SWMRE
Network Platform

SWMRE Configuration Guide

June 2019

Preface

This guide describes how to configure SWMRE.

Audience

This guide is intended for network administrators and other engineering professionals who configure SWMRE.

Conventions

Table P-1 shows the conventions used in this guide.

Table P-1: Conventions

Convention	Description
Italics	Emphasized terms; titles of books
Note:	Special instructions, suggestions, or warnings
`monospaced type`	Code elements such as commands, parameters, files, and directories

Chapter Organization

The chapters in command references are organized as described in Command Description Format.

The chapters in configuration guides are organized into these major sections:

- An overview that explains a configuration in words
- Topology with a diagram that shows the devices and connections used in the configuration
- Configuration steps in a table for each device where the left-hand side shows the commands you enter and the right-hand side explains the actions that the commands perform
- Validation which shows commands and their output that verify the configuration

Related Documentation

For information about installing of SWMRE, see the *Installation Guide* for your platform.

Command Line Interface

This chapter introduces the SWMRE Command Line Interface (CLI) and how to use its features.

Overview

You use the CLI to configure, monitor, and maintain SWMRE devices. The CLI is text-based and each command is usually associated with a specific task.

You can give the commands described in this manual locally from the console of a device running SWMRE or remotely from a terminal emulator such as `putty` or `xterm`. You can also use the commands in scripts to automate configuration tasks.

Command Line Interface Help

You access the CLI help by entering a full or partial command string and a question mark "?". The CLI displays the command keywords or parameters along with a short description. For example, at the CLI command prompt, type:

```
> show ?
```

The CLI displays this keyword list with short descriptions for each keyword: `show ?`

```
application-priority            Application    Priority
arp                             Internet Protocol (IP)
bfd                             Bidirectional Forwarding Detection (BFD)
bgp                             Border Gateway Protocol (BGP)
bi-lsp                          Bi-directional lsp status and configuration
bridge                          Bridge group commands
ce-vlan                         COS Preservation for Customer Edge VLAN
class-map                       Class map entry
cli                             Show CLI tree of current mode
clns                            Connectionless-Mode Network Service (CLNS)
control-adjacency               Control Adjacency status and configuration
control-channel                 Control Channel status and configuration
cspf                            CSPF Information
customer                        Display Customer spanning-tree
cvlan                           Display CVLAN information
debugging                       Debugging functions (see also 'undebug')
dot1x                           IEEE 802.1X Port-Based Access Control
etherchannel                    LACP etherchannel   ethernet
Layer-2 ...
```

If you type the ? in the middle of a keyword, the CLI displays help for that keyword only.

```
> show de? debugging Debugging functions (see
also 'undebug')
```

If you type the ? in the middle of a keyword, but the incomplete keyword matches several other keywords, SWMRE displays help for all matching keywords.

`> show i?` (CLI does not display the question mark).

```
interface  Interface status and configuration
ip         IP information isis       ISIS
information
```

Command Completion

The CLI can complete the spelling of a command or a parameter. Begin typing the command or parameter and then press the tab key. For example, at the CLI command prompt type `sh`:

```
> sh
```

Press the tab key. The CLI displays:

```
> show
```

If the spelling of a command or parameter is ambiguous, the CLI displays the choices that match the abbreviation. Type `show i` and press the tab key. The CLI displays:

```
> show i
  interface  ip          ipv6       isis
> show i
```

The CLI displays the `interface` and `ip` keywords. Type `n` to select `interface` and press the tab key. The CLI displays:

```
> show in
> show interface
```

Type ? and the CLI displays the list of parameters for the `show interface` command.

```
> show interface
  IFNAME  Interface name
  |       Output modifiers
  >       Output redirection
  <cr>
```

The CLI displays the only parameter associated with this command, the `IFNAME` parameter.

Command Abbreviations

The CLI accepts abbreviations that uniquely identify a keyword in commands. For example:

`> sh in xe0` is

an abbreviation for:

```
> show interface xe0
```

Command Line Errors

Any unknown spelling causes the CLI to display the error `Unrecognized command` in response to the ?. The CLI displays the command again as last entered.

```
> show dd?
% Unrecognized
command > show dd
```

When you press the Enter key after typing an invalid command, the CLI displays:

```
(config)#router ospf here
```

```
                                ^
% Invalid input detected at '^' marker.
```

where the ^ points to the first character in error in the command. If a command is incomplete, the CLI displays the following message:

```
> show
% Incomplete command.
```

Some commands are too long for the display line and can wrap mid-parameter or mid-keyword, as shown below. This does *not* cause an error and the command performs as expected:

```
area 10.10.0.18 virtual-link 10.10.0.19 authent ication-
key 57393
```

Command Negation

Many commands have a `no` form that resets a feature to its default value or disables the feature. For example:

- The `ip address` command assigns an IPv4 address to an interface
- The `no ip address` command removes an IPv4 address from an interface

Syntax Conventions

Table P-2 describes the conventions used to represent command syntax in this reference.

Table P-2: Syntax conventions

Convention	Description	Example
`monospaced font`	Command strings entered on a command line	`show ip ospf`
`lowercase`	Keywords that you enter exactly as shown in the command syntax.	`show ip ospf`
`UPPERCASE`	See Variable Placeholders	`IFNAME`
`()`	Optional parameters, from which you must select one. Vertical bars delimit the selections. Do not enter the parentheses or vertical bars as part of the command.	`(A.B.C.D|<0-4294967295>)`
`()`	Optional parameters, from which you select one or none. Vertical bars delimit the selections. Do not enter the parentheses or vertical bars as part of the command.	`(A.B.C.D|<0-4294967295>|)`

`()`	Optional parameter which you can specify or omit. Do not enter the parentheses or vertical bar as part of the command.	`(IFNAME|)`

Table P-2: Syntax conventions (Continued)

Convention	Description	Example
`{}`	Optional parameters, from which you must select one or more. Vertical bars delimit the selections. Do not enter the braces or vertical bars as part of the command.	`{intra-area <1-255>|inter-area <1-255>|external <1-255>}`
`[]`	Optional parameters, from which you select zero or more. Vertical bars delimit the selections. Do not enter the brackets or vertical bars as part of the command.	`[<1-65535>|AA:NN|internet|local-AS| no-advertise|no-export]`
`?`	Nonrepeatable parameter. The parameter that follows a question mark can only appear once in a command string. Do not enter the question mark as part of the command.	`?route-map WORD`
`.`	Repeatable parameter. The parameter that follows a period can be repeated more than once. Do not enter the period as part of the command.	`set as-path prepend .<1-65535>`

Variable Placeholders

Table P-3 shows the tokens used in command syntax use to represent variables for which you supply a value.

Table P-3: Variable placeholders

Token	Description
`WORD`	A contiguous text string (excluding spaces)
`LINE`	A text string, including spaces; no other parameters can follow this parameter
`IFNAME`	Interface name whose format varies depending on the platform; examples are: `eth0`, `Ethernet0`, `ethernet0`, `xe0`
`A.B.C.D`	IPv4 address
`A.B.C.D/M`	IPv4 address and mask/prefix
`X:X::X:X`	IPv6 address

`X:X::X:X/M`	IPv6 address and mask/prefix
`HH:MM:SS`	Time format
`AA:NN`	BGP community value

Table P-3: Variable placeholders

Token	Description
`XX:XX:XX:XX:XX:XX`	MAC address

`<1-5>`
`<1-65535>`
`<0-2147483647> <0-4294967295>`
	Numeric range

Command Description Format

Table P-4 explains the sections used to describe each command in this reference.

Table P-4: Command descriptions

Section	Description
Command Name	The name of the command, followed by what the command does and when should it be used
Command Syntax	The syntax of the command
Parameters	Parameters and options for the command
Default	The state before the command is executed
Command Mode	The mode in which the command runs; see Command Modes
Example	An example of the command being executed

Keyboard Operations

Table P-5 lists the operations you can perform from the keyboard.

Table P-5: Keyboard operations

Key combination	Operation
Left arrow or Ctrl+b	Moves one character to the left. When a command extends beyond a single line, you can press left arrow or Ctrl+b repeatedly to scroll toward the beginning of the line, or you can press Ctrl+a to go directly to the beginning of the line.
Right arrow or Ctrl-f	Moves one character to the right. When a command extends beyond a single line, you can press right arrow or Ctrl+f repeatedly to scroll toward the end of the line, or you can press Ctrl+e to go directly to the end of the line.
Esc, b	Moves back one word
Esc, f	Moves forward one word

Table P-5: Keyboard operations (Continued)

Key combination	Operation
Ctrl+e	Moves to end of the line
Ctrl+a	Moves to the beginning of the line
Ctrl+u	Deletes the line
Ctrl+w	Deletes from the cursor to the previous whitespace
Alt+d	Deletes the current word
Ctrl+k	Deletes from the cursor to the end of line
Ctrl+y	Pastes text previously deleted with Ctrl+k, Alt+d, Ctrl+w, or Ctrl+u at the cursor
Ctrl+t	Transposes the current character with the previous character
Ctrl+c	Ignores the current line and redisplays the command prompt
Ctrl+z	Ends configuration mode and returns to exec mode
Ctrl+l	Clears the screen
Up Arrow or Ctrl+p	Scroll backward through command history
Down Arrow or Ctrl+n	Scroll forward through command history

Show Command Modifiers

You can use two tokens to modify the output of a `show` command. Enter a question mark to display these tokens:

```
# show users ?
  | Output modifiers
  > Output redirection
```

You can type the | (vertical bar character) to use output modifiers. For example:

```
> show rsvp | ?
  begin       Begin with the line that matches
exclude    Exclude lines that match   include
Include lines that match    redirect   Redirect
output
```

Begin Modifier

The `begin` modifier displays the output beginning with the first line that contains the input string (everything typed after the `begin` keyword). For example:

```
# show running-config | begin xe1
...skipping interface
xe1
 ipv6 address fe80::204:75ff:fee6:5393/64
! interface xe2
ipv6 address
fe80::20d:56ff:
fe96:725a/64
! line con
0 login
! end
```

You can specify a regular expression after the `begin` keyword, This example begins the output at a line with either "xe2" or "xe4":

```
# show running-config | begin xe[3-4]

...skipping interface
xe3  shutdown
! interface
xe4 shutdown
!
interface svlan0.1 no
shutdown
!
route-map myroute permit 3
!
route-map mymap1 permit 10
!
route-map rmap1 permit 3
! line con 0
login line vty
0 4  login
! end
```

Include Modifier

The `include` modifier includes only those lines of output that contain the input string. In the output below, all lines containing the word “input” are included:

```
# show interface xe1 | include input
    input packets 80434552, bytes 2147483647, dropped 0, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 1, missed 0
```

You can specify a regular expression after the `include` keyword. This examples includes all lines with “input” or “output”:

```
#show interface xe0 | include (in|out)put
    input packets 597058, bytes 338081476, dropped 0, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 613147, bytes 126055987, dropped 0 output errors 0,
aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
```

Exclude Modifier

The `exclude` modifier excludes all lines of output that contain the input string. In the following output example, all lines containing the word “input” are excluded:

```
# show interface xe1 | exclude input
Interface xe1
  Scope: both
  Hardware is Ethernet, address is 0004.75e6.5393
  index 3 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Administrative Group(s): None   DSTE
Bandwidth Constraint Mode is MAM   inet6
fe80::204:75ff:fee6:5393/64
    output packets 4438, bytes 394940, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window
0 collisions 0
```

You can specify a regular expression after the `exclude` keyword. This example excludes lines with “output” or “input”:

```
# show interface xe0 | exclude
(in|out)put Interface xe0
  Scope: both
  Hardware is Ethernet Current HW addr: 001b.2139.6c4a
Physical:001b.2139.6c4a Logical:(not set)
  index 2 metric 1 mtu 1500 duplex-full arp ageing timeout 3000
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound Bandwidth
  100m
  DHCP client is disabled. inet
10.1.2.173/24 broadcast 10.1.2.255
  VRRP Master of :  VRRP is not configured on this interface.
inet6 fe80::21b:21ff:fe39:6c4a/64     collisions 0
```

Redirect Modifier

The `redirect` modifier writes the output into a file. The output is not displayed.

```
# show cli history | redirect /var/frame.txt
```

The output redirection token (>) does the same thing:

```
# show cli history >/var/frame.txt
```

Command Modes

Commands are grouped into modes arranged in a hierarchy. Each mode has its own set of commands. Table P-6 lists the command modes common to all protocols.

Table P-6: Common command modes

Name	Description
Executive mode	Also called *view* mode, this is the first mode to appear after you start the CLI. It is a base mode from where you can perform basic commands such as `show`, `exit`, `quit`, `help`, `list`, and `enable`.
Privileged executive mode	Also called *enable* mode, in this mode you can run additional basic commands such as `debug`, `write`, and `show`.

Table P-6: Common command modes (Continued)

Name	Description
Configure mode	Also called *configure terminal* mode, in this mode you can run configuration commands and go into other modes such as interface, router, route map, key chain, and address family.
Interface mode	In this mode you can configure protocol-specific settings for a particular interface. Any setting you configure in this mode overrides a setting configured in router mode.
Router mode	This mode is used to configure router-specific settings for a protocol such as RIP or OSPF.

Command Mode Tree

The diagram below shows the common command mode hierarchy.

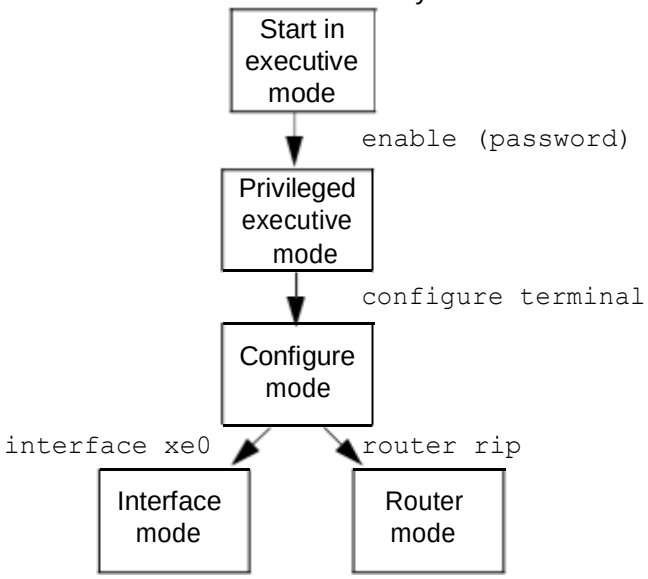


Figure P-1: Common command modes

To change modes:

1. Enter privileged executive mode by entering `enable` in Executive mode.
2. Enter configure mode by entering `configure terminal` in Privileged Executive mode.

The example below shows starting `imish` and then moving from executive mode to privileged executive mode to configure mode and finally to router mode:

```
# ./imish
> enable mypassword
# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
(config)# router rip
(config-router)#
```

Note: Each protocol can have modes in addition to the common command modes. See the command reference for the respective protocol for details.

SECTION 1 Architecture

Architecture Guide

Contents

This document contains this chapter:

- Chapter 1, *SWMRE Architecture*
- Chapter 2, *SWMRE Key Features*
- Chapter 3, *SWMRE Abstraction Layers*

CHAPTER 1 SWMRE Architecture

This chapter introduces SWMRE and describes its high-level architecture.

SWMRE Network Platform Overview

The SWMRE network platform is Layer 2 (data link) and Layer 3 (network layer) control plane software that allows network equipment manufacturers to rapidly add networking capabilities to communications products. SWMRE takes advantage of separate data plane processors (network processing units and switch ASICs). SWMRE is targeted at Tier 1 and Tier 2 network equipment manufacturers who provide solutions in:

- Carrier transport, access, and Carrier Ethernet
- Mobile backhaul and access
- Data center and cloud networking, including solutions for enterprise private clouds, hybrid clouds, and public clouds

The SWMRE networking protocol modules conform to leading IEEE, IETF, MEF, and industry-specific standards. SWMRE supports more than 200 protocols for:

- Layer 2 switching: Virtual Local Area Networks (VLANs), Spanning Tree, Data Center Bridging, TRILL, PTP
- Layer 3 routing: OSPFv2/v3, RIP/RIPng, BGP4+, ISIS
- Multi-Protocol Label Switching (MPLS) which operates at a layer between traditional definitions of Layer 2 and Layer 3
- Carrier Ethernet
- Data Center Ethernet

SWMRE is built on an SDN architecture that features:

- High degree of scalability
- Modularity and programmability
- Embedded abstraction layer to communicate with the underlying operating system
- Hardware abstraction layer to run on a variety of silicon switching chipsets for forwarding table updates

The modular architecture of SWMRE lets you select and integrate only the protocols you need. Each protocol module runs as a separate daemon with its own address space and stack. This isolates issues with one protocol module from all others. You can readily add a customized protocol module to address specific needs.

Note: For a list of all daemon file names, see the *SWMRE Installation Guide*.

SWMRE provides configuration management at multiple layers:

- Command line interface
- SNMP
- External simple management interface C API

Internal C API
SWMRE Architecture

High-Level Architecture

Figure 1-1 shows the high-level architecture of SWMRE.

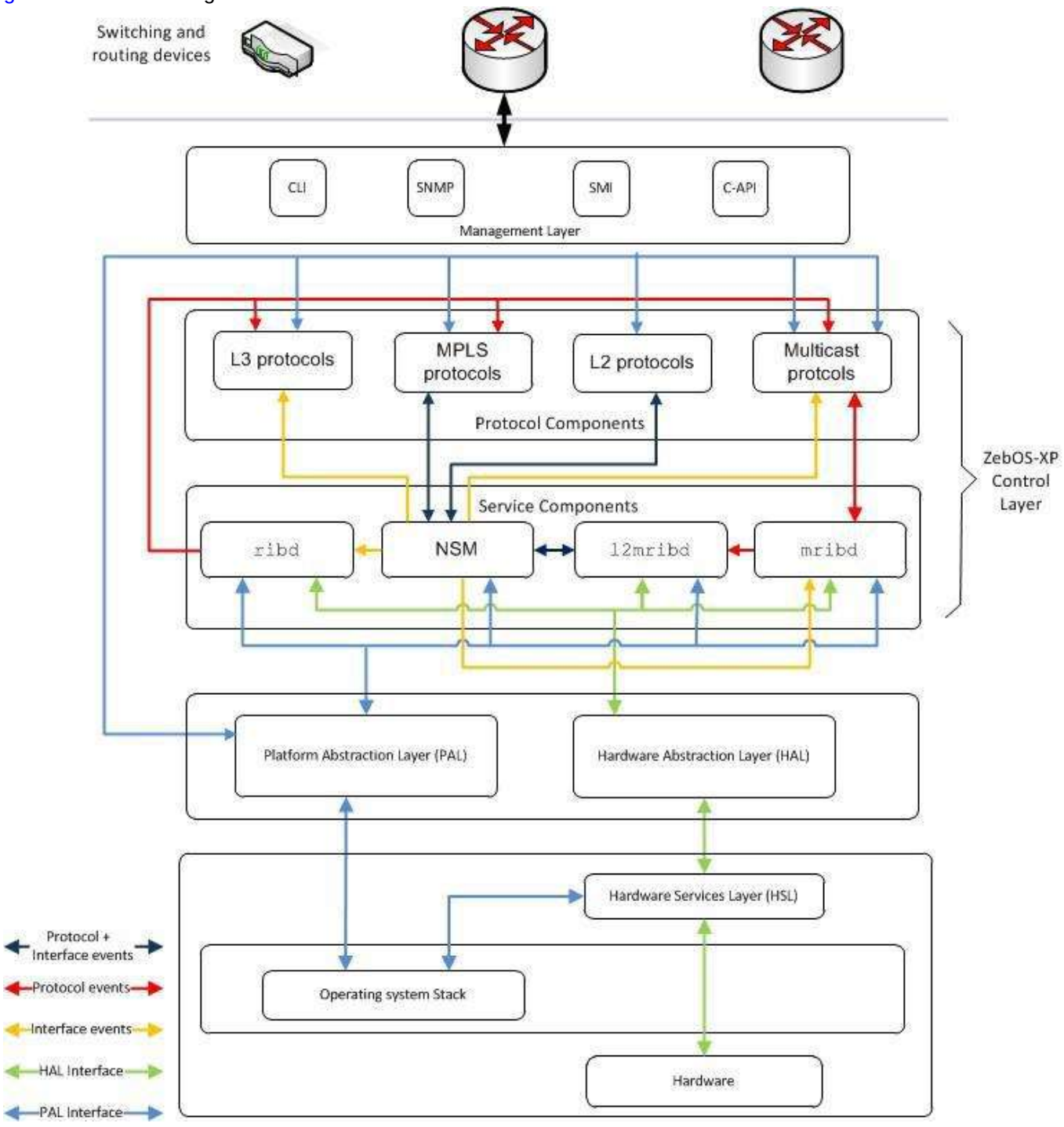


Figure 1-1: High-level architecture

SWMRE Architecture

At the top of Figure 1-1 is the Management Interface used to manage, configure, and operate the SWMRE routing and switching protocols.

The major components in the control layer of SWMRE are grouped into these categories:

- Protocol components, which include:

- Layer 3 Protocols
- Multi Protocol Label Switching Protocols
- Layer 2 Protocols
- Multicast Protocols
- Service components, which include:
- Network Services Module (NSM)
- Unicast Routing Information Base Daemon (ribd)
- Layer 2 Multicast Routing Information Base Daemon (l2mribd)
- Layer 3 Multicast Routing Information Base Daemon (mribd) The bottom of Figure 1-1 shows the abstraction layers of SWMRE:
- Platform Abstraction Layer
- Hardware Abstraction Layer

CHAPTER 2 SWMRE Key Features

This chapter describes the key features of SWMRE.

Management Interface

SWMRE provides a comprehensive set of tools to manage, configure, and operate the routing and switching protocols.

The management interface includes:

- Command Line Interface
- Simple Network Management Protocol
- Simple Management Interface
- C Language Application Programming Interface

Command Line Interface

The command line interface (CLI) offers complete, unified management of SWMRE. Each command is usually associated with a specific task. The CLI has two major components:

- The Integrated Management Interface process (`imi`) is a centralized, persistent daemon for managing the SWMREXP configuration that runs as a server of NSM and the protocols. The `imi` daemon connects to protocol daemons through inter-process communications.
- IMI shell (`imish`) is a interactive daemon program for the `imi` daemon that enables connection locally from the console of a device running SWMRE or remotely from terminal emulator programs such as `ssh` or `telnet`.

Through `imish`, a system administrator can configure and monitor all of the SWMRE daemons through one centralized connection. The `imish` daemon maintains a persistent connection to all protocol daemons, stores configuration data, and offers extensive monitoring and logging capabilities.

The CLI can use the secure authentication methods of the operating system to manage and validate user names and passwords.

Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) provides a standardized framework and a common language for monitoring and managing devices in a network. The SNMP framework has three parts:

- SNMP manager: A system used to control and monitor the activities of network devices. This is sometimes called a Network Management System (NMS).
- SNMP agent: The component within a managed device that maintains the data for the device and reports data to SNMP managers.
- Management Information Base (MIB): SNMP exposes management data in the form of variables on the managed device which network management agents can extract from the SWMRE protocols for all standard defined MIBs.

As shown in Figure 2-2, an SNMP manager on the network sends query packets to gather status data. Each protocol daemon responds to these queries as defined by the corresponding MIB for the protocol.

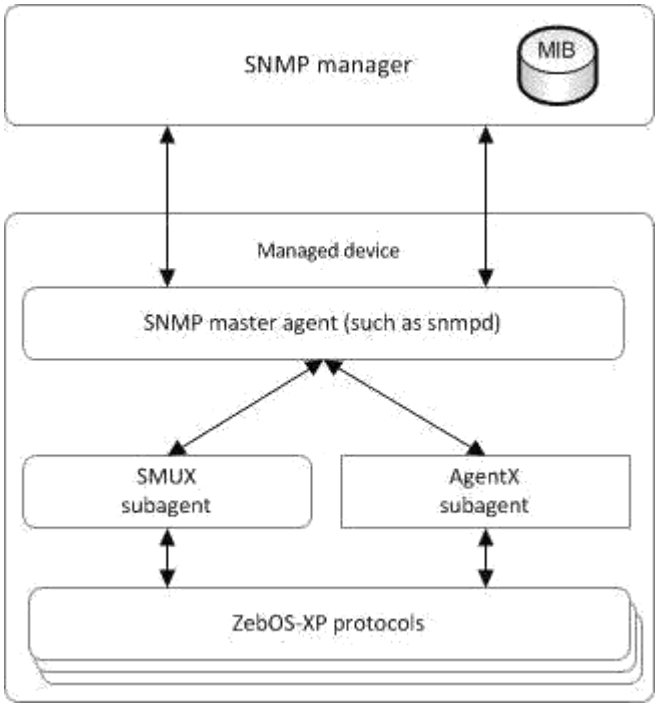


Figure 2-2: SNMP subagents SWMRE

supports these subagents:

- The SMUX (SNMP Multiplexing) protocol defined by RFC 1227 is enabled by default. The SMUX agent responds to UDP-161 packets, and transmits them to SWMRE over TELNET connections using port 199.
- The AgentX (Agent Extensibility) protocol defined by RFC 2741 uses TCP-705 for communication between the subagent and the master agent.

Note: You cannot configure SNMP with both SMUX and AgentX. One or the other must be used.

Each protocol daemon in SWMRE has an SNMP API that give developers the flexibility to integrate with any management plane. In addition, SWMRE can log both the systems' events and errors.

For more about installing and configuring SNMP agents and subagents, see the *Installation Guide*. For more about the MIBs a SWMRE protocol daemon supports, see the developer guide for the protocol.

Simple Management Interface

The Simple Management Interface (SMI) is a C language API that you use to write applications that configure and manage the SWMRE routing and switching protocols. For more see Chapter 6, *Management Modules*.

C Language Application Programming Interface

Every SWMRE protocol module provides a C language Application Programming Interface (API) for configuring properties of the protocol. For example, the `ospf_api.h` include file defines an API for configuring the OSPF protocol. Use these APIs to integrate with any management plane to control the SWMRE software.

Note: You must call the functions in a SWMRE C language API in the same process space as SWMRE (that is, from a SWMRE daemon).

Network Services Module

Network Services Module (NSM) is the core of the SWMRE architecture. NSM is the base module that simultaneously and independently communicates with every SWMRE routing and switching process. The protocol components use APIs exposed by the NSM client, which act as conduits to transfer data between the protocol modules and NSM.

NSM also interacts with the Platform Abstraction Layer (PAL) to communicate with the underlying operating system. Figure 2-3 shows NSM interacting with PAL and the protocols.

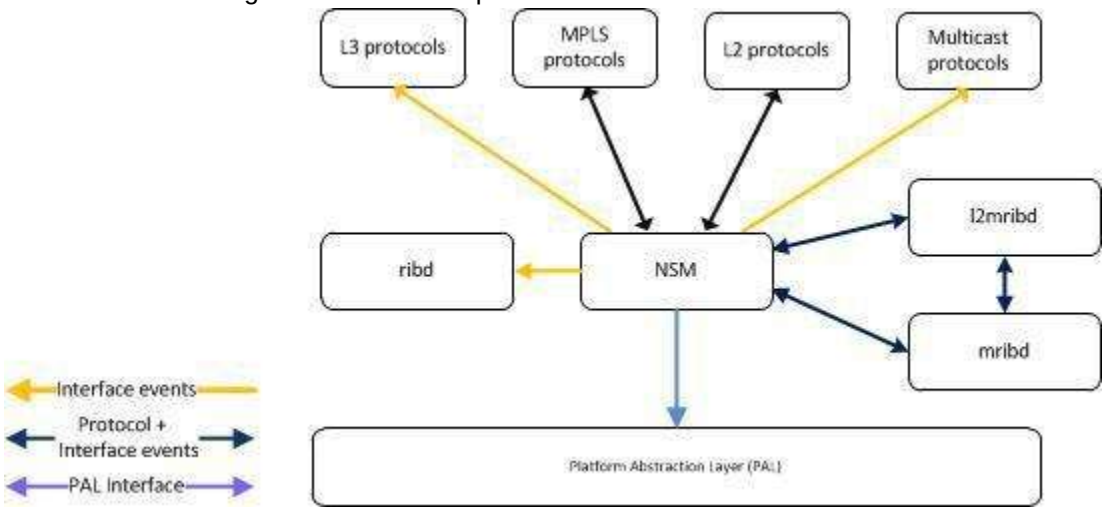


Figure 2-3: NSM

NSM provides the following services to the protocol components:

- Interface management
- Layer 2
- VLAN management for Layer 2 switching
- MPLS label management
- Traffic engineering
- QoS management
- Virtual Routing/Virtual Route Forwarding (VR/VRF) Management
- Virtual Private LAN Service (VPLS) and Virtual Private Wire Service (VPWS)

The protocol modules use the NSM client module to register for relevant services they want from NSM. The NSM server module manages the list of connected NSM clients and publishes information to them.

For more information about NSM, see the *Network Services Module Developer Guide.*

Interface Manager

The NSM Interface Manager provides a logical view of the interfaces in the system to the control plane. The Interface Manager configures and manages the physical and logical interface and provides the following functions:

- Manages and configures interfaces that are not managed by the network processor or ASIC
- Manages the learning, configuration, and management of the hardware interfaces present on the network processor or ASIC
  Provides an abstracted TCP/IP interface that can be populated by different TCP/IP stacks with the same operating system
- For Layer 3 interfaces, populates the interface in the TCP/IP stack for slow path and exception packet handling

- Maintains the database and hierarchies for all interface types and their relationships to each other and functions to maintain and change these hierarchies from the control plane
- Provides interfaces to link scanning tasks for interface up/down asynchronous events

Layer 2 Protocols

SWMRE includes these Layer 2 features:

- Virtual Local Area Networks
- Link Aggregation
- Multi-Chassis Link Aggregation
- Spanning Tree
- Data Center Bridging
- Port Authentication (authd)
- Precision Time Protocol
- Synchronous Ethernet
- Shortest Path Bridging (IEEE 802.1aq)
- Edge Virtual Bridging
- Ethernet Automatic Protection Switching
- Ethernet Local Management Interface
- Remote Monitoring

Figure 2-4 shows the SWMRE Layer 2 high-level architecture.

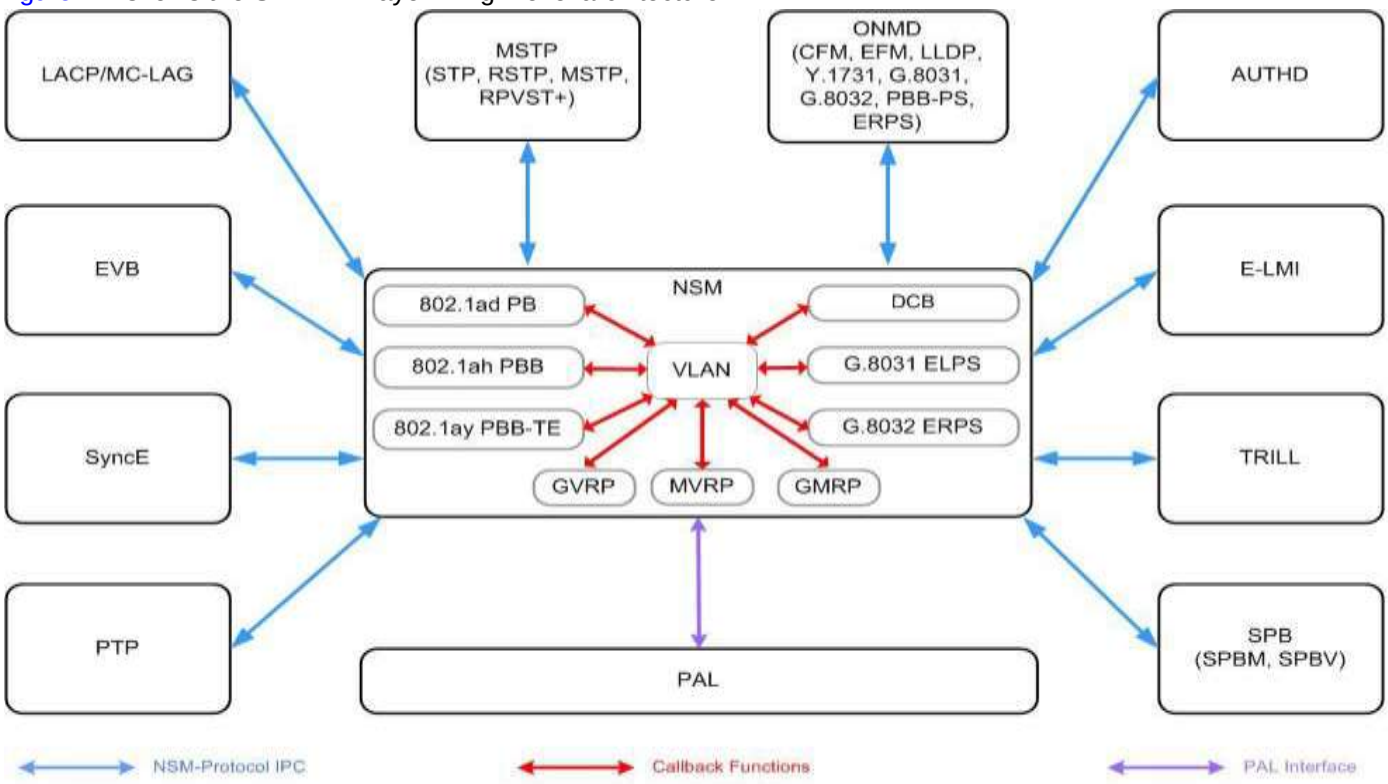


Figure 2-4: Layer 2 architecture

Virtual Local Area Networks

The VLAN modules offer a consistent network-wide management tools to manage virtual LANs (Local Area Networks) and bridged VLANs:

- VLAN bridging allows network devices to segment into VLANs, regardless of their physical location.
- VLANs, in accordance with IEEE 802.1Q, enable multiple bridged LANs to transparently share the same physical network link without leaking information between LANs. Traffic between VLANs is restricted to bridges that forward unicast, multicast, or broadcast traffic only on the LAN segments that serve the VLAN to which the traffic belongs.

SWMRE VLAN modules make it easy to administer logical groups of stations that can communicate as if they were on the same LAN. They make it easier to manage a move, add, delete, or other updates to members of these groups.

The following highlights the features of the VLAN modules.

MAC Bridging (802.1d)

The SWMRE VLAN modules support all IEEE 802.1D LAN MAC (Media Access Control) protocols, shared media, and point-to-point LANs. MAC bridging allows multiple LANs to be connected together. MAC bridging filters data sent between LAN segments, reduces network congestion, and allows networks to be partitioned for administrative purposes.

Identifying VLANS

VLAN identifiers (VIDs):

- Offer convenient, consistent, and network-wide methods for bridges to identify rules to classify user data for VLANs
- Extend source and destination MAC addresses by treating addressing for different VLANs independently

  Identify and select from multiple active topologies; and identify parameters that restrict access from one part of a network to another

Provider Bridging (802.1ad)

Provider Bridging (PB) enables a service provider to use the architecture and protocols of 802.Q to offer the equivalent of separate Local Area Networks (LANs), bridged LANs, or virtual bridged LANs to multiple customers. Provider bridging requires no active cooperation between customers and requires minimal cooperation between an individual customer and the service provider.

When VLANs were originally defined in the 802.1Q, the number of unique VLAN identifiers was limited to 4096. In large provider networks, each subscriber needs a separate address, thus this limit could prevent a provider from having more than 4096 subscribers.

To overcome the 4096 VLAN identifier limit, the frame format for 802.1ad inserts an additional VLAN header into a single 802.1Q Ethernet frame. There are two types of VLAN headers:

- The C-VLAN or inner header which is closest to the payload portion of the frame identifies the customer VLAN
- The S-VLAN or outer header which is closest to the Ethernet header identifier the provider VLAN The frame

  format for 802.1ad is also called “Q-in-Q” or “double tagged”.

With the two VLAN identifiers in combination for each provider-customer pair, it is possible to define up to 16,777,216 labels.

Provider Backbone Bridging (802.1ah)

Provider Backbone Bridging (PBB) adds the capability to create Ethernet backbones for service access networks. PBB extends 802.1ad Provider Bridging in these ways:

- The 802.1ah header adds a service instance identifier (I-SID) which is a label that maps to a customer VLAN identifier. An I-SID virtualizes VLANs across a network. VLANs are mapped into I-SIDs by configuring only the edge of the network at the Backbone Edge Bridges (BEBs). This makes the maximum number of service instances 16 million.
- The 802.1ah header encapsulates backbone source and destination MAC addresses (termed B-SA and B-DA) along with the customer source and destination MAC addresses (C-SA and C-DA). The 802.1ah format is sometimes called “MAC-in-MAC” because of this. The encapsulation of customer MAC addresses in backbone MAC addresses means that the backbone does not need to learn customer MAC addresses. Customer MAC addresses are learned at BEB ports only.

Provider Backbone Bridge-Traffic Engineering (802.1Qay)

The Provider Backbone Bridging-Traffic Engineering (PBB-TE) standard supports the construction of “traffic engineered” backbone topologies, load balancing, protection switching, bandwidth management, and so on to serve the needs of large service providers. Provider networks rely on direct control of path routing so that traffic engineering can be used to allocate bandwidth, ensure diverse backup path routing, and select path performance as required by service level agreements. The architecture of bridges and their associated protocols as specified by 802.1ah allows the further specification of interoperable bridge capabilities that support traffic engineering at the required scale.

Registration Frameworks

The Layer 2 support in SWMRE includes these registration frameworks:

- Generic Attribute Registration Protocol: GARP is a generic framework for bridges to register and de-register attributes, such as VLAN identifiers and multicast group membership.
- GARP VLAN Registration Protocol (802.1Q): GVRP is a GARP application that provides VLAN registration service.

  GVRP uses GARP Information Declaration (GID) and GARP Information Propagation (GIP), which provide the common state machine descriptions and the common information propagation mechanisms defined for GARPbased applications.

  GVRP provides support for VLAN pruning and dynamic VLAN creation. A switch can exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs.
- GARP Multicast Registration Protocol: GMRP allows participants to dynamically register and de-register information with the Media Access Control (MAC) bridges attached to the same LAN segment. A switch can exchange multicast group information with other GMRP switches, prune unnecessary broadcast traffic, and dynamically create and manage multicast groups.
- Multicast Registration Protocol (802.1ak): MRP has protocols, procedures, and managed objects to support multiple registrations, and allow the participants in an MRP application to register attributes with other participants in a bridged LAN.
- Multiple VLAN Registration Protocol (802.1ak): MVRP registers multiple VLANs and provides for the rapid healing of network failures without interrupting services to unaffected VLANs. In addition, MVRP improves the convergence time of the GVRP module.
- Multiple Multicast Registration Protocol (802.1ak) MMRP manages group Media Access Control (MAC) addresses. In addition, MMRP improves the convergence time of GMRP.

VLAN Prioritization (802.1p/Q)

SWMRE includes priority signaling for traffic at the data-link layer. IEEE 802.1Q specifies a priority value of between 0 and 7 inclusive that can be used by QoS (Quality of Service) disciplines to differentiate traffic. Although this technique is often called “802.1p”, there is no standard by that name published by the IEEE. Instead, the technique is incorporated into 802.1Q standard which specifies the tag inserted into an Ethernet frame.

Port and Protocol Classification (802.1v)

Port and Protocol Classification is an amendment to 802.1Q to classify incoming packets by methods other than source port information, specifically, classification based on data-link-layer protocol identification.

Link Aggregation

The Link Aggregation module allows one or more links to be aggregated together to form a Link Aggregation Group (LAG), such that a MAC client can treat the Link Aggregation Group as if it were a single link. The Link Aggregation Control Protocol (LACP) allows bundling of several physical interfaces to form a single logical channel providing enhanced performance and redundancy. The aggregated interface is viewed as a single link to each switch. The spanning tree also views it as one interface. When there is a failure in one physical interface, the remaining interfaces stay up, so there is no disruption.

Multi-Chassis Link Aggregation

Multi-Chassis Link Aggregation (also called MC-LAG, MLAG, or Distributed Resilient Network Interconnect [DRNI]) extends the link aggregation concept to ensure that connectivity between two networks can be maintained despite the failure of a node. With MC-LAG, at either one or both ends of a link aggregation group, a single aggregation system is replaced by a *portal* that is a collection of one to three portal systems.

Spanning Tree

The SWMRE Spanning Tree support are a combination of these modules:

- Spanning Tree Protocol (STP)
- Rapid Spanning Tree Protocol (RSTP)

  Multiple Spanning Tree Protocol (MSTP)

The following highlights the features of the Spanning Tree Protocol modules.

Note: All SWMRE spanning tree modules support 802.3x flow control, broadcast storm recovery, and port mirroring.

Spanning Tree Protocol (802.1d)

The SWMRE Spanning Tree Protocol (STP) module creates spanning trees within mesh networks of Layer 2 connected bridges, disabling any links that are not a part of the tree and leaving a single active connection between any two unique network nodes.

STP devices exchange BPDU (bridge protocol data unit) messages. The Spanning Tree Algorithm calculates the best path and prevents multiple paths between network segments. STP elects a root bridge, finds paths and determines the least cost path to the root bridge, then disables all other paths.

Network managers may design a topology that uses redundant links as automatic backup paths in the case of active link failure. Automatic backup takes place without the pitfalls of bridge loops, or the need to manually enable or disable backup links.

SWMRE STP supports all STP switch port states, including:

- Listening, learning, blocking, forwarding, disabled

For more information about the Spanning Tree modules, see the *Layer 2 Developer Guide*.

Rapid Spanning Tree Protocol (802.1w)

The Rapid Spanning Tree Protocol (RSTP) accelerates the re-configuration and restoration of a spanning tree after a link failure.

Multiple Spanning Tree Protocol (802.1s)

The Multiple Spanning Tree Protocol (MSTP) is a supplement to the IEEE 802.1ad standard. MSTP allows VLAN bridges to use multiple spanning trees, by providing the ability for traffic belonging to different VLANs to flow over potentially different paths within the virtual bridged LAN.

Data Center Bridging

Data Center Bridging (DCB) is a collection of standards-based extensions for Ethernet protocols. DCB is a lossless transport layer to allow the convergence of LANs and SANs into a single unified fabric. DCB is a flexible framework that defines the capabilities required for switches and end-points to be part of a data center environment. DCB protocols can carry Fibre Channel, TCP/IP, and Inter-process communication traffic over a single, converged Ethernet network.

SWMRE DCB provides these key benefits:

- Enables Fibre Channel over Ethernet (FCoE) to make possible the migration of SANS to more cost-effective Ethernet
- Enables high-speed connections over Carrier Ethernet between geographically dispersed data centers

Data center networks and backplane fabrics employ applications that depend on the delivery of data packets with a lower latency and lower probability of packet loss than is typical of IEEE 802 VLAN bridged networks. DCB supports the use of a single bridged local area network for these applications, as well as traditional LAN applications.

DCB features include:

- Lossless fabric for traffic on converged networks
- Virtual links by traffic class that includes pause-per-class technology, congestion management and event notification
- Improved performance, including stability, enhanced throughput, and robustness The following subsection highlights the features of DCB.

For more information about DCB, see the *Data Center Bridge Developer Guide.*

Priority-based Flow Control (IEEE 802.1Qbb)

The Priority-based Flow Control (PFC) standard specifies protocols, procedures and managed objects that enable flow control per traffic class on full-duplex links. Priority-based flow control helps eliminate frame loss due to congestion by operating on individual priorities. Along with other Data Center Bridging technologies, PFC helps the flow of higherlayer protocols, which are highly loss sensitive, while not affecting traditional LAN protocols that utilize other priorities. Data Center Bridging networks (bridges and end-nodes) include limited bandwidth-delay product and limited hop count.

VLAN tag priority values identify traffic classes. Priority-based flow control helps eliminate frame loss due to congestion by a mechanism similar to the IEEE 802.3x PAUSE, but operates on individual priorities.

Enhanced Transmission Selection (IEEE 802.1Qau)

The Enhanced Transmission Selection (ETS) standard supports the allocation of bandwidth among traffic classes. When the available load in a traffic class does not use its allocated bandwidth, ETS allows other traffic classes to use available bandwidth.

A network can prioritize traffic to offer different service characteristics to different traffic classes. However, a user may want to share bandwidth among the priorities that are carrying bursty, high-offered loads, instead of servicing them with a strict priority. Therefore, traffic set at a specific priority level that does not use its set allocation allows traffic set at other priorities to utilize the unused bandwidth.

Data Center Bridging eXchange (DCBx)

The Data Center Bridging eXchange (DCBx) protocol is used by DCB-enabled devices to exchange information with directly connected peers. The DCBx may also be used to detect mis-configurations and to configuring the peers. DCBx uses the Link Layer Discovery Protocol (LLDP) as a signaling mechanism.

Quantized Congestion Notification (802.1Qau)

Quantized Congestion Notification (QCN) addresses the problem of sustained congestion by moving corrective action to the network edge.

Port Authentication (authd)

The SWMRE Layer 2 802.1x module provides port-based network access control for LAN devices. The IEEE 802.1x standard offers centralized control of user authentication and access.

Precision Time Protocol

The Precision Time Protocol (PTP) is a protocol used to synchronize clocks throughout a computer network. On a local area network, PTP achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control

systems. PTP (IEEE 1588v2) introduced the concept of “boundary clocks” and “transparent clocks” that serve to further improve system and network scalability and the accuracy of clock synchronization.

PTP is an event-based protocol for time synchronization. PTP allows a better precision than other time synchronization protocol because of its “on-path support” and precision in sending the exact timestamp. On-path support in PTP is provided through boundary and transparent clocks. Boundary clocks synchronize time to the grandmaster and transmit it further on the network. There is no need for the grandmaster to send synchronization messages to all slave clocks. Boundary clocks in between can act as master.

Transparent clocks do not synchronize with the grandmaster or master. They just add correction to the timestamp by taking into account link delays and residence time.

For more information about PTP, see the *Precision Time Protocol Developer Guide.*

Synchronous Ethernet

Packet-switching networks such as Ethernet were designed to transport asynchronous data where strict synchronization is not needed because traffic is highly buffered. However, with Carrier Ethernet evolution, Ethernet is replacing the SONET/SDH/PDH infrastructure and carrying TDM traffic. This means that packet networks need frequency synchronization functions, especially at their edge. The adaptation of TDM signals into a packet network is called Circuit Emulation Services (CES). Synchronous Ethernet (SyncE) is an evolution of conventional Ethernet with SONET/SDH/PDH-based synchronization. Synchronous Ethernet is used to synchronize and send frequency information to nodes on the network. Synchronous Ethernet provides only frequency synchronization, not time or phase synchronization.

In Synchronous Ethernet, a reference-timing signal traceable to a Primary Reference Clock (PRC) is injected into the network element using an external clock port. The Synchronous Ethernet interface extracts the frequency of this reference-timing signal and locks it to a system clock. This reference frequency is distributed to downstream Synchronous Ethernet nodes. Using this method, timing originating from a PRC is distributed via the intermediate Ethernet equipment clocks (EEC), to the other nodes in the network.

For more information about SyncE, see the *Synchronous Ethernet Developer Guide.*

Shortest Path Bridging (IEEE 802.1aq)

SPB (Shortest Path Bridging) enables you to simplify how you create and configure networks—across the enterprise and for the cloud—by requiring service provisioning only at the edge of the network. Shortest Path Bridging (SPB) is a control plane protocol that combines an Ethernet data path with an Intermediate System To Intermediate System (ISIS) link state protocol running between bridges. SPB does not depend on spanning tree protocols to provide a loop-free topology, but instead uses IS-IS Link State Packets (LSPs) to discover and advertise the network topology and compute the shortest path trees from all bridges in the SPB area. RFC 6329 describes the IS-IS extensions to support 802.aq SPB.

There are two types of SPB depending on the type of Ethernet data path:

- Shortest Path Bridging - VID (SPBV) uses an 802.1ad “Q-in-Q” data path • Shortest Path Bridging - MAC (SPBM) uses an 802.1ah “MAC-in-MAC” data path For more information about SPB, see the *Shortest Path Bridging Developer Guide.*

SPB, like TRILL, uses the IS-IS link-state routing protocol to advertise both topology and logical network membership. SPB packets are encapsulated at the edge in either MAC-in-MAC 802.1ah or tagged 802.1Q/802.1ad frames and transported only to other members of the logical network. Unicast and multicast are supported and all routing is on symmetric shortest paths.

The key benefits of the SPB solution are:

- Supports thousands of multi-terabyte switches and enables a non-blocking two-tier network fabric

- Uses existing IS-IS protocol and interoperates with existing service provider equipment
- Already available through OAM, enabling service providers to quickly roll out managed services

IEEE 802.1aq can be used anywhere that Spanning Tree is currently being used. Operators can take existing STP/ MSTP-based networks and migrate to SPB.

With SPB, the data center network can be treated as one big Layer 2 switch by combining hundreds of smaller switches in a “non-blocking” topology. This big distributed switch can be used to interconnect hundreds of different customers cheaply with Layer 2 VPNs. The topology is fully compatible with all 802.1 data center bridging protocols. OAM (Operation, Administration, and Management) and address isolation is provided through MAC-in-MAC.

Edge Virtual Bridging

Software switches cannot achieve the level of network capabilities built into enterprise-class Layer 2 data center switches. To solve the management challenges with Virtual Ethernet Bridging (VEB), Edge Virtual Bridging (EVB) was developed with a primary goal to combine the best of VEBs with the best of external Layer 2 network switches.

EVB is based on VEPA (Virtual Ethernet Port Aggregator) technology. EVB enables the virtual switches to send all traffic and forwarding decisions to an adjacent physical switch. This moves the forwarding decisions and network operations from the host CPU to the switch. EVB also leverages the advanced management capabilities in the access or aggregation layer switches.

For more about EVB, see the *Edge Virtual Bridging Developer Guide.*

Ethernet Automatic Protection Switching

Ethernet Automatic Protection Switching (APS) detects signal failure or signal degrade on a working channel and switches traffic transmission to a protection channel.

Ethernet Linear Protection Switching

Ethernet Linear Protection Switching (ELPS) as defined by ITU-T G.8031 (2007) specifies these techniques:

- Linear 1+1 (One-plus-One) protection switching operates with either uni-directional or bi-directional switching; normal traffic is copied and fed to both working and protection transport entities
- Linear 1:1 (One-to-One) protection switching operates with bi-directional switching; normal traffic is transported either on the working transport entity or on the protection transport entity, using a selector bridge at the source For more about ELPS, see the *Carrier Ethernet Developer Guide*.

Ethernet Ring Protection Switching

Ethernet Ring Protection Switching (ERPS) protects Ethernet traffic in a ring topology by ensuring that no loops are within the ring. Loops are prevented by blocking traffic on either a predetermined link or a failed link. ERPS integrates Ethernet Operations, Administration, and Maintenance (OAM) functions with a simple APS protocol. An Ethernet ring uses normal learning, forwarding, filtering, and flooding mechanisms and a forwarding data base (FDB).

SWMRE supports multiple Ethernet ring instances, in accordance with ITU-T G.8032 (2012).

For more about ERPS, see the *Carrier Ethernet Developer Guide*.

Ethernet Local Management Interface

Ethernet Local Management Interface (E-LMI) is an OAM (Operation, Administration, and Management) protocol used for communications between two User Network Interfaces (that is, UNI-C and UNI-N). E-LMI provides both UNI and

EVC (Ethernet Virtual Connection) status information to customer edge (CE) devices. This information enables automatic configuration of CE operation based on the Metro Ethernet Network configuration. The SWMRE E-LMI module follows the Metro Ethernet Forum 16 specification.

For more about E-LMI, see the *Ethernet Local Management Interface Developer Guide*.

Remote Monitoring

Remote monitoring (RMON; defined by RFC RFC 2819) provides remote monitoring and management of network devices and enables these devices to communicate with each other to exchange network information.

For more about RMON, see the *Layer 2 Developer Guide*.

Layer 3 Protocols

SWMRE supports both IPv4 and IPv6 versions of:

- Border Gateway Protocol
- Open Shortest Path First
- Routing Information Protocol
- Intermediate System to Intermediate System
- Virtual Router Redundancy Protocol
- Bidirectional Forwarding Detection

Figure 2-5 shows how Layer 3 routing protocols interact with the Unicast Routing Information Base Daemon and Network Services Module.

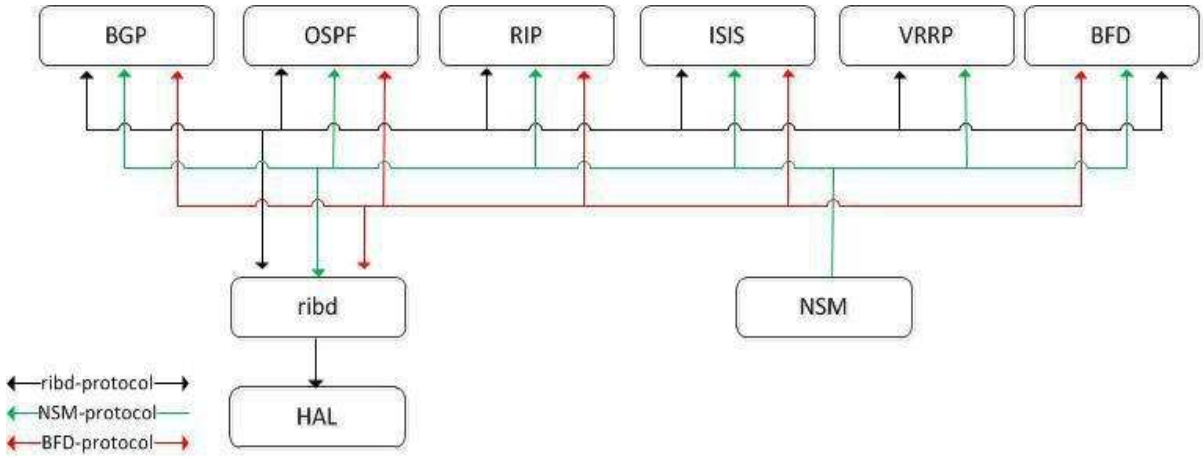


Figure 2-5: Layer 3 routing architecture

The protocol modules communicate with Network Services Module for interface updates and with the Unicast Routing Information Base Daemon for route updates and redistributed routes.

In addition to the standard Layer 3 routing protocols, SWMRE offers:

- Virtual Routing (VR) support
- Traffic Engineering (TE) extensions
- Constrained Shortest Path First (CSPF) topology support for the Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS) protocols

Unicast Routing Information Base Daemon

In SWMRE, the unicast Routing Information Base daemon (`ribd`) is responsible for maintaining a central unicast Routing Information Base.

A Routing Information Base (RIB) is a data structure stored in a network device that lists the routes to particular network destinations and metrics (distances) associated with those routes. A RIB contains information about the topology of the network immediately around it. Maintaining a RIB by discovering network topology is the primary purpose of dynamic routing protocols such as BGP, RIP, and OSPF. Static fixed routes are added to a RIB by commands. (A RIB is also called a routing table.)

A Forwarding Information Base (FIB) is used to find the proper interface to which an input interface should forward a packet. In contrast to RIBs, FIBs are optimized for fast lookup of destination addresses. (A FIB is also called a forwarding table.)

Protocol modules create their own routes, and communicate this protocol-specific information to `ribd` via InterProcess Communication (IPC) messaging functions. The `ribd` RIB contains all routing information received from routing peers, for example, destination prefix, nexthop information, and distance. Figure 2-6 shows how the Layer 3 protocols, `ribd`, and the kernel communicate.

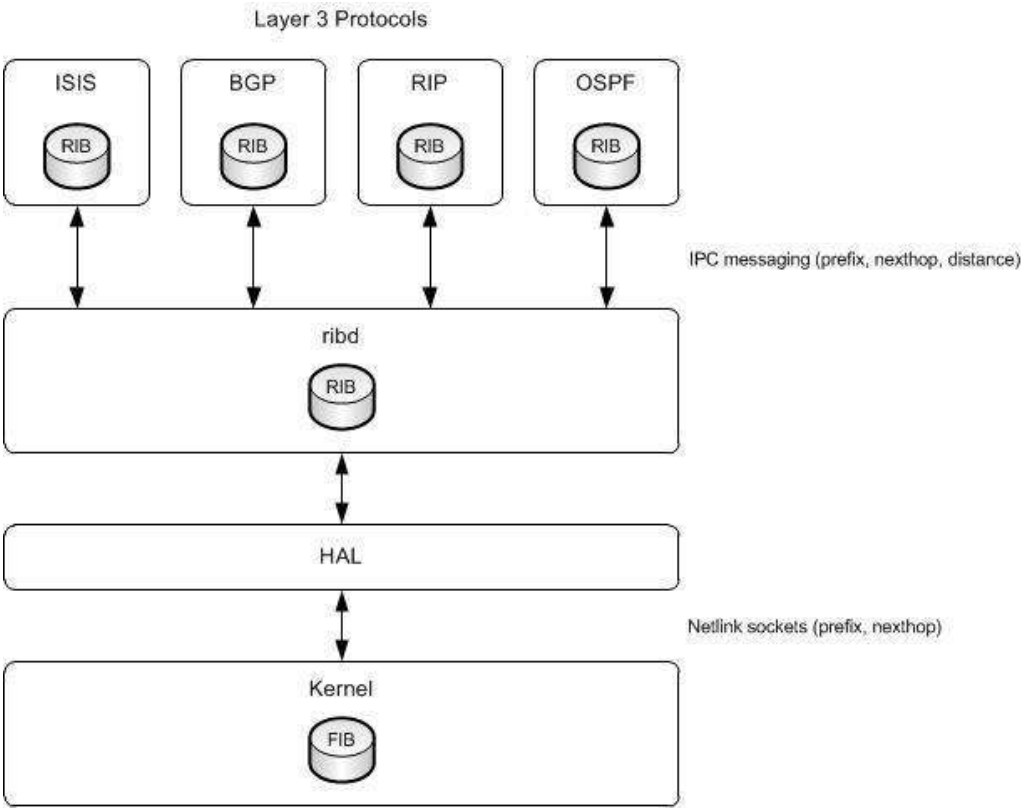


Figure 2-6: Protocol, ribd, and kernel interaction The

tasks of the `ribd` daemon are to:

- Communicate with SWMRE routing and switching modules to get routing information updates
- Provide configuration for static routes
- Process the routing information and maintain all the received routes from clients as part of the RIB • Maintain the FIB
- Process the routes and select the FIB route and program the kernel.

- Redistribute routes
- Handle interface up and down events

For every known prefix, `ribd` maintains a route node entry in its RIB. The `ribd` process populates this table upon receiving routes from:

- Protocols such as BGP, OSPF, and RIP
- Static routes configured using commands
- The kernel FIB
- Connected routes derived from interface information

Routing protocols use different metrics to calculate the best path for a destination. The best path is sent to the `ribd` process.

The kernel FIB contains the minimum amount of information required to make a forwarding decision on a particular packet, for example, destination prefix and nexthop information. This abbreviated form of the information in the RIB is transferred from `ribd` to the kernel FIB via Netlink sockets.

For more about the ribd daemon, see the *Unicast Routing Information Base Developer Guide*.

Border Gateway Protocol

Border Gateway Protocol (BGP) is a core exterior gateway protocol (EGP) used on the Internet. BGP maintains a table of IP networks, or prefixes, which designate network reachability among Autonomous Systems (AS). BGP is a pathvector protocol that makes routing decisions based on path, network policies, and/or rule sets.

SWMRE supports Border Gateway Protocol (BGP4+) versions 4 and 4+ and offers optional VPN extensions for MPLS-VPN support. The VPN extensions work with NSM, MPLS-LDP, RSVP-TE, and MPLS forwarder modules.

SWMRE BGP4+ features include:

- IPv4 and IPv6 support
- Route Reflection
- Route Refresh
- Community Attributes
- Community Attributes in Multi-Home Routing
- Extended Communities
- Protection of BGP Session via the TCP MD5 Signature Option
- Capabilities Advertisement
- Route Flap Damping
- E-BGP Multi hop
- Stateful implementation
- Multi-protocol BGP extensions
- BGP/MPLS VPNs
- BGP Graceful restart
- BGP4+ Inter-Domain Routing (IDR):
- Virtual Routing and Virtual Routing and Forwarding Support
- Full MIB support

For more information about BGP, see the *Border Gateway Protocol Developer Guide.*

Open Shortest Path First

Open Shortest Path First (OSPF) version 2 is a link-state routing protocol that runs internally on a single autonomous IPv4 system. Each router designated to run OSPF maintains an identical database describing the autonomous system's topology. From this database, a routing table is calculated by constructing a shortest-path tree. OSPF version 3 contains extensions to support IPv6 networks. The protocol is also extensible to other address families. SWMRE supports the following OSPF standards:

SWMRE OSPF features include:

- Opaque Link State Attributes (LSA)
- Multiple Instance Support
- Intra- and inter-area routing
- Type 1/2 external routing
- OSPF “not so stubby area” (NSSA) Option
- Inter domain Routing Protocol (IDRP) for IP-OSPF Interaction
- Opaque link state availability (LSA) Option
- Manual and automatic virtual links
- Equal Cost Multi Path (ECMP)
- Broadcast, point-to-point and point-to-multi-point models
- MD5 authentication
- Incremental SPF
- Traffic Engineering extensions
- Virtual Routing (VR) and Virtual Routing and Forwarding (VRF) support
- Graceful restart
- Full MIB support
- Optional Virtual Private Network (VPN) support
- Optional Constrained Shortest Path (CSPF) support

For more information about OSPF, see the *Open Shortest Path First Developer Guide.*

Routing Information Protocol

The Routing Information Protocol (RIP) version 2 is one of the most commonly used interior gateway protocols (IGP) for routing on internal IPv4 networks, and to a lesser extent, networks connected to the Internet. RIP employs a distributed variant of the Bellman-Ford algorithm to provide distance vector routing capabilities. RIP also supports subnet information, thus allowing Classless Inter-domain Routing (CIDR).

RIPng contains extensions to support IPv6 networks.

SWMRE RIP/RIPng features include:

- Split horizons with poisoned reverse
- Triggered updates
- ECMP (Equal Cost Multi path Routing) support
- Virtual Routing and Virtual Routing and Forwarding Support

- Full MIB support

For more information about RIP, see the *Routing Information Protocol Developer Guide.*

Intermediate System to Intermediate System

Intermediate System-to-Intermediate-System (IS-IS) is a link-state routing protocol that runs internally on a single autonomous system. IS-IS routers maintain identical databases that describe the autonomous system's topology. A routing table is calculated from the database by constructing a shortest-path tree.

SWMRE IS-IS features includes:

- Traffic Engineering extensions
- IS-IS MIB support
- Multi-protocol support for IPv4 and IPv6
- Equal cost Multi path
- Dynamic Host name Exchange Mechanism
- IS-IS Mesh Groups
- Traffic Engineering
- Restart Signaling
- Multi-topology routing
- Virtual Routing and Virtual Routing and Forwarding Support

For more information about IS-IS, see the *Intermediate System and Intermediate System Developer Guide.*

Virtual Router Redundancy Protocol

The Virtual Router Redundancy Protocol (VRRP) allows a virtual router composed of two or more VRRP routers on the same subnet to prevent failure by providing at least one standby virtual router if the master virtual router fails. VRRP eliminates the single point of failure most common in a static default routed environment.

In SWMRE, VRRP functions are handled by the `vrrpd` daemon whose tasks are to:

- Bring up or down VRRPv4 or VRRPv6 sessions in the respective VR mode
- Create and delete VRRP sessions dynamically
- Transmit and receive VRRP packets to and from the virtual-router peers based on the time-out value or the current state of the VRRP router and performs functions related to the VRRP Finite State Machine (FSM).

VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP addresses associated with a virtual router is called the master, and it forwards packets sent to these IP addresses. The election process manages dynamic fail-over in the forwarding responsibility should the master become unavailable. Any of the virtual router's IP addresses on a LAN can then be used as the default first-hop router by end-hosts. The advantage of using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.

The NSM client code in the VRRP daemon handles updates from NSM and builds the local interface table. The VRRP master sends the VIP and VMAC to HSL which is installed in the kernel. This allows the master to process the forward the traffic sent to VRRP Virtual Router.

SWMRE supports VRRP as specified in RFC 5798.

For more information about VRRP, see the *Virtual Router Redundancy Protocol Developer Guide.*

Bidirectional Forwarding Detection

Bidirectional Forwarding Detection (BFD) reduces the reliance upon the relatively slow Hello mechanism in routing protocols to detect failures where no hardware signaling is available to assist. BFD works with BGP, OSPFv2, and ISIS to enable them to configure BFD sessions, and for the sessions to receive the bidirectional forwarding failure notifications.

BFD provides the following features:

- A single mechanism to detect liveliness over any media and in any protocol layer
- Rapid detection of communication failures between adjacent systems to quickly establish alternative paths
- Passive, Active, Synchronous, Asynchronous, and Demand modes of operation
- Improved system performance when faster detection is required, because data-plane reachability detection is detached from control-plane functionality
- A separate process that works in tight conjunction with routing protocols and NSM to detect forwarding plane reachability to protocol next hops
- SWMRE protocol modules support BFD irrespective of where BFD packet-sending operations take place: in the interfaces, data links, or to some extent, in the forwarding engines themselves
- BFD is Graceful-Restart unaware: whenever BFD timers expire, a session-down event is triggered to the protocol module, and BFD maintains sessions for the protocol while it undergoes Graceful Restart
- A fast mechanism to detect liveliness of static next-hops

For more information about BFD, see the *Bidirectional Forwarding Detection Developer Guide.*

Equal Cost Multi-Path

Equal-Cost Multi-Path (ECMP) is a forwarding mechanism for routing packets along multiple paths of equal cost and ensures load balancing across multiple paths. The SWMRE implementation leverages Forwarding Plane Load Balancing. Link-state protocols which use a cost-based metric such as OSPF and ISIS explicitly allow ECMP routing.

SWMRE installs the maximum number of ECMP routes supported by a kernel. This allows for load balancing to be performed with more than one nexthop to reach a destination. If the router receives and installs multiple paths with the same administrative distance and cost to a destination, load-balancing is possible.

IPv6 Transition

With SWMRE, you can integrate into your existing gateways and Customer Premises Equipment (CPE), protecting your network investment. ISPs and other access providers require a migration strategy to enable them to continue to provide full connectivity throughout the transition to IPv6. The is applicable for both new IPv6-based services and existing IPv4 services moving to IPv6 with:

- IPv6 Rapid Deployment provides IPv6 tunnels over existing IPv4 access network between your CPEs and your gateways to provide your customers secure access to IPv6 networks and services.
- IPv4 Residual Deployment provides stateless IPv4 over IPv6 tunnels for your existing IPv4 customers with efficient global IPv4 address sharing. The advantage of stateless tunneling is that it does not require managing per user state; abusive users can easily be identified. Furthermore, stateless tunneling simplifies high availability and scalability of the gateway since the need to scale is only based on traffic volume.

Multicast Protocols

SWMRE provides these multicast protocol daemons:

- Layer 2 Multicast Routing Information Base Daemon
- Layer 3 Multicast Routing Information Base Daemon
- Protocol-Independent Multicast Daemon
- Multi Protocol Label Switching Protocols

Layer 2 Multicast Routing Information Base Daemon

The responsibilities of Layer 2 multicast Routing Information Base daemon (`l2mribd`) include:

- Updates hardware with snooping information.
- Interacts with NSM, for bridge, VLAN, and port related information and their association with each other.
- Interacts with MSTP for spanning tree related information.
- Interacts with MSTP to receive VLAN-to-instance mapping and TCN messages.
- Communicates with the `mribd` daemon to receive IGMP status on the VLANs. If IGMP is enabled on a VLAN, IGMP snooping functionality is disabled and vice versa.
- Processes IGMP and MLD packets and maintains group membership for all interfaces based on which multicast traffic forwarding is done. It also add/deletes the group membership information in hardware.

Figure 2-7 shows the Layer 2 multicast architecture.

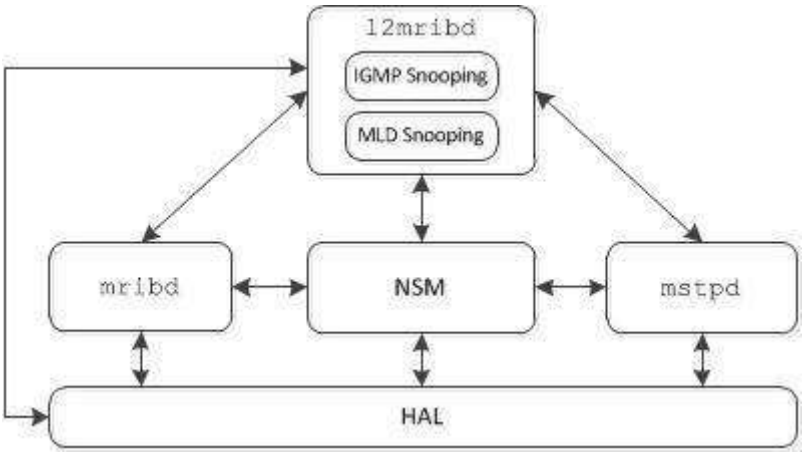


Figure 2-7: Layer 2 multicast architecture

The Layer 2 multicast modules support IPv4 or IPv6, or combination IPv4 and

IPv6. The features of the `l2mribd` daemon include:

- Internet Group Management Protocol (IGMP) Snooping: ability to passively snoop on IGMP packets to learn the IPv4 multicast group membership information. With IGMP snooping, multicast traffic in a group is only forwarded to ports that have members in that group. SWMRE supports IGMP snooping functionality for IGMP versions 1, 2, and 3.
- Multicast Listener Discovery (MLD) Snooping: ability to passively snoop on MLD packets to learn the IPv6 multicast group membership. With MLD snooping, multicast traffic is only forwarded to ports that request receipt of packets from the source. SWMRE supports MLD snooping functionality for MLD versions 1 and 2

For more information about Layer 2 multicast support, see the *Multicast Protocol Developer Guide.*

Layer 3 Multicast Routing Information Base Daemon

The multicast protocols communicate with the `mribd` daemon which communicates with the multicast forwarder. A common multicast routing information base allows multiple multicast protocols to function simultaneously.

Figure 2-8 shows the Layer 3 multicast architecture of SWMRE. The `mribd` daemon holds the multicast RIB and consolidates the routes from multicast routing protocols such as Protocol-Independent Multicast Daemon and Multi Protocol Label Switching Protocols and installs them in the kernel and sends them to HSL to install in the hardware. NSM provides the VR/VRF as well as the interface updates to the `mribd` daemon, the `pimd` daemon, and the kernel multicast forwarder.

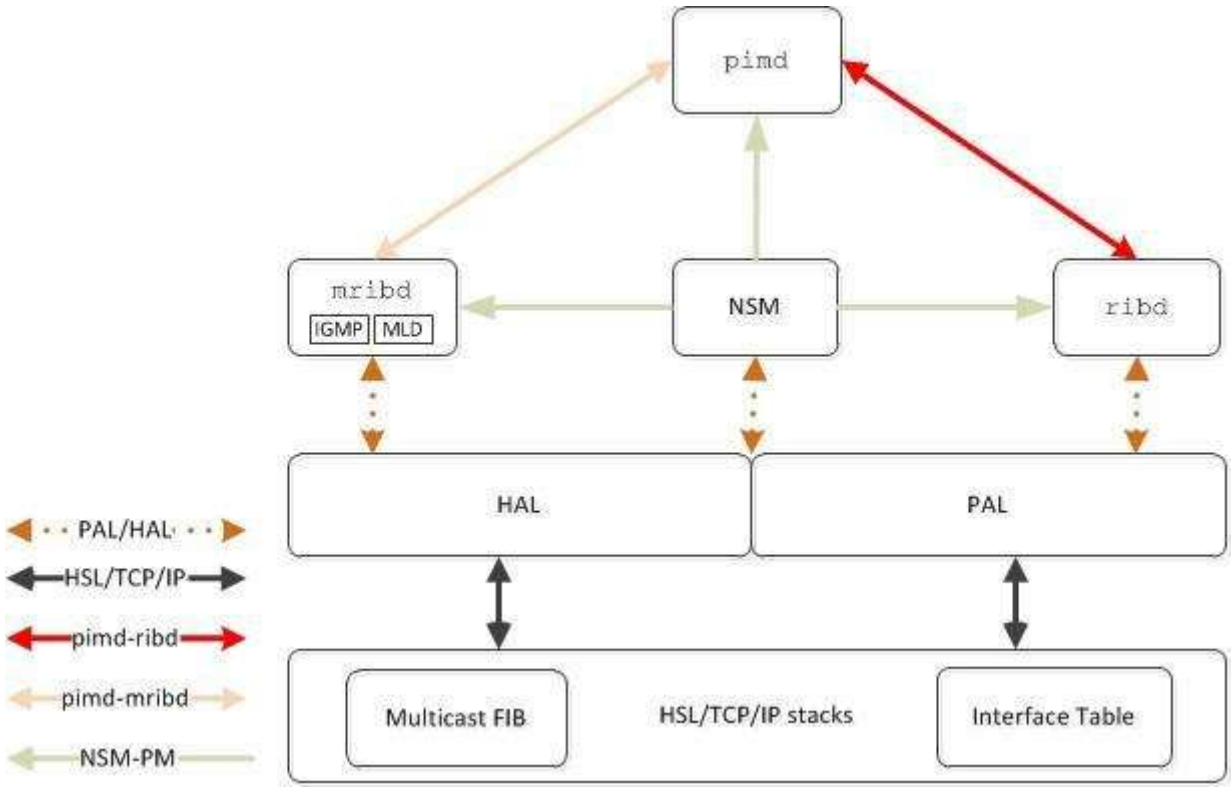


Figure 2-8: Layer 3 multicast architecture The

`mribd` daemon supports the following functions:

- Adds, deletes, and updates multicast routes in the route table and programs the kernel
- Multicast Virtual Interface (VIF) management for IPv4 networks
- Multicast Interface (MIF) management for IPv6 networks
- Multicast Route Entry management for IPv4 and IPv6
- Multicast Forwarder Event handling for IPv4 and IPv6
- Multicast Forwarding Entry statistics for IPv4 and IPv6
- Multicast Tunnel management for IPv4 only
- IGMP versions 1, 2, and 3 services (IPv4): Used by IP hosts and adjacent multicast routers to establish multicast group memberships
- IGMP Proxy

- Signals IGMP membership to multicast routing protocols like PIM
- MLD versions 1 and 2 services (IPv6): used by a by a device to discover listeners for a specific multicast group in the same manner as IGMP is used in IPv4
- MLD Proxy

For more information about Layer 3 Multicast, see the *Multicast Protocol Developer Guide.*

Protocol-Independent Multicast Daemon

Protocol-Independent Multicast (PIM) is a family of multicast routing protocols for IP networks that provides one-tomany and many-to-many distribution of data over a network. PIM is termed *protocol-independent* because it does not have its own topology discovery mechanism, but instead uses routing information supplied by other routing protocols.

SWMRE support these variants of PIM:

- PIM Sparse Mode (PIM-SM: RFC 4601) efficiently establishes distribution trees across wide area networks (WANs) by routing packets to multicast groups. PIM-SM constructs a tree from each sender to the receivers in a multicast group and packets from the sender follow the tree to interested recipients. PIM-SM is for situations where multicast groups are thinly populated across a large region. Although it can operate in LAN environments, it is most efficient in WAN environments.
- PIM Dense Mode (PIM-DM: RFC 3973) is a data-driven routing protocol that builds source-based multicast distribution trees that operate on the flood-and-prune principle. PIM-DM uses dense multicast routing and implicitly builds shortest-path trees by flooding multicast traffic domain wide, and then pruning back branches of the tree where no receivers are present. PIM-DM effectively distributes data to target recipients in a concentrated area. PIM-DM is straightforward to implement but generally has poor scaling properties.
- PIM Source-Specific Multicast (PIM-SSM: RFC 3569) is a subset of PIM-SM that allows deployment of SSM in a network with hosts that do not support IGMP version 3. PIM-SSM builds trees that are rooted in just one source, offering a more secure and scalable model for a limited amount of applications (mostly broadcasting of content). In PIM-SSM, an IP datagram is transmitted by a source S to an PIM-SSM destination address G, and receivers can receive this datagram by subscribing to channel (S,G).
- Bidirectional PIM (BIDIR-PIM: RFC 5015), is a variant of PIM-SM which dispenses with both encapsulation and source state by allowing packets to be natively forwarded from a source to the RP using shared tree state. These benefits can be observed when using a Many-Many multicast deployment.

The `pimd` daemon holds the PIM states and takes care of PIM packet processing. The `pimd` daemon also holds the Tree Information Base (TIB) with all multicast routes. The `pimd` daemon operations include:

- Interacts with NSM for interface updates
- Receives local group membership information from IGMP (MRIB). Installs multicast interfaces (VIF) and multicast routes to MRIB.
- Processes PIM packets from PIM neighbor routers The PIM features are:
- Any Cast RP
- Bootstrap router
- PIM MSDP • PIM border

For more, see the *Protocol Independent Multicasting Developer Guide*.

Multi Protocol Label Switching Protocols

Multi-Protocol Label Switching (MPLS) operates at a layer operated between traditional definitions of Layer 2 (data link layer) and Layer 3 (network layer). The MPLS modules provide integration into enterprise, edge, and core communications equipment.

The SWMRE MPLS module supports the following protocols and features:

- Label Distribution Protocol
- Traffic Engineering
- Resource ReSerVation Protocol-Traffic Engineering
- Differentiated Services
- Layer 2 Virtual Private Network
- Layer 3 Virtual Private Network
- MPLS-TP Operation, Administration and Management

For more information about MPLS, see the *Multi Protocol Label Switch Developer Guide*

Figure 2-9 shows the MPLS high-level architecture.

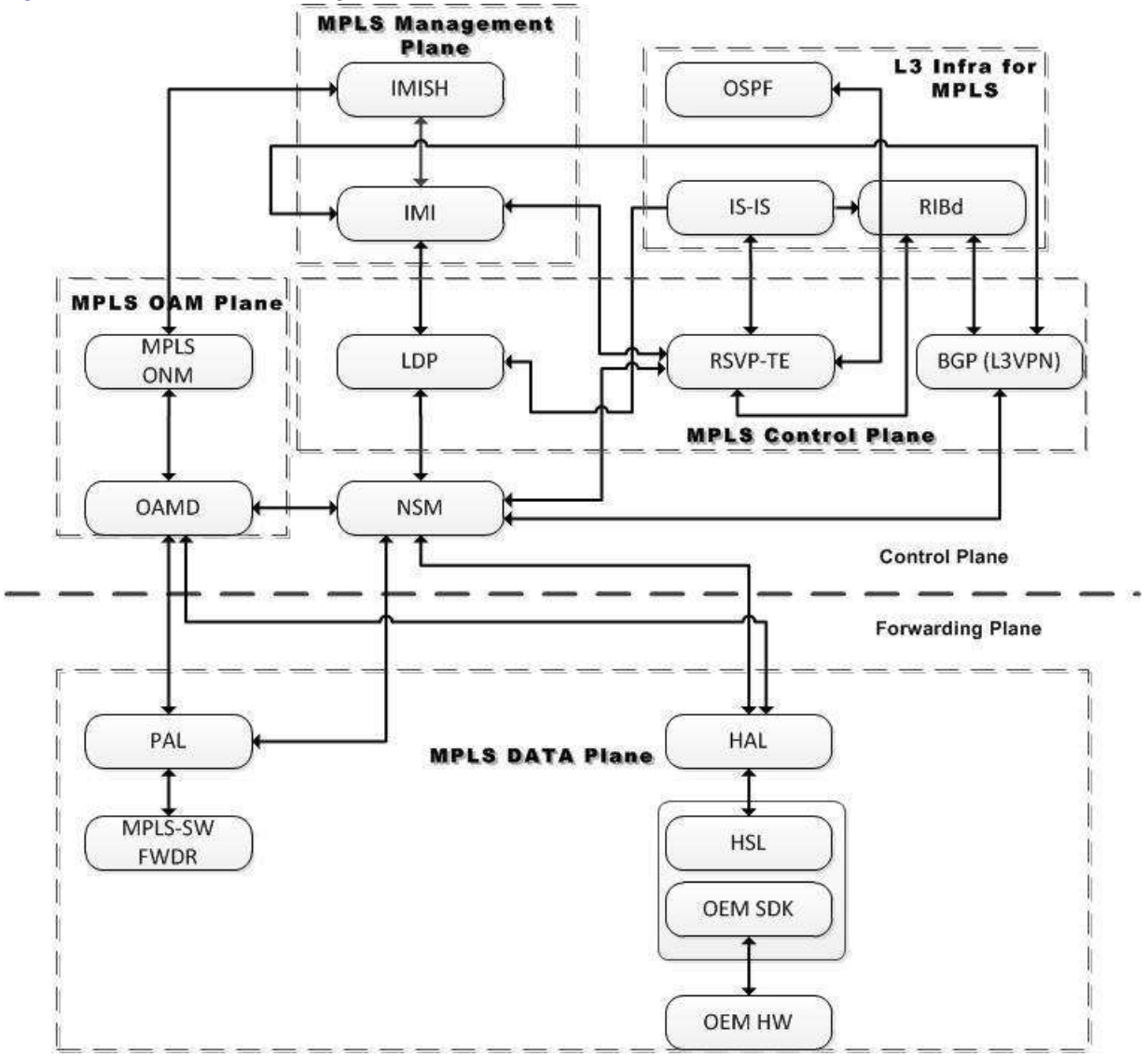


Figure 2-9: MPLS High Level Architecture

The following summarizes the architecture.

- IMISH: Provides the commands to configure the MPLS/MPLS-TP on-demand OAMs. This module interacts with the MPLS ONM to interface with the OAMD module to configure an on-demand OAM.
- MPLS ONM: Interface between IMISH and OAMD, which performs the OAM functionality. The OAMD uses the MPLS ONM to send the results of an active on-demand OAM session to IMISH to display the results to the enduser.
- OAMD: Performs on-demand and proactive OAM activities. It also provides the configuration and show commands for all proactive OAMs. This module interacts with NSM when the MPLS/MPLS-TP transport path information is required to transmit an OAM payload and to act on a received OAM payload. It uses PAL to send and receive the OAM payloads via the MPLS software forwarder.
- NSM: Houses all the MPLS/MPLS-TP transport path information. It handles the OAMD module, providing the required transport path information for OAM payload transmission and reception.

- LDP: Distributes labels between peers to form a Label Switched Path (LSP). NSM houses the MPLS Routing Information Base. LDP sends FTN/ILM obtained as result of LSP signaling to NSM. NSM installs these routes in MPLS software forwarder/hardware which will be used to forward data packets. This module also establishes LDP sessions between non-directly connected peers (T-LDP).
- RSVP-TE: Establishes traffic engineered label switched path. RSVP-TE queries CSPF to compute the explicit routes. Similar to LDP, RSVP-TE also sends FTN/ILM to NSM and NSM installs in MPLS software forwarder/ hardware.
- PAL: Interface between the OAMD and the MPLS software forwarder. It provides the necessary APIs to OAMD to send the OAM payloads to the MPLS software forwarder. It also aids the OAMD in registering for callbacks required to process incoming OAM payloads.
- MPLS software forwarder: Transmits OAM payloads received from OAMD over an MPLS/MPLS-TP transport path. This module also de-multiplexes any MPLS/MPLS-TP OAM payload received over a transport path and sends it to the OAMD for further processing.

Label Distribution Protocol

With the Label Distribution Protocol (LDP), two label-switched routers (LSR) exchange label mapping information. The two LSRs are called LDP peers and the exchange of information is bi-directional. LDP is used to build and maintain databases of LSRs that are used to forward traffic through MPLS networks.

LDP works with other routing protocols (RIP, OSPF, and BGP) to create the label-switched paths (LSP) used when forwarding packets. An LSP is the path taken by all packets that belong to the Forwarding Equivalence Class (FEC) corresponding to that LSP. In this way, SWMRE LDP assigns labels to every destination address and destination prefix provided by the `ribd` daemon. The LDP interface to the MPLS forwarder adds labels to and deletes labels from the forwarding tables.

Traffic Engineering

Traffic Engineering (TE) is a signaling protocol that supports explicit routing capability to establish Label-Switched Paths (LSPs) in a MPLS network. RSVP-TE creates explicitly routed paths, which might not agree with the route suggested by the Interior Gateway Protocol (IGP) such as OSPF or IS-IS.

Resource ReSerVation Protocol-Traffic Engineering (RSVP-TE) provides signaling information for traffic engineering in an MPLS network. A router that supports MPLS as either an LER or an LSR uses RSVP-TE to request quality of service (QoS) tasks from the network for a flow that a network operator has provisioned.

TE extensions use the RSVP and LDP dynamic-signaling protocols to communicate to the SWMRE MPLS forwarder or a third-party MPLS forwarder. The RSVP-TE extension enables MPLS to scale into large and complex IP-based communications equipment.

For computing explicit routes to reach the destination:

1. RSVP-TE queries Constrained Shortest Path First (CSPF) (OSPF or IS-IS) for a complete, end-to-end, explicit route based on constraints specified by the network administrator.
2. CSPF refers to the Traffic Engineering Database (TED) for computing the explicit route.
3. The resulting explicit route is used by a signaling protocol (RSVP-TE or LDP) to set up LSPs.

NSM maintains local TE parameters and it updates the TED of IS-IS and OSPF. If there is any change in TEparameters, NSM updates the same in IS-IS/OSPF. IGPs exchange the TE parameters with their peers.

MPLS for Traffic Engineering has these advantages:

- LSPs are not constrained because of destination based forwarding paradigm can be created through manually or through automatically by the underlying protocols
- LSPs can be efficiently maintained
- MPLS allows traffic aggregation and disaggregation unlike classical destination which only allows IP forwarding and permits only aggregation
- Easy integration of “constraint-based routing” framework with MPLS Figure 2-10 shows the MPLS Traffic Engineering high level architecture.

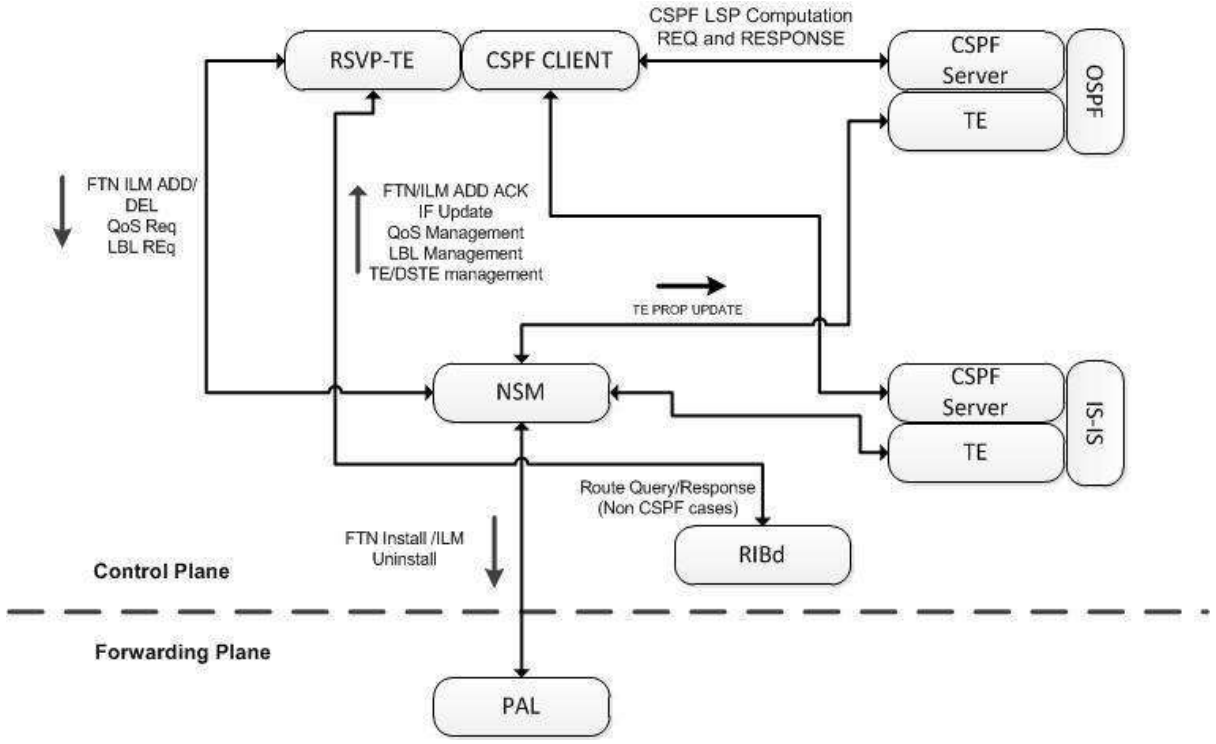


Figure 2-10: MPLS Traffic Engineering

Resource ReSerVation Protocol-Traffic Engineering

Resource ReSerVation Protocol-Traffic Engineering (RSVP-TE) communicates with the QoS module in NSM to:

- Find if the requested bandwidth is available
- Reserve bandwidth for an LSP
- Release a reserved resource

To manage labels, RSVP-TE communicates with the label pool manger in NSM. NSM provides a label block and RSVP-TE assigns a label for each LSP within the label range provided by NSM. If all labels in a label block are exhausted, RSVP queries and gets the next available label block from NSM.

- RSVP-TE gets interface up/down events from NSM
- RSVP-TE queries RIB for next hop information
- RSVP-TE sends FTN/ILM (obtained as result of LSP signaling) to NSM
- NSM maintains MPLS RIB information (FTN/ILM) and installs it in hardware

Differentiated Services

Differentiated Services (DiffServ) specifies a simple, scalable and coarse-grained mechanism to classify and manage network traffic and provides Quality of Service (QoS) guarantees for service providers. To provide a flexible DiffServeover-MPLS solution, DiffServ extends the RSVP-TE module. The DiffServ module enables network traffic to be specified and prioritized by class, so that certain kinds of traffic, for example voice traffic, attain precedence over other types of traffic.

Because DiffServ by itself lacks the ability to efficiently use network transmission resources. The DiffServ-TE module performs traffic engineering per DiffServ class, rather than at an aggregate level. By combining DiffServ with MPLS-TE, routing devices can simultaneously classify and prioritize traffic and achieve fined-grained optimization of transmission resources.

The SWMRE implementation of DiffServ supports RFC 3270 and RFC 4124.

Layer 2 Virtual Private Network

SWMRE offers MPLS Layer 2 Virtual Private Network (VPN) and Virtual Private LAN Service (VPLS) protocol modules that enhance MPLS by providing transparent LAN access between VPN sites. The VPN infrastructure for provider-edge equipment uses the IP routing, traffic engineering, and MPLS switching features of SWMRE.

Figure 2-11 shows the MPLS Layer 2 VPN high-level architecture.

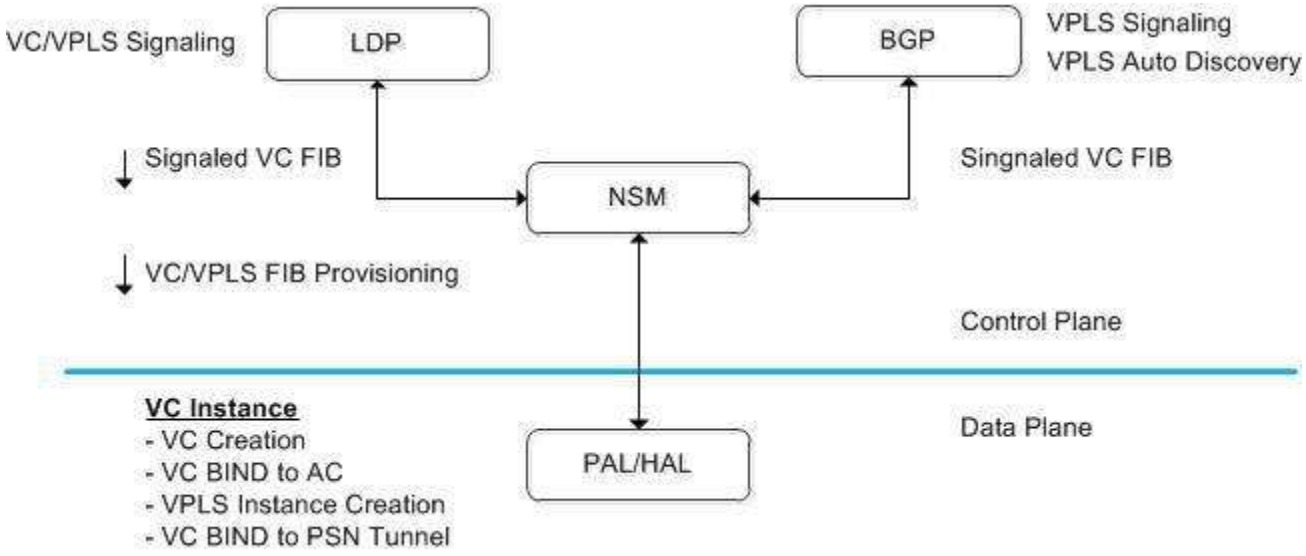


Figure 2-11: Layer 2 VPN

MPLS Layer 2 VPN provides end-to-end connection over a MPLS tunnel. Virtual Circuits (VC) addresses the problem of point-to-point VPN connections in MPLS VPNs. VPLS presents a solution for multipoint connectivity for the Layer 2 MPLS VPN.

In SWMRE, MPLS-Layer 2VPN is achieved using signaling protocols such as LDP, BGP, or by static configuration. During VC/VPLS configuration, IMI relays all the VC/VPLS configuration information to NSM. NSM creates a VC/VPLS instance and bind this instance to the attachment circuit and PSN tunnel. Additionally, NSM sends this information to LDP and BGP which starts the signals:

- LDP provides signaling of VC/VPLS information and establishes targeted session and VC label exchange. The exchanged VC labels (FIB) are then sent to NSM.
- BGP uses auto-discovery to learn peers participating in a VPLS instances. Once the peers are discovered, VC labels are exchanged. The exchanged VC labels (FIB) are then sent to NSM.

NSM maintains the VC and PSN label information and installs the FIB information in the hardware.

Note: The SWMRE Layer 2VPN solution has signaling extensions for both VPWS (Virtual Private Wire Service) and VPLS.

Layer 3 Virtual Private Network

The MPLS Layer 3 Virtual Private Network (Layer 3 VPN) is a PE-based technology for service provider VPN solutions. It uses BGP to advertise VPN routes and uses MPLS to forward VPN packets on service provider backbones. A CE first establishes adjacency with a directly connected PE and advertises its VPN routes to the PE and learns remote VPN routes from that PE. A CE and a PE use BGP/IGP to exchange routing information

The SWMRE Layer 3 MPLS-VPN solution is supported by the SWMRE MPLS forwarder and LDP modules by tightly integrating BGP-VPN extensions. It provides address space and routing separation through the use of per-VPN routing tables (VPN Routing and Forwarding) and MPLS switching in the MPLS core.

Figure 2-12 shows the MPLS Layer 3 VPN high level architecture.

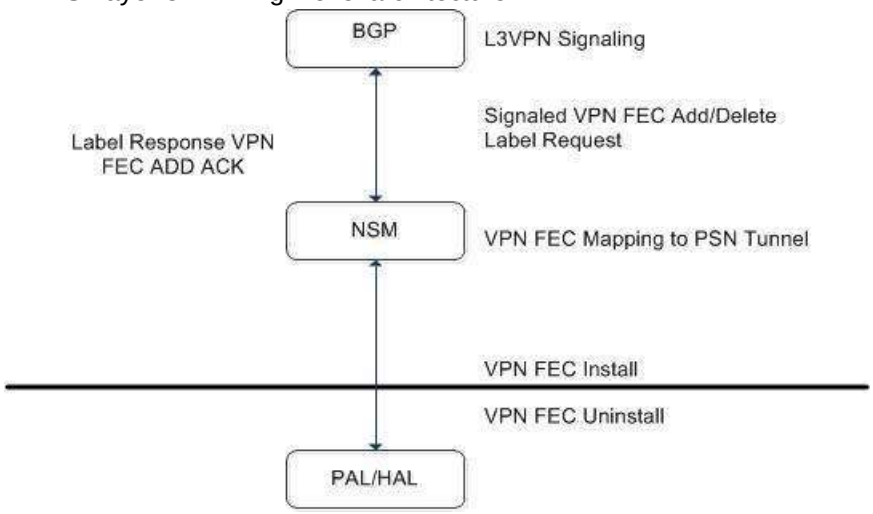


Figure 2-12: Layer 3 VPN

SWMRE supports BGP-MPLS VPNs for both IPv4 and IPv6. Customer data packets are tunneled through the backbone, so that core routers are unaware of IPv4 and IPv6 VPN routes. NSM gives the routes it has learned from IGPs to BGP. BGP allocates the labels for these prefixes and then informs its peer about these labels. BGP then interacts with NSM to install the labels in the forwarder and to map the VPN prefix to the underlying MPLS tunnel. Data traffic is encapsulated with BGP labels and sent on the MPLS tunnel.

Virtualization

SWMRE supports different virtualization concepts like Virtual Router (VR) and Multi-Tenancy (MT).

Virtual Router (VR)

The Virtual Router (VR) feature logically subdivides a physical router into multiple virtual routers, with each virtual router independently monitored and managed by the network administrator. Each VR can have multiple VRFs (Virtual Routing and Forwarding instances) supporting multiple routing tables (RIBs) co-existing within the same router at same time. A single instance of SWMRE manages all the VRs and its VRFs. SWMRE offers VR support for both IPv4 and IPv6 routing protocols.

VR/VRF with Namespaces

Multiple Forward Information Base (FIB) tables in x86 platforms (using Linux kernel versions 3.0 and later) are supported using Linux namespaces. Each VRF is essentially mapped to one network namespace which has a Forwarding Information Base. SWMRE supports the segregation of VRF routes at the control plane level which is extended to the FIB in the Linux IP stack using the namespace concept.

Multi-Tenancy

Multi-tenancy (MT) is a virtualization concept to create independent slices of a device, each of which can be individually managed and configured. Multi-tenancy is based on file system partitioning using `chroot` jails and Linux namespace support. This namespace allows the user of the Linux kernel to create multiple instances of a given resources. For example, the network namespace can be used to create multiple IP stacks.

In each tenant or logical partition, a complete instance of SWMRE control plane (Layer 3 and Layer 2) can be executed.

The high level modules in the system are:

- Logical Switch Router (LSR): A LSR is one partition of a physical switch and provides virtualization for management plane, control plane and data plane. Each LSR has an instance of the control plane processes (OSPF, BGP, RIP, STP, RIB, MRIB, NSM), management plane processes (SNMPD, IMI) and system services processes (SYSLOGD) running in the LSR under a `chroot` jail.
- Default LSR/ Privileged LSR: The default/ privileged LSR (LSR 0) is always active and enabled and can never be deleted. This LSR comprises the LSM which manages the multi-LSR eco-system.
- Logical System Manager (LSM): This module is a separate Linux process that is responsible for LSR management:
- Creating and deleting LSRs
- Setting up the environment for the LSR such as the root file system
- Loading/unloading individual processes in a LSR

  LSM is only present in the default/privileged LSR. When the LSR is created, all processes needed for the the LSR are loaded (imi, nsm, rib, mrib, syslogd, vlogd, snmpd).
- `syslogd`: Linux logger daemon. One instance of `syslogd` runs per LSR.

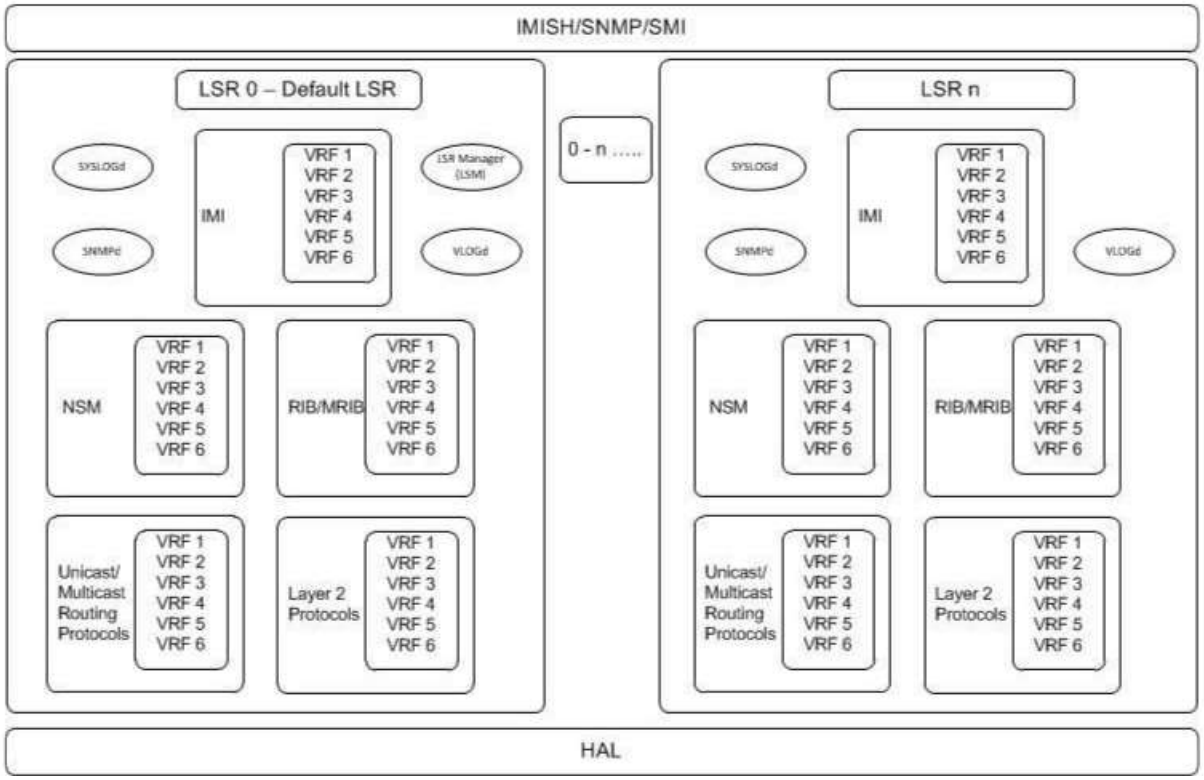


Figure 2-14: Multi-Tenancy

CHAPTER 3 SWMRE Abstraction Layers

This chapter describes the abstraction layers in SWMRE that enable hardware and software portability:

- The Platform Abstraction Layer (PAL) enables SWMRE to be ported to different operating systems and CPUs
- The Hardware Abstraction Layer (HAL) decouples the SWMRE protocol modules from the underlying data plane, enabling portability across multiple silicon switching chipsets

These abstraction layers isolate hardware and operating system specific interactions to a small set of well-defined function calls for the control plane. The abstraction layers provide a unified interface for the control plane to interact with the data plane for all Layer 2, Layer 3, multicast, and MPLS forwarding needs. The functions calls above the abstraction layer run unmodified for any switching and routing hardware platform.

Additionally, this chapter describes the Hardware Services Layer (HSL) which implements the hardware system-related functions.

Platform Abstraction Layer

SWMRE provides platform independence with the Platform Abstraction Layer (PAL) functions. The PAL functions call the system services specific to the platform to isolate SWMRE daemons from the operating system.

PAL allows SWMRE to support multiple operating systems. The complexity of each component is handled by a PAL module for each OS. This allows a SWMRE component to make an OS-independent call and then the compile-time options link the appropriate PAL module that fulfills that call.

SWMRE comes with a set of production-quality, fully-tested PAL modules for the most common operating systems. Any porting efforts to non-supported platforms can be modelled on these PAL modules.

Features

The features of PAL are as follows.

Memory Management

A memory management in PAL gives developers more control over memory, including setting the class and size of the requested storage.

Sockets

Sockets services are used to create TCP sockets. PAL sockets handle all socket functionality. For example, creating and deleting, reading and writing; and synchronizing. In addition, there are extensions to the socket calls that handle layer 2 and raw sockets.

String

The string abstraction includes string operations such as copying, scanning, parsing, and comparing. It interacts with the memory abstraction to create or move memory cells.

Standard Library

The standard library (`stdlib`) abstraction takes advantage of the most effective functions on the system. If there is an enhanced or particular functionality available for a feature, that functionality can be used in preference to the standard function.

Configuration Storage

PAL abstracts storage of configuration files. This allows platforms without a file system to store configuration information in any available memory model, including linear memory or flash memory.

Logging

Logging facilities are abstracted so that the system can log to any available facility, for example syslog, file, or console. These outputs can also run in parallel so that each output can be set independently to different log trap levels.

Interfaces and Routes

PAL abstracts kernel routes and interfaces. This allows SWMRE to not directly perceive how routes are manipulated.

Daemons

Process daemons are abstracted so that they are automatically handled on systems with this functionality.

Source

The source tree layout puts each protocol in its own directory. There is no platform-specific source in these directories. All calls, data types, and other components that are operating-system-specific or platform-specific are in subdirectories of the `pal` directory. All included modules either document other required included modules or automatically include the necessary modules.

Dummy Build Environment

A “dummy” build environment helps determine if the module include any system-dependent functions. The dummy environment excludes the system header files, and each module that builds with the dummy environment does not include any system-dependent functions. This ensures that all modules run in any PAL supported environment, even if that environment does not support the standard library feature.

Module Compatibility

Changes, additional features, and enhancements to protocols are restricted to the source for that module. Changes made necessary by a platform are restricted to the PAL module for that platform. A PAL API can change to support an operating system feature. This ensures backward compatibility for protocol modules with later versions of an API.

Hardware Abstraction Layer

As shown in Figure 3-15, the Hardware Abstraction Layer (HAL) enables the control plane to run on different hardware platforms, regardless of the type of chip set or operating system being used. Additionally, HAL makes the control plane fully independent of the specific TCP/IP stack implementation used with the operating system.

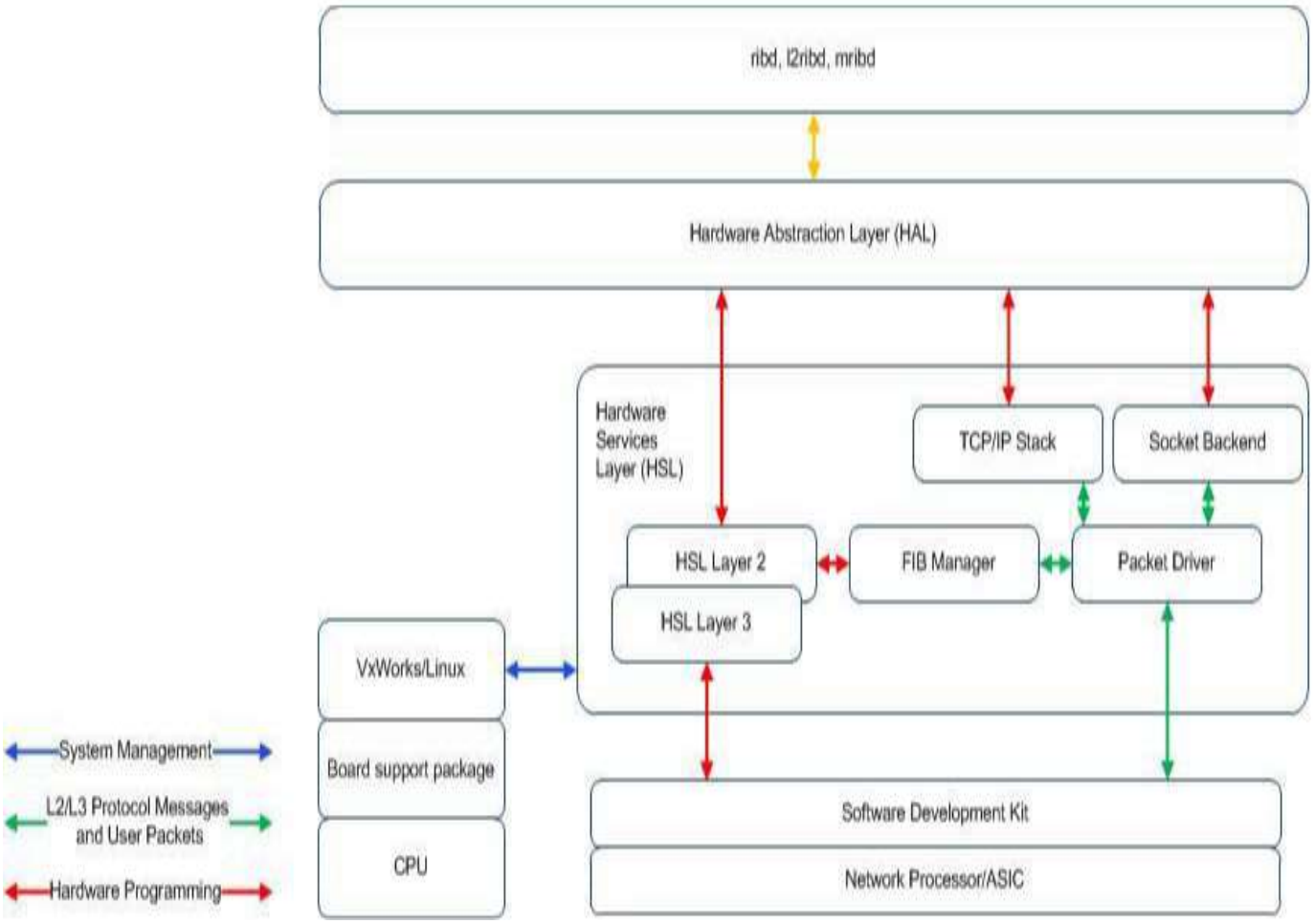


Figure 3-15: HAL and HSL HAL

has two major functions:

- Encapsulating and sending control messages: These messages originate from `ribd`, `l2ribd`, and `mribd`.
- Processing System Responses: HAL processes system responses and events, and calls the appropriate module in the control plane based on the type of event. The processing of system layer responses includes parsing or decoding of the message, and then notifying the appropriate module in the control plane, if required.

To accomplish these tasks, HAL has the following components:

- Socket communication layer
- Hardware Services Layer (HSL)
- Packet driver
- FIB manager
- Ethernet driver

Each component is described in the following sections.

Socket Communication Layer

HAL communicates with the Hardware Services Layer (HSL) through the socket communication layer. In other words, the control plane communicates with the forwarding plane through the socket communication layer. The communication tasks are:

Deliver hardware and operating system configuration messages

- Handle event messages generated by the forwarding plane • Poll forwarding plane information (such as interface information) The communication is based on a client/server model:
- The control plane implements the client side
- The forwarding plane implements the server side

During hardware initialization, the forwarding plane creates a server socket to which control plane clients connect once they start. All communication between the control plane and the forwarding plane is message-based.

SWMRE provides one proprietary `AF_HSL` family socket mechanism which is registered with the operating system.

Each message contains the following:

- Message type
- Message length
- Message data in the TLV encoded (length/field) format

The sender is responsible for preparing the message header and encoding the data. The receiver is responsible for decoding messages, acknowledging receipt of the message to the sender, and performing an integrity check.

Bulk Messaging and Asynchronous Messaging

With bulk messaging, several requests are sent in a single group or a few groups, relieving the burden on the IPC channel and optimizing performance. Bulk messaging is deployed across applications such as NSM, `mstpd`, `ribd`, and `mribd` that have intensive message transactions.

There is a mechanism to bulk information when programming the hardware in the HAL layer. This mechanism can be used by an application layer to bulk information when programming the hardware. However, this feature is not available on x86 platforms, but only for specific silicon vendor hardware.

With asynchronous messaging, the application layer can program the hardware to respond quickly and process the success or failure of a request later. Asynchronous messaging is implemented using message sequencing, a success/ failure callback mechanism, and timers. However, this feature is not available on x86 platforms, but only for specific silicon vendor hardware.

Hardware Services Layer

The Hardware Services Layer (HSL) implements the hardware system-related functions.

Note: Depending of the platform, portions of HSL run in user space or kernel space.

HSL has four main interfaces to the system which are described below:

- Socket Interface to control plane
- SDK interface to hardware
- Operating system Interface
- Event interface

Socket Interface to Control Plane

The socket interface receives control plane messages (such as configuration messages) and sends the response and notification.

SDK Interface to Hardware

The SDK (software development kit) interface configures the hardware chip set (fast path) according to the control plane messages. It is also retrieves counters and statistics.

Operating System Interface

The operating system interface configures the slow path according to control plane messages. The operating system interface also maintains a full forwarding information base (FIB), which is not restricted by hardware limitations.

Event Interface

The event interface registers callbacks with the hardware and the operating system to receive and process system events. Examples of callbacks are:

- Hardware module attachment/detachment
- Link/auto-negotiation status update,
- New address addition/notification from the operating system

HSL processes these events and notifies the control modules and system modules of the change.

For example, to detach an interface, a notification to the control plane is sent to stop all the protocols running on the detached interface. This also notifies the interface manager to delete the detached interface and any associated configuration.

A socket interface receives configuration updates and then sends responses and notifications. Message encapsulation and sending are similar to HAL; however, HSL does not require a response or acknowledgement message. Moreover, HSL acknowledges or sends a response to all messages.

HSL Operating System Functions

HSL uses abstracted operating function calls to provide services for the control plane.These functions are broadly abstracted for the following system services:

- Logging
- Memory allocation
- Synchronization mechanisms (semaphores)
- Thread/process management
- Inter-process communication (IPC)

FIB Manager

Networking devices store forwarding information in two databases:

- RIB (Routing Information Database) which represents a collection of all forwarding possibilities known to a device, learned from different sources, including identical and overlapping entries
- FIB (Forwarding Information Database) which represents an active selection of forwarding entries, used by a device to forward data

Traditionally, there are two paths for traffic forwarding:

- Fast Path where traffic moves via pre-programmed entries on a network processor or ASIC chip

Slow Path forwarding: the network processor or ASIC chip is unable to forward the traffic and data is sent to the CPU/OS before being processed

The FIB manager database contains all forwarding entries, learned dynamically and statically by the system:

- The FIB manager stores and programs forwarding entries selected for forwarding to the network processor or ASIC and operating system.
- The FIB manager removes forwarding entries from the network processor or ASIC and operating system if an entry was withdrawn from the FIB.

As shown in Figure 3-16, the FIB manager database maintains two radix trees:

- A prefix tree that contains all active routes
- A nexthop tree that maintains a tree of attached hosts

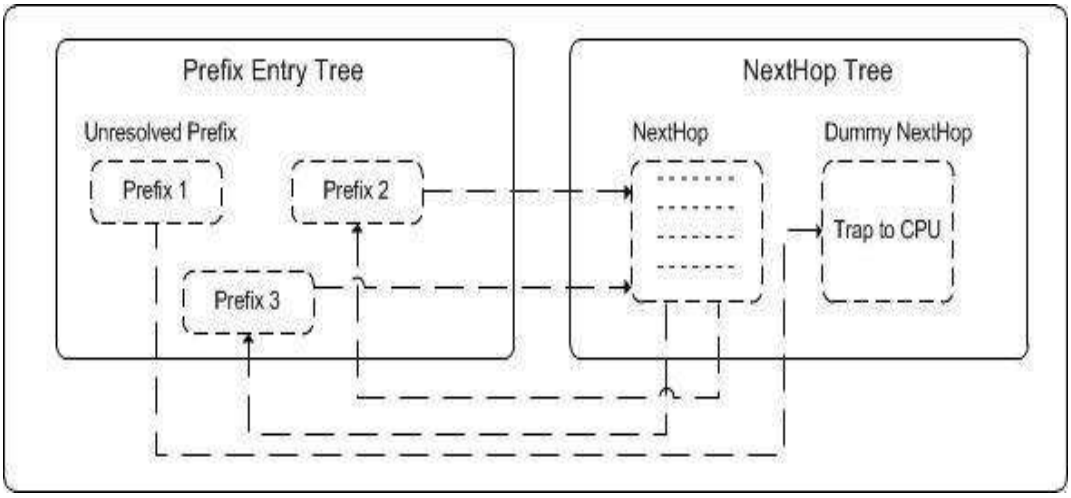


Figure 3-16: FIB manager database

Each prefix with a resolved next-hop points to the next-hop entry in the nexthop tree. Each next-hop points to all prefixes pointing to it. Prefixes with an unresolved next-hop point to a dummy next-hop entry, which indicates to send that traffic to the CPU. Once the CPU receives the traffic, the operating system stack attempts to resolve the next-hop and update the hardware.

The FIB manager performs these major tasks:

- Operating system programing: All prefixes and resolved next-hops are stored in the operating system.
- Hardware programming: Every prefix is installed in the hardware, based on the resolved or dummy nexthop.
- Keeping a shadow of all programmed and un-programmed prefixes.

Every time a new hop is resolved, or an existing nexthop is updated, the nexthop tree is updated, and all prefixes pointing to it are updated with relevant information.

For un-programmed prefix storage:

- The FIB manager stores prefixes and nexthops that cannot be programmed to the hardware due to hardware FIB table size limitations. If the hardware FIB is full, only entries used by traffic are stored; and others are removed.
- The FIB manager monitors prefix usage in hardware to identify and remove unused entries. The FIB Manager uses the ARP aging mechanism to remove unused nexthop entries.
- The FIB Manager handles nested routes to ensure proper forwarding.
- Each time an exception packet is received, the FIB Manager attempts to program a relevant entry to the hardware, making sure that the next time, forwarding occurs through the fast path.

Typically, both the operating system and chip are identically programmed, and only control traffic goes to the CPU. In addition, there is a memory limitation on processors for the number of prefixes a chip can accommodate. Modules keep a

shadow of installed forwarding entries in both the chip and operating system. The FIB manager database has additional fields specific to the hardware, since the processor and ASIC programming require additional information.

Packet Driver

The packet driver module processes packets. Packet receipt occurs in the hardware-interrupt context, when the packet descriptor is passed to the user-callback function. To avoid a packet drop in case of bulk, the packet driver does not immediately start parsing and processing packets. Instead, the packet driver implements a first-in, first out (FIFO) queue for packets to be processed. During hardware interrupt, the packet descriptor is stored in the queue, and the packet-ready semaphore is released. If the queue is full, or the system is not ready for traffic, packets are dropped. Packet processing is based on the hardware CPU error code.

The packet driver is responsible for receiving packets. Packet receipt usually occurs in the hardware-interrupt context. As shown in Figure 3-17, the packet driver implements a first-in, first out (FIFO) queue for packets to be processed.

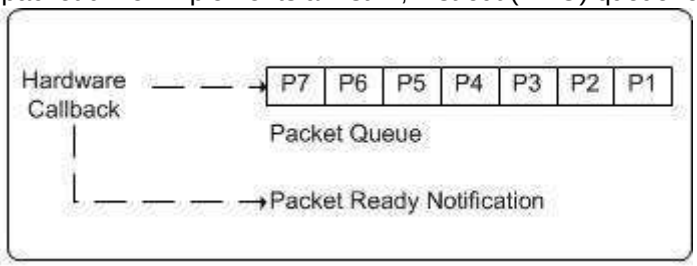


Figure 3-17: Packet driver When

the packet queue is not empty, the packet driver does the following:

1. Gets the packet from the head.
2. Resolves the receiving interface based on the port and the VLAN in the packet.
3. Verifies the packet validity for the interface based on the CPU error code or the packet Ether type.
4. If the packet is a Layer 2 control type (BPDU), it duplicates the packet descriptor, and sends it to a protocol socket.
5. Verifies whether learning is required. If required, it attempts to learn the new neighbor hosts.
6. Verifies if a valid forwarding entry exists. If it exists, the packet driver attempts to program the fast-path FIB.
7. Prepares the packet (CRC/VLAN tag).
8. Uploads the packet to the TCP/IP stack.

Note the following:

- Layer 2 control messages are passed to the protocol modules directly through the sockets.
- Layer 3 data traffic and control messages are passed to the operating system TCP/IP stack.
- Before passing the traffic to the socket or the operating system, the packet driver translates the hardware receive port to the operating system interface, based on the received port and VLAN.
- If the packet is not specific to the interface, the packet driver drops the packet.
- The packet driver removes the VLAN tag if the TCP/IP stack does not support the VLAN interfaces.
- The packet driver removes the packet CRC, if needed.
  The packet driver learns about the neighbor hosts and local FIB updates from the ARP and neighbor solicitation messages.
- The packet driver tries to program the fast path for packets not handled by the hardware.

Ethernet Driver

The Ethernet driver has these functions:

- Handling interfaces in the operating system
- Passing traffic between the hardware and the operating system stack
- Managing network buffer pools

The Ethernet driver registers interfaces in the operating system based on the interface type. Each interface type is represented as a separate device driver. Each device registers a set of driver functions for device handling (start-stop and send-receive). Interfaces of the same type are treated as multiple instances of the device. The Ethernet driver manages the network buffer pool to pass traffic between the hardware SDK and the operating system stack.

The Ethernet driver resolves the destination hardware logical port and modifies packets, if necessary. Possible modifications include VLAN tag insertion and CRC recalculation. Based on the operating system transmitting interface, the Ethernet driver resolves destination hardware ports, updates the packets based on (destination port and VLAN) pair and transmits the packets on the interface.

If the destination interface is the VLAN termination interface including multiple ports, the following logic is applied:

The Ethernet Driver performs a lookup in the Layer 3 FIB:

1. If the destination interface has multiple ports:
    - If the destination port is found in the packet, it is transmitted to that port
    - If the destination port is not found in the packet, the packet is transmitted to all participating ports
2. If the destination interface is an aggregator, the Ethernet driver finds the first participating port where it transmits the packet.

SECTION 2 System Management

System Management Configuration Guide

Contents

This guide contains these chapters:

- Chapter 1, *User Configuration*
- Chapter 2, *Using the Management Interface*
- Chapter 3, *SSH Client Server Host Configuration*
- Chapter 4, *Telnet Configuration*
- Chapter 5, *Syslog Configuration*
- Chapter 6, *DNS Configuration*
- Chapter 7, *DHCP Client Configuration*
- Chapter 8, *Software Monitoring and Reporting*
- Chapter 9, *TACACS Client Configuration*
- Chapter 10, *RADIUS Client Configuration*
- Chapter 11, *DHCP Relay Agent Configuration*
- Chapter 12, *NTP Client Configuration*
- Chapter 13, *Simple Network Management Protocol*
- Chapter 14, *Access Control Lists Configurations*
- Chapter 15, *Show Tech Support Configurations*

CHAPTER 1 User Configuration

Overview

User management is an authentication feature that provides administrators with the ability to identify and control the users who log into the network.

SWMRE provides 4 different roles for users.

- Network Administrator: can make permanent changes to switch configuration. Changes are persistent across reset/reboot of switch.
- Network Engineer: can make permanent changes to switch configuration. Changes are persistent across reset/ reboot of switch.
- Network Operator: can make permanent changes to switch configuration. Changes are not persistent across reset/ reboot of switch.
- Network User: displays information; cannot modify configuration.

User Configuration

`#configure terminal`	Enter configure mode.
`(config)#username user1 password user12345`	Create Username “user1” with password user12345 which will have default role as network-user. Password should be <8-32> char, username <2-15>char.
`(config)#username user1 role networkoperator password user12345`	Changing the role for user1 to network-operator. Password should be <8-32> char, username <2-15>char.
`(config)#username user2 role networkoperator password user12345`	Create a user “user2” with role as network-operator. Password should be <8-32> char, username <2-15>char.
`(config)#username user3 role network-admin password user12345`	Create a user “user3” with role as network-admin. Password should be <8-32> char, username <2-15>char.
`(config)#username user4 role networkengineer password user12345`	Create a user “user4” with role as network-engineer. Password should be <8-32> char, username <2-15>char.
`(config)#exit`	Exit configure mode.

Validation Commands

`show user-account, show user-account <username>, show role`

```
#show user-account
User:user1
                roles: network-operator
User:user2
```

```
                roles: network-operator
User:user3
                roles: network-admin
User:user4
                roles: network-engineer

#show role
Role Name                              Info
```
User Configuration

```
------------------------------------------------------------------------
network-admin                          Network Administrator - Have all
permissions
network-engineer                       Network Engineer - Can save
configuration
network-operator                       Network Operator - Can not save
configuration
network-user                           Network User - Can not change
configuration

#show user-account user1 User:user1
                roles: network-operator
```

CHAPTER 2 Using the Management Interface

Overview

SWMRE provides support for different types of Management Interfaces. The management interface can be the standard out of band (OOB) port, or any in-band port.

To provide segregation between management traffic and data traffic, SWMRE provides a Management VRF. The Management VRF is created by default when SWMRE boots. This VRF cannot be deleted. All ports used as Management Interface needs to be in Management VRF. The management VRF is used for all types of Management applications listed below

- Remote access to router (SSH/Telnet)
- File transfer applications (SFTP/SCP)
- Login Authentication via Radius/Tacacs
- Network management protocols (SNMP, Netconf)

Apart from this, DHCP, DNS, NTP, Syslog, License/Software upgrade also uses ports mapped to management VRF for their operations. Also LLDP protocol can be run on any ports mapped to this Management VRF.

Note: If the management interface flaps, the device becomes unreachable.

Management Port

The Out of Band (OOB) Management Port in SWMRE is identified as “eth0.” This port is automatically mapped to the Management VRF when SWMRE boots, and will remain in same VRF throughout. It cannot be moved out of this VRF.

The IP address of the management port can be configured statically or via DHCP.

Static IP Configuration

A static IP can be configured on the management port during ONIE installation itself, or after installation using the SWMRE CLIs commands. To configure a static IP during ONIE installation, do the following

```
#onie-discovery-stop
#ifconfig eth0 <ip address> netmask <subnet mask> up
```

Please check the *Install Guide* for details.

The IP address configured during ONIE installation will be applied to the management port and the same will be retained when SWMRE boot up, and the port becomes part of Management VRF.

```
#show running-config interface
eth0 ! interface eth0
```

```
 ip vrf forwarding management
ip address 10.12.44.109/24
```

After getting the SWMRE prompt, this IP address can be changed from the CLI.

Using the Management Interface

`#configure terminal`	Enter Configure mode.
`(config)#interface eth0`	Change mode to interface eth0
`(config-if)# ip address 10.12.44.120/24`	Set a ipv4 address on this interface
`(config-if)#exit`	Exit from the interface mode
`(config)#exit`	Exit from the configuration mode.

If a static IP is not configured during ONIE installation the same can be configured via CLI by following the above steps. Using the SWMRE CLI, DHCP can also be enabled on the Management port.

`#configure terminal`	Enter Configure mode.
`(config)#interface eth0`	Change mode to interface eth0
`(config-if)# ip address dhcp`	Enable DHCP on interface eth0
`(config-if)#exit`	Exit from the interface mode
`(config)#exit`	Exit from the configuration mode.

Obtaining IP Address via DHCP

During onie installation, the management port attempts to acquire IP address via DHCP automatically unless stopped explicitly using “onie-discovery-stop”. So, if management port is getting IP via DHCP, after SWMRE boots, the management port will continue to use DHCP, even when it’s part of the Management VRF.

```
#show running-config interface eth0Zeb
!   interface
eth0
 ip vrf forwarding management
ip address dhcp
```

After SWMRE comes up, the IP address can be changed to any static IP via CLI as shown earlier.

In-Band Ports

Any front-end ports of the device (In-Band ports) can be made part of the management VRF. Once they are part of the management VRF they can also support all management applications such as SSH/Telnet and others as listed in Overview.

Once the ports are part of the management VRF, they should not be used for data traffic and routing or switching purposes. In-Band ports can be added or removed from Management VRF as and when required.

`#configure terminal`	Enter Configure mode.
`(config)#interface xe1/1`	Change mode to interface xe1/1

(config-if)# ip vrf forwarding management	Add In-Band port as part of Management VRF
(config-if)#exit	Exit from the interface mode
(config)#exit	Exit from the configuration mode.

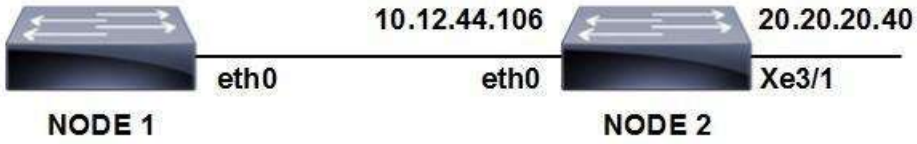
Using the Management Interface

#configure terminal	Enter Configure mode.
(config)#interface xe1/1	Change mode to interface xe1/1
(config-if)# no ip vrf forwarding management	Remove In-Band port from Management VRF
(config-if)#exit	Exit from the interface mode
(config)#exit	Exit from the configuration mode.

Using Ping in Management VRF

To check reachability to any node in the management network, you need to explicitly mention the VRF name as “management.”

In the following example, Node-1 has management interface eth0 and Node-2 has management interfaces eth0 and xe3/1. In order to reach the network 20.20.20.40/24 from Node-1 a static route needs to added.



#configure terminal	Enter Configure mode.
(config)# ip route vrf management 20.20.20.0/24 10.12.44.106 eth0	Add static route in management VRF to reach 20.20.20.0/24 network
(config)#exit	Exit from the configuration mode.

```
Node-1#show ip route vrf management
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
area,        inter v - vrf leaked * - candidate default

IP Route Table for VRF "management"
C       10.12.44.0/24 is directly connected, eth0
S20.20.20.0/24 [1/0] via 10.12.44.106, eth0

Gateway of last resort is not set

Node-1#ping 20.20.20.40 vrf management
PING 20.20.20.40 (20.20.20.40) 56(84) bytes of data.
```

```
64 bytes from 20.20.20.40: icmp_seq=1 ttl=64 time=0.494 ms
64 bytes from 20.20.20.40: icmp_seq=2 ttl=64 time=0.476 ms
```

CHAPTER 3 SSH Client Server Host Configuration

Overview

SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices.SSH was designed as a replacement for Telnet and other insecure remote shells, which send information, notably passwords, in plain text, rendering them susceptible to packet analysis.[2] The encryption used by SSH is intended to provide confidentiality and integrity of data over an unsecured network, such as the Internet.SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user.

SSH is typically used to log into a remote machine and execute commands, but it also supports tunneling, forwarding TCP ports and X11 connections; it can transfer files using the associated SFTP or SCP protocols. SSH uses the client- server model

The standard TCP port 22 has been assigned for contacting SSH servers. Here in this document covering the ssh server configuration to enable ssh service and key generation CLI commands and ssh client configuration for remote login to server.

Topology

Figure 3-22: SSH sample topology

`#configure terminal`	Enter Configure mode.
`(config)#no feature ssh vrf management`	Disable the feature ssh.
`(config)# ssh login-attempts 2 vrf management`	Set Login-attempts 2. Default is 3.
`(config)#feature ssh vrf management`	Enable the feature ssh.
`(config)#exit`	Exit from the configuration mode.

The login-attempt is set to 2 which means that the five times the password can be re-entered. The feature ssh should be disabled while configuring the login-attempts and it should be enabled before creating the SSH session.

Validation Commands

`show ssh server, show running-config ssh server`

```
#sh ssh server
```

```
ssh server enabled port: 22
authentication-retries 2

#sh running-config ssh server
feature ssh
```

SSH Client Server Host Configuration

Support for In-band Management over default VRF

SWMRE offers support for SSH over default and management VRFs via in-band management interface & OOB management interface, respectively.

The feature can be enabled to run on default and management VRF simultaneously. By default, it runs on the management VRF.

SSH Keys

`#configure terminal`	Enter Configure mode.
`(config)#no feature ssh [vrf management]`	Disable the feature ssh.
`(config)# ssh login-attempts 2 [vrf management]`	Set Login-attempts 2. Default is 3.
`(config)#feature ssh [vrf management]`	Enable the feature ssh.
`(config)#exit`	Exit from the configuration mode.

Use this SSH keys to generates new RSA/DSA keys for SSH server. This command can only be executed when the SSH server is disabled. By default the system has RSA/DSA public/private key pair placed in /etc/ssh/. If the user wants to regenerate the keys the force option must be specified. The length option can only be used with RSA keys; DSA has a constant key length of 1024bits.

`#configure terminal`	Enter Configure mode.
`(config)#no feature ssh vrf management`	Disable the feature ssh.
`(config)# ssh key rsa force vrf management`	The force option is used if the user wants to regenerate the ssh rsa keys. The same thing applies for dsa also.
`(config)#feature ssh vrf management`	Enable the feature ssh.
`(config)#exit`	Exit from the configuration mode.

Validation Commands

`show ssh key`

```
#sh ssh key
****************RSA KEY********************
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDMuVc0jpNgMyNzaqzIELX6LlsaK/
1q7pBixmwHAGDsZm/
dClTLb18AIB27W68YD8k0+Yw0LR0rHuPtNeSFMEsMaQxsaLkSi7yg86xSJaqgLQTyOUTS/
OC9hreXkJ73ay
n0yXa8+bre0oyJq1NWxAI9B1jEhfSSAipoDSp/
```

```
dmc93VJyV+3hgy1FMTAheyebQaUVeLBEMH7siRlSfyo7OHsBYSF6GzAmSuCm6PAelpHm/
3L4gChcnPL+0outQOifCSLdUOXEZhTFXrzC61l+14LGt8pR6YN+2uEnU6kq1i
aDLEffIWK4dWCp67JUIef1BTOvxRurpssuRdslhJQXDFaj
bitcount: 2048 fingerprint: a4:23:5d:8a:5a:54:8b:3e:0b:38:06:79:82:e9:83:48
************************************
****************DSA KEY*******************
ssh-dsa AAAAB3NzaC1kc3MAAACBALpY6MFhFPYI+VcAHzHppnwVnNXv9oR/
EGHUM50BBqdQE1Qi1mlt1rft4oa4tYR46P4gazKnnNfVE/
97FwEbCZaXaz9Wzfcfa3ALtsvGdyNQQk2BebYiRnmeWnS3wGV0M/D64bAiV0
2p/
LyF6D0ygMnZ3up3ttTN5QfHeyYQtwyzAAAAFQD+k6wQyr51IhXIQSsQD8by8qxjUwAAAIB0LxP3ljn
```

SSH Client Server Host Configuration

```
fzxEXyEkNNzlxCcJ7ZZkFYUmtDJxRZlDceuSf4QipMrQVrdrgdqZNhrUiDWM/
HaCMO9LdEQxfPh5TaIwPyccngn
VUS83Tx577ofBW6hellTey3B3/3I+FfiGKUXS/
mZSyf5FW3swwyZwMkF0mV0SRCYTprnFt5qx8awAAAIEAjDNqMkyxUvB6JBqfo7zbGqXjBQmJ+dE8fG
jI2znlgq4lhYcMZJVNwTiydDIgMVNFfKc1dAT3zr6qMZfGv56EbK
1qUu103K5CF44XfVkYNcHJV+/
fcfAJasGU8W6oSbU5Q08abyMsIGRYTurOMkRhvif6sxvieEpVnVK2/nPVVXA=
bitcount: 1024 fingerprint: d9:7a:80:e0:76:48:20:72:a6:5b:1c:67:da:91:9f:52
************************************
```

Note: The newly created rsa/dsa key can be verified by logging into DUT from remote machine and checking whether the newly created key's fingerprint matches with the logging session fingerprint.

SSH Client session

When the device is acting as an SSH client, it supports both SSH ipv4 sessions to login to remote machine.

SSH Client

`#ssh root@10.10.10.1 vrf management`	Logging into remote machine using ipv4 address.

SSH Encryption Cipher

Use this SSH cipher to set which cipher is to be used to encrypt an ssh session. By default, all the ciphers are supported for a new ssh client to connect to the ssh server.

SSH server supports the encryption algorithms Advanced Encryption Standard Counter Mode [AES-CTR], Advanced Encryption Standard Cipher Block Chaining [AES-CBC], and Triple Data Encryption Standard [3DES].

The following is a list of standards:

1. aes128-ctr
2. aes192-ctr
3. aes256-ctr
4. aes128-cbc

5. 3des-cbc
6. aes192-cbc
7. aes256-cbc

Configuring an Encryption Cipher

`#configure terminal`	Enter Configuration Mode.
`(config)#ssh server algorithm encryption aes128-ctr`	Set ssh server cipher encryption algorithm to AES 128 bit Counter Mode.

SSH Client Server Host Configuration

`(config)# ssh server algorithm encryption aes128-cbc`	Set ssh server cipher encryption algorithm to AES 128 Cipher block chaining.
`(config)#exit`	Exit from the configuration mode.

Validation

The newly configured cipher encryption algorithm will take effect for a new incoming ssh client connection.

```
#show running-config ssh server
```

SSH Client Session

`#ssh cipher aes128-ctr root@1.1.1.1`	AES 128-bit Counter Mode to establish ssh connection to a remote machine using ipv4 address.

CHAPTER 4 Telnet Configuration

Overview

Telnet is a TCP/IP protocol used on the Internet and local area networks to provide a bidirectional interactive text-oriented communications facility using a virtual terminal connection. The Telnet program runs, connects it to a server on the network. A user can then enter commands through the Telnet program and they will be executed as if the user were entering them directly on the server console.Telnet enables users to control the server and communicate with other servers on the network. The default port number for Telnet protocol is 23.Telnet offers users the capability of running programs remotely and facilitates remote administration.

Support for In-band Management Over Default VRF

SWMRE offers support for Telnet over default and management VRFs via in-band management interface & OOB management interface, respectively.

The feature can be enabled to run on default and management VRFs simultaneously. By default, it runs on management VRF.

Topology

Figure 4-23: Telnet sample topology

Enable and Disable the Telnet Server

`#configure terminal`	Enter Configure mode.
`(config)#no feature telnet vrf management`	Disable Telnet feature.
`(config)#feature telnet vrf management`	Enable Telnet feature.
`(config)#exit`	Exit configure mode.

Configure the Telnet Server Port

`#configure terminal`	Enter Configure mode.

(config)#no feature telnet vrf management	Disable Telnet feature.
(config)#telnet server port 6112 vrf management	Set Telnet port to 61112. Default is 23.

Telnet Configuration

(config)#feature telnet vrf management	Enable Telnet feature.
(config)#exit	Exit configure mode.

Telnet Client session

#telnet root@10.10.10.1 vrf management	Logging into remote machine using ipv4 address.

Validation Commands

```
#show telnet server telnet server enabled port: 6112

#show running-config telnet server feature telnet
```

CHAPTER 5 Syslog Configuration

Syslog is a standard for logging program messages. It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It also provides devices which would otherwise be unable to communicate, a means to notify administrators of problems or performance.

SWMRE supports logging messages to a syslog server in addition to logging to a file or the console (local or ssh/telnet console). SWMRE messages can be logged to a local syslog server (the machine on which SWMRE executes) as well as to one or more remote syslog servers. Remote syslog servers can either be configured with IPv4 addresses or host names.

Support for In-band management over default VRF

SWMRE now offers support for Syslog over default and management VRFs via in-band management interface & OOB management interface, respectively.

The feature can either be running on the default or management VRFs. By default, it runs on the management VRF using a new CLI feature `rsyslog` [vrf management].

Topology

Figure 5-24: Syslog sample topology

Enabling rsyslog

`#configure terminal`	Enter Configure mode.
`config)#feature rsyslog [vrf management]`	Enable feature on default or management VRF. By default this feature runs on management VRF.
`config)#exit`	Exit from the configuration mode

Logging to a File

The below configurations shows how to enable debug logs for a particular protocol. In this case, LACP is shown.

`#debug lacp all`	This enables the debugging on LACP.
`#configure terminal`	Enter Configure mode.
`(config)#logging level lacp 7 [vrf management]`	This enable debug messages for LACP module. This is configurable either if default of management VRF.

`(config)#logging logfile xyz 7`	This creates the log file where the logs will be saved. The path of the file will be in the directory /log/xyz. Log File size 40964194304 bytes.

Syslog Configuration

`(config)#interface xe1`	Enter interface mode.
`(config-if)#switchport`	Make port as switchport.
`(config-if)#channel-group 1 mode active`	Make port as part of port-channel 1.
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit configure mode.

To verify this, do some lacp configuration and view the messages in the log file or with the show logging logfile command.

Validation Commands

```
show logging logfile, show logging level
    #show logging logfile
    File logging : enabled File Name : /log/xyz Severity : (7)
    2016 Mar 03 00:02:32 x86_64-debian NSM-3: AgentX: failed to send open message:
    Connection refused
    2016 Mar 03 00:02:33 x86_64-debian OSPF-3: AgentX: failed to send open
    message: Connection refused
    2016 Mar 03 00:02:33 x86_64-debian OSPFv3-3: AgentX: failed to send open
    message: Connection refused
    2016 Mar 03 00:02:33 x86_64-debian IS-IS-3: AgentX: failed to send open
    message: Connection refused
    2016 Mar 03 00:02:33 x86_64-debian BGP-3: AgentX: failed to send open message:
    Connection refused
    2016 Mar 03 00:02:33 x86_64-debian RIP-3: AgentX: failed to send open message:
    Connection refused

#show logging level

    Facility         Default Severity        Current Session
    Severity nsm                     3                          3
    ripd                    3                          3 ospfd
    3                          3 ospf6d                  3
    3 isisd                   3                          3 hostpd
    3                          3 ldpd                    2
    2 rsvpd                   2                          2 mribd
    2                          2 pimd                    2
    2 authd                   2                          2 mstpd
    2                          2 imi                     2
    2 onmd                    2                          2 oamd
    2                          2 vlogd                   2
    2 vrrpd                   2                          2 ribd
    2                          2 bgpd                    3
    3 l2mribd                 2                          2 lagd
```

```
2                              2 sflow                    2
2 pservd                     2                            2
```

Syslog Configuration

Logging to the Console

`#configure terminal`	Enter Configure mode.
`(config)#logging level ospf 7`	This enable debug messages for OSFP module.
`(config)#logging console 7`	This enables the console logs.
`(config)#debug ospf`	This enables the debugging on OSPF configurations.
`(config)#router ospf`	Enabling ospf for process 1.
`(config-router)#exit`	Exit router mode.
`(config)#exit`	Exit configure mode.

To verify this, do some OSPF configuration and view the messages in the console.

Validation Commands

```
#show logging console
    Console logging      : enabled Severity: (debugging)

#show logging level

    Facility         Default Severity        Current Session
    Severity nsm                      3                          3
    ripd                     3                          3 ospfd
    3                           7 ospf6d                   3
    3 isisd                    3                           3 hostpd
    3                           3 ldpd                     2
    2 rsvpd                    2                           2 mribd
    2                           2 pimd                     2
    2 authd                    2                           2 mstpd
    2                           2 imi                      2
    2 onmd                     2                           2 oamd
    2                           2 vlogd                    2
    2 vrrpd                    2                           2 ribd
    2                           2 bgpd                     3
    3 l2mribd                  2                           2 lagd
    2                           2 sflow                    2
    2 pservd                   2                           2
```

Syslog Configuration

Logging to Remote Server

#configure terminal	Enter Configure mode.
(config)#logging level bgp 7	This enable debug messages for BGP module.
(config)#logging server 10.16.2.1 vrf management	Redirects the log messages to the server configured.
(config)#debug bgp	This enables the debugging on BGP configurations.
(config)#router bgp 1	Enabling BGP process 1.
(config-router)#exit	Exit router mode.
(config)#exit	Exit configure mode.

Validation Commands

```
#show logging server
      Remote Servers:
                  10.16.2.1                  severity:
    (debugging)                facility: local7
    VRF: management

    #show logging level

    Facility        Default Severity        Current Session Severity nsm
    3                           3 ripd                    3
    3 ospfd                   3                           3 ospf6d
    3                           3 isisd                   3
    3 hostpd                  3                           3 ldpd
    2                           2 rsvpd                   2
    2 mribd                   2                           2 pimd
    2                           2 authd                   2
    2 mstpd                   2                           2 imi
    2                           2 onmd                    2
    2 oamd                    2                           2 vlogd
    2                           2 vrrpd                   2
    2 ribd                    2                           2 bgpd
    3                           7 l2mribd                 2
    2 lagd                    2                           2 sflow
    2                           2 pservd                  2
    2
```


© Symanitron

CHAPTER 6 DNS Configuration

Overview

The Domain Name System (DNS) is an Internet service that translates domain names into IP addresses. When a domain name is used, DNS service translates the name into the corresponding IP address. If one DNS server does not know how to translate a particular domain name, it gathers information from other Domain Name Systems to obtain the correct IP address.

Support for In-band Management over default VRF

SWMRE offers support for DNS over default and management VRFs via in-band management interface & OOB management interface, respectively.

The feature can be enabled to run on default and management VRF simultaneously. By default, it runs on management VRF.

Topology

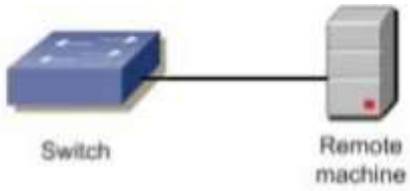


Figure 6-25: DNS sample topology

Configuration

`#configure terminal`	Enter Configure mode.
`(config)#ip name-server vrf management 10.12.17.11  10.1.1.2`	This add a IPv4 Name Server to the DNS.
`(config)#ip host BINGO vrf management 10.1.1.1`	This will add IPv4 host to the DNS
`(config)#exit`	Exit configure mode.

Validation Commands

```
#show hosts
             VRF: default

     DNS lookup is disabled
     Default domain is empty
     DNS domain list is empty

     Name Servers        : 10.12.17.11 10.1.1.2
```

```
Host                                                    Address
----                                                    ------BINGO
10.1.1.1

 * - Values assigned by DHCP Client.
```

CHAPTER 7 DHCP Client Configuration

Overview

Dynamic Host Configuration Protocol (DHCP) protocol is used for assigning dynamic IP addresses to systems on a network. Dynamic addressing allows a system to have an IP address each time it connects to the network. DHCP makes network administration easier by removing the need to manually assign a unique IP address every time a new system is added to the network. It is especially useful to manage mobile users. Once a system is configured to use DHCP, it can be automatically configured on any network that has a DHCP server.

DHCP uses a client-server model, in which the DHCP server centrally manages the IP addresses used in the network. DHCP clients obtain an IP address on lease from the DHCP server.

DHCP Client Configuration for IPv4

Before configuring the DHCP in client, make sure that DHCP server is ready and also dhcpd is running on the server machine.

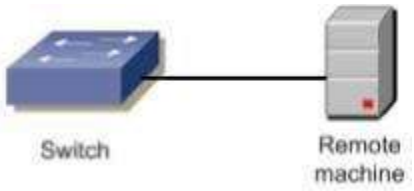


Figure 7-26: DHCP sample topology

`#configure terminal`	Enter Configure mode.
`(config)#feature dhcp`	Enable the feature dhcp. This will be enabled by default.
`(config)#interface xe1`	Specify the interface(xe1) to be configured and enter the interface mode.
`(config-if)#ip address dhcp`	The client requests for the IP address to the server, once it receives the acknowledgment from the server, it assigns the IP address to the interface in which this command is enabled.
`(config if)#exit`	Exit interface mode.
`(config)#interface eth0`	Enter management interface mode.
`(config-if)#ip address dhcp`	The client requests for the IP address to the server, once it receives the Acknowledgement from the server, it assigns the IP address to the management interface.
`(config if)#exit`	Exit interface mode.

Validation Commands

```
#show running-config dhcp
    interface  xe2    ip
    address dhcp
    ! ip dhcp relay
    information option
```

DHCP Client Configuration

```
    #sh ip interface brief

    Interface            IP-Address      Admin-Status          Link-Status
    GMPLS Type
    eth0                  10.12.44.20     up                    up
    -
    lo                    127.0.0.1       up                    up
    -
    lo.4                  127.0.0.1       up                    up
    -
    vlan1.1               unassigned      up                    down
    -
    xe1/1                 2.2.2.3         up                    up
    -
    xe1/2                 unassigned      down                  down
    -
    xe1/3                 unassigned      down                  down
    -
    xe1/4                 unassigned      up                    down
    -
    xe2                  *40.40.40.40     up                    down
    -
    xe3/1                 20.20.30.1      up                    up
    -
```

CHAPTER 8 Software Monitoring and Reporting

Overview

SWMRE provides a mechanism (called “watchdogging”) to monitor all SWMRE modules and provides the following functions.

1. Periodic heart beat check.
2. Automatic restarts of a module upon a hung state or crash detection.
3. Upon hanging or crashing of a module, a crash report (including system states) is logged.
4. A proprietary SNMP trap is sent to the trap manager, if configured, after a fault is detected in a protocol module. Similarly a trap is sent when the module recovers.

By default, the software watchdog is enabled and the keep-alive time interval is 30 seconds. All SWMRE processes periodically send keep-alive messages to a monitoring module at the configured keep-alive time interval.

This functionality can be disabled for a particular module or all SWMRE modules by using CLI commands. In order to permanently disable software monitoring functionality, the user has to disable the watchdog feature. If, however, software watchdogging is disabled the monitoring module doesn’t take any action upon a hang or crash of any SWMRE module.

Software Monitoring

`#configure terminal`	Enter Configure mode.
`(config)#feature software-watchdog`	Enable software watchdog for all SWMRE modules — This is the default.
`(config)#no software-watchdog imi`	To disable software watchdog for only imi modules.
`(config)#software-watchdog keep-alive-time 100`	The keep-alive time interval in seconds. Default is 60 seconds and applies to all SWMRE modules.
`#show software-watchdog status`	Display the keep-alive time interval and list of SWMRE process names with watchdog status for each SWMRE modules.

Validation

```
#show software-watchdog status
Software Watchdog timeout in seconds : 100
Process name         Watchdog
status ============
=============== nsm
```

```
Enabled   ripd
Enabled   ospfd
Enabled   isisd
Enabled   hostpd
Enabled   ldpd
Enabled   rsvpd
Enabled   Software Monitoring and
Reporting

mribd              Enabled   pimd              Enabled   authd             Enabled
mstpd              Enabled   imi               Disabled  onmd              Enabled
HSL                Enabled   oam               Enabled   vlogd             Enabled
vrrpd              Enabled   ndd               Enabled   ribd              Enabled
bgpd               Enabled   l2mribd           Enabled   lagd              Enabled
sflow                Enabled
```

CHAPTER 9 TACACS Client Configuration

Overview

Terminal Access Controller Access Control System (TACACS) is a remote authentication protocol that is used to communicate with an authentication server. With TACACS, a network device communicates to an authentication server to determine whether a particular user should be allowed access to the device. TACACS+ listens at port 49.

TACACS Server Authentication

Figure 9-27: TACACS Server Host Configuration

Authenticating Device

`#configure terminal`	Enter Configure mode.
`(config)#feature tacacs+ vrf management`	Enable the feature TACACS+ for management vrf
`(config)#feature tacacs+ vrf`	Enable the feature TACACS+. for default vrf
`(config)#tacacs-server login key testing101 vrf management`	Specify the global key for tacacs servers that are not configured with their respective keys for management vrf This key should match the one present in the config file of tacacs server
`(config)#tacacs-server login key testing101`	Specify the global key for tacacs servers that are not configured with their respective keys for default vrf This key should match the one present in the config file of tacacs server
`(config)#tacacs-server host 10.16.19.2 vrf management key testing123`	Specify the tacacs server ipv4 address to be configured with shared key. The same key should be present on the server config file
`(config)#tacacs-server login host 10.16.19.2 key testing123`	Specify the tacacs server ipv4 address to be configured with shared local key for default vrf The same key should be present on the server config file.
`(config)#tacacs-server host 10.12.30.135 vrf management seq-num 1 key testing123`	Specify the tacacs server ipv4 address to be configured with the sequence number and the shared key. The key should match the one present in the server config file
`(config)#tacacs-server host 10.12.30.86 vrf management seq-num 2 port 1045`	Specify the tacacs server ipv4 address to be configured with the sequence and port number.The tacacs server should be started with same port number
`config)#tacacs-server login host 10.12.30.86 seq-num 2 port 1045`	Specify the tacacs server ipv4 address to be configured with the sequence and port number for default vrf. The tacacs server should be started with same port number

(config)#tacacs-server login host 10.12.17.11 vrf management seq-num 8 key 7 65535 port 65535	Specify the tacacs server ipv4 address to be configured with the sequence, key and port number for management vrf. The tacacs server should be started with same port number.
(config)#tacacs-server login host 10.12.17.11 seq-num 8 key 7 65535 port 65535	Specify the tacacs server ipv4 address to be configured with the sequence, key and port number for default vrf. The tacacs server should be started with same port number.
(config)#tacacs-server login host Tacacs-Server-1 vrf management seq-num 7 key 7 65535 port 65535	Specify the tacacs server configured with host-name sequence number key and port number for management vrf. The tacacs server should be started with same port number
(config)#tacacs-server login host Tacacs-Server-1 seq-num 7 key 7 65535 port 65535	Specify the tacacs server configured with host-name sequence number key and port number for default vrf. The tacacs server should be started with same port number
(config)#aaa authentication login default vrf management group tacacs+	Enable authentication for TACACS+ server configured for management vrf. Authorization is also enabled by default
(config)#aaa authentication login default group tacacs+	Enable authentication for TACACS+ server configured for default vrf. Authorization is also enabled by default.
(config)#aaa authentication login default vrf management group tacacs+ local	Enable authentication for TACACS+ and fall-back to local configured for management vrf. Authorization is also enabled by default
(config)#aaa authentication login default vrf management group tacacs+ local none	Enable authentication for TACACS+ fall-back to local followed by fall-back to none configured for management vrf. Authorization is also enabled by default
(config)#aaa authentication login default vrf management group tacacs+ none	Enable authentication for TACACS+ fall-back to none configured for management vrf. Authorization is also enabled by default
(config)#aaa authentication login default group tacacs+ none	Enable authentication for TACACS+ fall-back to none , configured for default vrf. Authorization is also enabled by default
(config)#aaa group server tacacs+ G1 vrf management	Create aaa group G1 for management vrf
(config)#aaa group server tacacs+ G1	Create aaa group G1 for default vrf
(config-tacacs)#server 10.12.30.86 vrf management	Make the tacacs-server 10.12.30.86 a part of this group G1
(config-tacacs)#server 10.12.30.86	Make the tacacs-server 10.12.30.86 a part of this group G1 for default vrf
(config-tacacs)#server Tacacs-Server-1 vrf management	Make the tacacs-server Tacacs-Server-1 a part of this group G1 for management vrf
(config-tacacs)#server Tacacs-Server-1	Make the tacacs-server Tacacs-Server-1 a part of this group G1 for default vrf
(config)#exit	Exit the tacacs-config
(config)#aaa authentication login default vrf management group G1	Authenticate the tacacs+ group G1 with aaa authentication for management vrf
(config)#aaa authentication login default group G1	Authenticate the tacacs+ group G1 with aaa authentication for default vrf

Users are mapped as shown as shown in Table 9-2 :

Table 9-2: Role/privilege level mapping

Role	Privilege level
Network administrator	15
Network engineer	14
Network operator	1 to 13
Network user	0 or any other values (>15 or negative values or any character)

Validation

```
 #show tacacs-server vrf management        VRF: management
    total number of servers:2

    Tacacs+ Server                 : Tacacs-Server-1/65535(*)
                Sequence Number    : 7
           Failed Auth Attempts    : 0
          Success Auth Attempts    : 1
       Failed Connect Attempts     : 0
     Last Successful authentication: 2018 October 30, 10:10:22

    Tacacs+ Server                 : 10.12.17.11/65535
                Sequence Number    : 8
           Failed Auth Attempts    : 0
          Success Auth Attempts    : 0
       Failed Connect Attempts     : 0  Last Successful
    authentication:

    (*) indicates last active.
#


#show tacacs-server vrf all
            VRF: management total number of servers:2
     Tacacs+ Server                : Tacacs-Server-1/65535(*)
                Sequence Number    : 7
           Failed Auth Attempts    : 0
          Success Auth Attempts    : 1
       Failed Connect Attempts     : 0
     Last Successful authentication: 2018 October 30, 10:10:22

     Tacacs+ Server                : 10.12.17.11/65535
                Sequence Number    : 8
           Failed Auth Attempts    : 0
          Success Auth Attempts    : 0
       Failed Connect Attempts     : 0
     Last Successful authentication:
```

```
        VRF: default total number of servers:2

    Tacacs+ Server                  : Tacacs-Server-1/2222
                Sequence Number     : 7
           Failed Auth Attempts     : 0
          Success Auth Attempts     : 0
        Failed Connect Attempts     : 0  Last Successful
    authentication:

    Tacacs+ Server                  : 100.0.0.1/2222
                Sequence Number     : 8
           Failed Auth Attempts     : 0
          Success Auth Attempts     : 0
        Failed Connect Attempts     : 0  Last Successful
    authentication:


    (*) indicates last active.
#


    #
#show tacacs-server
        VRF: default total number of servers:2

    Tacacs+ Server                  : Tacacs-Server-1/2222
                Sequence Number     : 7
           Failed Auth Attempts     : 0
          Success Auth Attempts     : 0
       Failed Connect Attempts      : 0  Last Successful
    authentication:

    Tacacs+ Server                  : 100.0.0.1/2222
                Sequence Number     : 8
           Failed Auth Attempts     : 0
          Success Auth Attempts     : 0
       Failed Connect Attempts      : 0  Last Successful
    authentication:

    (*) indicates last active.

#show tacacs-server vrf management groups G1         VRF: management

        group G1:                 server Tacacs-Server-1:
    seq-num 7                port is 65535                 key is
    ********

                server 10.12.17.11:
                seq-num 8                port is 65535
    key is ********
#show tacacs-server vrf all groups G1         VRF: management
```

```
        group G1:                  server Tacacs-Server-1:
    seq-num 7                port is 65535                  key is
    ********

                server 10.12.17.11:                 seq-
    num 8                port is 65535                  key is
    ********


        VRF: default

        group G1:                  server Tacacs-Server-1:
    seq-num 7                port is 2222                  key is
    ********

                server 100.0.0.1:
                seq-num 8                port is 2222
    key is ********



#
#show  tacacs-server  groups  G1             VRF:  default  group  G1:
    server Tacacs-Server-1:
                seq-num 7                port is 2222
    key is ********

                server 100.0.0.1:
                seq-num 8                port is 2222
    key is ********
    #show tacacs vrf management         VRF: management
    total number of servers:2

    Tacacs+ Server                  : Tacacs-Server-1/65535(*)
              Sequence Number     : 7
         Failed Auth Attempts     : 0
        Success Auth Attempts     : 1
       Failed Connect Attempts     : 0
     Last Successful authentication: 2018 October 30, 10:10:22

    Tacacs+ Server                  : 10.12.17.11/65535
           Sequence Number     : 8
      Failed Auth Attempts     : 0
     Success Auth Attempts     : 0
   Failed Connect Attempts     : 0  Last Successful
authentication:

(*) indicates last active.



#show tacacs vrf all         VRF: management total
number of servers:2
```

```
Tacacs+ Server                  : Tacacs-Server-1/65535(*)
            Sequence Number     : 7
       Failed Auth Attempts     : 0
      Success Auth Attempts     : 1
    Failed Connect Attempts     : 0
 Last Successful authentication: 2018 October 30, 10:10:22

Tacacs+ Server                  : 10.12.17.11/65535
            Sequence Number     : 8
       Failed Auth Attempts     : 0
      Success Auth Attempts     : 0
    Failed Connect Attempts     : 0   Last Successful
authentication:


        VRF: default total number of servers:2

Tacacs+ Server                  : Tacacs-Server-1/2222(*)
            Sequence Number     : 7
       Failed Auth Attempts     : 0
      Success Auth Attempts     : 1
    Failed Connect Attempts     : 0
 Last Successful authentication: 2018 October 30, 10:32:52

Tacacs+ Server                  : 100.0.0.1/2222
            Sequence Number     : 8
       Failed Auth Attempts     : 0
      Success Auth Attempts     : 0
    Failed Connect Attempts     : 0   Last Successful
authentication:


(*) indicates last active.
#

#show tacacs         VRF: default total number of
servers:2

Tacacs+ Server                  : Tacacs-Server-1/2222(*)
           Sequence Number      : 7
      Failed Auth Attempts      : 0
          Success Auth Attempts     : 1
        Failed Connect Attempts     : 0
     Last Successful authentication: 2018 October 30, 10:32:52

     Tacacs+ Server                 : 100.0.0.1/2222
                Sequence Number     : 8
           Failed Auth Attempts     : 0
          Success Auth Attempts     : 0
        Failed Connect Attempts     : 0  Last Successful
     authentication:
```

```
    (*) indicates last active.

    #show tacacs vrf management         VRF: management
    total number of servers:2

    Tacacs+ Server                  : Tacacs-Server-1/65535(*)
                Sequence Number     : 7
           Failed Auth Attempts     : 0
          Success Auth Attempts     : 1
        Failed Connect Attempts     : 0
      Last Successful authentication: 2018 October 30, 10:10:22

    Tacacs+ Server                  : 10.12.17.11/65535
                Sequence Number     : 8
           Failed Auth Attempts     : 0
          Success Auth Attempts     : 0
        Failed Connect Attempts     : 0  Last Successful
    authentication:

    (*) indicates last active.

#show tacacs vrf all
             VRF: management total number of servers:2

    Tacacs+ Server                  : Tacacs-Server-1/65535(*)
                Sequence Number     : 7
           Failed Auth Attempts     : 0
          Success Auth Attempts     : 1
        Failed Connect Attempts     : 0
      Last Successful authentication: 2018 October 30, 10:10:22

    Tacacs+ Server                  : 10.12.17.11/65535
                Sequence Number     : 8
           Failed Auth Attempts     : 0
          Success Auth Attempts     : 0
        Failed Connect Attempts     : 0   Last Successful
    authentication:


             VRF: default total number of servers:2

    Tacacs+ Server                  : Tacacs-Server-1/2222(*)
                Sequence Number     : 7
           Failed Auth Attempts     : 0
          Success Auth Attempts     : 1
        Failed Connect Attempts     : 0
      Last Successful authentication: 2018 October 30, 10:32:52

    Tacacs+ Server                  : 100.0.0.1/2222
                Sequence Number     : 8
           Failed Auth Attempts     : 0
          Success Auth Attempts     : 0
```

```
      Failed Connect Attempts     : 0  Last Successful
    authentication:


    (*) indicates last active.
#

#show tacacs
            VRF: default total number of servers:2

    Tacacs+ Server                  : Tacacs-Server-1/2222(*)
                Sequence Number     : 7
             Failed Auth Attempts   : 0
            Success Auth Attempts   : 1
          Failed Connect Attempts   : 0
     Last Successful authentication: 2018 October 30, 10:32:52

    Tacacs+ Server                  : 100.0.0.1/2222
                Sequence Number     : 8
             Failed Auth Attempts   : 0
            Success Auth Attempts   : 0
          Failed Connect Attempts   : 0   Last Successful
    authentication:

     (*) indicates last active.

#show aaa authentication vrf management                    VRF:
    management   default: group G1   console: local

#show aaa authentication vrf all
                    VRF: management    default: group G1
    console: local

                    VRF: default   default: group tacacs+
    console: local

#show aaa authentication
                    VRF: default   default: group tacacs+
    console: local
#
# show aaa groups vrf management
                    VRF: management
    radius tacacs+ G1

#
    # show aaa groups vrf all
    VRF: management radius tacacs+ G1

                    VRF: default
    radius tacacs+ G1
```

```
#show aaa groups
                    VRF: default
    radius tacacs+ G1

#show running-config tacacs+ feature
    tacacs+ vrf management
    tacacs-server login host Tacacs-Server-1 vrf management seq-num 7 key 7 65535
    po rt 65535
    tacacs-server login host 10.12.17.11 vrf management seq-num 8 key 7 65535 port
    6 5535

    feature tacacs+
    tacacs-server login host Tacacs-Server-1 seq-num 7 key 7 65535 port 2222 tacacs-
    server login host 100.0.0.1 seq-num 8 key 7 65535 port 2222

#show running-config aaa aaa authentication login default vrf
    management group G1 aaa group server tacacs+ G1 vrf
    management server Tacacs-Server-1 vrf management
    server 10.12.17.11 vrf management

    aaa authentication login default group tacacs+
    aaa group server tacacs+ G1     server Tacacs-
    Server-1     server 100.0.0.1

#show running-config aaa all aaa authentication login default
    vrf management group G1 aaa authentication login console
    local aaa accounting default vrf management local
    no aaa authentication login default fallback error local vrf management no
    aaa authentication login console fallback error local
    no aaa authentication login error-enable vrf management aaa
    local authentication attempts max-fail 3  vrf management aaa
    local authentication unlock-timeout 1200  vrf management aaa
    group server tacacs+ G1 vrf management      server Tacacs-
    Server-1 vrf management     server 10.12.17.11 vrf management

    aaa authentication login default group
    tacacs+ aaa authentication login console
    local aaa accounting default local
    no aaa authentication login default fallback error local
    no aaa authentication login console fallback error local
    no aaa authentication login error-enable aaa local
    authentication attempts max-fail 3 aaa local
    authentication unlock-timeout 1200 aaa group server
    tacacs+ G1     server Tacacs-Server-1     server 100.0.0.1
```

TACACS Server Accounting

After authentication, the user can configure accounting to measure the resources that the user consumes during access.

Authenticating Device

#configure terminal	Enter Configure mode.
(config)#feature tacacs+ vrf management	Enable the feature TACACS+ for vrf management
(config)#feature tacacs+	Enable the feature TACACS+ for default vrf
(config)#tacacs-server host 10.16.19.2 vrf management key testing123	Specify the TACACS server IPv4 address to be configured with shared key for vrf management. The same key should be present in the server configuration file.
(config)#tacacs-server login host 10.16.19.2 key testing123	Specify the TACACS server IPv4 address to be configured with shared key default vrf. The same key should be present in the server configuration file.
(config)#aaa accounting default vrf management group tacacs+	Enable accounting for TACACS server configured for vrf management.
(config)#aaa accounting default group tacacs+	Enable accounting for TACACS server configured for default vrf
#clear tacacs-server counters vrf management	Clear tacacs server counters for management vrf
#clear tacacs-server counters vrf all	Clear tacacs server counters for management and default vrf
#clear tacacs-server counters	Clear tacacs server counters for default vrf

To verify the TACACS accounting process, connect using SSH or Telnet from the host to the client with the user created and provided TACACS server password, and check whether the client validates the user with corresponding username and password.

Validation Commands

show tacacs-server, show aaa accounting, show aaa accounting

```
#show aaa accounting vrf management
                    VRF: management       default: group tacacs+
#

#show aaa accounting vrf all
                    VRF: management       default: group tacacs+

                    VRF: default       default: group tacacs+

#show aaa accounting
                    VRF: default       default: group tacacs+
          #
```

```
    #show running-config aaa aaa authentication login default vrf management group G1
 aaa accounting default vrf management group tacacs+ aaa group server tacacs+ G1 vrf
    management server Tacacs-Server-1 vrf management server 10.12.17.11 vrf
    management

    aaa authentication login default group tacacs+ aaa accounting default
    group tacacs+ aaa group server tacacs+ G1 server Tacacs-Server-1
    server 100.0.0.1
```

Sample TACACS Config File Contents

```
#tacacs configuration file #set the key

    key = "testing123"
    accounting file = /var/log/tac_acc.log

    user = test1 {
            default service = permit         login = cleartext
    "12345"
    }

    group = netadmin {
            service = ppp protocol = ip {          priv-lvl = 1
            } }

    user = test2 {
            default service = permit         login = cleartext
    "12345"         member = netadmin
    }

    user = test3 {
            default service = permit
    login = cleartext "12345"
    service = ppp protocol = ip {
    priv-lvl = 15
    }
    }
```

TACACS Server Authorization

Authorization is realized by mapping the authenticated users to one of the existing predefined roles as shown in Table 9-2.

The privilege information from the TACACS+ server is retrieved for the authenticated users and is mapped onto one of the roles as shown in Table 9-2.

Each authenticated user is mapped to one of the pre-defined privilege level.

Users with priv-level <=0 and priv-level > 15 are treated as read-only user mapped onto the pre-defined network-user role.

There is no command to enable authorization. Authorization functionality is enabled by default when remote authentication is enabled with TACACS+.

Authorization is “auto-enabled”. After successful authentication, a user can enter into privilege exec mode, irrespective of its privilege level and such user is not prompted with enable mode password, if configured. However based on their role, commands are rejected if not allowed to perform certain operations.

Example

A network-user has read-only access and can only execute show commands. A network-user cannot enter configuration mode. An error message is displayed upon executing any command which is not allowed.

```
#write
% Access restricted for user %
```

```
#configure terminal
% Access restricted for user %
```

The following attribute value pair in TACACS+ server is used to fetch user privilege information.

```
service = ppp protocol = ip {          priv-lvl = <0…15>
}
```

Sample TACACS+ Configuration File

```
#tacacs configuration file from “tac_plus version F4.0.3.alpha
” #set the key

key = "testing123"
accounting file = /var/log/tac_acc.log

#Read only user “test1”, without any priv-lvl, mapped to role “network-user”
user = test1 { default service =
permit login = cleartext "12345"
}

#We can create a group of users mapped to a privilege group
= netadmin { service = ppp protocol = ip { priv-lvl = 15
} }

#User “test2” with highest priv-lvl=15, mapped to role “network-admin” user =
test2 { default service = permit login = cleartext "12345" member = netadmin }

#User “test3” with priv-lvl= 1…13, mapped to role “network-operator” user
= test3 { default service = permit login = cleartext "12345" service = ppp
protocol = ip { priv-lvl = 10
} }
#User “test4” with priv-lvl=14, mapped to role “network-engineer” user = test4 {
default service = permit login = cleartext "12345" service = ppp protocol = ip { priv-
lvl = 14 } }
```

CHAPTER 10 RADIUS Client Configuration

Overview

Remote Authentication Dial In User Service (RADIUS) is a remote authentication protocol that is used to communicate with an authentication server.

A RADIUS server is responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user.

The key points for RADIUS authentication are:

- Transactions between client and server are authenticated through the use of a shared key and this key is never sent over the network.
- The password is encrypted before sending it over the network.

RADIUS Server Authentication

Figure 10-28: RADIUS Server Host Configuration

Host

`#configure terminal`	Enter configure mode.
`(config)# radius-server login key testing101 vrf management`	Specify the global key for radius servers that are not configured with their respective keys for management vrf. This key should match the one present in the config file of tacacs server.
`(config)# radius-server login key testing101`	Specify the global key for radius servers that are not configured with their respective keys for default vrf. This key should match the one present in the config file of tacacs server
`(config)# radius-server login host 10.16.19.2 vrf management key testing123`	Specify the radius server ipv4 address to be configured with shared local key for management vrf. The same key should be present on the server config file.
`(config)# radius-server login host 10.16.19.2 key testing123`	Specify the radius server ipv4 address to be configured with shared local key for default vrf. The same key should be present on the server config file.

(config)# radius-server login host 10.12.30.86 vrf management auth-port 1045	Specify the radius server ipv4 address to be configured with port number for management vrf. The radius server should be started with same port number.

(config)# radius-server login host 10.12.30.86 auth-port 1045	Specify the radius server ipv4 address to be configured with port number for default vrf.The radius server should be started with same port number
(config)#radius-server login host 10.12.17.11 vrf management key 7 wawyanb123 auth-port 60000 acct-port 60000 timeout 6	Specify the radius server ipv4 address to be configured with authentication port number, accounting port number, shared key for management vrf. The radius server should be started with same port number.
(config)#radius-server login host 10.12.17.11 key 7 wawyanb123 auth-port 60000 acct-port 60000 timeout 6	Specify the radius server ipv4 address to be configured with authentication port number, accounting port number, shared key for default vrf. The radius server should be started with same port number. The radius server should be started with same port number
(config)# radius-server login host Tacacs-Server-1 vrf management seq-num 7 key 7 65535 port 65535	Specify the radius server configured with hostname, key authentication port number, accounting port number, for management vrf. The radius server should be started with same port number
(config)# radius-server login host Radius-Server-1 seq-num 7 key 7 65535 port 65535	Specify the radius server configured with hostname sequence number, key and port number for default vrf. The radius server should be started with same port number.
(config)#aaa authentication login default vrf management group radius	Enable authentication for radius server configured for management vrf. Authorization is also enabled by default
(config)#aaa authentication login default group radius	Enable authentication for radius server configured for default vrf. Authorization is also enabled by default.
(config)#aaa authentication login default vrf management group radius local	Enable authentication for radius server and fallback to local configured for management vrf. Authorization is also enabled by default
(config)#aaa authentication login default group radius local	Enable authentication for radius server and fallback to local configured for default vrf. Authorization is also enabled by default
(config)#aaa authentication login default vrf management group radius local none	Enable authentication for radius server, fallback to local followed by fallback to none ,configured for management vrf. Authorization is also enabled by default
(config)#aaa authentication login default radius local none	Enable authentication for radius server, fallback to local followed by fallback to none, configured for default vrf. Authorization is also enabled by default
(config)#aaa authentication login default vrf management group radius none	Enable authentication for radius, fallback to none, configured for management vrf. Authorization is also enabled by default
(config)#aaa authentication login default group radius none	Enable authentication for radius, fallback to none, configured for default vrf. Authorization is also enabled by default
(config)#aaa group server radius G1 vrf management	Create aaa radius group G1 for management vrf
(config)#aaa group server radius G1	Create aaa radius group G1 for default vrf
(config-radius) #server 10.12.30.86 vrf management	Make the radius-server 10.12.30.86 a part of this group G1 for management vrf

(config-radius)#server 10.12.30.86	Make the radius server 10.12.30.86 a part of this group G1 for default vrf
(config-radius)#server Radius-Server-1 vrf management	Make Radius-Server-1 a part of this group G1 for management vrf
(config-radius)#server Tacacs-Server-1	Make the radius server Radius-Server-1 a part of this group G1 for default vrf
(config)#aaa authentication login default vrf management group radius tacacs+	Enable authentication for radius, fallback to tacacs+, configured for management vrf. Authorization is also enabled by default
(config)#aaa authentication login default group radius tacacs+	Enable authentication for radius, fallback to tacacs+, , configured for default vrf. Authorization is also enabled by default
(config)#aaa authentication login default vrf management group tacacs+ radius	Enable authentication for tacacs+ fallback to radius configured for management vrf. Authorization is also enabled by default
(config)#aaa authentication login default group tacacs+ radius	Enable authentication for tacacs+ fallback to radius configured for default vrf. Authorization is also enabled by default
(config)#username test password test12345	Create username and password for authentication purpose. The same user should be present in the radius server config file.

Validation

To verify the RADIUS authentication process, use SSH or Telnet from the host machine to Host IP with the authenticating user created, and provide a RADIUS server password and check whether the client validates the user with the corresponding username and password.

```
#sh radius-server vrf management
VRF: management         timeout
value: 5

        Total number of servers:2

         Following RADIUS servers are configured:

               100.0.0.1:                  available for
authentication on port:60000                  available for
accounting on port:60000
                 RADIUS shared secret:********

               Radius-Server-1:
                 available for authentication on
port:60000 available for accounting on port:60000 RADIUS
shared secret:********

#sh radius-server vrf all
VRF: management timeout
value: 5
```

```
Total number of servers:2

Following RADIUS servers are configured:

                100.0.0.1:
                  available for authentication on port:60000
available for accounting on port:60000 RADIUS shared
secret:********

                Radius-Server-1:                    available for authentication on
port:60000                    available for accounting on port:60000
                  RADIUS shared secret:********
        VRF: default timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:

                Radius-Server-1:                    available for authentication on
port:60000                    available for accounting on port:60000
RADIUS shared secret:********

               100.0.0.1:                       available for authentication
port:60000                    on available for accounting on port:60000
RADIUS shared secret:********

#sh radius-server         VRF: default timeout
value: 5

Total number of servers:2

Following RADIUS servers are configured:

                Radius-Server-1:                    available for authentication on
port:60000                    available for accounting on port:60000
RADIUS shared secret:********

                100.0.0.1:
                  available for authentication on port:60000
available for accounting on port:60000                    RADIUS shared secret:********

#sh radius-server vrf management sorted
        VRF: management timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:

                100.0.0.1:
```

```
                  available for authentication on port:60000                  available
for accounting on port:60000
                  RADIUS shared secret:********


                Radius-Server-1:                    available for authentication on
port:60000                    available for accounting on port:60000
                  RADIUS shared secret:********

#sh radius-server vrf all sorted         VRF: management
timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:

                100.0.0.1:                    available for authentication on
     port:60000         available for accounting on port:60000
                  RADIUS shared secret:********


                Radius-Server-1:                    available for authentication on
port:60000                    available for accounting on port:60000
                  RADIUS shared secret:********

        VRF: default timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:

                100.0.0.1:
                  available for authentication on port:60000                  available
for accounting on port:60000
                  RADIUS shared secret:********


                Radius-Server-1:
                  available for authentication on port:60000
available for accounting on port:60000                    RADIUS shared secret:********

#sh radius-server sorted         VRF: default timeout
value: 5
Total number of servers:2

Following RADIUS servers are configured:

                100.0.0.1:                    available for authentication on
     port:60000         available for accounting on port:60000
                  RADIUS shared secret:********
```

```
                Radius-Server-1:                    available for authentication on
port:60000                    available for accounting on port:60000
RADIUS shared secret:********

#sh radius-server vrf management groups          VRF: management

        group radius:
                server: all configured radius servers

        group rad1:                  server Radius-Server-1:
auth_port is 60000                 acct_port is 60000
key is ********

                server 100.0.0.1:                  auth_port is
60000                  acct_port is 60000                  key is
********

#sh radius-server vrf all groups         VRF: management

        group radius:
                server: all configured radius servers

        group rad1:
                server Radius-Server-1:                  auth_port
is 60000                   acct_port is 60000                   key
is ********

                server 100.0.0.1:                  auth_port is
60000                  acct_port is 60000                  key is
********          VRF: default

        group radius:
                server: all configured radius servers

        group rad1:                  server Radius-Server-1:
auth_port is 60000                 acct_port is 60000
key is ********

                server 100.0.0.1:                  auth_port is 60000
acct_port is 60000                 key is ********

#sh radius-server groups         VRF: default

        group radius:
                server: all configured radius servers

        group rad1:                  server Radius-Server-1:
auth_port is 60000                 acct_port is 60000
key is ********
```

```
                server 100.0.0.1:                   auth_port is 60000
acct_port is 60000                 key is ********

#sh radius-server vrf management groups rad1          VRF: management

        group rad1:
                server Radius-Server-1                 auth_port is
60000                 acct_port is 60000                 key is
********

                server 100.0.0.1                 auth_port is 60000
acct_port is 60000                 key is ********

#sh radius-server vrf all groups rad1
        VRF: management
        group rad1:                   server Radius-Server-1
auth_port is 60000                 acct_port is 60000
key is ********

                server 100.0.0.1                 auth_port is
60000                 acct_port is 60000                 key is
********


        VRF: default

        group rad1:
                server Radius-Server-1                 auth_port
is 60000                   acct_port is 60000                   key
is ********

                server 100.0.0.1                 auth_port is
60000                 acct_port is 60000                 key is
********

#sh radius-server groups rad1          VRF: default

        group rad1:                   server Radius-Server-1
auth_port is 60000                 acct_port is 60000
key is ********

                server 100.0.0.1                 auth_port is
60000                 acct_port is 60000                 key is
********

#sh radius vrf management         VRF: management
timeout value: 5

Total number of servers:2
```

```
Following RADIUS servers are configured:

                100.0.0.1:                    available for authentication on
port:60000 available for accounting on port:60000 RADIUS shared
secret:********

                Radius-Server-1:                    available for authentication on
port:60000                    available for accounting on port:60000
                  RADIUS shared secret:********

#sh radius vrf all         VRF: management
timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:

                100.0.0.1:
                  available for authentication on port:60000                    available
for accounting on port:60000
                  RADIUS shared secret:********

                Radius-Server-1:                    available for authentication on
port:60000                    available for accounting on port:60000
                  RADIUS shared secret:********
        VRF: default timeout value: 5

Total number of servers:2

Following RADIUS servers are configured:

                Radius-Server-1:                    available for authentication on
port:60000                    available for accounting on port:60000
RADIUS shared secret:********

                100.0.0.1:
                  available for authentication on port:60000
available for accounting on port:60000                    RADIUS shared secret:********

#sh radius         VRF: default timeout value:
5

Total number of servers:2

Following RADIUS servers are configured:

                Radius-Server-1:
                  available for authentication on port:60000
available for accounting on port:60000                    RADIUS shared secret:********
```

```
                100.0.0.1:                    available for authentication on
port:60000 available for accounting on port:60000 RADIUS shared
secret:********

#sh aaa authentication vrf management                   VRF:
management   default: group radius    console: local

#sh aaa authentication vrf all                   VRF:
management   default: group radius    console: local

                VRF: default    default: group radius
console: local

#sh aaa authentication                   VRF: default
default: group radius    console: local

#sh aaa groups vrf management                   VRF:
management radius rad1 rad1

#sh aaa groups vrf all                   VRF: management
radius rad1

                VRF: default radius rad1

#sh aaa groups
                VRF: default radius rad1
#sh running-config radius
radius-server login host 100.0.0.1 vrf management key 7 wawyanb123 auth-port 600
00 acct-port 60000
radius-server login host Radius-Server-1 vrf management key 7 wawyanb123 auth-po rt
60000 acct-port 60000


radius-server login host Radius-Server-1 key 7 wawyanb123 auth-port 60000 acctport
60000

radius-server login host 100.0.0.1 key 7 wawyanb123 auth-port 60000 acct-port 6 000

#sh running-config aaa
aaa authentication login default vrf management group radius
aaa group server radius rad1 vrf management
server Radius-Server-1 vrf management     server
100.0.0.1 vrf management

aaa authentication login default group radius aaa
group server radius rad1 server Radius-Server-1
server 100.0.0.1

#sh running-config aaa all
```

```
aaa authentication login default vrf management group radius
aaa authentication login console local aaa accounting default
vrf management local
no aaa authentication login default fallback error local vrf management no
aaa authentication login console fallback error local no aaa authentication
login error-enable vrf management aaa local authentication attempts max-fail
3 vrf management aaa local authentication unlock-timeout 1200 vrf management
aaa group server radius rad1 vrf management
server Radius-Server-1 vrf management     server
100.0.0.1 vrf management

aaa authentication login default group radius aaa
authentication    login    console    local    aaa
accounting default local
no aaa authentication login default fallback error local no aaa
authentication login console fallback error local
no aaa authentication login error-enable aaa local
authentication attempts max-fail 3 aaa local
authentication unlock-timeout 1200 aaa group
server radius rad1     server Radius-Server-1
server 100.0.0.1
```

RADIUS Server Accounting

You can configure accounting to measure the resources that another user consumes during access.

User

`#configure terminal`	Enter Configure mode.
`(config)#radius-server login host 10.12.17.11 vrf management key 7 wawyanb123 auth-port 60000 acct-port 60000 timeout 6`	Specify the radius server ipv4 address to be configured with authentication port number, accounting port number, shared key for management vrf. The radius server should be started with same port number.
`(config)#radius-server login host 10.12.17.11 key 7 wawyanb123 auth-port 60000 acct-port 60000 timeout 6`	Specify the radius server ipv4 address to be configured with port number for default vrf.The radius server should be started with same port number
`(config)#aaa accounting default vrf management group radius`	Enable accounting for radius server configured for vrf management
`(config)#aaa accounting default group radius`	Enable accounting for radius server configured for default vrf
`(config)#username test password test12345`	Create username and password for accounting purpose.The same user should be present in the radius server config file.

Validation

```
#sh aaa accounting vrf management
VRF: management   default: group radius
```

```
#sh aaa accounting vrf all
VRF: management   default: group radius

                VRF:  default     default:  group
radius

#sh aaa accounting                 VRF:
default   default: group radius
#
#sh running-config aaa
aaa authentication login default vrf management group radius aaa
accounting default vrf management group radius aaa group server radius
rad1 vrf management     server Radius-Server-1 vrf management     server
100.0.0.1 vrf management

aaa authentication login default group radius aaa
accounting default group radius aaa group server radius
rad1     server Radius-Server-1
    server 100.0.0.1
```

Sample Radius Clients.conf File

```
client 10.12.58.20 {   secret    = testing123   shortname =
localhost
} client 192.168.1.2 {   secret    = testing123
shortname = localhost
} client 10.12.37.196 {   secret    = testing123
} client 100.0.0.2 {   secret    = testing123   shortname
= localhost }

# IPv6 Client #client ::1 {
#       secret          = testing123
#       shortname       = localhost
#}
#
# All IPv6 Site-local
clients #client fe80::/16 {
#       secret          = testing123
#       shortname       = localhost
```

Sample Radius Users Configuration File

```
#
#DEFAULT
#       Service-Type = Login-User,
#       Login-Service = Rlogin,
#       Login-IP-Host = shellbox.ispdomain.com
```

```
# #
# # Last default: shell on the local terminal server.
# #
# DEFAULT
#       Service-Type = Administrative-User # On no match, the user is denied

access. selftest Cleartext-Password := "password" testuser1 Cleartext-

Password := "user1@101" testuser2 Cleartext-Password := "user2@202"

testuser3 Cleartext-Password := "user3@303"
```

CHAPTER 11 DHCP Relay Agent Configuration

Overview

The DHCP Relay feature was designed to forward DHCP broadcast requests as unicast packets to a configured DHCP server or servers for redundancy.

DHCP Relay for IPv4

Before configuring DHCP Relay, make sure DHCP server and client configurations are done.

Figure 11-29: DHCP Relay Configuration

DHCP Agent

`#configure terminal`	Enter Configure mode.
`(config)#feature dhcp`	Enable the feature dhcp. This is enabled by default.
`(config)#ip dhcp relay`	By default this will be enabled. It starts the ip dhcp relay service.
`(config)#interface xe1`	Specify the interface(xe1) to be configured and enter the interface mode.
`(config-if)#ip address 10.10.10.1/24`	Configure ipv4 address on the interface xe1.
`(config if)#exit`	Exit from the interface mode.
`(config)#interface xe2`	Specify the interface(xe2) to be configured and enter the interface mode.
`(config-if)#ip address 20.20.20.1/24`	Configure ipv4 address on the interface xe2.
`(config-if)#ip dhcp relay address 10.10.10.2`	The relay address configured should be server interface address connected to DUT machine.
`(config if)#exit`	Exit from the interface mode.

Validation Commands

```
#show running-config dhcp

interface xe2
 ip dhcp relay address 10.10.10.2

#show ip dhcp relay
```

DHCP Relay Agent Configuration

```
DHCP relay service is Enabled.
Insertion of option 82 is Disabled.
Helper addresses are configured on the following interfaces:
 Interface         Relay Address
--------          ----------- xe2
10.10.10.2

#show ip dhcp relay address
 Interface         Relay Address
--------          ----------- xe2
10.10.10.2

#show ip dhcp relay address interface ethernet eth1
 Interface         Relay Address  -
-------           ------------ xe2
10.10.10.2
```

DHCP Relay for IPv6

DHCP Agent

`#configure terminal`	Enter Configure mode.
`(config)#feature dhcp`	Enable the feature dhcp. This is enabled in default.
`(config)#ipv6 dhcp relay`	By default this will be enabled. It starts the ipv6 dhcp relay service.
`(config)#interface xe1`	Specify the interface(xe1) to be configured and enter the interface mode.
`(config-if)#ipv6 address 2001::1/64`	Configure ipv6 address on the interface xe1.
`(config if)#exit`	Exit from the interface mode.
`(config)#interface xe2`	Specify the interface(xe2) to be configured and enter the interface mode.
`(config-if)#ipv6 address 2002::1/64`	Configure ipv6 address on the interface xe2.
`(config-if)#ipv6 dhcp relay address 2001::2`	The relay address configured should be server interface address connected to DUT machine.
`(config if)#exit`	Exit from the interface mode.

Validation Commands

```
#sh ipv6 dhcp relay address
Interface            Relay Address                              Output Interface
--------             -------------                              ---------------
Xe2                   2001::1
```


CHAPTER 12 NTP Client Configuration

Overview

NTP modes differ based on how NTP allows communication between systems. NTP communication consists of time requests and control queries. Time requests provide the standard client/server relationship in which a client requests time synchronization from an NTP server. Control queries provide ways for remote systems to get configuration information and reconfigure NTP servers.

SNTP is a simplified form of NTP that does not reach the level of accuracy compared to a full implementation of NTP. SNTP can be used for simple applications where the requirements for accuracy and reliability are not too demanding. SWMRE supports SNTP version 4, defined in RFC 2030.

Note: SWMRE uses "`ntp`" for the SNTP command names instead of "`sntp`."

Support for Default VRF via In-band Management

SWMRE now offers support for NTP over default and management VRFs via in-band management interface & OOB management interface, respectively.

The feature can either be running on the default or management VRF. By default, it runs on the management VRF.

NTP Modes

The following describes the various NTP node types.

Client

An NTP client is configured to let its clock be set and synchronized by an external NTP timeserver. NTP clients can be configured to use multiple servers to set their local time and are able to give preference to the most accurate time sources. They do not, however, provide synchronization services to any other devices.

Server

An NTP server is configured to synchronize NTP clients. Servers can be configured to synchronize any client or only specific clients. NTP servers, however, will accept no synchronization information from their clients and therefore will not let clients update or affect the server's time settings.

Peer

With NTP peers, one NTP-enabled device does not have authority over the other. With the peering model, each device shares its time information with the others, and each device can also provide time synchronization to the others.

Access Lists

Once a router is synchronized to an NTP time source, it acts automatically as an NTP for any client that requests synchronization or informational control queries.

NTP Client Configuration

NTP allows you to configure ACLs to restrict access to the NTP services on the router. These ACLs can be configured to restrict access based on IP and the following four restrictions:

- Peer – Allows time synchronization requests and control queries and allows the router to synchronize itself to remote systems that pass the ACL.
- Server – Allows time synchronization requests and control queries, but does not allow the router to synchronize itself to remote systems that pass the ACL.
- Serve-only – Allows only time synchronization requests from systems that pass the ACL.
- Query-only – Allows only NTP control queries from systems that pass the ACL.

The two ACLs generally used to restrict access for security reasons are the `peer` and `serve-only` options. For example, if you are using the hierarchical model with the core routers `RouterOne and RouterTwo` providing NTP services for the rest of the routers in your network.

Authentication

For additional security, you can configure your NTP servers and clients to use authentication. Routers support MD5 authentication for NTP. To enable a router to do NTP authentication:

1. Enable NTP authentication with the `ntp authenticate` command.
2. Define an NTP authentication key with the ntp authentication-key vrf management command. A unique number identifies each NTP key. This number is the first argument to the ntp authentication-key vrf management command.
3. 3.Use the ntp trusted-key vrf management command to tell the router which keys are valid for authentication. If a key is trusted, the system will be ready to synchronize to a system that uses this key in its NTP packets. The trusted key should already be configured and authenticated.

NTP Configuration

NTP client, user can configure an association with a remote server. In this mode the client clock can synchronize to the remote server

After configuring the NTP servers, wait a few minutes before you verify that clock synchronization is successful. When the clock synchronization has actually happened, there will be an '*' symbol along with the interface while you give the "`show ntp peers`" command.

Topology

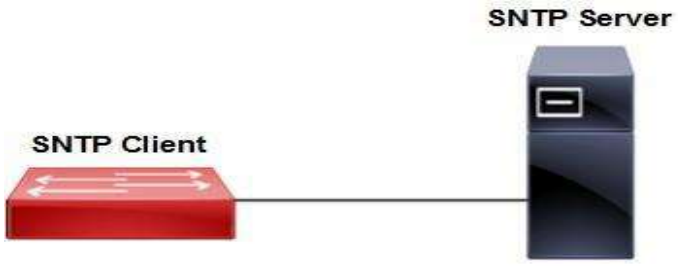


Figure 12-30: SNTP Client and Server

NTP Client Configuration

NTP Client

`#configure terminal`	Enter Configure mode.
`(config)#feature ntp vrf management`	Configure feature on default or management VRF. By default this feature runs on management VRF.
`(config)# ntp enable vrf management`	This feature enables ntp. This will be enabled in default.
`(config)#ntp server 10.1.1.1 vrf management`	Configure ntp server ip address.
`(config)#exit`	Exit from the Configure Mode.

Validation Commands

```
#show ntp peers
    ------------------------------------------------------------
    Peer IP Address Serv/Peer
    ------------------------------------------------------------
    10.1.1.1 Server (configured)

    #show ntp peer-status
    Total peers : 1
    * - selected for sync, + -  peer mode(active), -
    - peer mode(passive), = - polled in client mode
         remote           refid      st t when poll reach   delay   offset  jitter
    ==============================================================================
    *10.1.1.1        LOCAL(0)         7 u   14   32   37    0.194   -4.870   3.314
```

Maxpoll and Minpoll Configuration

The maximum poll interval are specified in defaults to 6 (64 seconds), but can be increased by the `maxpoll` option to an upper limit of 16 (18.2 hours). The minimum poll interval defaults to 4 (16 seconds), and this is also the minimum value of the `minpoll` option.

The client will retry between `minpoll` and `maxpoll` range configured for synchronization with the server.

Client

`#configure terminal`	Enter Configure mode.
`(config)#feature ntp vrf management`	Configure feature on default or management VRF. By default this feature runs on management VRF.
`(config)#ntp server 10.1.1.1 maxpoll 7 minpoll 5 vrf management`	Configure `minpoll` and `maxpoll` range for ntp server.
`(config)#exit`	Exit from the Configure Mode.

Validation Commands

```
#show ntp peers
    ------------------------------------------------------------
    Peer IP Address Serv/Peer
    ------------------------------------------------------------10.1.1.1
    Server (configured)
```

NTP Client Configuration

```
#show   ntp   peer-status
    Total peers : 1
    * - selected for sync, + -  peer mode(active), -
    - peer mode(passive), = - polled in client mode
         remote           refid      st t when poll reach   delay   offset  jitter
    ==============================================================================
    *10.1.1.1        LOCAL(0)         7 u   14   32   37    0.194   -4.870   3.314
```

NTP Authentication

When you enable NTP authentication, the device synchronizes to a time source only if the source carries the authentication keys specified with the source by key identifier. The device drops any packets that fail the authentication check, and prevents them from updating the local clock.

Client

`#configure terminal`	Enter Configure mode.
`(config)#feature ntp vrf management`	Enable feature on default or management VRF. By default this feature runs on management VRF..

(config)#ntp server 10.1.1.1 vrf management	Configure ntp server ip address.
(config)#ntp authenticate vrf management	Enable NTP Authenticate. NTP authentication is disabled by default.
(config)#ntp authentication-key 1234 md5 text vrf management	Configure ntp authentication key along with md5 value.
(config)#ntp trusted-key 1234 vrf management	Configure trusted key <1-65535>
(config)#exit	Exit from the Configure Mode.

Validation Commands

```
#show ntp authentication-status
    Authentication enabled

#show ntp authentication-keys
    --------------------------
     Auth Key       MD5 String
    --------------------------
    1234              SWWX

#show    ntp    trusted-keys
    Trusted Keys:
    1234
```


CHAPTER 13 Simple Network Management Protocol

Overview

SNMP provides a standardized framework and a common language for monitoring and managing devices in a network. The SNMP framework consists of three parts:

- An SNMP manager: The system used to control and monitor the activities of network devices. This is sometimes called a Network Management System (NMS).
- An SNMP agent: The component within a managed device that maintains the data for the device and reports these data SNMP managers.
- Management Information Base (MIB): SNMP exposes management data in the form of variables which describe the system configuration. These variables can be queried (and sometimes set) by SNMP managers.

In SNMP, administration groups are known as communities. SNMP communities consist of one agent and one or more SNMP managers. You can assign groups of hosts to SNMP communities for limited security checking of agents and management systems or for administrative purposes. Defining communities provides security by allowing only management systems and agents within the same community to communicate.

A host can belong to multiple communities at the same time, but an agent does not accept a request from a management system outside its list of acceptable community names.

SNMP access rights are organized by groups. Each group is defined with three accesses: read access, write access, and notification access. Each access can be enabled or disabled within each group.

The SNMP v3 security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The security levels are:

- noAuthNoPriv: No authentication or encryption
- authNoPriv: Authentication but no encryption
- authPriv: Both authentication and encryption SNMP is defined in RFCs 3411-3418.

Topology

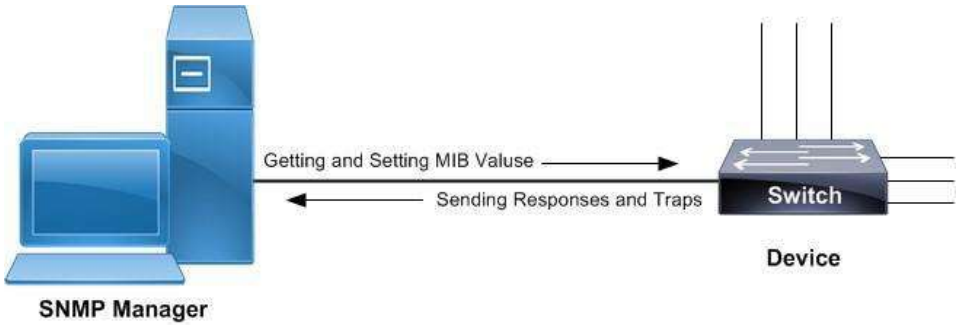


Figure 13-31: SNMP sample topology

Simple Network Management Protocol

Standard SNMP Configurations

`#configure terminal`	Enter Configure mode.
`(config)#snmp-server view all .1 included vrf management`	Creates SNMP view labeled as “all” for OID-Tree as “.1” for vrf management.
`(config)#snmp-server community test group network-operator vrf management`	Set community string as “test” for group of users having “network-operator” privilege.
`(config)#snmp-server host 10.12.6.63 traps version 2c test udp-port 162 vrf management`	Specify host “10.12.6.63” to receive SNMP version 2 notifications at udp port number 162 with community string as “test”.
`(config)#exit`	Exit configure mode.

Validation

Use the below commands to verify the SNMP configuration:

```
#show running-config snmp snmp-server view all
.1 included vrf management
snmp-server community test group network-operator vrf management snmp-server
host 10.12.6.63 traps version 2c test udp-port 162 vrf management
```

```
#show snmp group
-------------------------------------------------------------------------------
community/user    group          version   Read-View    Write-view    Notify-view
-------------------------------------------------------------------------------
test          network-operator    2c/1       all         none            all

#show snmp host
-------------------------------------------------------------------------------
Host                Port    Version   Level          Type            SecName
-------------------------------------------------------------------------------
10.12.6.63          162     2c        noauth         trap            test
```

SNMP GET Command

```
# snmpget -v2c -c test 10.12.45.238
.1.3.6.1.2.1.6.13.1.2.10.12.45.238.22.10.12.6.63.52214

TCP-MIB::tcpConnLocalAddress.10.12.45.238.22.10.12.6.63.52214 = IpAddress:
10.12.45.238
```

SNMP WALK Command

SNMP WALK for particular OID

```
#snmpwalk -v2c -c test 10.12.45.238 .1.3.6.1.2.1.25.3.8.1.8 HOST-
RESOURCES-MIB::hrFSLastFullBackupDate.1 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.4 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.5 = STRING: 0-1-1,0:0:0.0
```



```
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.6 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.10 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.12 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.13 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.14 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.15 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.16 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.17 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.18 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.19 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.20 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.21 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.22 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.23 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.24 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.25 = STRING: 0-1-1,0:0:0.0
HOST-RESOURCES-MIB::hrFSLastFullBackupDate.26 = STRING: 0-1-1,0:0:0.0
```

Complete SNMP WALK

```
#snmpwalk -v2c -c test 10.12.45.238 .1
```

SNMP WALK Command

```
#snmpset -v2c -c test 10.12.45.102 1.3.6.1.2.1.10.246.1.2.1.30.1 u 123
iso.3.6.1.2.1.10.246.1.2.1.30.1 = Gauge32: 123
```

CHAPTER 14 Access Control Lists Configurations

This chapter contains a complete example of access control list (ACL) configuration.

Overview

An Access Control List is a list of Access Control Entries (ACE). Each ACE in ACL specifies the access rights allowed or denied.

Each packet that arrives at the device is compared to each ACE in each ACL in the order they are defined. The device continues to look until it has a match. If no match is found and the device reaches the end of the list, the packet is denied. For this reason, place the most frequently occurring specifications at the top of the list.

The device stops checking the specifications after a match occurs.

Note: If there is no match, the packet is dropped (implicit deny). Therefore, an ACL intended to deny a few selected packets should have at least one permit filter of lower priority; otherwise, all traffic is dropped because of the default implicit deny filter.

Topology

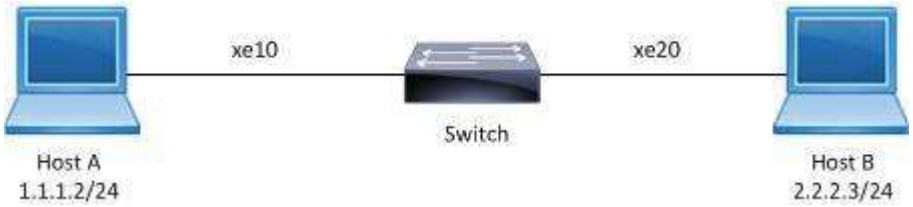


Figure 14-32: ACL sample topology

IPv4 ACL Configuration

`#configure terminal`	Enter configure mode.
`(config)#ip access-list T1`	Create an IP access list named T1.
`(config-ip-acl)#deny any host 1.1.1.1 any`	Create an access rule to deny IP packets with source address 1.1.1.1.
`(config-ip-acl)#permit any host 1.1.1.1/24 any`	Create an access rule to permit IP packets with source address 1.1.1.1.
`(config-ip-acl)#exit`	Exit access list mode.
`(config)#interface xe10`	Enter interface mode.
`(config-if)#no switchport`	Configure the interface as Layer 3.
`(config-if)#ip address 1.1.1.3/24`	Assign an IP address.
`(config-if)#ip access-group T1 in`	Apply access group T1 for inbound traffic to the interface.
`(config-if)#end`	Exit interface and configure mode.

Validation

Use the commands below to verify the match count. When inbound IP packets reach interface xe10 with source address 1.1.1.1, then the match count for access rule 10 increases equal to the number of packets sent.

```
#show ip access-lists T1
    IP access list T1
            10 deny any host 1.1.1.1 any [match=200]
            20 permit any 1.1.1.1/24 any
            default deny-all
```

When inbound IP packets reach interface xe10 with a source address in the range from 1.1.1.1 to 1.1.1.254, then the match count for access rule 20 increases equal to the number of packets sent.

```
#show ip access-lists T1
    IP access list T1
        10 deny any host 1.1.1.1 any
        20 permit any 1.1.1.1/24 any
    [match=2000] default deny-all
```

Note: Use the command `clear ip access-list counters` to clear the statistics of all ACLs or `clear ip access-list <access-list name> counters` to clear statistics of a particular ACL.

ICMP ACL Configuration

`#configure terminal`	Enter configure mode.
`(config)#ip access-list icmp-acl-01`	Create an IP access list named icmp-acl-01.
`(config-ip-acl)#10 deny icmp 1.1.1.2/24 2.2.2.2/24 dscp af11 fragments`	Create an access rule with sequence number 10 to deny ICMP packets from a specific source towards a specific destination with a DSCP value of af11. Note: The sequence number is optional.
`(configip-acl)#20 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash`	Create an access rule with sequence number 20 to permit ICMP packets from a specific source towards a specific destination with precedence as flash.
`(config-ip-acl)#exit`	Exit access list mode.
`(config)#interface xe10`	Enter interface mode.
`(config-if)#no switchport`	Configure the interface as Layer 3.
`(config-if)#ip address 1.1.1.3/24`	Assign an IP address.
`(config-if)#ip access-group icmp-acl-01 in`	Apply access group icmp-acl-01 for inbound traffic to the interface.
`(config-if)#end`	Exit interface and configure mode.

Validation

Use the commands below to verify the match count. When inbound IP packets reach interface xe10 with source address 1.1.1.X, destination address 2.2.2.X, DSCP value af11, and are fragmented, then the count for access rule 10 increases equal to the number of packets sent.

```
#show ip access-lists icmp-acl-01
IP access-list icmp-acl-01
```

```
    10 deny icmp 1.1.1.2/24 2.2.2.2/24 dscp af11 [match=200]
    20 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash
default deny-all
```

When inbound IP packets reach interface xe10 with source address as 1.1.1.X, destination address 2.2.2.X, and precedence value flash, then the count for access rule 20 increases equal to the number of packets sent.

```
#show ip access-lists icmp-acl-01
IP access-list icmp-acl-01
    10 deny icmp 1.1.1.2/24 2.2.2.2/24 dscp af11
    20 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash
[match=200] default deny-all
```

Note: Use the command `clear ip access-list counters` to clear statistics of all ACLs configured or `clear ip access-list <access-list name> counters` to clear statistics of a particular ACL.

Access List Entry Sequence Numbering

You can change the sequence numbers of rules in an access list.

Note: Re-sequencing an ACL attached to a management interface clears the ACL counters associated to it.

`#configure terminal`	Enter configure mode.
`(config)#ip access-list icmp-acl-01`	Enter access list mode for ACL icmp-acl-01.
`(config-ip-acl)#resequence 100 200`	Re-sequence the access list, starting with sequence number 100 and incrementing by 200.
`(config-ip-acl)#1000 deny icmp 1.1.1.2/24 2.2.2.2/24 dscp af11`	Re-sequencing specific access rule 100 with sequence number 1000
`(config-ip-acl)#exit`	Exit access list mode.

Validation

Before re-sequencing:

```
#show access-lists icmp-acl-01
IP access list icmp-acl-01
        10 deny icmp 1.1.1.2/24 2.2.2.2/24 dscp af11 log
20 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash
default deny-all
```

After re-sequencing the access list, starting with sequence number 100 and incrementing by 200

```
#show access-lists icmp-acl-01
IP access list icmp-acl-01
        100 deny icmp 1.1.1.2/24 2.2.2.2/24 dscp af11 log
300 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence
flash default deny-all
```

After re-sequencing specific access rule 100 with sequence number 1000

```
 #show access-lists icmp-acl-01
IP access list icmp-acl-01
```

```
300 permit icmp 1.1.1.1/24 2.2.2.2/24 precedence flash
1000 deny icmp 1.1.1.2/24 2.2.2.2/24 dscp af11
log default deny-all
```

IPv6 ACL Configuration

`#configure terminal`	Enter configure mode.
`(config)#ipv6 access-list ipv6-acl-01`	Create an IPv6 access list named as icmp-acl-01.
`(config-ipv6-acl)#11 deny ip any any flow-label 100`	Create access rule sequence number 11 to deny IPv4 encapsulated packets in IPv6 with any source address to any destination address with flow label 100.
`(config-ipv6-acl)#default permit-all`	Update the default rule to permit all.
`(config-ipv6-acl)#exit`	Exit access list mode
`(config)#interface xe10`	Enter interface mode.
`(config-if)#no switchport`	Configure the interface as Layer 3.
`(config-if)#ipv6 address 1:1::1:3/64`	Assign an IPv6 address.
`(config-if)# ipv6 access-group ipv6-acl-01 in`	Apply access group ipv6-acl-01 for inbound traffic to the interface.
`(config-if)#end`	Exit interface and configure mode.

Validation

Use the commands below to verify the match count. When inbound IPv6 packets reach interface xe10 with IPv4 packets encapsulated with flow label 100, then count for access rule 11 increases equal to the number of packets sent.

```
#show ipv6 access-lists ipv6-acl-01
IPv6 access-list ipv6-acl-01
    11 deny ip any any flow-label 100
[match=1000] default permit all
```

For all other IPv6 packets, access rule 100 is invoked and the match counts increase equal to the number of packets sent.

```
#show ipv6 access-lists ipv6-acl-01
IPv6 access-list ipv6-acl-01
    11 deny ip any any flow-label 100
default permit-all [match=2000]
```

Note: Use the command `clear ipv6 access-list counters` to clear statistics of all IPv6 ACLs configured or `clear ipv6 access-list <ipv6 access-list name> counters` to clear statistics of the particular IPv6 ACL.

MAC ACL Configuration

`#configure terminal`	Enter configure mode.
`(config)#mac access-list mac-acl-01`	Create a MAC access list named mac-acl-01.

(config-mac-acl)#22 permit host 0000.0011.1212 host 0000.1100.2222 vlan 2	Create an access rule with sequence number 22 to permit packets from a host with a specific MAC towards a host with a specific MAC with VLAN 2.
(config-mac-acl)#exit	Exit access list mode.
(config)#bridge 1 protocol rstp vlanbridge	Create a VLAN-aware RSTP bridge.
(config)#vlan 2 bridge 1 state enable	Create VLAN 2.
(config)#interface xe10	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)# mac access-group mac-acl-01 in	Applies the MAC access list mac-acl-01 to ingress traffic.
(config-if)#end	Exit interface and configure mode.

Validation

Use the commands below to verify the match count. When inbound packets reach interface xe10 with the specific source and destination MAC with the VLAN as 2, then the count for access rule 22 increases equal to the number of packets sent.

```
#show mac access-lists
    MAC access list mac-acl-01
        22 permit mac host 0000.0011.1212 host 0000.1100.2222 vlan 2 [match=3000]
    default deny-all
```

For all other packets, default rule is invoked and the match counts increases equal to the number of packets sent.

```
#show mac access-lists mac-acl-01
    MAC access list mac-acl-01
        22 permit mac host 0000.0011.1212 host 0000.1100.2222 vlan 2
    default deny-all [match=2000]
```

Note: As per the present design, ARP/ND packets will be filtered based on the source MAC address only (host mac address).

Note: Use the command `clear mac access-list counters` to clear statistics of all MAC ACLs or `clear mac access-list <mac access-list name> counters` to clear statistics of a particular MAC ACL.

Management ACL Overview

Management Port ACL can be used to provide basic level of security for accessing the management network. ACLs can also be used to decide which types of management traffic to be forwarded or blocked at the management port.

When configuring access list on a router or a switch, each access list needs to be identified by a unique name or a number. Each access list entry can have permit or deny actions. Each entry will be associated with a sequence number in the range of <1-268435453>. Lower the sequence number, higher the priority.

User should be able to configure the system to allow certain IP address for a protocol and don't allow any other IP address matching for that protocol.

Note: If there is no match, the packet is dropped (implicit deny). Therefore, an ACL intended to deny a few selected packets should have at least one permit filter of lower priority; otherwise, all traffic is dropped because of the default implicit deny filter.

Topology

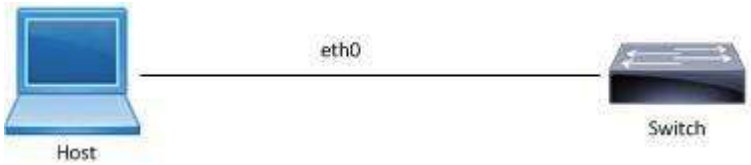


Figure 14-33: Management ACL Sample Topology

Management ACL Configuration

`#configure terminal`	Enter configure mode.
`(config)#ip access-list mgmt`	Create an IP access list named mgmt
`(config-ip-acl)#permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh`	Create an access rule to permit TCP connection with source address 10.12.45.57 with destination address 10.12.29.49 on destination port equal to SSH.
`(config-ip-acl)#permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet`	Create an access rule to permit TCP connection with source address 10.12.45.58 with Destination address 10.12.29.49 on destination port equal to Telnet.
`(config-ip-acl)#permit udp any host 10.12.29.49 eq snmp`	Create an access rule to permit UDP packet with any source address with Destination address 10.12.29.49 on destination port equal to SNMP.
`(config-ip-acl)#permit udp any host 10.12.29.49 eq ntp`	Create an access rule to permit UDP packet with any source address with Destination address 10.12.29.49 on destination port equal to NTP.
`(config-ip-acl)#permit udp host 10.12.29.49 any eq snmptrap`	Create an access rule to permit UDP packet with source address 10.12.29.49 with any Destination address on destination port equal to SNMPTrap.
`(config-ip-acl)#permit tcp host 10.12.29.49 eq ssh host 10.12.45.57`	Create an access rule to permit TCP connection with source address 10.12.29.49 on source port equal to ssh with Destination address 10.12.45.57 .
`(config-ip-acl)#deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh`	Create an access rule to deny TCP connection with source address 10.12.45.58 with Destination address 10.12.29.49 on destination port equal to SSH.
`(config-ip-acl)# deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet`	Create an access rule to deny TCP connection with source address 10.12.45.57 with Destination address 10.12.29.49 on destination port equal to Telnet.
`(config-ip-acl)#exit`	Exit access list mode.
`(config)#interface eth0`	Enter interface mode of Management Interface.
`(config-if)#no switchport`	Configure the interface as Layer 3.
`(config-if)#ip address 10.12.29.49/24`	Assign an IP address.

(config-if)#ip access-group mgmt in	Apply access group mgmt for inbound traffic to the interface.
(config-if)#end	Exit interface and configure mode.

Validation

Use the commands below to verify the match count. When a TCP connection for Destination Port SSH reach interface eth0 with source address 10.12.45.57, then the match count for access rule 10 increases equal to the number of packets sent.

```
#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh [match=9]
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
    80 deny tcp host 10.12.45.57 host 10.12.29.49 eq
    telnet default deny-all
```

When a TCP connection for Destination Port Telnet reach interface eth0 with source address 10.12.45.58, then the match count for access rule 20 increases equal to the number of packets sent.

```
#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet [match=10]
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
    80 deny tcp host 10.12.45.57 host 10.12.29.49 eq
    telnet default deny-all
```

When a UDP packet for Destination Port SNMP reach interface eth0 with any source address, then the match count for access rule 30 increases equal to the number of packets sent. Prior to this SNMP should be configured on Device (10.12.29.49).

```
    Example: snmp-server community SNMPTEST group network-admin vrf
    management snmp-server host 10.12.6.86 traps version 2c SNMPTEST udp-
    port 162 vrf management
    snmp-server enable snmp  vrf management

    #show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp [match=50]
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
```

```
        70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
    80 deny tcp host 10.12.45.57 host 10.12.29.49 eq
    telnet default deny-all
```

When a UDP packet for Destination Port NTP reach interface eth0 with any source address, then the match count for access rule 40 increases equal to the number of packets sent. Prior to this NTP should be configured on Device (10.12.29.49).

```
    Example:
    ntp enable vrf management ntp
    authenticate vrf management
    ntp authentication-key 123 md5 swwx 7 vrf
    management ntp trusted-key 123 vrf management ntp
    server 10.12.45.36 vrf management ntp server
    10.12.16.16 prefer vrf management
    ntp server 10.12.16.16 key 123 vrf management

#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp [match=1]
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
    80 deny tcp host 10.12.45.57 host 10.12.29.49 eq
    telnet default deny-all
```

When a TCP connection request for Destination Port SSH reach interface eth0 with source address 10.12.45.58, this should deny the connection and the match count for access rule 70 increases equal to the number of packets sent.

```
#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
    [match=1]         80 deny tcp host 10.12.45.57 host 10.12.29.49 eq
    telnet         default deny-all
```

When a TCP connection request for Destination Port Telnet reach interface eth0 with source address 10.12.45.57, this should deny the connection and the match count for access rule 80 increases equal to the number of packets sent.

```
#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
```

```
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq
    telnet[match=1] default deny-all
```

To enable SNMPTRAPS, apply the ACL outbound to the Management interface.

`#configure terminal`	Exit access list mode.
`(config)#interface eth0`	Enter interface mode of Management Interface.
`(config-if)#ip access-group mgmt out`	Apply access group mgmt for outbound traffic to the interface.
`(config-if)#end`	Exit interface and configure mode.

When a UDP packet for Destination Port SNMPTrap sends out of interface eth0 with any Destination address, then the match count for access rule 50 increases equal to the number of packets received. Prior to this SNMPTrap should be configured on Device (10.12.29.49) to listen to port 162.

```
    Example: snmp-server community SNMPTEST group network-admin vrf
    management snmp-server host 10.12.6.86 traps version 2c
    SNMPTEST udp-port 162 vrf management snmp-server enable snmp
    vrf management

#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap [match=5]
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
    80 deny tcp host 10.12.45.57 host 10.12.29.49 eq
    telnet default deny-all
```

When an ACL is applied on interface eth0 outbound and inbound together, then we must configure an ACL to establish a TCP connection between source 10.12.29.49 with source Port SSH to destination address 10.12.45.57. When a TCP connection is established on port SSH, then the match count for access rule 10 and 60 increases equal to the number of packets sent and received.

```
#show ip access-lists mgmt
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh [match=9]
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57[match=9]
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
    80 deny tcp host 10.12.45.57 host 10.12.29.49 eq
    telnet default deny-all
```

Note: Use the command `clear ip access-list counters` to clear the statistics of all ACLs or `clear ip access-list <access-list name> counters` to clear statistics of a particular ACL.

```
#show access-lists
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
            80 deny tcp host 10.12.45.57 host 10.12.29.49 eq telnet


#show   access-lists   summary
    IPV4 ACL mgmt
           statistics enabled
           Total ACEs Configured: 8
    Configured on interfaces:
              eth0 - ingress (Router ACL)
           Active on interfaces:
    eth0 - ingress (Router ACL)

#show access-lists expanded
    IP access list mgmt
            10 permit tcp host 10.12.45.57 host 10.12.29.49 eq ssh
            20 permit tcp host 10.12.45.58 host 10.12.29.49 eq telnet
            30 permit udp any host 10.12.29.49 eq snmp
            40 permit udp any host 10.12.29.49 eq ntp
            50 permit udp host 10.12.29.49 any eq snmptrap
            60 permit tcp host 10.12.29.49 eq ssh host 10.12.45.57
            70 deny tcp host 10.12.45.58 host 10.12.29.49 eq ssh
    80 deny tcp host 10.12.45.57 host 10.12.29.49 eq
    telnet default deny-all [match=4]
```

ARP ACL Overview

ARP ACL can be used to permit or deny the ARP packets, based on the ARP request or response option configured.

Topology

Figure 14-34: ARP ACL Sample Topology

ARP ACL Configuration

#configure terminal	Enter configure mode.
(config)#interface ge4	Enter interface mode.
(config-if)#ip address	Assign IPv4 address.
(config-if)#exit	Exit access list mode.
(config)# mac access-list mac1	Enter mac access list mode.
(config-mac-acl)#permit 0000.3ae0.456d.0000.0000.0000 any arp request	Create an access rule to permit specific ARP request.
(config-mac-acl)#permit 0000.3ae0.456d.0000.0000.0000 any arp response	Create an access rule to permit specific ARP response.
(config-mac-acl)#permit any any ipv4	Create an access rule to permit any IPv4 packet.
(config-mac-acl)#exit	Exit access list mode.
(config)#interface ge4	Enter interface mode.
(config-if)#mac access-group mac1 in	Apply access group mac1 for inbound traffic to the interface.
(config-if)#end	Exit interface and configure mode.

Validation

Use the commands below to assign IP address on IXIA and ping from IXIA.

```
#show mac access-lists
    MAC access list mac1
            10 permit host 0000.3AE0.456D any arp request [match=1]
            20 permit host 0000.3AE0.456D any arp response [match=1]
            30 permit any any ipv4 [match=1] default deny-
    all
```

CHAPTER 15 Show Tech Support Configurations

Overview

SWMRE maintains a collection of consolidated information about system configurations and statistics. This information is for debugging and diagnosing system issues, and can be uploaded to a remote server. You generate a file with this information via the `show techsupport` command.

Note: Output is not displayed on the terminal.

The default directory (`/var/log/`) is where the stored information is saved. The filename has the form:

`tech_support_YYYY_MMM_DD_HH_MM_SS.tar.gz`. If a file name is specified, the information will be saved to `filename_YYYY_MMM_DD_HH_MM_SS_.tar.gz`. Date stamps are in the `YYYY_MM_DD` form, and time stamps are in the form `HH_MM_SS`.

The collected system data contains the following logs:

- Saved start-up configuration of the system.
- The `running-config`, and statistics for a specified module or all modules.
- The last 100 commands.
- Memory and CPU usage of the process.
- Process Id and process name.
- The user account running the process.

Tech Support Samples

`#show techsupport all`	Collects system configurations and statistics for all modules, and saves it in `tech support date timestamp.tar.gz` in the `/var/log/` directory.
`#show techsupport all log-path /home/filename`	Collects system configurations and statistics for all modules, and saves it in `filename date timestamp.tar.gz` in the `/home/directory`.
`#show techsupport nsm`	Collects `nsm` protocol configurations and statistics, and saves it in `tech support date timestamp.tar.gz` in the `/var/log/` directory.
`#show techsupport nsm log-path /home/filename`	Collects `nsm` protocol configurations and statistics, and saves it at `filename_date_timestamp.tar.gz` in the `/home/directory`.
`#show techsupport hostpd authd imi`	Collects `hostp`, `authd`, and `imi` protocol configurations and statistics and saves it at `tech_support_date_timestamp.tar.gz` in the `/var/log/` directory.

`#show techsupport hostpd authd imi logpath /home/filename`	Collects `hostp, authd, imi` protocol configurations and statistics, saves it as `filename date timestamp.tar.gz` in the `/home/` directory.

Show Tech Support Configurations

Validation Commands

You can display the status of a `show techsupport` command given earlier which indicates the protocol modules that have completed, are in progress, or have not executed. If the command has completed, it lists the last five generated tech support files with their path.

```
#show techsupport status

Tech Support Command Execution Is Complete
##Generated Tech Support File-list
/var/log/tech_support_18_Dec_2017_20_39_02.tar.gz #
```

Note: the running `show techsupport` operation has not completed, reentering the `show techsupport` command is ignored.

CHAPTER 16 Route-map Continue Configuration

This section contains Route-map continue configuration with BGP.

Overview

The continue clauses allow you to configure and organize more modular policy definitions to reduce the number of policy configurations that are repeated within the same route map.

Continue clause under a route-map provides the capability to execute additional entries in a route map after an entry is executed with a successful match and set clauses. The continue command allows multiple entries to be evaluated within a single route-map. Continue commands can be assigned optional sequence numbers that indicates the order in which clauses are to be evaluated.

Using Continue with Match Clauses

When a `match` clause exists in a route-map with continue clause then `continue` clause is executed only when a successful match occurs. If a `match` clause does not exist in the route-map and if a `continue` clause exists, the `continue` clause will be evaluated and will go to the specified route-map entry. When a successful match occurs and we have a `continue` clause, the route-map executes the `set` clauses and then goes to the specified route-map entry. If a `continue` clause does not exist in the next route map, then the route-map will behave normally. If a `continue` clause exists in the next route-map but a match is not successful, the route-map will not continue and will “fall through” to the next sequence number if one exists

Using Continue with Set Actions

`Set` clauses are executed after the route-map evaluation is done. The `set` clauses are evaluated and executed in the order in which they were configured. `Set` clauses are only executed after a successful match occurs. The `continue` statement proceeds to the specified route-map entry only after configured `set` actions are performed. If a `set` action is configured in the first route-map and then the same `set` action occurs again but with a different value, in a subsequent route-map entry, then the last `set` action will override the previous `set` actions which were configured with the same set command.

Topology

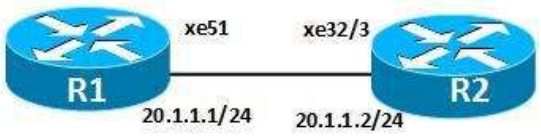


Figure 16-35: Route-map continue

Configure Route-map *continue* on R1

In the below example we will apply route-map `continue` on R1 under BGP 100, with redistributed connected routes from R2 on R1. Here, 10.1.0.0/16 is a superset, while 10.1.1.0/24, 10.1.2.0 /24, 10.1.3.0/24, 10.1.4.0/24, and 10.1.5.0/24 are subsets and will filter PF1, which is a superset and sets several prefixes.

R1

R1#configure terminal	Enter configure mode.
R1(config)#interface xe51	Enter interface mode.
R1(config-if)#ip address 20.1.1.1/24	Configure the IP address of the interface.
R1(config-if)#exit	Exit interface mode.
R1(config)#ip prefix-list PF1 seq 5 permit 10.1.0.0/16 le 32	Configure super set prefix PF1
R1(config)#ip prefix-list P1 seq 5 permit 10.1.1.0/24 le 32	Configure subset prefix P1
R1(config)#ip prefix-list P2 seq 5 permit 10.1.2.0/24 le 32	Configure subset prefix P2
R1(config)#ip prefix-list P3 seq 5 permit 10.1.3.0/24 le 32	Configure subset prefix P3
R1(config)#router bgp 100	Configure bgp process 100
R1(config-router)#bgp router-id 1.1.1.1	Configure bgp router id
R1(config-router)#neighbor 20.1.1.2 remoteas 100	Configure bgp remote-as 100 with neighbor IP
R1(config-router)#neighbor 20.1.1.2 routemap myid1 in	Configure bgp route-map myid1 as In bound policy with neighbor ip
R1(config-routed)#exit	Exit the router bgp mode
R1(config)#route-map myid1 permit 1	Configure route-map myid1 with sequence number 1
R1(config-route-map)match ip address prefixlist PF1	Match for prefix PF1
R1(config-route-map)continue	Configure continue command without sequence number
R1(config-route-map)set metric 10	Set metric as 10
R1(config-route-map)set weight 3465789	Set weight as 3465789
R1(config-route-map)route-map myid1 permit 2	Configure route-map myid1 with sequence number 2
R1(config-route-map)match ip address prefixlist P1	Match for IP prefix-list P1
R1(config-route-map)continue 3	Configure continue with sequence number 3
R1(config-route-map)set metric 20	Set metric as 20.
R1(config-route-map)set origin igp	Set origin as IGP protocol
R1(config-route-map)route-map myid1 permit 3	Configure route-map myid1 with sequence number 3
R1(config-route-map)match ip address prefixlist P2	Match for IP prefix-list P2
R1(config-route-map)continue 4	Configure continue with sequence number 4
R1(config-route-map)set metric 30	Set metric as 30.
R1(config-route-map)set as-path prepend 600	Set as-path prepend as 600
R1(config-route-map)route-map myid1 permit 4	Configure route-map myid1 with sequence number 4

R1(config-route-map)match ip address prefixlist P3	Match for IP prefix-list P3.
R1(config-route-map)set local-preference 400	Set local preference as 400
R1(config-route-map)set weight 400	Set weight as 400
R1(config-route-map)end	End the route-map

R2

R2#configure terminal	Enter configure mode.
R2(config)#interface xe32/1	Enter interface mode.
R2(config-if)#ip address 10.1.1.1/24	Configure the IP address of the interface on an interface which is up and running
R2(config-if)#interface xe32/2	Enter interface mode.
R2(config-if)#ip address 10.1.2.1/24	Configure the IP address of the interface on an interface which is up and running
R2(config-if)#interface xe32/4	Enter interface mode.
R2(config-if)#ip address 10.1.3.1/24	Configure the IP address of the interface on an interface which is up and running
R2(config-if)#interface xe17/1	Enter interface mode.
R2(config-if)#ip address 10.1.4.1/24	Configure the IP address of the interface on an interface which is up and running
R2(config-if)#interface xe21/1	Enter interface mode.
R2(config-if)#ip address 10.1.5.1/24	Configure the IP address of the interface on an interface which is up and running
R2(config-if)#interface xe32/3	Enter interface mode.
R2(config-if)#ip address 20.1.1.2/24	Configure the IP address on the connected interface.
R2(config-if)#exit	Exit interface mode.
R2(config)#router bgp 100	Configure BGP process 100
R2(config-router)#bgp router-id 2.2.2.2	Configure BGP router id
R2(config-router)#redistribute connected	Redistribute the connected routes which are 10 networks here.

Validation

```
R1#show ip bgp summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 5
2 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V    AS    MsgRcv     MsgSen TblVer    InQ    OutQ    Up/
 Down   State/PfxRcd
20.1.1.2                  4    100   145         177       5       0       0
00:40:05                5
```

```
    Total number of neighbors 1

    Total number of Established sessions 1

    Note: Check the prefixes learnt here are 5.

    R1#

    R1#show ip bgp
    BGP table version is 5, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network          Next Hop            Metric     LocPrf      Weight Path
*>i   10.1.1.0/24      20.1.1.2              20         100          3465789  i *>i
10.1.2.0/24       20.1.1.2             30        100          3465789 600 ?
*>i   10.1.3.0/24      20.1.1.2              10         400          400      ?
*>i   10.1.4.0/24      20.1.1.2              10         100          3465789  ?
*>i   10.1.5.0/24      20.1.1.2              10         100          3465789  ?

Total number of prefixes 5
R1#

Note: In the above example, 10.1.4.0/24 and 10.1.5.0/24 prefixes will match only on
PF1 which is a super set prefix and metric is set as 10, while the 10.1.1.0/24,
10.1.2.0/24 and 10.1.3.0/24 prefixes will match in P1,P2 and P3 prefix-lists and
execute the set clauses respectively.

R1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,        ia -
IS-IS inter area, E - EVPN,        v - vrf leaked        * -
candidate default

IP Route Table for VRF "default"
B     10.1.1.0/24 [200/20] via 20.1.1.2, xe51, 00:45:05
B     10.1.2.0/24 [200/30] via 20.1.1.2, xe51, 00:45:05
B     10.1.3.0/24 [200/10] via 20.1.1.2, xe51, 00:45:05
B     10.1.4.0/24 [200/10] via 20.1.1.2, xe51, 00:25:05
B     10.1.5.0/24 [200/10] via 20.1.1.2, xe51, 00:24:35
C     20.1.1.0/24 is directly connected, xe51, 01:00:40
C     127.0.0.0/8 is directly connected, lo, 02:26:41

Gateway of last resort is not set R1#

R1#show ip bgp route-map myid1
BGP table version is 5, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
```

```
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network          Next Hop            Metric     LocPrf      Weight Path
*>i   10.1.1.0/24       20.1.1.2              20          100          3465789  i *>i
10.1.2.0/24       20.1.1.2             30        100          3465789 600 ?
*>i   10.1.3.0/24       20.1.1.2              10          400          400      ?
*>i   10.1.4.0/24       20.1.1.2              10          100          3465789  ?
*>i   10.1.5.0/24       20.1.1.2              10          100          3465789  ?
Total number of prefixes 5
R1#
R1#


R2#show ip bgp summary
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 3
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv     MsgSen TblVer    InQ   OutQ   Up/ Down
State/PfxRcd
20.1.1.1                  4   100  133         133       3      0      0
00:39:57                0

Total number of neighbors 1

Total number of Established sessions 1
R2#
R2#


R2#show ip bgp
BGP table version is 3, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network          Next Hop            Metric     LocPrf      Weight Path *>
10.1.1.0/24       0.0.0.0              0          100          32768    ?
*>    10.1.2.0/24       0.0.0.0              0          100          32768    ?
*>    10.1.3.0/24       0.0.0.0              0          100          32768    ?
*>    10.1.4.0/24       0.0.0.0              0          100          32768    ?
*>    10.1.5.0/24       0.0.0.0              0          100          32768    ?
*>    20.1.1.0/24       0.0.0.0              0          100          32768    ?

Total number of prefixes 6
R2#

R2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
```

```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2,         ia -
IS-IS inter area, E - EVPN,        v - vrf leaked         * -
candidate default

IP Route Table for VRF "default"
C     10.1.1.0/24 is directly connected, xe32/1, 01:02:22
C10.1.2.0/24 is directly connected, xe32/2, 01:01:46
C10.1.3.0/24 is directly connected, xe32/4, 01:02:21
C10.1.4.0/24 is directly connected, xe17/1, 00:26:52
C10.1.5.0/24 is directly connected, xe21/1, 00:26:32
    C20.1.1.0/24 is directly connected, xe32/3, 01:02:22
    C127.0.0.0/8 is directly connected, lo, 01:34:40

    Gateway of last resort is not set R2#
```

Route-map Show Commands

```
R1#show running-config route-map
    ! route-map myid1 permit 1 match ip address prefix-list
    PF1 continue set metric 10 set weight 3465789 ! route-
    map myid1 permit 2 match ip address prefix-list P1
    continue 3 set metric 20 set origin igp ! route-map
    myid1 permit 3 match ip address prefix-list P2 continue
    4 set metric 30 set as-path prepend 600 ! route-map
    myid1 permit 4 match ip address prefix-list P3 set
    local-preference 400 set weight 400
!
    R1#
R1#show route-map route-map myid1, permit, sequence 1   Match
    clauses:     ip address prefix-list: PF1   Continue
    clause:  next sequence
Set clauses:                                                metric 10   weight 3465789 rou
    myid1, permit, sequence 2   Match clauses:
        ip address prefix-list: P1   Continue clause:
    sequence 3:   Set clauses:     metric 20     origin
    igp
    route-map myid1, permit, sequence 3   Match clauses:
        ip address prefix-list: P2   Continue clause:
    sequence 4:   Set clauses:     metric 30
    as-path prepend 600 route-map myid1, permit, sequence 4   Match clauses:
    ip address prefix-list: P3
  Set clauses:     local-preference 400     weight 400
R1#
```

System Management Command Reference

Contents

This document contains these chapters and appendices:

- Chapter 1, *Dynamic Host Configuration Protocol Client*
- Chapter 2, *Domain Name System*
- Chapter 3, *Secure Shell*
- Chapter 4, *Simple Network Management Protocol*
- Chapter 6, *Syslog*
- Chapter 5, *Telnet*
- Chapter 7, *User Management*
- Chapter 8, *Network Time Protocol*
- Chapter 9, *Dynamic Host Configuration Protocol Relay*
- Chapter 10, *Remote Management*
- Chapter 11, *Software Monitoring and Reporting*

CHAPTER 1 Dynamic Host Configuration Protocol Client

This chapter describes the Dynamic Host Configuration Protocol (DHCP) client commands.

DHCP is used to configure devices that are connected to a network so they can communicate on that network using the Internet Protocol (IP). DHCP is implemented in a client-server model where DHCP clients request configuration data, such as an IP address, a default route, or DNS server addresses from a DHCP server.

This chapter contains these commands:

- feature dhcp
- ip address dhcp
- ip dhcp client request

feature dhcp

Use this command to enable the DHCP client and DHCP relay on the device.

Use the `no` form of this command to disable the DHCP client and DHCP relay and delete any DHCP-related configuration.

Command Syntax `feature dhcp`

`no feature dhcp`

Parameters

None

Default

By default, feature dhcp is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#feature dhcp
```


ip address dhcp

Use this command to get an IP address from a DHCP server for this interface.

Use the `no` form of this command to disable the DHCP client for this interface.

You can give the ip dhcp client request command before giving this command to request additional options.

Command Syntax `ip address dhcp no ip address dhcp`

Parameters

None

Default

No default value is specified.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip address dhcp
(config-if)#
```

Dynamic Host Configuration Protocol Client

ip dhcp client request

Use this command to add an option to a DHCP request.

Use the `no` form of this command to remove an option from a DHCP request.

Command Syntax `ip dhcp client request dns-nameserver ip dhcp client request host-name ip dhcp client request log-server ip dhcp client request ntp-server no ip dhcp client request dns-nameserver no ip dhcp client request host-name no ip dhcp client request log-server no ip dhcp client request ntp-server`

Parameters `dns-nameserver` List of DNS name servers (DHCP option 6) `host-name` Name of the client (DHCP option 12) `ntp-server` List of NTP servers (DHCP option 42) `log-server` List of log servers (DHCP option 7)

Default

By default, ip dhcp client request is enabled

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip dhcp client request ntp-server
```

CHAPTER 2 Domain Name System

This chapter describes Domain Name System (DNS) commands. DNS translates easily-to-remember domain names into numeric IP addresses needed to locate computer services and devices. By providing a worldwide, distributed keyword-based redirection service, DNS is an essential component of the Internet.

The DNS database is hierarchical. When a client such as a Web browser gives a request that specifies a host name, the DNS resolver on the client first contacts a DNS server to determine the server's IP address. If the DNS server does not contain the needed mapping, it forwards the request to a different DNS server at the next higher level in the hierarchy. After potentially several forwarding and delegation messages are sent within the DNS hierarchy, the IP address for the given host eventually arrives at the resolver, that in turn completes the request over Internet Protocol (IP).

Note: The commands below are supported only on the “management” VRF.

The chapter contains these commands:

- debug dns client
- ip domain-list
- ip domain-lookup
- ip domain-name
- ip host
- ip name-server
- show hosts
- show running-config dns

© Symanitron

debug dns client

Use this command to display DNS debugging messages.

Use the `no` form of this command to stop displaying DNS debugging messages.

Command Syntax `debug dns client no debug dns client`

Parameters

None

Default

By default, disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#debug dns client
```

ip domain-list

Use this command to define a list of default domain names used to complete unqualified host names. Each domain in the list is to be tried in turn.

The `ip domain-list` command is similar to the ip domain-name command, except that with the `ip domain-list` command you can define a list of domains, each to be tried in turn.

If there is no domain list, the default domain name specified with the `ip domain-name` command is used. If there is a domain list, the default domain name is not used. Use the `no` form of this command to remove a domain.

Command Syntax `ip domain-list (vrf management|)`
`DOMAIN-NAME no ip domain-list (vrf management|)`
`DOMAIN-NAME`

Parameters

`management`	Virtual Routing and Forwarding name
`DOMAIN-NAME`	Domain name, such as company.com

Default

No default is specified.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip domain-list mySite.com
```

ip domain-lookup

Use this command to enable DNS host name-to-address translation.

Use the `no` form of this command to disable DNS.

Command Syntax `ip domain-lookup (vrf management|) no ip domain-lookup (vrf management|)`

Parameters `management` Virtual Routing and Forwarding name

Default

No default is specified.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip domain-lookup
```

ip domain-name

Use this command to set the default domain name used to complete unqualified host names (names without a dotteddecimal domain name).

The ip domain-list command is similar to the `ip domain-name` command, except that with the `ip domain-list` command you can define a list of domains, each to be tried in turn.

If a domain list has been created with `ip domain-list`, the default domain name is not used. If there is no domain list, the default domain name is used.

Use the `no` form of this command to disable DNS.

Command Syntax `ip domain-name (vrf management|) DOMAIN-NAME no ip domain-name (vrf management|) DOMAIN-NAME`

Parameters

`management`	Virtual Routing and Forwarding name
`DOMAIN-NAME`	Domain name, such as company.com

Default

No default is specified.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip domain-name company.com
```

ip host

Use this command to define static hostname-to-address mappings in DNS. You can specify one or two mappings in a command.

Use the `no` form of this command remove a hostname-to-address mapping.

Command Syntax `ip host (vrf management|) WORD A.B.C.D ip host (vrf management|) WORD A.B.C.D A.B.C.D ip host (vrf management|) WORD (X:X::X:X | A.B.C.D) ip`

```
host (vrf management|) WORD (X:X::X:X | A.B.C.D) (X:X::X:X | A.B.C.D) no
ip host (vrf management|) WORD A.B.C.D no ip host (vrf management|) WORD
A.B.C.D A.B.C.D no ip host (vrf management|) WORD (X:X::X:X | A.B.C.D)
```

```
no ip host (vrf management|) WORD (X:X::X:X | A.B.C.D) (X:X::X:X | A.B.C.D)
```

Parameters

`management`	Virtual Routing and Forwarding name
`WORD`	Host name, such as company.com
`X:X::X:`	IPv6 address of the host
`X`	IPv4 address of the host
`A.B.C.D`	

Default

No default is specified.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip host company.com 192.0.2.1
```

ip name-server

Use this command to add 1-3 DNS server addresses that are used to translate hostnames to IP addresses.

Use the `no` form of this command to remove 1-3 DNS server addresses.

Command Syntax `ip name-server (vrf management|) A.B.C.D ip name-server (vrf management|)(A.B.C.D) (A.B.C.D) ip name-server (vrf management|) (A.B.C.D) (A.B.C.D) (A.B.C.D) ip name-server (vrf management|) (X:X::X:X | A.B.C.D) ip name-server (vrf management|) (X:X::X:X | A.B.C.D) (X:X::X:X | A.B.C.D) ip name-server (vrf management|) (X:X::X:X | A.B.C.D) (X:X::X:X | A.B.C.D) (X:X::X:X | A.B.C.D) no ip name-server (vrf management|) A.B.C.D no ip name-server (vrf management|) A.B.C.D A.B.C.D no ip name-server (vrf management|) A.B.C.D A.B.C.D A.B.C.D no ip name-server (vrf management|) (X:X::X:X | A.B.C.D) no ip name-server (vrf management|) (X:X::X:X | A.B.C.D) (X:X::X:X | A.B.C.D) no ip name-server (vrf management|) (X:X::X:X | A.B.C.D) (X:X::X:X | A.B.C.D) (X:X::X:X | A.B.C.D)`

Parameters

`management`	Virtual Routing and Forwarding name
`A.B.C.D`	IPv4 address of the host
`X:X::X:X`	IPv6 address of the host

Default

No default is specified.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip name-server 123.70.0.23
```

show hosts

Use this command to display the DNS name servers and domain names.

Command Syntax `show hosts (vrf management|all)`

Parameters

`vrf`	management or all VRFs

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following is a sample output of this command displaying two name servers: 10.10.0.2 and 10.10.0.88.

```
#show hosts
Default domain is mySite.com
Domain list: myOtherSite.com
Name/address lookup uses domain service
Name servers are 10.10.0.2 10.10.0.88
```

show running-config dns

Use this command to show the DNS settings of the running configuration.

Command Syntax `show running-config dns (vrf management|)`

Parameters

`vrf`	management

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show running-config dns ip domain-lookup ip name-server
10.10.10.10 !
```

CHAPTER 3 Secure Shell

This chapter describes Secure Shell (SSH) commands.

SSH is a cryptographic protocol for secure data communication, remote login, remote command execution, and other secure network services between two networked computers.

Note: The commands below are supported only on the “management” VRF.

This chapter contains these commands:

- clear ssh hosts
- debug ssh server
- feature ssh
- show debug ssh-server
- show running-config ssh server
- show ssh key
- show ssh server
- show username
- ssh
- ssh6
- ssh algorithm encryption
- ssh key
- ssh login-attempts
- ssh server port

- username sshkey
- username keypair

clear ssh hosts

Use this command to clear the `known_hosts` file.

This command clears all trusted relationships established with SSH servers during previous connections. When a client downloads a file from an external server the first time, the client stores the server keys in the `known_hosts` file. After that, other connections to the same server will use the server keys stored in the `known_hosts` file. In other words, a trusted relationship is created when a client accepts the server keys the first time.

An example of when you need to clear a trusted relationship is when SSH server keys are changed.

Command Syntax `clear`

```
ssh hosts
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear ssh hosts
```

debug

ssh server

Use this command to display SSH server debugging information.

Use the `no` form of this command to stop displaying SSH server debugging information.

Command Syntax `debug ssh server no debug ssh server`

Parameters

None

Default

By default, disabled.

Command Mode

Executive mode and configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#debug ssh server
```

feature ssh

Use this command to enable the SSH server.

Use the `no` form of this command to disable the SSH server.

Command Syntax `feature ssh (vrf management|) no feature ssh (vrf management|)`

Parameters `management` Virtual Routing and Forwarding name

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)feature ssh
```

show

debug ssh-server

Use this command to display whether SSH debugging is enabled.

Command Syntax `show debug ssh-server`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show debug ssh-server ssh server debugging enabled
```

show running-config ssh server

Use this command to display SSH settings in the running configuration.

Command Syntax `show running-config ssh server`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show running-config ssh server feature ssh
```

show ssh key

Use this command to display the SSH server key.

Command Syntax `show`

```
ssh key
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show ssh key
******************RSA KEY*********************
 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDMuVc0jpNgMyNzaqzIELX6LlsaK/
1q7pBixmwHAGDsZm/
dClTLb18AIB27W68YD8k0+Yw0LR0rHuPtNeSFMEsMaQxsaLkSi7yg86xSJaqgLQTyOUTS/
OC9hreXkJ73ay
n0yXa8+bre0oyJq1NWxAI9B1jEhfSSAipoDSp/
dmc93VJyV+3hgy1FMTAheyebQaUVeLBEMH7siRlSfyo7OHsBYSF6GzAmSuCm6PAelpHm/
3L4gChcnPL+0outQOifCSLdUOXEZhTFXrzC61l+14LGt8pR6YN+2uEnU6kq1i
aDLEffIWK4dWCp67JUIef1BTOvxRurpssuRdslhJQXDFaj bitcount: 2048 fingerprint:
a4:23:5d:8a:5a:54:8b:3e:0b:38:06:79:82:e9:83:48

************************************
******************DSA KEY*********************
 ssh-dsa AAAAB3NzaC1kc3MAAACBALpY6MFhFPYI+VcAHzHppnwVnNXv9oR/
EGHUM50BBqdQE1Qi1mlt1rft4oa4tYR46P4gazKnnNfVE/
97FwEbCZaXaz9Wzfcfa3ALtsvGdyNQQk2BebYiRnmeWnS3wGV0M/D64bAiV0
2p/
LyF6D0ygMnZ3up3ttTN5QfHeyYQtwyzAAAAFQD+k6wQyr51IhXIQSsQD8by8qxjUwAAAIB0LxP3ljn
fzxEXyEkNNzlxCcJ7ZZkFYUmtDJxRZlDceuSf4QipMrQVrdrgdqZNhrUiDWM/
HaCMO9LdEQxfPh5TaIwPyccngn
VUS83Tx577ofBW6hellTey3B3/3I+FfiGKUXS/
mZSyf5FW3swwyZwMkF0mV0SRCYTprnFt5qx8awAAAIEAjDNqMkyxUvB6JBqfo7zbGqXjBQmJ+dE8fG
jI2znlgq4lhYcMZJVNwTiydDIgMVNFfKc1dAT3zr6qMZfGv56EbK
1qUu103K5CF44XfVkYNcHJV+/
fcfAJasGU8W6oSbU5Q08abyMsIGRYTurOMkRhvif6sxvieEpVnVK2/nPVVXA=  bitcount: 1024

fingerprint: d9:7a:80:e0:76:48:20:72:a6:5b:1c:67:da:91:9f:52
```

```
**************************************
```

show ssh server

Use this command to display the SSH server status.

Command Syntax `show ssh server`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show ssh server ssh server enabled port: 22 authentication-retries 3
```

show

username

Use this command to display the RSA or DSA key pair for a user.

Command Syntax `show username USERNAME`

`keypair`

Parameters

`USERNAME`	User identifier

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3 1.

Examples

```
#show username kedar keypair
***************RSA KEY******************* ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDCnWo/3Y7LlVkw/Z43dbVIm+I3o25JlgUTmwa9ll
T35+2gNvDbIPfYAqUKYgrmXKDc9vg7f4SAsmXS+4ZwrrQSTTsHk8PNLA+4lEcufFNl3jpfXTuhphN9 N9
i+uFHGYIIviWZksiRqpMZmDlALyzAIOzyCfG44hlRm3/ pYfhBNhHruvxYVhbP4wHsmrWfcFb+HZCWQGM
CJupxu8bouGd2UW5/BlVy1yuYNIhdo2NHjUI+ameETV+Wroki8+OLVA6eXp5/ KY3Bj9x2+AxOCiKcpU0
axwFSoCbP3+29wrp4JJhl4ssSqM+19+VbUtpuXAM0cR7VQ7mJ0JDZ9tBvK4l8/
bitcount: 2048 fingerprint: 2b:ac:17:a4:ef:1d:79:4e:2d:17:af:72:4c:c7:e4:2f
************************************ ***************DSA
KEY*******************
ssh-dss AAAAB3NzaC1kc3MAAACBAP0npAm+Pw8t7OpO+KQ0Vx3ayXavHHVPPAKOo8RTmquE8zUSjn
/XiZ+vP2343RpXu9/
jLwAcCUMfNBZyE8NbmGKxMMk2PqMz10VtfvDOn5LSNurXL4lypZLG2hR2PNva4w
6b4Adpd+E1fEoUncIgOun2i4SO8N5TCMYVyusKjYzDAAAAFQCWeAzeahZeoIzBlnSo87madxfL3QAA AI
EA4b86l/
nHoWobRoYBrkeOGtjyWLRKk1P2T+rGH+j0rqqJiD0sh2PVfppylliNvqLtYSmXyMCxzEEeFd
HH1cVXgrgQjtUOeCPhF+2We2ummmlCwg4v71Z358FRjsi9VgJ/vQUpOq1hRDhwjJHtEHSA+NkX/ ccW9J
ww8YOoNhCI7DcAAACANuYiP6tKGSU9LeClF1F65Tq1blVHfLp3TSeZYPldqonDoZ1qo3NNvOOH5KN8
Lj
MRtTCN1GaXow1QccS941XFy3efuWXxC00HZ64FhmjCyOYYv2Wsvn4UGCAG3ikiu6M1xjOLl6b53H4m B3
w7O6bkcjH1GnytwrgR0D/nlsZ/9fs=
bitcount: 1024 fingerprint: c1:0a:e5:e1:a1:78:ae:c2:4a:07:4a:50:07:4b:d5:84
************************************
```

ssh

Use this command to open an ssh session to a ipv4 address or host name resolved to an ipv4 address.

Command

Syntax `ssh WORD (vrf (NAME | management)) ssh WORD <1-65535> (vrf (NAME | management)) ssh (cipher (aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc |aes192-cbc| aes256-cbc | 3des-cbc)) WORD (vrf (NAME | management)) ssh (cipher (aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc |aes192-cbc | aes256-cbc | 3des-cbc)) WORD <1-65535> (vrf (NAME | management))`

Parameters

`WORD`	User and Destination Host name to resolve into IPV4 Address or IPv4 Address to open a ssh session as user@ipv4-address/Hostname
`1-65535`	Destination Port to open a ssh session. Default is 22
`cipher`	Specify algorithm to encrypt ssh session
`aes128-ctr`	Advanced Encryption Standard 128 bit Counter Mode
`aes192-ctr`	Advanced Encryption Standard 192 bit Counter Mode
`aes256-ctr`	Advanced Encryption Standard 256 bit Counter Mode
`aes128-cbc`	Advanced Encryption 128 bit Standard Cipher Block Chaining
`aes192-cbc`	Advanced Encryption Standard 192 bit Cipher Block Chaining
`aes256-cbc`	Advanced Encryption Standard 256 bit Cipher Block Chaining
`3des-cbc`	Triple Data Encryption Standard Cipher Block Chaining
`vrf`	Specify the VPN routing/forwarding instance.
`NAME`	Specify the name if the VPN routing/forwarding instance.
`management`	Management VPN routing/forwarding instance name.

Default

By default, ssh WORD option is 22

Command Mode

Privileged Exec mode

Applicability

This command was introduced in version before SWMRE version 1.3.

Examples

```
#ssh cipher aes128-ctr 10.12.16.17 22 vrf management
   The authenticity of host '10.12.16.17 (10.12.16.17)' can't be established.
  RSA key fingerprint is 93:82:98:ce:b7:20:1a:85:a5:9a:2e:93:13:84:ea:9e.
Are you sure you want to continue connecting (yes/no)?
```

ssh6

Use this command to open an ssh session to an ipv6 address or host name resolved to an ipv6 address.

Command Syntax `ssh6 (X:X::X:X | HOSTNAME) (vrf (NAME | management)) ssh6 (X:X::X:X | HOSTNAME) <1-65535> (vrf (NAME | management)) ssh6 (cipher (aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc |aes192-cbc | aes256-cbc | 3des-cbc)) (X:X::X:X | HOSTNAME) (vrf (NAME | management))`

```
                                                                    ssh6
    (cipher (aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc |aes192-cbc | aes256-
    cbc | 3des-cbc))  (X:X::X:X | HOSTNAME) <1-65535> (vrf (NAME | management))
```

Parameters

X:XX::X:X	User and Destination IPv6 Address to open a ssh session as user@ipv6-address
HOSTNAME	User and Destination Host name to resolve into IPv6 Address to open an ssh session as user@ipv4-address/Hostname
1-65535	Destination Port to open a ssh session. Default is 22
cipher	Specify algorithm to encrypt ssh session
aes128-ctr	Advanced Encryption Standard 128 bit Counter Mode
aes192-ctr	Advanced Encryption Standard 192 bit Counter Mode
aes256-ctr	Advanced Encryption Standard 256 bit Counter Mode
aes128-cbc	Advanced Encryption 128 bit Standard Cipher Block Chaining
aes192-cbc	Advanced Encryption Standard 192 bit Cipher Block Chaining
aes256-cbc	Advanced Encryption Standard 256 bit Cipher Block Chaining
3des-cbc	Triple Data Encryption Standard Cipher Block Chaining
vrf	Specify the VPN routing/forwarding instance.
NAME	Specify the name if the VPN routing/forwarding instance.
management	Management VPN routing/forwarding instance name.

Default

No default value is specified.

Command Mode

Privileged Exec mode

Applicability

This command was introduced in version before SWMRE version 1.3.

Examples

```
        #ssh6 cipher aes128-ctr 2:2::2:2 22 vrf management
        The authenticity of host '2:2::2:2 (2:2::2:2)' can't be established.
          RSA key fingerprint is 93:82:98:ce:b7:20:1a:85:a5:9a:2e:93:13:84:ea:9e.
    Are you sure you want to continue connecting (yes/no)?
```

ssh algorithm encryption

SSH server authorizes connection of only those algorithms that are configured from the list below. If a client tries establishing a connection to the server with the algorithm encryption that are not part of the list, the connection will not established.

SSH server supports the encryption algorithms Advanced Encryption Standard Counter Mode [AES-CTR], Advanced Encryption Standard Cipher Block Chaining [AES-CBC], and Triple Data Encryption Standard [3DES].

and they are as follows:

1. aes128-ctr
2. aes192-ctr
3. aes256-ctr
4. aes128-cbc
5. 3des-cbc
6. aes192-cbc
7. aes256-cbc

Use this command to set an algorithm encryption to establish ssh session.

Use the `no` form of this command to remove an algorithm encryption.

Command Syntax:

```
ssh server algorithm encryption {aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc
|aes192-cbc | aes256-cbc | 3des-cbc} (vrf management|) no ssh server algorithm
encryption {aes128-ctr | aes192-ctr | aes256-ctr | aes128-
cbc |aes192-cbc | aes256-cbc | 3des-cbc} (vrf management|)
```

Parameters

`aes18-ctr`	AES 128 bit Counter Mode
`aes192-ctr`	AES 192 bit Counter Mode
`aes256-ctr`	AES 256 bit Counter Mode
`aes128-cbc`	AES 128 bit Cipher block chaining
`aes192-cbc`	AES 192 bit Cipher block chaining
`aes256-cbc`	AES 256 bit Cipher block chaining
`3des-cbc`	Triple DES Cipher block chaining
`vrf`	Virtual Routing and Forwarding
`NAME`	Virtual Routing and Forwarding name

Default

No default value is specified.

By default, all the ciphers are supported for a new ssh client to connect to the ssh server.

Command Mode

Configure mode

Applicability

This command was introduced in version before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ssh server algorithm encryption aes128-ctr
```

Note: After configuring the ssh server algorithm encryption, if you disable the previous encryption algorithm, the command is rejected, and the following message is displayed:

```
"% There must be at least one session encryption alogirthm."
```

ssh key

Use this command to create a SSH server key.

Use the `no` form of this command remove a SSH server key. The `no ssh key` form (with no other parameters) deletes both RSA and DSA keys.

You can only give this command when the SSH server is disabled. See the feature ssh command.

Command Syntax `ssh key dsa (vrf management|) ssh key dsa force (vrf management|) ssh key rsa (vrf management|) ssh key rsa length <768-2048> (vrf management|) ssh key rsa length <768-2048> force (vrf management|) ssh key rsa force (vrf management|) no ssh key (vrf management|) no ssh key dsa (vrf management|) no ssh key rsa (vrf management|)`

Parameters

`dsa`	Digital System Algorithm (DSA) SSH key
`management`	Virtual Routing and Forwarding name
`force`	Forces the replacement of an SSH key
`rsa`	Rivest, Shamir, and Adelman (RSA) public-key cryptography SSH server key
`<768-2048>`	Number of bits to use when creating the SSH server key; this parameter is only valid for RSA keys (DSA keys have a default length of 1024)

Default

DSA keys have a default value of 1024.

RSA keys have a minimum key length of 768 bits and the default length is 2048.

By default the system has RSA/DSA public/private key pair placed in /etc/ssh/. The force option is used if the user wants to regenerate the ssh rsa keys. The same thing applies for dsa also.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ssh key dsa
```

ssh login-attempts

Use this command to set the number of times that a user can try to log in to a SSH session.

Use the `no` form of this command to set the number of login attempts to its default (3).

You can only give this command when the SSH server is disabled. See the feature ssh command.

Command Syntax `ssh login-attempts RETRIES (vrf management|) no ssh login-attempts (vrf management|)`

Parameters

`RETRIES` Number of retries <1-3> `management` Virtual Routing and Forwarding name

Default

By default, the device attempts to negotiate a connection with the connecting host three times.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ssh login-attempts 3
```

ssh server port

Use this command to set the port number on which the SSH server listens for connections. The default port on which the SSH server listens is 22.

You can only give this command when the SSH server is disabled. See the feature ssh command.

Use the `no` form of this command to set the default port number (22).

Command Syntax `ssh server port <1024-65535> (vrf management|) no ssh server port (vrf management|)`

Parameters

`<1024-65535>` Port number

`management` Virtual Routing and Forwarding name

Default

By default, SSH server port is 22.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ssh server port 1720
```

username sshkey

Use this command to create a user account.

Command Syntax `username USERNAME sshkey LINE`

Parameters

`USERNAME`	User identifier
`LINE`	Digital System Algorithm (DSA) key or Rivest, Shamir, and Adelman (RSA) key in OpenSSH format; this key is written to the `authorized_keys` file

Default

By default, SSHKEY is 1024.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#username fred sshkey
AAAAB3NzaC1kc3MAAAEBAIirweZzCdyITqbMWB8Wly9ivGxY1JBVnWTVtcWKi6uc
CPZyw3I6J6/+69LEkPUSAyO+SK8zj0NF2f25FFc2YDMh1KKHi5gK7iXF3/ran54j
nP2byyLeo8rnuVqfEDLaBI1qQaWBcDQvsZc14t5SEJfsOQSfR03PDqPYAisrZRvM
5pWfzo486Rh33J3+17OuARQtZFDP4wA5zZoFxhl4U3RK42JzKNUiYBDrH3lSgfkv
XLWLXz9WcxY6zuKvXFwUpOA9PRXwUsKQqWuyywZQLNavENqFyoQ8oZnNKLCYE0h8
QnUe62NGxb3jQXKLflOL04JFNiii9sACG1Y/ut4ANysAAAAVAJbM7Z4chRgiVahN
iwXFJNkBmWGZAAABAAuF1FlI6xy0L/pBaIlFw34uUL/mh4SR2Di2X52eK70VNj+m
y5eQdRC6cxpaVqpS3Q4xTN+W/kaBbIlX40xJP5lcjMvfn/nqiuIeEodmVIJMWxOD
fh3egeGuSW614Vzd1RGrxpYInIOygMULRcxhmbX+rPliuUIvhg36iH0UR7XBln6h
uyKFvEmaL7bGlRvELjqaj0y6iiCfP1yGBc5vavH5X+jOWqdsJHsCgcIzPF5D1Ybp
w0nZmGsqO+P55mjMuj0O2uI7Ns1sxyirbnGhd+ZZ1u03QDy6MBcUspai8U5CIe6X
WqvXY+yJjpuvlW9GTHowCcGd6Z/e9IC6VE/kNEAAAAEAFIe6kLGTALR0F3AfapYY
/M+bvkmkkhOJUZVdLiwMjcvtJb9fQpPxqXElS3ZvUNIEElUPS/V7KgSsj8eg3FKN
```

```
iUGICkTwHIK7RTLC8k4IE6U3V3866JtxW+Znv1DB7uwnbZgoIZuVt3r1+h8O0ah8
UKwDUMJT0fwu9cuuS3G8Ss/gKi1HgByrcxXoK51/r4Bc4QmR2VQ8sXOREv/SHJeY
JGbEX3OxjRgXC7GlpbrdPiL8zs0dPiZ0ovAswsBOYlKYhd7JvfCcvWRjgP5h55aw
GNSmNs3STKufbIqYGeDAISYNYY4F2JzR593KIBnWgyhokyYybyEBh8NwTTO4J5rT ZA==
```

username keypair

Use this command to create a user account.

Command Syntax `username USERNAME keypair rsa username USERNAME keypair dsa username USERNAME keypair rsa length <768-2048> username USERNAME keypair rsa length <768-2048> force username USERNAME keypair rsa force username USERNAME keypair dsa force`

Parameters

`USERNAME`	User identifier
`rsa`	Rivest, Shamir, and Adelman (RSA) public-key cryptography SSH server key
`dsa`	Digital System Algorithm (DSA) SSH key
`<768-2048>`	Number of bits to use when creating the SSH server key; this parameter is only valid for RSA keys (DSA keys have a default length of 1024)
`force`	Forces the replacement of an SSH key

Default

DSA keys have a default value of 1024.

RSA keys have a minimum key length of 768 bits and the default length is 2048.

By default the system has RSA/DSA public/private key pair placed in /etc/ssh/. The force option is used if the user wants to regenerate the ssh rsa keys. The same thing applies for dsa also.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#username fred keypair rsa
```

CHAPTER 4 Simple Network Management Protocol

This chapter is a reference for Simple Network Management Protocol (SNMP) commands.

SNMP provides a standardized framework and a common language for monitoring and managing devices in a network. The SNMP framework consists of three parts:

- An SNMP manager: The system used to control and monitor the activities of network devices. This is sometimes called a Network Management System (NMS).
- An SNMP agent: The component within a managed device that maintains the data for the device and reports these data SNMP managers.
- Management Information Base (MIB): SNMP exposes management data in the form of variables which describe the system configuration. These variables can be queried (and sometimes set) by SNMP managers.

In SNMP, administration groups are known as *communities*. SNMP communities consist of one agent and one or more SNMP managers. You can assign groups of hosts to SNMP communities for limited security checking of agents and management systems or for administrative purposes. Defining communities provides security by allowing only management systems and agents within the same community to communicate.

A host can belong to multiple communities at the same time, but an agent does not accept a request from a management system outside its list of acceptable community names.

SNMP access rights are organized by groups. Each group is defined with three accesses: read access, write access, and notification access. Each access can be enabled or disabled within each group.

The SNMP v3 security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The security levels are:

- noAuthNoPriv: No authentication or encryption
- authNoPriv: Authentication but no encryption
- authPriv: Both authentication and encryption SNMP is defined in RFCs 3411-3418.

Note: The commands below are supported only on the “management” VRF.

This chapter contains these commands:

- clear snmp hostconfig
- debug snmp-server
- show running-config snmp
- show snmp
- show snmp community
- show snmp engine-id
- show snmp group
- show snmp host
- show snmp user
- show snmp view
- snmp-server community
- snmp-server contact
- snmp-server enable snmp

- snmp-server enable traps
- snmp-server host
- snmp-server location
- snmp-server tcp-session
- snmp-server user
- snmp-server view

clear snmp hostconfig

Use this command to remove all SNMP trap hosts.

Command Syntax `clear snmp hostconfig`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear snmp hostconfig
```

debug snmp-server

Use this command to display SNMP debugging information.

Use the `no` form of this command to stop displaying SNMP debugging information.

Command Syntax `debug snmp-server no debug snmp-server`

Parameters

None

Default

By default, disabled.

Command Mode

Exec and configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#debug snmp-server
```

show running-config snmp

Use this command to display the SNMP running configuration.

Command Syntax `show running-config snmp`

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show running-config snmp snmp-server view all .1 included snmp-server
community abc group network-admin snmp-server enable snmp
```

show snmp

Use this command to display the SNMP configuration, including session status, system contact, system location, statistics, communities, and users.

Command Syntax

```
show snmp
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show snmp
SNMP
Protocol:Enabled sys
Contact: sys
Location:

--------------------------------------------------------------------------------
Community Group/Access Context acl_filter
--------------------------------------------------------------------------------
public network-admin
________________________________________________________________________________

                         SNMP USERS
________________________________________________________________________________
User Auth Priv(enforce) Groups
________________________________________________________________________________

SNMP Tcp-session :Disabled
```

show snmp community

Use this command to display SNMP communities.

Command Syntax `show snmp`

```
community
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show snmp community

  ---------------------------------------------------------------------------
Community               Group/Access        view-name        version
  ---------------------------------------------------------------------------
```

show snmp engine-id

Use this command to display the SNMP engine identifier.

The SNMP engine identifier is a unique string used to identify the device for administration purposes. You do not specify an engine identifier for a device; SWMRE generates a default string. For more about the SNMP engine identifier, see RFC 2571.

Command Syntax

```
show
snmp engine-id
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show snmp engine-id
SNMP ENGINE-ID : 80 00 8f 41 03 00 00 00 00 00 00
```

show snmp group

Use this command to display SNMP server groups and associated views.

Command Syntax `show`

```
snmp group
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show snmp group
-------------------------------------------------------------------------------
------------------------------
community/user    group         version   Read-View   Write-view   Notify-view
-------------------------------------------------------------------------------
------------------------------

test          network-operator    2c/1      all          all          all
kedar         network-operator    3         all          none         all
tamil         network-operator     3        all          none         all
```

show snmp host

Use this command to display the SNMP trap hosts.

Command Syntax `show`

```
snmp host
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show snmp host
-------------------------------------------------------------------------
```

```
Host            Port    Version    Level       Type      SecName
-------------------------------------------------------------------------

10.10.26.123    162     2c         noauth      trap      test
```

Table 4-3: Show snmp host output

Entry	Description
Host	The IP address of the SNMP host server.
Port	The port being used for SNMP traffic.
Version	SNMP version number.
Level	The security level being used.
Type	The type of SNMP object being sent.
SecName	Secure Name for this SNMP session.

show snmp user

Use this command to display SNMP users and associated authentication, encryption, and group.

Command Syntax `show snmp`

`user`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show snmp user

SNMP USERS

_____________________________________________________________________
User            Auth     Priv(enforce)     Groups
_____________________________________________________________________
ntwadmin        MD5      AES               network-admin
```

```
#
```

Table 4-4: Show snmp user output

Entry	Description
User	The person attempting to use the SMNMP agent.
Auth	The secure encryption scheme being used.
Priv(enforce)	What enforcement privilege is being used (in this case, it is the Advance Encryption Standard).
Group	The group to which the user belongs.

show snmp view

Use this command to display SNMP views.

Command Syntax `show snmp view`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show snmp view

View : all
  OID : .1
  View-type : included
```

snmp-server community

Use this command to create an SNMP community string and access privileges.

Use the `no` form of this command to remove an SNMP community string.

Command Syntax

```
snmp-server community WORD (| (view VIEW-NAME version (v1 | v2c ) ( ro | rw)) |
(group WORD) |( ro | rw) | (use-acl WORD) ) (vrf management|) no
snmp-server community COMMUNITY-NAME (vrf management|)
```

Parameters

`WORD`	SNMP community string; maximum length 32 characters
`VIEW-NAME`	Defined view that defines the objects available to the SNMP community
`v1`	SNMP v1
`v2c`	SNMP v2c
`ro`	Read-only access
`rw`	Read-write access
`group`	Community group
`WORD`	Community group name; maximum length 32 characters
`ro`	Read-only access
`rw`	Read-write access
`use-acl`	Access control list (ACL) to filter SNMP requests
`WORD`	ACL name; maximum length 32 characters
`management`	Virtual Routing and Forwarding name

Default

No default value specified.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
  (config)#snmp-server community MyComm view MyView1 version v2c rw vrf management
```

snmp-server contact

Use this command to set the system contact information for the device (`sysContact` object).

Use the `no` form of this command to remove the system contact information.

Command Syntax `snmp-server contact (vrf management|) (TEXT|)`

`no snmp-server contact (vrf management|) (TEXT|)`

Parameters `management` Virtual Routing and Forwarding name

`TEXT` System contact information; maximum length 32 characters without spaces

Default

No default value specified.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#snmp-server contact vrf management Irving@555-0150
```

snmp-server enable snmp

Use this command to start the SNMP agent daemon over UDP.

Use the `no` form of this command to stop the SNMP agent daemon over UDP.

Command Syntax `snmp-server enable snmp (vrf management|) no snmp-server enable snmp (vrf management|)`

Parameters `management` Virtual Routing and Forwarding name

Default

No default value specified.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#snmp-server enable snmp vrf management
```

snmp-server enable traps

Use this command to enable or disable SNMP traps and inform requests.

Command Syntax

```
snmp-server enable traps (link(linkDown|linkUp|)|snmp(authentication|)|) (vrf
  management|)

no snmp-server enable traps ((link(linkDown|linkUp|))|(snmp(authentication|))|)
  (vrf management|)
```

Parameters

`link`	Module notifications enable
`linkDown`	IETF Link state down notification
`linkUp`	IETF Link state up notification
`snmp`	Enable RFC 1157 notifications
`authentication`	Send SNMP authentication failure notifications
`management`	Virtual Routing and Forwarding name

Default

By default, snmp server enable traps is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#snmp-server enable traps vrf management
```

snmp-server host

Use this command to configure an SNMP trap host. An SNMP trap host is usually a network management station (NMS) or an SNMP manager.

Use the `no` form of this command to remove an SNMP trap host.

Command Syntax

IPv4/SNMP v2:

```
snmp-server host (A.B.C.D|HOSTNAME) (traps | informs) version ((1
  | v2c) WORD) (|udp-port <1-65535>) (vrf management|)
```

IPv4/SNMP v3:

```
snmp-server host (A.B.C.D|HOSTNAME) (traps | informs)
  version(( (1 | 2c) WORD | (3 (noauth | auth | priv) WORD)) (|udp-port <1-65535>)
   (vrf management|)
```

Parameters

A.B.C.D	IPv4 address
HOSTNAME	DNS host name
traps	Send notifications as traps
informs	Send notifications as informs
version	Version
v1	SNMP v1
1	SNMP v1
v2c	SNMP v2c
2c	SNMP v2c
WORD	SNMP community string
<1-65535>	Host UDP port number; the default is 162
management	Virtual Routing and Forwarding name
3	SNMP v3 security level
noauth	No authentication and no privacy (noAuthNoPriv) security model: messages transmitted as clear text providing backwards compatibility with earlier versions of SNMP
auth	Authentication and no privacy (authNoPriv) security model: use message digest algorithm 5 (MD5) or Secure Hash Algorithm (SHA) for packet authentication; messages transmitted in clear text
priv	Authentication and privacy (authPriv) security model: use authNoPriv packet authentication with Data Encryption Standard (DES) Advanced Encryption Standard (AES) for packet encryption
WORD	SNMPv3 user name

Default

The default SNMP version is v2c and the default UDP port is 162.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#snmp-server host 10.10.10.10 traps version 3 auth MyUser udp-port 512 vrf
management
```

snmp-server location

Use this command to set the physical location information of the device (`sysLocation` object).

Use the `no` form of this command to remove the system location information.

Command Syntax `snmp-server location (vrf management|) (LINE|)`

`no snmp-server location (vrf management|) (LINE|)`

Parameters `management` Virtual Routing and Forwarding name `LINE` Physical location information

Default

No system location string is set.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
          (config)#snmp-server location vrf management Bldg. 5, 3rd floor, northeast
```

snmp-server tcp-session

Use this command to start the SNMP agent daemon over TCP.

Use the `no` form of this command to close the SNMP agent daemon over TCP.

Command Syntax `snmp-server tcp-session (vrf management|) no snmp-server tcp-session (vrf management|)`

Parameters `management` Virtual Routing and Forwarding name

Default

By default, snmp server tcp session is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#snmp-server tcp-session vrf management
```

snmp-server user

Use this command to create an SNMP server user.

Use the `no` form of this command to remove an SNMP server user.

Command Syntax

```
snmp-server user WORD (|WORD) ((auth (md5 | sha ) AUTH-PASSWORD) ((priv (des | aes)
 PRIV-PASSWORD) |) |) (vrf management|) no snmp-
server user USER-NAME (vrf management|)
```

Parameters

`WORD`	User name; length 5-32 characters
`WORD`	Name of the group to which the user belongs; maximum length 35 characters
`auth`	Packet authentication type
`md5`	Message Digest Algorithm 5 (MD5)
`sha`	Secure Hash Algorithm (SHA)
`AUTH-PASSWORD`	Authentication password; length 8-32 characters
`priv`	Packet encryption type (“privacy”)
`des`	Data Encryption Standard (DES)
`aes`	Advanced Encryption Standard (AES)
`PRIV-PASSWORD`	Encryption password; length 8-33 characters
`management`	Virtual Routing and Forwarding name

Default

By default, snmp server user word is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#snmp-server user Fred auth md5 J@u-b;l2e`n,9p_ priv des t41VVb99i8He{Jt vrf
management
```

snmp-server view

Use this command to create or update a view entry

Use the `no` from of this command to remove a view entry.

Command Syntax `snmp-server view VIEW-NAME OID-TREE (included | excluded) (vrf management|) no snmp-server view VIEW-NAME (vrf management|)`

Parameters

`VIEW-NAME`	View name; maximum length 32 characters
`OID-TREE`	Object identifier of a subtree to include or exclude from the view; specify a text string consisting of numbers and periods, such as 1.3.6.2.4
`included`	Include `OID-TREE` in the SNMP view
`excluded`	Exclude `OID-TREE` from the SNMP view
`management`	Virtual Routing and Forwarding name

Default

By default, snmp-server view VIEW-NAME OID-TREE `is` disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example creates a view named `myView3` that excludes the `snmpCommunityMIB` object (1.3.6.1.6.3.18).

```
#configure terminal
(config)#snmp-server view myView3 1.3.6.1.6.3.18 excluded vrf management
```

CHAPTER 5 Telnet

This chapter describes telnet commands.

Telnet is a client/server protocol that establishes a session between a user terminal and a remote host:

- The telnet client software takes input from the user and sends it to the server's operating system
- The telnet server takes output from the host and sends it to the client to display to the user

While telnet is most often used to implement remote login capability, the protocol is general enough to allow it to be used for a variety of functions.

Note: The commands below are supported only on the "management" VRF.

This chapter contains these commands:

- debug telnet server
- feature telnet
- show debug telnet-server
- show running-config telnet server
- show telnet-server
- telnet
- telnet6
- telnet server port

debug telnet server

Use this command to display telnet debugging information.

Use the `no` form of this command to stop displaying telnet debugging information.

Command Syntax `debug telnet server no debug telnet server`

Parameters

None

Default

By default, disabled.

Command Mode

Executive mode and configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show debug telnet-server

telnet server debugging is on
#
```

feature telnet

Use this command to enable the telnet server.

Use the `no` form of this command to disable the telnet server.

Command Syntax `feature telnet (vrf management|) no feature telnet (vrf management|)`

Parameters `management` Virtual Routing and Forwarding name

Default

By default, feature telnet is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
                    (config)#feature telnet vrf management
```

show debug telnet-server

Use this command to display whether telnet debugging is enabled.

Command Syntax `show debug telnet-server`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show debug telnet-server
```

show running-config telnet server

Use this command to display telnet settings in the running configuration.

Command Syntax `show running-config telnet server`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show running-config telnet server feature telnet
```

show telnet-server

Use this command to display the telnet server status.

Command Syntax `show telnet server`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show telnet server telnet server enabled port: 23
```

telnet

Use this command to open a telnet session to an ipv4 address or host name resolved to ipv4 address.

Command Syntax `telnet (A.B.C.D | HOSTNAME) (vrf (NAME|management))` `telnet (A.B.C.D | HOSTNAME) (<1-65535>) (vrf (NAME|management))`

Parameters

`A.B.C.D`	Destination IPv4 Address to open a telnet session.
`HOSTNAME`	Destination Hostname to resolve into IPv4 address to open a telnet session.
`1-65535`	Destination Port to open a telnet session. Default is 23.
`vrf`	Specify the VPN routing/forwarding instance.
`NAME`	Specify the name if the VPN routing/forwarding instance.
`management`	Management VPN routing/forwarding instance name.

Default

By default, telnet is 23

Command Mode

Privileged Exec mode

Applicability

This command was introduced in version before SWMRE version 1.3.1.

Examples

```
#telnet 10.12.16.17 2543 vrf management Trying 10.12.16.17...
```

telnet6

Use this command to open a telnet session to an ipv6 address or host name resolved to ipv6 address.

Command Syntax `telnet6 (X:X::X:X| HOSTNAME) (vrf (NAME|management)) telnet6 (X:X::X:X | HOSTNAME) (<1-65535>) (vrf (NAME|management))`

Parameters

`X:X::X:X`	Destination IPv6 Address to open a telnet session.
`HOSTNAME`	Destination Host name to resolve into IPv6 address to open a telnet session.
`1-65535`	Destination Port to open a telnet session. Default is 23.
`vrf`	Specify the VPN routing/forwarding instance.
`NAME`	Specify the name if the VPN routing/forwarding instance.
`management`	Management VPN routing/forwarding instance name.

Default

By default, telnet is 23.

Command Mode

Privileged Exec mode

Applicability

This command was introduced in version before SWMRE version 1.3.1.

Examples

```
#telnet6 2:2::2:2 2543 vrf management Trying
2:2::2:2...
```

telnet server port

Use this command to set the port number on which the telnet server listens for connections. The default port on which the telnet server listens is 23.

You can only give this command when the telnet server is disabled. See the feature telnet command.

Use the `no` form of this command to set the default port number (23).

Command Syntax `telnet server (port <1024-65535>) (vrf management|) no telnet server port (vrf management|)`

Parameters

`<1024-65535>`	Port number
`management`	Virtual Routing and Forwarding name

Default

By default, telnet server port number is 23

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#telnet server port 1157 vrf management
```

© Symanitron

CHAPTER 6 Syslog

This chapter is a reference for the `syslog` commands.

Linux applications use the `syslog` utility to collect, identify, time-stamp, filter, store, alert, and forward logging data. The `syslog` utility can track and log all manner of system messages from informational to extremely critical. Each system message sent to a `syslog` server has two descriptive labels associated with it:

- The function (facility) of the application that generated it. For example, an application such as `mail` and `cron` generates messages with a facility names “mail” and “cron”.
- Eight degrees of severity (numbered 0-7) of the message which are explained in Table 6-5.

This chapter contains these commands:

- feature rsyslog
- debug logging
- log syslog
- logging console
- logging level
- logging logfile
- logging monitor
- logging server
- logging timestamp
- show logging
- show logging last
- show logging logfile
- show logging logfile last-index
- show logging logfile start-seqn end-seqn
- show logging logfile start-time end-time
- show running-config logging

Syslog Severities

Table 6-5: Syslog severities (Sheet 1 of 2)

Severity Level	Keyword	Description

0	emergency	The whole system is unusable and needs operator intervention to recover. If only a particular port or component is unusable, but the system as a whole is still usable it is not categorized at an emergency level.
		Examples of this type of message:
		`Output Power of PSU XX (psu_no) XX Watt] has exceeded Maximum Output Power Limit[XX Watt]`
		`OSPF Initialization failed.`

1	alert	The operator needs to act immediately or the system might go into emergency state. The system or one of its component's functionality might be critically affected. Examples of this type of message:
		`Temperature of sensor is (curr_temp)C. It is nearing Emergency Condition.`
		`OSPF has exceed lsdb limit`
		`OSPF Detected router with duplicate router ID [ID]`

2	critical	A critical system event happened which requires the operator's attention. The event might not require immediate action, but this event can affect functionality or behavior of a system component. Examples of this type of message:
		`OSPF Neighbor session went down.`
		`Interface %s changed state to down`

3	error	An error event happened which does not require immediate attention. This log message provides details about error conditions in the system or its components which you can use to troubleshoot problems.
		These events are not logged directly even if the logging level is set to include this level. You also need to enable the protocol debug filters (such as `debug ospf all`). Examples of this type of message:
		`Device i2c bus open error.!!!`
		`[DECODE] Attr ASPATH: Invalid AS Path value.`
		`OSPF MD5 authentication error`

4	notification	Notifications about important system and protocol events to assure the operator that the system is running properly. If a critical/alert condition has happened and has been corrected, that is also logged at this level.
		Warning messages are also logged in this level.
		These events are not logged directly even if the logging level is set to include this level. You also need to enable the protocol debug filters (such as `debug ospf all`). Examples of this type of message:
		`OSPF Received link up for interface: xe1`
		`OSPF neighbour [10.1.1.1] Status change Exstart -> Exchange`
		`Interface %s changed state to UP`

Table 6-5: Syslog severities (Sheet 2 of 2)

Severity Level	Keyword	Description

5	informational	Detailed informational events happening across the system and protocol modules. These events are not necessarily important and are useful only to find details about the functionality being executed in the system and its components. Some of these events might be periodic events like hello or keep alive messages along with packet dumps. Also, this level includes logs for control packets that are ignored and do not impact the protocol states.
		Symanitron recommends to use proper debug filters to log only relevant events and switch off other events; otherwise the logs can get verbose. For example: `debug ospf all`
		`no debug ospf packet hello`
		The above enables all OSPF debugging, but disables the periodic hello messages.
		Examples of this type of message:
		`Successfully added dynamic neighbour`
		`[DECODE] KAlive: Received!`
		`[FSM] Ignoring Unsupported event <EVENT> in state <STATE>`
		`Unknown ICMP packet type"`
		`OSPF RECV[%s]: From %r via %s: Version number mismatch`
		`OSPF RECV[%s]: From %r via %s: Network address mismatch`

6	debug informational	Developer notification events that might not be readable by an operator. However these logs are useful for debugging by a developer and if required, this level needs to be enabled and provided to technical support for analysis.
7	debug detailed	Developer notification events that might not be readable by an operator. However these logs are useful for debugging by a developer and if required, this level needs to be enabled and provided to technical support for analysis.

Log File Rotation

SWMRE rotates `/var/log/message` every three hours. When the log file is 100 megabytes or more, the current log file is backed up and a new log file is started. With four rotations, there can be four backup log files and one current log file.

feature rsyslog

Use this command to enable the rsyslog server.

Use the `no` form of this command to disable the rsyslog server.

Command Syntax `feature rsyslog vrf (management|) no feauture rsyslog vrf (management|)`

Parameters `management` Virtual Routing and Forwarding name

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced in SWMRE version 1.3.5

Example

```
#configure terminal
                    (config)#feature rsyslog vrf management
```

debug logging

Use this command to display logging debugging information.

Use the `no` form of this command stop displaying logging debugging information.

Command Syntax `debug logging host no  debug logging host`

Parameters

None

Command Mode

Exec and configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#debug logging host
```

log syslog

Use this command to begin logging to the system log and set the level to debug.

Syslog enables centrally logging and analyzing of configuration events and system error messages. This helps monitor interface status, security alerts, and CPU process overloads. It also allows real-time capturing of client debug sessions. The command instructs the `VLOGD` daemon to forward all PVR debug output from all active `terminal monitor` sessions to the syslog file.

Use the `no` parameter to disable logging to the system log.

Command Syntax

```
log syslog no
log syslog
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#log syslog
```

logging console

Use this command to set the severity level that a message must reach before the messages is sent to the console. The severity levels are from 0 to 7 as shown in Table 6-5.

Use the `no` form of this command to disable logging console messages.

Note: Below message will be displayed if console severity is set to 6 or 7:

% Warning : If debug volume is huge it can degrade system performance and makes console to be nonresponsive

Command Syntax `logging`

```
console (<0-7>|) no
logging console
```

Parameters

`<0-7>`	Maximum logging level for console messages as shown in Table 6-5.

Note: Setting the level above 5 might affect performance and is not recommended in a production network.

Default

If not specified, the default logging level is 2 (Critical).

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#logging console 6

(config)#2015 Dec 23 03:13:26 SWMRE    BGP-6: [RIB] Scanning BGP Network Route
s...
2015 Dec 23 03:13:41 SWMRE BGP-6: [RIB] Scanning BGP Network Routes...
2015 Dec 23 03:13:56 SWMRE BGP-6: [RIB] Scanning BGP Network Routes...
2015 Dec 23 03:14:00 SWMRE BGP-6: [RIB] Scanning BGP RIB...
2015 Dec 23 03:14:11 SWMRE BGP-6: [RIB] Scanning BGP Network Routes...
2015 Dec 23 03:14:26 SWMRE BGP-6: [RIB] Scanning BGP Network Routes...
2015 Dec 23 03:14:41 SWMRE BGP-6: [RIB] Scanning BGP Network Routes...
2015 Dec 23 03:14:56 SWMRE BGP-6: [RIB] Scanning BGP Network Routes...
2015 Dec 23 03:15:00 SWMRE BGP-6: [RIB] Scanning BGP RIB...

(config)#no logging console
```

logging level

Use this command to set the severity level that a message for a specific process must reach before the messages is logged. The severity levels are from 0 to 7 as shown in Table 6-5. Logging happens for the messages less than or equal to the configured severity level.

Use the `no` form of this command to disable logging messages.

Note: SWMRE shell takes level of CMLD module. Any updates in severity of CMLD will be taken into effect for the next SWMRE session.

Command Syntax

```
logging level (all|auth|bgp|dvmrp|hostp|hsl|isis|l2mrib|lacp|lagd|ldp|mrib|
  mstp|ndd|nsm|onm|oam|ospf|ospf6|pim|pservd|ptp|rib|rip|ripng|rmon|rsvp|sflow
  | trill|vrrp) <0-7>

no logging level (all|auth|bgp|dvmrp|hostp|hsl|isis|l2mrib|lacp|lagd|ldp|mrib|
  mstp|ndd|nsm|oam|onm|ospf|ospf6|pim|pservd|ptp|rib|rip|ripng|rmon|rsvp|sflow
  | trill|vrrp)
```

Parameters

`all`	All messages

`auth`	Auth messages
`bgp`	BGP messages
`dvmrp`	DVMRP messages
`hostp`	Hostp messages
`hsl`	HSL messages
`isis`	ISIS messages
`l2mrib`	L2MRIB messages
`lacp`	LACP messages
`lagd`	LAGD messages
`ldp`	LDP messages
`mrib`	MRIB messages
`mstp`	MSTP messages
`ndd`	NDD messages
`nsm`	NSM messages
`oam`	OAM messages
`onm`	ONM messages
`ospf`	OSPF messages
`ospf6`	OSPF6 messages
`pim`	PIM messages
`pservd`	PSERVD messages
`ptp`	PTP messages
`rib`	RIB messages
`rip`	RIP messages
`ripng`	RIPNG messages
`rmon`	RMON messages
`rsvp`	RSVP messages
`sflow`	Sflow messages
`trill`	TRILL messages
`vrrp`	VRRP messages
`<0-7>`	Severity level as shown in Table 6-5.

Default

By default, logging monitor is 2 (critical).

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#logging level all 5

#configure terminal
(config)#logging level bgp 6

(config)#no logging monitor
```

logging logfile

Use this command to specify the log file controls and where to save the logs in a configuration file. This command enables writing debug output and command history to the disk file in the directory `/log/`.

When logging logfile is enabled, SWMRE log information is stored in user configured logging file which is present in "/log" directory. The log is spread across four files total of these files size is the user configured size.

For example, if the name of the logging log file is “mylogFile” and logging file size configured is 4 MB then each file will be maximum size of 1MB. The logging file names will be "mylogFile", "mylogfile.0", "mylogfile.1" and "mylogfile.2".

"mylogFile" will have the latest log information. As soon as it’s size becomes 1 MB this file is renamed as mylogFile.0 and newlog information is written to new "mylogFile". As a result oldest log information stored in mylogfile.2 and is lost in order to accommodate new set of logs in mylogFile.

Use option no to cancel writing to a specific log file.

Note:Changing logfile paramenters (name/size/severity) will be taken into effect for the next SWMRE session.

Command Syntax `logging logfile LOGFILENAME <0-7> ((size <4096-4194304>)|) no logging logfile`

Parameter

`LOGFILENAME`	Name of the log file.
`<0-7>`	Severity level as shown in Table 6-5.
`<4096-4194304>`	Log file size in bytes.

Default

By default, log file size is 4194304 bytes.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

This command is used to log the debug messages of a particular protocol daemon to the specified file.

```
#configure terminal
(config)#logging logfile test123 7
```

logging monitor

Use this command to set the severity level that a message must reach before a monitor message is logged. The severity levels are shown in Table 6-5.

Use the `no` parameter to disable logging monitor messages.

Command Syntax `logging monitor`

```
(<0-7>|) no logging monitor
```

Parameters

`<0-7>` Maximum logging level for monitor messages as shown in Table 6-5.

Note: Setting the level above 5 might affect performance and is not recommended in a production network.

Default

If not specified, the default logging level is 3 (error).

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#logging monitor 6

(config)#no logging monitor
```

logging server

Use this command to set a syslog server.

SWMRE supports logging messages to a syslog server in addition to logging to a file or the console (local or ssh/telnet console). SWMRE messages can be logged to a local syslog server (the machine on which SWMRE executes) as well as to one or more remote syslog servers.

Use the `no` form of this command to remove a syslog server.

Command Syntax

```
logging server (A.B.C.D|HOSTNAME) (|((<0-7>) (|facility (local0| local1 | local2 |
  local3| local4 |local5 | local6 | local7 |user)))) (vrf management|)
no logging server (A.B.C.D | HOSTNAME ) (vrf management|)
```

Parameters

A.B.C.D	IPv4 address
HOSTNAME	Host name; specify localhost to log locally
<0-7>	Severity at which messages are logged as shown in Table 6-5. If not specified, the default is 3.
facility	Entity logging the message (user defined); if not specified, the default is local7
local0	Local0 entity
local1	Local1 entity
local2	Local2 entity
local3	Local3 entity
local4	Local4 entity
local5	Local5 entity
local6	Local6 entity
local7	Local7 entity (default)
user	User entity
management	Virtual Routing and Forwarding name

Default

If not specified, the default severity at which messages are logged is 3 (error).

If not specified, the default facility is local7.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
    #configure terminal
(config)#logging server MyLogHost vrf management
```

logging timestamp

Use this command to set the logging timestamp granularity.

Use the `no` form of this command to reset the logging timestamp granularity to its default (milliseconds).

Note: Any change in timestamp configurations will result in timestamp configured for event logged by protocol modules except for CLI history for the current and active sessions. The timestamp configuration is reflected in CLI history for new CLI sessions.

Changing logging timestamp will be taken into effect for the next SWMRE session.

Command Syntax `logging timestamp (microseconds|milliseconds|seconds)` `no logging timestamp`

Parameters `microseconds` Microseconds granularity `milliseconds` Milliseconds granularity `seconds` Seconds granularity

Default

By default, logging time stamp granularity is milliseconds.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#logging timestamp milliseconds
```

show logging

Use this command to display the logging configuration.

Command Syntax `show logging (info|level|server|console|timestamp|monitor)`

Parameters

`info`	Show server logging configuration
`level`	Show facility logging configuration
`server`	Syslog server configuration
`console`	Console configuration
`timestamp`	Timestamp configuration
`monitor`	Monitor configuration

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show logging console
Console logging     : enabled Severity: Operator (critical) Level : 2


#show logging monitor
Logging monitor     : enabled Severity: Operator (debugging) Level: 7


#show logging server
  Remote Servers:
               1.1.1.1
               severity: Operator (informational)
facility: local7                VRF : management

#sh logging info    Remote
Servers:
               1.1.1.1
               severity: Operator (informational)
facility: local7                VRF : management
Logging console     : enabled Severity: operator (critical) Level : 2
Logging monitor     : enabled Severity: Operator (debugging) Level : 7
Logging timestamp   : seconds
File logging          : enabled   File Name   : /log/abc   Severity    : Operator (de
bugging)  Level   : 7  Size   : 4194304 Cli logging         : enabled
```

```
Facility         Default Severity       Current Session Severity nsm
2                           2 ripd                    2                           2
ripngd                  2                           2 ospfd                    2
2 ospf6d                  2                           2 isisd                    2
2 hostpd                  2                           2 mribd                    2
2 pimd                    2                           2 authd                    2
2 mstpd                   2                           2 onmd                     2
2 HSL                     2                           2 oamd                     2
2 vlogd                   2                           2 vrrpd                    2
2 ndd                     2                           2 ribd                     2
2 bgpd                    2                           2 l2mribd                  2
2 hslrasmgr               2                           2 lagd                     2
2 pservd                  2                           2 cmmd                     2
2
```

show logging last

Use this command to display lines from the end of the log file.

Command Syntax `show logging last (<1-9999>)`

Parameters

`<1-9999>`	Number of lines to display from end of the log file

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show logging last 100
2016 Mar 03 00:02:32 x86_64-debian NSM-3: AgentX: failed to send open message:
Connection refused
2016 Mar 03 00:02:33 x86_64-debian OSPF-3: AgentX: failed to send open message:
Connection refused
2016 Mar 03 00:02:33 x86_64-debian OSPFv3-3: AgentX: failed to send open message:
Connection refused
2016 Mar 03 00:02:33 x86_64-debian IS-IS-3: AgentX: failed to send open message:
Connection refused
2016 Mar 03 00:02:33 x86_64-debian BGP-3: AgentX: failed to send open message:
Connection refused
2016 Mar 03 00:02:33 x86_64-debian RIP-3: AgentX: failed to send open message:
Connection refused
```

show logging logfile

Use this command to display whether logging is enabled, the log file name, and the logging severity.

Command Syntax `show logging logfile`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#sh logging logfile
File logging          : enabled   File Name    : /log/abc   Severity    : (7) 2017 Sep 25
17:18:14 : SWMRE : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : ' logging server
1.1.1.1 5 vrf management '

2017 Sep 25 17:18:14 : SWMRE : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : ' ex'

2017 Sep 25 17:18:17 : SWMRE : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : ' sh
logging info '

2017 Sep 25 17:19:15 : SWMRE : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : ' sh
logging console '

2017 Sep 25 17:19:20 : SWMRE : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : ' sh
logging monitor '

2017 Sep 25 17:19:32 : SWMRE : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : ' sh
logging logfile '

2017 Sep 25 17:19:44 : SWMRE : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : ' sh
logging server '

2017 Sep 25 17:28:26 : SWMRE : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : ' sh
logging info '

2017 Sep 25 17:29:02 : SWMRE : CMLSH : CLI_HIST : User root@/dev/ttyS1 : CLI : ' sh
logging console
```

show logging logfile last-index

Use this command to display the number of line in the log file.

Command Syntax `show logging logfile last-index`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show logging logfile last-index
```

show logging logfile start-seqn end-seqn

Use this command to display a range of lines in the log file.

Command Syntax `show logging logfile start-seqn (<0-2147483647>) (|(end-seqn <0-2147483647>))` **Parameters**

`start-seqn`	Starting line number
`end-seqn`	Ending line number

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show logging logfile start-seqn 500 end-seqn 750
```

show logging logfile start-time end-time

Use this command to display lines from the log file within a given date-time range.

Command Syntax

```
show logging logfile start-time (<2000-2030> WORD <1-31> WORD) (|(end-time
  <20002030> WORD <1-31> WORD))
```

Parameters `start-time` Starting date and time:

`<2000-2030>` Year in YYYY format

`WORD` Month as `jan`, `feb`, `mar`,..., `oct`, `nov`, or `dec` (maximum length 3 characters)

`<1-31>` Day of month in DD format

`WORD` Hour, minutes, seconds in HH:MM:SS format (maximum length 8 characters); range <0-23>:<0-59>:<0-59>

`end-time` Ending date and time:

`<2000-2030>` Year in YYYY format

`WORD` Month as `jan`, `feb`, `mar`,..., `oct`, `nov`, or `dec` (maximum length 3 characters)

`<1-31>` Day of month in DD format

`WORD` Hour, minutes, seconds in HH:MM:SS format (maximum length 8 characters); range <023>:<0-59>:<0-59>

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show logging logfile start-time 2015 mar 15 12:10:00 end-time 2015 apr 15
12:10:00
```

show running-config logging

Use this command to display the logging configuration.

Command Syntax `show running-config logging`

Parameters

None

Command Mode

Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show running-config logging no Logging console no Logging monitor logging
timestamp milliseconds
```

CHAPTER 7 User Management

This chapter is a reference for user management commands.

This chapter includes these commands:

- clear aaa local user lockout username
- debug user-mgmt
- show user-account
- username

clear aaa local user lockout username

Use this command to unlock the locked user due to three times wrong password login attempt.

Command Syntax `clear aaa local user lockout username USERNAME`

Parameters

`USERNAME`	User name; length 2-15 characters

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear aaa local user lockout username testuser
```

debug user-mgmt

Use this command to display user management debugging information.

Use the `no` form of this command stop displaying user management debugging information.

Command Syntax `debug user-mgmt no debug user-mgmt`

Parameters

None

Default

By default, disabled.

Command Mode

Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#debug user-mgmt

#config t
(config)#debug user-mgmt
```

show user-account

Use this command to display information about all users or a given user.

Command Syntax `show user-account (WORD|)`

Parameters

`WORD`	User name

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show user-account User:user1
                roles: network-operator User:user2
                roles: network-operator User:user3
                roles: network-operator
```

username

Use this command to add a user or to change a user password.

The `role` parameter maps to privilege levels in the TACACS+ server as shown in Table 7-6

Table 7-6: Role/privilege level mapping

Role	Privilege level
Network administrator	15
Network engineer	14
Network operator	1 to 13
Network user	0 or greater then 15

Use the `no` form of this command to remove a user.

Command Syntax `username USERNAME username USERNAME password (encrypted|) PASSWORD`

```
username USERNAME role (network-admin|network-engineer|network-
operator|networkuser)
 username USERNAME role (network-admin|network-engineer|network-
  operator|network-user) password (encrypted|) PASSWORD
no username USERNAME
```

Parameters

`USERNAME` User name; length 2-15 characters

`encrypted` Password is encrypted

`PASSWORD` Password; length 5-32 characters

`network-admin` Network administrator role with all access permissions that can make permanent changes to the configuration. Changes persist after a reset/reboot of the switch.

Only network administrators can manage other users with the enable password, Authentication, Authorization and Accounting, RADIUS, and TACACS+ commands.

`network-engineer`

Network engineer role with all access permission that can make permanent changes to the configuration. Changes persist after a reset/reboot of the switch.

`network-operator`

Network operator role with all access permissions that can make temporary changes to the configuration. Changes do not persist after a reset/reboot of the switch.

`network-user` Network user role with access permissions to display the configuration, but cannot change the configuration.

Default

By default, user name is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
          (config)#username fred_smith password encrypted W3g7y&6yV}JH6&5EYIah?779IT9iV2
```


© Symanitron

CHAPTER 8 Network Time Protocol

This chapter is a reference for Network Time Protocol (NTP) commands.

NTP synchronizes clocks between computer systems over packet-switched networks. NTP can synchronize all participating computers to within a few milliseconds of Coordinated Universal Time (UTC).

NTP uses a hierarchical, layered system of time sources. Each level of this hierarchy is called a “stratum” and is assigned a number starting with zero at the top. The number represents the distance from the reference clock and is used to prevent cyclical dependencies in the hierarchy.

Note: The commands below are supported only on the “management” VRF.

This chapter contains these commands:

- clear ntp statistics
- debug ntp
- feature ntp
- ntp authenticate
- ntp authentication-key
- ntp enable
- ntp logging
- ntp peer
- ntp server
- ntp trusted-key
- show ntp authentication-keys
- show ntp authentication-status
- show ntp logging-status
- show ntp peer-status
- show ntp peers
- show ntp statistics

- show ntp trusted-keys
- show running-config ntp

clear ntp statistics

Use this command to reset NTP statistics.

Command Syntax `clear ntp statistics (all-peers | io | local | memory)`

Parameters

`all-peers`	Counters associated with all peers
`io`	Counters maintained in the input-output module
`local`	Counters maintained in the local protocol module
`memory`	Counters related to memory allocation

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear ntp statistics all-peers
```

debug ntp

Use this command to display NTP debugging messages.

Use the `no` form of this command to stop displaying NTP debugging messages.

Command Syntax `debug ntp no debug ntp`

Parameters

None

Command Mode

Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal (config)#debug ntp

(config)#no debug ntp
```

feature ntp

Use this command to enable NTP.

Use the `no` form of this command to disable NTP.

Command Syntax `feature ntp (vrf management|) no feature ntp (vrf management|)`

Parameters `management` Virtual Routing and Forwarding name

Default

By default, feature ntp is enabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#feature ntp vrf management
```

```
(config)#no feature ntp vrf management
```

ntp authenticate

Use this command to enable NTP authentication.

Use the `no` form of this command to disable authentication.

Command Syntax `ntp authenticate (vrf management|) no ntp authenticate (vrf management|)`

Parameters `management` Virtual Routing and Forwarding name

Default

By default, ntp authenticate is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
                    (config)#ntp authenticate vrf management
```

ntp authentication-key

Use this command to set an NTP Message Digest Algorithm 5 (MD5) authentication key.

Use the `no` form of this command to delete an authentication key.

Command Syntax `ntp authentication-key <1-65534> md5 WORD (vrf management|) ntp authentication-key <1-65534> md5 WORD 7 (vrf management|) no ntp authentication-key <1-65534> md5 WORD (vrf management|)`

Parameters

`<1-65534>`	Authentication key number
`WORD`	MD5 string (maximum 8 characters)
`7`	Encrypt using weak algorithm
`management`	Virtual Routing and Forwarding name

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
                    (config)#ntp authentication-key 535 md5 J@u-b;l2 vrf management
```

ntp enable

Use this command to enable NTP.

Use the `no` form of this command to disable NTP.

Command Syntax `ntp enable (vrf management|) no ntp enable (vrf management|)`

Parameters `management` Virtual Routing and Forwarding name

Default

By default, ntp is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ntp enable vrf management
```

ntp logging

Use this command to log NTP events.

Use the `no` form of this command to disable NTP logging.

Command Syntax `ntp logging (vrf management|) no ntp logging (vrf management|)`

Parameters `management` Virtual Routing and Forwarding name

Default

By default, ntp logging message is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ntp logging vrf management
```

ntp peer

Use this command to configure a peer association. In a peer association, this system can synchronize with the other system or the other system can synchronize with this system.

Use the `no` command to remove a peer association.

Command Syntax

```
ntp peer (A.B.C.D | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-
  16>}|) (vrf management|) ntp peer (A.B.C.D | X:X::X:X | HOSTNAME)
({prefer|key <1-65534>|minpoll <4-
  16>|maxpoll <4-16>}|) (vrf management|) no ntp peer (A.B.C.D | HOSTNAME)
({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-
  16>}|) (vrf management|) no ntp peer (A.B.C.D | HOSTNAME)
({prefer|key|minpoll|maxpoll}|) (vrf management|) no ntp peer (A.B.C.D
| X:X::X:X | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-
  16>|maxpoll <4-16>}|) (vrf management|) no ntp peer (A.B.C.D | X:X::X:X |
HOSTNAME) ({prefer|key|minpoll|maxpoll}|) (vrf
  management|)
```

Parameters

`A.B.C.D`	IPv4 address of peer
`HOSTNAME`	Host name of peer
`X:X::X:X`	IPv6 address of peer
`prefer`	Prefer this peer; preferred peer responses are discarded only if they vary dramatically from other time sources
`key`	Peer authentication key
`<1-65534>`	Peer authentication key value
`minpoll`	Minimum poll interval
`<4-16>`	Minimum poll interval value in seconds raised to a power of 2 (default 4 = 16 seconds)
`maxpoll`	Maximum poll interval
`<4-16>`	Maximum poll interval value in seconds raised to a power of 2 (default 6 = 64 seconds)
`management`	Virtual Routing and Forwarding name

Default

By default, value of `minpoll` is 4 and `maxpoll` is 6.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ntp peer 10.10.0.23 vrf management
                    (config)#ntp peer 10.10.0.23 prefer key 12345 vrf management

(config)#no ntp peer 10.10.0.23 vrf management
```

ntp

server

Use this command to configure an NTP server so that this system synchronizes with the server, but not vice versa.

Use the `no` option with this command to remove an NTP server.

Command Syntax

```
ntp server (A.B.C.D | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-16>|maxpoll <4-
  16>}|) (vrf management|) ntp server (A.B.C.D | X:X::X:X | HOSTNAME) ({prefer|key
<1-65534>|minpoll <4-
  16>|maxpoll <4-16>}|) (vrf management|) no ntp server (A.B.C.D | HOSTNAME)
({prefer|key <1-65534>|minpoll <4-16>|maxpoll
  <4-16>}|) (vrf management|) no ntp server (A.B.C.D | HOSTNAME)
({prefer|key|minpoll|maxpoll}|) (vrf
  management|)
no ntp server (A.B.C.D | X:X::X:X | HOSTNAME) ({prefer|key <1-65534>|minpoll <4-
  16>|maxpoll <4-16>}|) (vrf management|) no ntp server (A.B.C.D | HOSTNAME)
({prefer|key|minpoll|maxpoll}|) (vrf
  management|)
```

Parameters

`A.B.C.D`	IPv4 address of the server
`HOSTNAME`	Host name of the server
`X:X::X:X`	IPv6 address of the server
`prefer`	Prefer this server; preferred server responses are discarded only if they vary dramatically from other time sources
`key`	Server authentication key
`<1-65534>`	Server authentication key
`minpoll`	Minimum poll interval
`<4-16>`	Minimum poll interval value in seconds raised to a power of 2 (default 4 = 16 seconds)
`maxpoll`	Maximum poll interval
`<4-16>`	Maximum poll interval value in seconds raised to a power of 2 (default 6 = 64 seconds)
`management`	Virtual Routing and Forwarding name

Default

By default, `minpoll` is 4 and `maxpoll` is 6.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ntp server 10.10.0.23 vrf management
                    (config)#ntp server 10.10.0.23 prefer key 12345 vrf management

(config)#no ntp server 10.10.0.23 vrf management
```

ntp

sync-retry

Use this command to retry NTP synchronization with configured servers.

Command Syntax `ntp sync-retry (vrf management|)`

Parameters `management` Virtual Routing and Forwarding name

Default

No default value is specified

Command Mode

Exec mode Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ntp sync-retry vrf management
```

ntp trusted-key

Use this command to define a “trusted” authentication key. If a key is trusted, the device will synchronize with a system that specifies this key in its NTP packets.

Use the `no` option with this command to remove a trusted key.

Command Syntax `ntp trusted-key <1-65534> (vrf management|) no ntp trusted-key <1-65534> (vrf management|)`

Parameter

`<1-65534>` Authentication key number `management` Virtual Routing and Forwarding name

Default

By default, ntp trusted key is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ntp trusted-key 234676 vrf management
```

show ntp authentication-keys

Use this command to display authentication keys.

Command Syntax `show ntp authentication-keys`

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ntp authentication-keys
--------------------------
 Auth Key       MD5 String
```

```
--------------------------
14                SWWX
```

Table 8-7 explains the output fields.

Table 8-7: show ntp authentication-key fields

Entry	Description
Auth key	Authentication key (password). Use the password to verify the authenticity of packets sent from this interface or peer interface.
MD5 String	One or more MD5 key strings. The MD5 key values can be from 1 through 16 characters long. You can specify more than one key value within the list.

show ntp authentication-status

Use this command to display whether authentication is enabled or disabled.

Command Syntax `show ntp authentication-status`

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ntp authentication-status
Authentication enabled
```

show ntp logging-status

Use this command to display the NTP logging status.

Command Syntax `show ntp logging-status`

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ntp logging-status
NTP logging enabled
```

show ntp peer-status

Use this command to display the peers for which the server is maintaining state along with a summary of that state.

Command Syntax `show ntp peer-status`

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ntp peer-status
```

show ntp peers

Use this command to display NTP peers.

Command Syntax `show ntp peers`

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ntp peers
```

show ntp statistics

Use this command to display NTP statistics.

Command Syntax

```
show ntp statistics (io | local | memory | peer ( ipaddr (A.B.C.D | X:X::X:X ) |
  name (HOSTNAME)) )
```

Parameters

io	Counters maintained in the input-output module
local	Counters maintained in the local protocol module
memory	Counters related to memory allocation
peer	Counters associated with the specified peer
A.B.C.D	Peer IPv4 address
X:X::X:X	Peer IPv6 address
HOSTNAME	Peer host name

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ntp statistics local
time since restart:     1685
time since reset:       1685
packets received:       4
packets processed:      0
current version:        0
previous version:       0
declined:               0
access denied:          0 bad
length or format:    0 bad
authentication:     0 rate
exceeded:          0 #show
ntp statistics memory time
since reset:     1698 total
peer memory:     15 free peer
memory:      15 calls to
findpeer:     0 new peer
allocations: 0 peer
demobilizations: 0
 hash table counts:       0   0   0   0   0   0   0   0
                          0   0   0   0   0   0   0   0
                         0   0   0   0   0   0   0   0
                         0   0   0   0   0   0   0   0
```

0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Table 8-8 explains the output fields.

Table 8-8: show ntp statisticsfields

Entry	Description
Time since restart	Time when the ntp protocols were last started and how long they have been running.
Time since reset	Time when the ntp protocols were last reset and how long they have been running.
Packets received	Number of packets received from the peers.
Packets processed	Number of packets processed to the peers.
Current version	Current version of the protocol that is being used.
Previous version	Previous version of the protocol that has been used.
Declined	Access to the protocol declined
Access denied	Number of attempts denied to access protocol
Bad length or format	Number of messages received with length or format errors so severe that further classification could not occur.
Bad authentication	Number of messages received with incorrect authentication.

Rate exceeded	Exceed the configured rate if additional bandwidth is available from other queues
Total peer memory	Actual memory available to the peer system.
Free peer memory	Free memory available to the peer system.
Calls to find peer	Number of calls to find peer.
New peer allocations	Number of allocations from the free peer list.
Peer demobilizations	Number of structures freed to free peer list.
Hash table counts	Peer hash table's each bucket count.

show ntp trusted-keys

Use this command to display keys that are valid for authentication.

Command Syntax `show ntp trusted-keys`

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ntp trusted-keys

Trusted Keys:
333
#
```

show running-config ntp

Use this command to display the NTP running configuration.

Command Syntax `show running-config`

`ntp (|all)`

Parameters `all` Reserved for future use

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show running-config ntp

ntp enable vrf management ntp
authenticate vrf management ntp
logging vrf management
ntp authentication-key 333 md5 3gid 7 vrf management
ntp trusted-key 333 vrf management
```

CHAPTER 9 Dynamic Host Configuration Protocol Relay

This chapter describes the Dynamic Host Configuration Protocol (DHCP) relay commands.

In small networks with only one IP subnet, DHCP clients communicate directly with DHCP servers. To allow DHCP clients on subnets not directly served by DHCP servers to communicate with DHCP servers, DHCP relay agents can be installed on these subnets. The DHCP client broadcasts on the local link and the relay agent receives the broadcast and transmits it to one or more DHCP servers using unicast. The DHCP server replies to the client and the relay agent then retransmits the response on the local network.

This chapter contains these commands:

- ip dhcp relay
- ip dhcp relay address
- ip dhcp relay information option
- ipv6 dhcp relay
- ipv6 dhcp relay address
- show ip dhcp relay
- show ip dhcp relay address
- show ipv6 dhcp relay
- show ipv6 dhcp relay address
- show ipv6 dhcp relay address interface
- show running-config dhcp

ip dhcp relay

Use this command to enable the DHCP relay agent.

Use the `no` form of this command to disable the DHCP relay agent.

Command Syntax `ip dhcp relay no ip dhcp relay`

Parameters

None

Default

By default, the ip dhcp relay is enabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip dhcp relay
```

```
#configure terminal
(config)#no ip dhcp relay
```

ip dhcp relay address

Use this command to set an IP address of a DHCP server on an interface.

Use the `no` form of this command to remove the IP address of a DHCP server.

You must give the ip dhcp relay command before you give this command.

Command Syntax `ip dhcp relay address A.B.C.D (remote-id REMOTE_ID |) no ip dhcp relay address A.B.C.D`

Parameters

`A.B.C.D` IPv4 address of the DHCP server

`REMOTE_ID` Remote host identifier. Use option 82 to provide the DHCP server information about the DHCP client.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3 and was changed in SWMRE version 1.3.5.

Examples

```
#configure terminal
(config)#interface eth2
(config-if)#ip address 2.2.2.2/24
(config-if)#ip dhcp relay address 198.51.100.127
```

ip dhcp relay information option

Use this command to enable the device to insert and remove option-82 information on DHCP packets forwarded by the relay agent.

Use the `no` form of this command to disable inserting and removing option-82 information.

Command Syntax `ip dhcp relay information option no ip dhcp relay information option`

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip dhcp relay information option

#configure terminal
(config)#no ip dhcp relay information option
```

ipv6 dhcp relay

Use this command to enable the DHCP relay agent.

Use the `no` form of this command to disable the DHCP relay agent.

Command Syntax `ipv6 dhcp relay no ipv6 dhcp relay`

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ipv6 dhcp relay

#configure terminal
(config)#no ipv6 dhcp relay
```

ipv6 dhcp relay address

Use this command to set an IPv6 address of a DHCP server on an interface.

Use the `no` form of this command to remove an IPv6 address of a DHCP server.

You must give the ip dhcp relay command before you give this command.

Note:Global IPv6 address should be configured before configuring DHCPv6 relay address on an interface.

Command Syntax `ipv6 dhcp relay address X:X::X:X ipv6 dhcp relay address X:X::X:X interface IFNAME no ipv6 dhcp relay address X:X::X:X`

`ipv6 dhcp relay address X:X::X:X`

`no ipv6 dhcp relay address X:X::X:X interface IFNAME`

Parameters

`X:X::X:X` IPv6 address of the DHCP server `IFNAME` Source interface name

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth2
(config-if)#ipv6 address 1000:ad1::30/64
(config-if)#ipv6 dhcp relay address 2001:db8::7F
```

show ip dhcp relay

Use this command to display DHCP snooping relay status including DHCP server addresses configured on interfaces.

Command Syntax `show ip dhcp relay`

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show ip dhcp relay
DHCP relay service is Enabled.
Insertion of option 82 is Disabled.
Helper addresses are configured on the following interfaces:
 Interface        Relay Address
--------         ----------- xe2
10.10.10.2
```

Table 9-9 explains the output fields.

Table 9-9: show ip dhcp relay fields

Entry	Description
Interface	Name of the interface in dhcp relay.
Relay Address	Relay address in the dhcp server.

show ip dhcp relay address

Use this command to display DHCP relay addresses.

Command Syntax `show ip dhcp relay address`

```
show ip dhcp relay address interface IFNAME
```

Parameters

`IFNAME` Interface name

Command Mode

Executive mode

Applicability

This command was introduced before SWMRE version 1.3 and changed in SWMRE version 1.3.5.

Examples

```
#show ip dhcp relay address interface eth1

Interface          Relay Address --------
------------ eth1              10.10.10.10
```

Table 9-10 explains the output.

Table 9-10: show ip dhcp relay address interface fields

Entry	Description
Interface	Interface name.
Relay Address	Relay address.

show ipv6 dhcp relay

Use this command to display DHCP snooping relay status including DHCP server addresses configured on interfaces.

Command Syntax `show ipv6 dhcp relay`

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show ipv6 dhcp relay

DHCPv6 relay service is Enabled.
Helper addresses are configured on the following interfaces:
Interface            Relay Address                              Output Interface
--------             -------------                              --------------
xe5/1                 10:10::10:1                                    xe3/1
```

Table 9-11 explains the output fields.

Table 9-11: show ipv6 dhcp relay fields

Entry	Description
Interface	Name of the interface in dhcp relay.
Relay Address	Relay address in the dhcp server.

Output Interface	Name of the output interface in dhcp relay.

show ipv6 dhcp relay address

Use this command to display DHCP server addresses configured on interfaces.

Command Syntax `show ipv6 dhcp relay address`

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show ipv6 dhcp relay address
 Interface            Relay Address                          Output Interface
--------             -------------                          --------------
xe4/2                20:10::10:2                                xe4/3
```

Table 9-12 explains the output fields.

Table 9-12: show ipv6 dhcp relay address fields

Entry	Description
Interface	Name of the interface in dhcp relay.
Relay Address	Relay address in the dhcp server.
Output Interface	Name of the output interface in dhcp relay.

show ipv6 dhcp relay address interface

Use this command to display DHCP server addresses configured on the device.

Command Syntax `show ipv6 dhcp relay address interface ethernet`
`show ipv6 dhcp relay address interface ethernet <1-4096> show`

```
ipv6 dhcp relay address interface vlan show ipv6 dhcp relay
address interface vlan <1-4096> show ipv6 dhcp relay address
interface port-channel show ipv6 dhcp relay address
interface port-channel <1-4096>
```

Entry	Description
Interface	Name of the interface in dhcp relay.

Relay Address	Relay address in the dhcp server.
Output Interface	Name of the output interface in dhcp relay.

Parameters

`ethernet`	Display DHCP server addresses configured on Ethernet interfaces
`<1-4096>`	Ethernet interface number
`port-channel`	Display DHCP server addresses configured on port-channel interfaces
`<1-4096>`	Port-channel number
`vlan`	Display DHCP server addresses configured on VLAN interfaces
`<1-4096>`	VLAN identifier

Command Mode

Executive mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show ipv6 dhcp relay address interface ethernet 1
 Interface            Relay Address                          Output Interface
--------             -------------                          --------------
Ethernet1            3ffe::2
```

Table 9-13 explains the output fields.

Table 9-13: show ipv6 dhcp relay address interface fields

show running-config dhcp

Use this command to display DHCP settings in the running configuration.

Command Syntax `show running-config dhcp`

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show running-config dhcp !

interface xe2  ip dhcp relay address 10.10.10.2 !
```

CHAPTER 10 Remote Management

This chapter is a reference for commands that copy these types of files:

- Start-up configuration and running configuration
- System files such as boot files, core dumps, and debug logs

You can use these commands to copy files locally or to copy between the local device and a remote system.

The commands in this chapter use the techniques in Table 10-14 to remotely transfer files: **Table 10-14: File transfer techniques**

Trivial File Transfer Protocol (TFTP)	No authentication or encryption; dangerous to use over the Internet, but might be acceptable in a trusted environment Address format: `tftp:[//server[:port]][/path]`
File Transfer Protocol (FTP)	Authenticates, but does not encrypt Address format: `ftp:[//server][/path]`
Secure copy (SCP)	Authenticates and encrypts using Secure Shell (SSH1) Address format: `scp:[//server][/path]`
SSH File Transfer Protocol (SFTP)	Authenticates and encrypts using Secure Shell (SSH2); this is the most secure technique Address format: `sftp:[//server][/path]`
Hyper text Transfer Protocol (HTTP)	Address format: `http:[//server][/path]` For download of running and startup configurations

This chapter contains the command listed below.

- copy running-config
- copy running-config (interactive)
- copy startup-config
- copy startup-config (interactive)
- copy system file
- copy system file (interactive)
- copy ftp startup-config
- copy ftp running-config
- copy scp startup-config
- copy scp running-config
- copy sftp startup-config
- copy sftp running-config
- copy tftp startup-config
- copy tftp running-config
- copy http startup-config
- copy http running-config

- copy scp running-config (interactive)
- copy sftp running-config (interactive)
- copy http startup-config (interactive)
- copy ftp startup-config (interactive)
- copy scp startup-config (interactive)
- copy sftp running-config (interactive)
- copy tftp startup-config (interactive)
- copy http startup-config (interactive)
- copy startup-config running-config
- copy file running-config

copy running-config

Use this command to copy the running configuration to an FTP server, an SCP server, an SFTP server, or a TFTP server.

Command Syntax

```
copy running-config (tftp TFTP-URL|ftp FTP-URL|scp SCP-URL|sftp SFTP-URL) (vrf
  (NAME|management)|)
```

Parameters

`TFTP-URL`	Destination: `tftp:[//server[:port]][/path]`
`FTP-URL`	Destination: `ftp:[//server][/path]`
`SCP-URL`	Destination: `scp:[//server][/path]`
`SFTP-URL`	Destination: `sftp:[//server][/path]`
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#copy running-config sftp sftp://sftp.mysite.com/running_conf vrf management
```

copy running-config (interactive)

Use this command to copy the running configuration to an FTP server, an SCP server, an SFTP server, or a TFTP server.

Command Syntax `copy running-config (ftp|tftp|scp|sftp) (vrf (NAME|management)|)`

Parameters `ftp` Destination: FTP server `tftp` Destination: TFTP server `scp` Destination: SCP server `sftp` Destination: SFTP server `NAME` Virtual Routing and Forwarding name `management` Management Virtual Routing and Forwarding

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#copy running-config sftp vrf management
```

copy startup-config

Use this command to copy the running configuration to an FTP server, an SCP server, an SFTP server, or a TFTP server.

Command Syntax

```
copy startup-config (tftp TFTP-URL|ftp FTP-URL|scp SCP-URL|sftp SFTP-URL) (vrf
  (NAME|management)|)
```

Parameters

TFTP-URL	Destination: tftp:[//server[:port]][/path]
FTP-URL	Destination: ftp:[//server][/path]
SCP-URL	Destination: scp:[//server][/path]
SFTP-URL	Destination: sftp:[//server][/path]
NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#copy startup-config sftp sftp://sftp.mysite.com/start-up_conf vrf management
```

copy startup-config (interactive)

Use this command to copy the running configuration to an FTP server, an SCP server, an SFTP server, or a TFTP server.

Command Syntax `copy startup-config (ftp|tftp|scp|sftp) (vrf (NAME|management)|)`

Parameters `ftp` Destination: FTP server `tftp` Destination: TFTP server `scp` Destination: SCP server `sftp` Destination: SFTP server

`NAME` Virtual Routing and Forwarding name `management` Management Virtual Routing and Forwarding

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#copy startup-config sftp vrf management
```

copy system file

Use this command to copy a system file to an FTP server, an SCP server, an SFTP server, or a TFTP server.

Note: The names of the options for the source in the first parameter refer to symbolic locations. The specific locations for Linux are noted below. The locations on a specific device can vary depending on the platform.

Command Syntax

```
copy (core|debug|log) FILE (tftp TFTP-URL|ftp FTP-URL|scp SCP-URL|sftp SFTP-URL)
  (vrf (NAME|management)|)
```

Parameters

`core`	Core file storage; on Linux this refers to `/var/log/crash/cores/`
`debug`	Debug file storage; on Linux this refers to `/log/`
`log`	Log file storage; on Linux this refers to
`FILE`	`/var/log/` Source file name
`TFTP-URL`	Destination: `tftp:[//server[:port]][/path]`
`FTP-URL`	Destination: `ftp:[//server][/path]`
`SCP-URL`	Destination: `scp:[//server][/path]`
`SFTP-URL`	Destination: `sftp:[//server][/path]` Virtual
`NAME`	Routing and Forwarding name Management Virtual
`managemen t`	Routing and Forwarding

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#copy core myFile sftp sftp://sftp.mysite.com/dst_filename vrf management
```

copy system file (interactive)

Use this command to copy a system file to an FTP server, an SCP server, an SFTP server, or a TFTP server.

Note: The names of the options for the source in the first parameter refer to symbolic locations. The specific locations for Linux are noted below. The locations on a specific device can vary depending on the platform.

Command Syntax `copy (core|debug|log) FILE (ftp|tftp|scp|sftp) (vrf (NAME|management)|)`

Parameters `core` Core file storage; on Linux this refers to `/var/log/crash/cores/`

`debug` Debug file storage; on Linux this refers to `/log/` `log` Log file storage; on Linux this refers to `/var/log/`

`FILE` Source file name `ftp` Destination: FTP server `tftp` Destination: TFTP server `scp` Destination: SCP server

`sftp` Destination: SFTP server `NAME` Virtual Routing and Forwarding name `management` Management Virtual Routing and Forwarding

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#copy log myFile sftp vrf management
```

copy ftp startup-config

Use this command to copy the start up configuration from an FTP server to the local device.

Command Syntax `copy ftp FTP-URL startup-config (vrf (NAME|management)|)`

Parameters

`FTP-URL` Configuration source: `ftp:[//server][/path] NAME`

Virtual Routing and Forwarding name `management` Management

Virtual Routing and Forwarding

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#copy ftp ftp://ftp.mysite.com/scr filename startup-config vrf management
```

copy ftp running-config

Use this command to append the running configuration from an FTP server to the local device.

Command Syntax `copy ftp FTP-URL running-config append (store|) (vrf (NAME|management)|)` **Parameters**

`FTP-URL` Configuration source: `ftp:[//server][/path]`

`store`	Store the running-configuration
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#copy ftp ftp://ftp.mysite.com/scr filename running-config appen store vrf
management
```

copy scp startup-config

Use this command to copy the start up configuration from a SCP server to the local device.

Command Syntax `copy scp SCP-URL startup-config (vrf (NAME|management)|)`

Parameters

`SCP-URL` Configuration source: `scp:[//server][/path] NAME`

Virtual Routing and Forwarding name `management` Management

Virtual Routing and Forwarding

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#copy scp scp://scp.mysite.com/scr filename startup-config vrf management
```

copy scp running-config

Use this command to append the running configuration from an SCP server to the local device.

Command Syntax `copy scp SCP-URL running-config append (store|) (vrf (NAME|management)|)`

Parameters

`SCP-URL`	Configuration source: `SCP:[//server][/path]`
`store`	Store the running configuration
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#copy scp scp://scp.mysite.com/scr filename running-config appen store vrf
management
```

copy sftp startup-config

Use this command to copy the start up configuration from a SFTP server to the local device.

Command Syntax `copy sftp SFTP-URL startup-config (vrf (NAME|management)|)`

Parameters

SFTP-URL	Configuration source: sftp:[//server][/path] NAME
	Virtual Routing and Forwarding name management Management
	Virtual Routing and Forwarding

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#copy sftp sftp://sftp.mysite.com/scr filename startup-config vrf management
```

copy sftp running-config

Use this command to append the running configuration from an SFTP server to the local device.

Command Syntax copy sftp SFTP-URL running-config append (store|) (vrf (NAME|management)|)

Parameters

SFTP-URL	Configuration source: sftp:[//server][/path]
store	Store the running-configuration
NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#copy sftp sftp://sftp.mysite.com/sftp filename running-config appen store vrf
management
```

copy tftp startup-config

Use this command to copy the start up configuration from a TFTP server to the local device.

Command Syntax `copy tftp TFTP-URL startup-config (vrf (NAME|management)|)`

Parameters

`TFTP-URL` Configuration source: `tftp:[//server][/path] NAME`

Virtual Routing and Forwarding name `management` Management

Virtual Routing and Forwarding

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#copy tftp tftp://tftp.mysite.com/scr filename startup-config vrf management
```

copy tftp running-config

Use this command to append the running configuration from an FTP server to the local device.

Command Syntax `copy tftp TFTP-URL running-config append (store|) (vrf (NAME|management)|)` **Parameters**

`TFTP-URL` Configuration source: `tftp:[//server][/path]`

`store` Store the running-configuration

NAME	Virtual Routing and Forwarding name
management	Management Virtual Routing and Forwarding

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#copy tftp tftp://tftp.mysite.com/scr filename running-config appen store vrf
management
```

copy http startup-config

Use this command to copy the start up configuration from a HTTP server to the local device.

Command Syntax `copy http HTTP-URL startup-config (vrf (NAME|management)|)`

Parameters

`HTTP-URL` Configuration source: `http:[//server][/path] NAME`

Virtual Routing and Forwarding name `management` Management

Virtual Routing and Forwarding

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#copy http http://http.mysite.com/scr filename startup-config vrf management
```

copy http running-config

Use this command to append the running configuration from an FTP server to the local device.

Command Syntax `copy http HTTP-URL running-config append (store|) (vrf (NAME|management)|)`

Parameters

`HTTP-URL`	Configuration source: `http:[//server][/path]`
`store`	Store the running-configuration
`NAME`	Virtual Routing and Forwarding name
`management`	Management Virtual Routing and Forwarding

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#copy http http://http.mysite.com/scr filename running-config appen store vrf
management
```

copy scp running-config (interactive)

Use this command to copy and store the running configuration from an SCP server to the local device.

Command Syntax `copy scp running-config (append|) store (vrf (NAME|management)|)`

Parameters `append` Append the configuration into running-config `NAME` Virtual Routing and Forwarding name `management` Management Virtual Routing and Forwarding

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#copy scp running-config append store vrf management
```

copy sftp running-config (interactive)

Use this command to copy and store the running configuration from an SFTP server to the local device.

Command Syntax `copy sftp running-config (append|) store (vrf (NAME|management)|)`

Parameters `append` Append the configuration into running-config `NAME` Virtual Routing and Forwarding name `management` Management Virtual Routing and Forwarding

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#copy sftp running-config append store vrf management
```

copy tftp running-config (interactive)

Use this command to copy and store the running configuration from a TFTP server to the local device.

Command Syntax `copy tftp running-config (append|) store (vrf (NAME|management)|)`

Parameters `append` Append the configuration into running-config `NAME` Virtual Routing and Forwarding name `management` Management Virtual Routing and Forwarding

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#copy tftp running-config append store vrf management
```

copy http running-config (interactive)

Use this command to copy and store the running configuration from a TFTP server to the local device.

Command Syntax `copy http running-config (append|) store (vrf (NAME|management)|)`

Parameters `append` Append the configuration into running-config `NAME` Virtual Routing and Forwarding name `management` Management Virtual Routing and Forwarding

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#copy http running-config append store vrf management
```

copy ftp startup-config (interactive)

Use this command to copy the start up confguration from an FTP server to the local device.

Command Syntax `copy ftp startup-config (vrf (NAME|management)|)`

Parameters

`NAME` Virtual Routing and Forwarding name `management` Management Virtual Routing and Forwarding

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#copy ftp startup-config vrf management
```

copy scp startup-config (interactive)

Use this command to copy the start up confguration from a SCP server to the local device.

Command Syntax `copy scp startup-config (vrf (NAME|management)|)`

Parameters

`NAME` Virtual Routing and Forwarding name `management` Management Virtual Routing and Forwarding

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#copy scp startup-config vrf management
```

copy sftp startup-config (interactive)

Use this command to copy the start up confguration from an SFTP server to the local device.

Command Syntax `copy sftp startup-config (vrf (NAME|management)|)`

Parameters

`NAME` Virtual Routing and Forwarding name `management` Management Virtual Routing and Forwarding

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#copy sftp startup-config vrf management
```

copy tftp startup-config (interactive)

Use this command to copy the start-up confguration from a TFTP server to the local device.

Command Syntax `copy tftp startup-config (vrf (NAME|management)|)`

Parameters

`NAME` Virtual Routing and Forwarding name `management` Management Virtual Routing and Forwarding

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#copy tftp startup-config vrf management
```

copy http startup-config (interactive)

Use this command to copy the start-up confguration from a TFTP server to the local device.

Command Syntax `copy http startup-config (vrf (NAME|management)|)`

Parameters

`NAME` Virtual Routing and Forwarding name `management` Management Virtual Routing and Forwarding

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#copy http startup-config vrf management
```

copy startup-config running-config

Use this command to copy the start-up configuration to the running configuration.

Command Syntax `copy startup-config running-config`

Parameters

None

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#copy startup-config running-config
```

copy file running-config

Use this command to copy and store a file into the running configuration.

Command Syntax `copy file FILE running-config (append|) store`

Parameters

`FILE`	File name
`append`	Append the configuration into running-config

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#copy file myFile running-config append store
```

© Symanitron

CHAPTER 11 Software Monitoring and Reporting

This document describes software watchdog and reporting related commands.

- feature software-watchdog
- show bootup-parameters
- show cores
- show software-watchdog status
- show system log
- show system login
- show system reboot-history
- show system resources
- show system uptime
- show techsupport
- software-watchdog
- software-watchdog keep-alive-time

feature software-watchdog

Use this command to enable software watchdog functionality for all SWMRE modules. This feature is enabled by default.

Use the `no` form of this command to disable software watchdog functionality.

Command Syntax

```
feature software-watchdog
no feature software-watchdog
```

Parameter

None

Default

By default, software watchdog is enabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
#(config)feature software-watchdog
```

show bootup-parameters

Use this command to show SWMRE kernel bootup parameters.

Command Syntax `show bootup-parameters`

Parameter

None

Command Mode

Execution mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show bootup-parameters
BOOT_IMAGE=/boot/vmlinuz-3.16.0-41-generic root=/dev/sda4
console=ttyS0,115200n8 ro
```

show cores

Use this command to list core files in the system or to display information about a given core file.

Command Syntax `show cores`

`(|WORD details)`

Parameter

`WORD`	Core file name

Command Mode

Execution mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show cores
Core file and Crash log location :/var/log/crash/cores
Process Name    PID             Core-File-Name      -----------
-     ---             --------------     sflow            29355
core_sflow.29355_20130531_044219 vrrpd           6792
core_vrrpd.6792_20130531_044236


>show details
core_vrrpd.6792_20130531_044236 /* This
shows output of following commands top -n 1
-b gdb output of bt full info proc info
sharedlib info target info registers info
threads thread apply all bt full netstat -
apn netstat -avs
*/
```

Table 11-15 explains the output fields.

Table 11-15: show cores fields

Entry	Description
Process Name	String that identifies the process.
PID	Process ID, a number that identifies a process.
Core-File-Name	Core dump-file where the file resides and the filename.

show software-watchdog status

Use this command to display the software watchdog status for each SWMRE module.

Command Syntax `show software-watchdog status show software-watchdog status detail`

Parameter

None

Command Mode

Execution mode

Applicability

This command was introduced before SWMRE version 1.3 and updated in SWMRE version 1.3.4.

Examples

```
#show software-watchdog status
Software Watchdog timeout in seconds : 60
Process name         Watchdog status
============         ===============
nsm                  Enabled ripd
Enabled ripngd               Enabled
ospfd                Enabled ospf6d
Enabled isisd                Enabled
hostpd               Enabled ldpd
Enabled rsvpd                Enabled
mribd                Enabled pimd
Enabled authd                Enabled
mstpd                Enabled imi
Enabled onmd                 Enabled
HSL                  Enabled oamd
Enabled vlogd                Enabled
vrrpd                Enabled ndd
Enabled ribd                 Enabled
bgpd                 Enabled l2mribd
Enabled lagd                 Enabled
sflow                Enabled
cmld             Enabled
cmmd             Enabled

#show software-watchdog status detail
Software Watchdog timeout in seconds : 60

Process Watchdog   Process   Disconnect Connect         Last Restart
```

```
 Name     Status      Status      Count      Count                Reason
=======       ========       ===========        ==========        =======
================================ nsm     Enabled   Running     0          1
Fresh bootup ripd    Enabled  Running      0         1        Fresh bootup
ripngd   Enabled  Running      0             1        Fresh   bootup ospfd
Enabled   Running      0           1        Fresh bootup   ospf6d  Enabled
Running      0           1        Fresh bootup isisd     Enabled  Running
0          1       Fresh bootup hostpd  Enabled   Running      0          1
Fresh bootup ldpd    Enabled  Running      0         1        Fresh bootup
rsvpd    Enabled  Running      0             1        Fresh   bootup mribd
Enabled   Running      0           1        Fresh bootup   pimd     Enabled
Running      0           1        Fresh bootup authd     Enabled  Running
0          1       Fresh bootup mstpd   Enabled  Running      0          1
Fresh bootup imi     Enabled  Running      0         1        Fresh bootup
onmd     Enabled   Running      0             1          Fresh bootup HSL
Enabled   Running      0           1        Fresh bootup   oamd     Enabled
Running      0           1        Fresh bootup vlogd     Enabled  Running
0          1       Fresh bootup vrrpd   Enabled  Running      0          1
Fresh bootup ndd     Enabled  Running      0         1        Fresh bootup
ribd     Enabled   Running      0             1        Fresh   bootup bgpd
Enabled   Running      0           1        Fresh bootup   l2mribd Enabled
Running      0           1        Fresh bootup lagd      Enabled  Running
0          1       Fresh bootup sflow   Enabled  Running      0          1
Fresh bootup cmld    Enabled  Running      0         1        Fresh bootup
cmmd     Enabled  Running     0           1       Fresh bootup
```

Table 11-16 explains the output fields.

Table 11-16: show software-watchdog status output fields

Field	Description
Process Name	The name of a protocol module.
Watchdog Status	Status of a protocol module (Enabled or Disabled).
Process Status	Status of the protocol module Running/Not-running).
Disconnect Count	Number of times the protocol module disconnected from monitoring module.

Table 11-16: show software-watchdog status output fields (Continued)

	Description
Count	Number of times the protocol module connected to monitoring module.
tart Reason	Reason why a module disconnected from monitoring module.

show system log

Use this command to display the system's log file.

Command Syntax

```
show system log
```

Parameters

None

Command Mode

Execution mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show system log
Syslog              : enabled      File Name   : /var/log/messages
Oct 18 18:10:18 localhost rsyslogd: [origin software="rsyslogd"
swVersion="8.4.2
" x-pid="541" x-info="http://www.rsyslog.com"] start
Oct 18 18:10:18 localhost systemd[1]: Started Apply Kernel Variables. Oct 18
18:10:18 localhost systemd[1]: Started Create Static Device Nodes in / dev
.
Oct 18 18:10:18 localhost systemd[1]: Starting udev Kernel Device Manager...
Oct 18 18:10:18 localhost systemd[1]: Started udev Kernel Device Manager. Oct
18 18:10:18 localhost systemd[1]: Starting Copy rules generated while the ro
ot was ro...
Oct 18 18:10:18 localhost systemd[1]: Starting LSB: Set preliminary keymap...
Oct 18 18:10:18 localhost systemd[1]: Started Copy rules generated while the
roo t was ro.
Oct 18 18:10:18 localhost nfs-common[163]: Starting NFS common utilities:.
Oct 18 18:10:18 localhost systemd[1]: Found device /dev/ttyS0.
Oct 18 18:10:18 localhost systemd[1]: Found device 16GB_SATA_Flash_Drive
SWMRE-CONFIG.
Oct 18 18:10:18 localhost systemd[1]: Starting File System Check on
/dev/disk/ by
-label/SWMRE-CONFIG...
Oct 18 18:10:18 localhost systemd[1]: Starting system-ifup.slice.
Oct 18 18:10:18 localhost systemd-fsck[217]: SWMRE-CONFIG: clean, 85/128016
file
s, 27057/512000 blocks
Oct 18 18:10:18 localhost systemd[1]: Created slice system-ifup.slice. --More-
-
```

Table 11-17 explains the output fields.

Table 11-17: show system log fields

	Description
	Status of the protocol (enabled or disabled).
	Specifies the name of the system log files that you configured.

show system login

Use this command to display the system's login history.

Command Syntax `show system login`

Parameters

None

Command Mode

Execution mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show system login
eric      ttyS0                         Wed Oct 19 18:31   still logged in takayuki
ttyS0                         Wed Oct 19 18:14 - 18:25  (00:10) girish    ttyS0
Wed Oct 19 16:46 - 17:01  (00:14) wtmp begins Wed Oct 19 16:46:18 2016
```

show system reboot-history

Use this command to show the SWMRE reboot history.

Command Syntax `show system reboot-history`

Parameters

None

Command Mode

Execution mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show system reboot-history
#) On Thu Jun 6 06:16:03 2013
Reason: Reset Requested by Active User
Service: NONE
#) On Thu Jun 6 06:21:30 2015
Reason: Reset Requested due to Process Crash
Service: nsm
#
```

Table 11-17 explains the output fields.

Table 11-18: show system reboot-history fields

Entry	Description
Reason	Displays the reason, why the fields are reset.
Service	Name of the service in this protocol.

show system resources

Use this command to display the system's current resources.

Command Syntax `show system resources (iteration <1-5>|)`

Parameters

`<1-5>` The number of times to check the resources before they are displayed.

Command Mode

Execution mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
DELL-6K3#show system resources load
average: 0.11, 0.08, 0.05
Tasks: 113 total,   1 running, 112 sleeping,   0 stopped,   0 zombie
%Cpu(s):   1.1 us,  0.4 sy,  0.0 ni, 98.5 id,   0.0 wa,   0.0 hi,  0.0 si,  0.0
st
KiB Mem:    8181040 total,    736124used,   7444916 free,    133012 buffers


#show system resources iteration 5 load
average: 0.03, 0.06, 0.05
Tasks: 112 total,   3 running, 109 sleeping,   0 stopped,   0 zombie
%Cpu(s):   1.0 us,  0.6 sy,  0.0 ni, 98.4 id,   0.0 wa,   0.0 hi,  0.0 si,  0.0
st
KiB Mem:    8181040 total,    736608used,   7444432 free,    132976 buffers
KiB Swap:         0 total,         0used,         0 free.    252416 cached Mem
```

Table 11-19 explains the output fields.

Table 11-19: show system resource fields

Entry	Description
Load Average	Number of processes that are running. The average reflects the system load the past 1, 5, and 15 minutes.
Tasks	Number of processes in the system and how many processes are actually running when the command is issued.
CPU	Displays the CPU utilization information for processes on the device.

Table 11-19: show system resource fields

	Description
	The memory field (Mem) shows the virtual memory used by processes. The value in the memory field is in KB and MB, and is broken down as follows: Total: The total amount of available virtual memory, in kibibytes (KiBs). Used:The total amount of used virtual memory, in kibibytes (KiBs). Free: The total amount of free virtual memory, in kibibytes (KiBs) Buffers: The size of the memory buffer used to hold data recently called from disk.
	The Swap field shows the total swap space available and how much is unused and is broken down as follows: Total: The total amount of available swap memory, in kibibytes (KiBs). Used: The total amount of used swap memory, in kibibytes (KiBs). Free: The total amount of free swap memory, in kibibytes (KiBs). Cache Memory: Memory that is not associated with any program and does not need to be swapped before being reused.

show system uptime

Use this command to display how lone the system has been up and running.

Command Syntax `show system uptime`

Parameters

None

Command Mode

Execution mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
DELL-6K3#show system uptime
            19:10:22 up 1 day,  1:01,  1 user,  load average: 0.08, 0.05, 0.05
```

Table 11-20 explains the output fields.

Table 11-20: show system uptime fields

Entry	Description
Time and up	Current time, in the local time zone, and how long the router or switch has been operational.
Users	Number of users logged in to the router or switch.
Load Average	Number of processes that are running. The average reflects the system load the past 1, 5, and 15 minutes.

show techsupport

Use this command to collect system data for technical support to save support information in a compressed (.gz) file.

The default file path is `/var/log/` and the filename is `tech_support_YYYY_MMM_DD_HH_MM_SS.tar.gz`.

The filename given can be the same as another file; to distinguish them, each of the filenames are appended with a date and timestamp.

If a `show techsupport` command execution is in progress, any newly issued `show techsupport` commands are ignored.

If a `show techsupport` command is executing, and the `show running-config` command is given, the displayed information is copied from the `show techsupport` command.

Command Syntax

```
show techsupport
  ({bgp|authd|isis|lag|ldp|mstp|ospf|pim|hostpd|hsl|l2mribd|mribd|nsm|oam|onm|os
p6   |rib|ripng|sflow|vrrp|rip|rsvp|imi|trill|all|cmmd})(log-path   WORD)(status)
```

Parameters:

`daemon`	Protocol/daemon name
`WORD`	The path and filename (log-path) where the technical support information is saved.
`status`	Displays the status of the completion of the technical support `tar_.gz` file.
`all`	Include all protocol information in the technical support `tar_.gz` file.

Default

The default file path for show techsupport is /var/log/.

Command Mode

Privileged EXEC

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show techsupport all
#show techsupport all log-path /home/filename
#show techsupport nsm
#show techsupport nsm log-path /home/filename
#show techsupport hostpd authd imi
#show techsupport hostp authd imi log-path /home/filename
#show techsupport status
```

software-watchdog

Use this command to enable the software watchdog feature for an SWMRE module.

Use the `no` form of this command to disable the software watchdog feature.

Command Syntax

```
software-watchdog (nsm|authd|bgpd|cmld|hostpd|imi|isisd|lagd|l2mribd|
  mstpd|mribd|ndd|oamd|onmd|ospfd|ospf6d|pimd|ribd|ripd|ripngd|sflow|vlogd|vrrpd
  | | ldpd|rsvpd||trilld|hsl|cmmd)

no software-watchdog (nsm|authd|bgpd|cmld|hostpd|imi|isisd|lagd|l2mribd|
  mstpd|mribd|ndd|oamd|onmd|ospfd|ospf6d|pimd|ribd|ripd|ripngd|sflow|vlogd|vrrpd
  | | ldpd|rsvpd||trilld|hsl|cmmd)
```

Parameters

`nsm`	NSM module
`authd`	AUTH module
`bgpd`	BGP module
`cmld`	CML module
`hostpd`	HOSTP module

imi	IMI module
isisd	ISIS module
lagd	LAG module
l2mribd	L2MRIB module
mstpd	MSTP module
mribd	MRIB module
ndd	NDD module
oamd	OAM module
onmd	ONM module
ospfd	OSPF module
ospf6d	OSPF6 module
pimd	PIM module
ribd	RIB module
ripd	RIP module
ripngd	RIPNG module
sflow	SFLOW module
vlogd	VLOG module
vrrpd	VRRP module
ldpd	LDP module
rsvpd	RSVP module
trilld	TRILL module
hsl	HSL module
cmmd	CMM module

Default

By default, software watchdog is enabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
                    #(config)no software-watchdog imi
#(config)software-watchdog nsm
```

software-watchdog keep-alive-time

Use this command to set the software watchdog keep-alive time interval in seconds. The default keep-alive time interval is 60 seconds.

Use the `no` form of this command to set default keep-alive time interval.

Command Syntax `software-watchdog keep-alive-time <30-1800> no software-watchdog keep-alive-time`

Parameters

`<30-1800>`	Keep-alive time interval in seconds

Default

By default, software watchdog is enabled and the keep-alive time interval is 60 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
#(config)software-watchdog keep-alive-time 100
```

Authentication Command Reference

Contents

This document contains these chapters:

- Chapter 1, *Authentication, Authorization and Accounting*
- Chapter 2, *RADIUS*
- Chapter 3, *TACACS+*

© Symanitron

Authentication Command Reference

CHAPTER 1 Authentication, Authorization and Accounting

This chapter is a reference for the authentication:

- Authentication identifies users by challenging them to provide a user name and password. This information can be encrypted if required, depending on the underlying protocol.
- Authorization provides a method of authorizing commands and services on a per user profile basis.

Note: Authorization will be auto-enabled if user enables the Authentication.

- Accounting collects detailed system and command information and stores it on a central server where it can be used for security and quality assurance purposes.

The authentication feature allows you to verify the identity and, grant access to managing devices. The authentication feature works with the access control protocols as described in these chapters:

- Chapter 2, *RADIUS*
- Chapter 3, *TACACS+*

Note: Only network administrators can execute these commands. For more, see the username command.

Note: The commands below are supported only on the “management” VRF.

This chapter describes these commands:

- aaa authentication login default
- aaa accounting details
- aaa authentication login console
- aaa authentication login default
- aaa authentication login default fallback error
- aaa group server
- aaa local authentication attempts max-fail
- aaa local authentication unlock-timeout
- debug aaa
- server
- show aaa authentication
- show aaa authentication login
- show aaa accounting
- show aaa groups
- show running-config aaa

aaa authentication login

Use this command to set login authentication behavior.

Use the `no` form of this command to disable either authentication behavior.

Command Syntax `aaa authentication login error-enable (vrf management|) no aaa authentication login error-enable (vrf management|)`

Parameters `error-enable` Display login failure messages `management`

Management VRF

Default

By default, aaa authentication login is local

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
                (config)#aaa authentication login error-enable vrf management
```

aaa accounting details

Use this command to set a list of server groups to which to redirect accounting logs.

Use the `no` form of this command to only log locally.

Command Syntax `aaa accounting default (vrf management|) ((group LINE)|local) no aaa accounting default (vrf management|) ((group LINE)|local)`

Parameters `group` Server group list for authentication

`LINE` A space-separated list of up to 8 configured RADIUS or TACACS+ server group names `local` Use local authentication `management` Management VRF

Default

Default AAA method is local

Default groups: RADIUS or TACACS+

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#aaa accounting default vrf management group radius
```

aaa authentication login console

Use this command to set the AAA authentication methods for console log ins.

Use the `no` form of this command to set the default AAA authentication method (local).

Command Syntax `aaa authentication login console ((group LINE) | (local (|none)) | (none)) no aaa authentication login console ((group LINE) | (local (|none)) | (none))`

Parameters `group` Use a server group list for authentication

`LINE` Specify a space-separated list of up to 8 configured RADIUS or TACACS+ server group names followed by `local` or `none` or both `local` and `none`. The list can also include:

`radius` All configured RADIUS servers

`tacacs+` All configured TACACS+ servers

`local` Use local authentication `none` No authentication

Default

Default AAA authentication method is local Default

groups: RADIUS or TACACS+

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#aaa authentication login console group radius
```

aaa authentication login default

Use this command to set the AAA authentication methods.

Use the `no` form of this command to set the default AAA authentication method (local).

Command Syntax

```
aaa authentication login default (vrf management|) ((group LINE) | (local (|none))
  | (none)) no aaa authentication login default (vrf management|) ((group
LINE) | (local (|none)) | (none))
```

Parameters

`group`		Use a server group list for authentication
	`LINE`	A space-separated list of up to 8 configured RADIUS or TACACS+, server group names followed by `local` or `none` or both `local` and `none`. The list can also include:
		`radius` All configured RADIUS servers
		`tacacs+` All configured TACACS+ servers
`local`		Use local authentication
`none`		No authentication
`management`		Management VRF

Default

By default, AAA authentication method is local

By default, groups: RADIUS or TACACS+

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#aaa authentication login default vrf management group radius
```

aaa authentication login console fallback error

Use this command to enable fallback to local authentication for the console login if remote authentication is configured and all AAA servers are unreachable.

Use the `no` form of this command to disable fallback to local authentication.

Command Syntax `aaa authentication login console fallback error local`

`no aaa authentication login console fallback error local`

Parameters

None

Default

By default, AAA authentication is local

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#aaa authentication login console fallback error local
```

aaa authentication login default fallback error

Use this command to enable fallback to local authentication for the default login if remote authentication is configured and all AAA servers are unreachable.

Use the `no` form of this command to disable fallback to local authentication.

Command Syntax `aaa authentication login default fallback error local (vrf management|) no aaa authentication login default fallback error local (vrf management|)`

Parameters `management` Management

VRF

Default

By default, AAA authentication is local.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#aaa authentication login default fallback error local vrf management
```

aaa group server

Use this command to create a server group and enter server group configuration mode.

Use the `no` form of this command to remove a server group.

Command Syntax `aaa group server (radius|tacacs+) WORD (vrf management|) no aaa group server (radius|tacacs+) WORD (vrf management|)`

Parameters

`radius`	RADIUS server group
`tacacs+`	TACACS+ server group
`WORD`	Server group name; maximum 127 characters
`management`	Management VRF

Default

By default, the AAA group server option is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#aaa group server radius maxsmart
(config-radius)#
```

aaa local authentication attempts max-fail

Use this command to set the number of unsuccessful authentication attempts before a user is locked out.

Use the `no` form of this command to disable the lockout feature.

Command Syntax `aaa local authentication attempts max-fail <1-25> (vrf management|) no aaa local authentication attempts max-fail (vrf management|)`

Parameters

`<1-25>` Range of number of unsuccessful authentication attempts `management` Management VRF

Default

By default, the maximum number of unsuccessful authentication attempts before a user is locked out is 3.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#aaa local authentication attempts max-fail 2 vrf management
```

aaa local authentication unlock-timeout

Use this command to set timeout value in seconds to unlock local user-account.

Use the no form of this command to set default timeout value in seconds.

Note: This command is applicable only to local user but not for user/s present at the server end to authenticate using TACACS+ or RADIUS.

Command Syntax `aaa local authentication unlock-timeout <1-3600> (vrf management|)` `no aaa local authentication unlock-timeout (vrf management|)`

Parameters

`<1-3600>` Range of timeout value in seconds to unlock local user-account. Default value is 1200

`management` Management VRF

Default

By default, the unlock timeout is 1200 seconds

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#aaa local authentication unlock-timeout 1800
```

debug aaa

Use this command to display AAA debugging information.

Use the `no` form of this command to stop displaying AAA debugging information.

Command Syntax `debug aaa no debug aaa`

Parameters

None

Command Mode

Executive mode and configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#debug aaa
```

server

Use this command to add a server to a server group.

Use the `no` form of this command to remove from a server group.

Command Syntax `server (A.B.C.D | X:X::X:X | HOSTNAME) no server (A.B.C.D | X:X::X:X | HOSTNAME)`

Parameters

`A.B.C.D`	IPv4 address
`X:X::X:X`	IPv6 address

Default

None

Command Modes

RADIUS server group configure mode

TACACS+ server group configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#feature tacacs+
                                    (config)#aaa group server tacacs+ TacacsGroup4
(config-tacacs)#server 203.0.113.127
```

show aaa authentication

Use this command to display AAA authentication configuration.

Command Syntax `show aaa authentication (|vrf(management|all))`

Parameters

None

Command Modes

Executive mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show aaa authentication                VRF: default
default: local   console: local
```

Table 1-21 explains the output fields.

Table 1-21: show aaa authentication fields

Entry	Description
VRF	Virtual Routing and Forwarding (VRF) default support.
Default	Displays the aaa authentication method list.
Console	Authentication setting for the console access.

show aaa authentication login

Use this command to display AAA authentication configuration for login default and login console.

Command Syntax `show aaa authentication login error-enable (|vrf management|all))`

Parameters `error-enable` Display setting for login failure messages `vrf`

Management VRF or all VRFs

Command Modes

Executive mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show aaa authentication login error-enable
                VRF: default disabled
```

show aaa groups

Use this command to display AAA group configuration.

Command Syntax `show aaa groups (vrf (management|all)|)`

Parameters

`vrf`	Management VRF or all VRFs

Command Modes

Executive mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show aaa groups VRF: default radius
```

show aaa accounting

Use this command to display AAA accounting configuration.

Command Syntax `show aaa accounting (vrf (management|all)|)`

Parameters

`vrf`	Management VRF or all VRFs

Command Modes

Executive mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show aaa accounting
                VRF: default
```

show running-config aaa

Use this command to display AAA settings in the running configuration.

Command Syntax `show running-config aaa (vrf(management|all)|)`

Parameters

`vrf`	Management VRF or all VRFs

Command Modes

Executive mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show aaa accounting                VRF: default
default: local
```

Table 1-22 explains the output fields.

Table 1-22: show aaa accounting fields

Entry	Description
VRF	Virtual Routing and Forwarding (VRF) default support.
Default	Displays the aaa authentication method list.

© Symanitron

CHAPTER 2 RADIUS

This chapter is a reference for Remote Authentication Dial In User Service (RADIUS) commands, RADIUS provides centralized Authentication, Authorization management for users that connect to and use a network service. RADIUS is specified in RFC 2865.

Note: Only network administrators can execute these commands. For more, see the username command.

Note: The commands below are supported only on the “management” VRF.

- debug radius
- radius-server login host
- radius-server login host acct-port
- radius-server login host auth-port
- radius-server login host key
- radius-server login key
- radius-server login timeout
- show debug radius
- show radius-server
- show running-config radius

debug radius

Use this command to display RADIUS debugging information.

Use the `no` form of this command stop displaying RADIUS debugging information.

Command Syntax `debug radius no debug radius`

Parameters

None

Command Mode

Executive mode and configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#debug radius
```

radius-server login host

Use this command to configure a RADIUS server for both accounting and authentication.

Use the `no` form of this command to remove a RADIUS server.

Command Syntax `radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|)`

```
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) timeout
  <1-60> no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf
management|) no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME)
(vrf management|)
  timeout
```

Parameters

`login`	Remote login
`A.B.C.D`	IPv4 address of RADIUS server
`X:X::X:X`	IPv6 address of RADIUS server
`HOSTNAME`	DNS host name of RADIUS server
`timeout`	How long to wait for a response from the RADIUS server before declaring a timeout failure
`<1-60>`	Range of time out period in seconds
`vrf`	Virtual Routing and Forwarding
`management`	Management VRF

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#radius-server login host 203.0.113.15 vrf management
```

radius-server login host acct-port

Use this command to configure a RADIUS server and specify a UDP port to use for RADIUS accounting messages.

Use the `no` form of this command to remove a RADIUS server.

Command Syntax

```
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) acct-
```

```
port <0-65535> |) | timeout <1-60> |)
```

```
no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) acct-
port |) | timeout <1-60> |)
```

Parameters

`login`	Remote login
`A.B.C.D`	IPv4 address of RADIUS server
`X:X::X:X`	IPv6 address of RADIUS server
`HOSTNAME`	DNS host name of RADIUS server
`acct-port`	UDP port to use for RADIUS accounting messages
`<0-65535>`	Range of UDP port numbers
`timeout`	How long to wait for a response from the RADIUS server before declaring a timeout failure
`<1-60>`	Range of timeout period in seconds
`vrf`	Virtual Routing and Forwarding
`management`	Management VRF

Default

By default, radius-server login host acct-port is 1813

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#radius-server login host 192.168.2.3 vrf management acct-port 23255
```

radius-server login host auth-port

Use this command to configure a RADIUS server and specify a UDP port to use for RADIUS authentication messages.

Use the `no` form of this command to remove a RADIUS server.

Command Syntax

```
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (|(auth-
port <0-65535> (|(acct-port <0-65535> (|(timeout <1-60>))))))
```

```
no radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|)
(auth-port (|(acct-port (|timeout))))
```

Parameters

`login`	Remote login
`A.B.C.D`	IPv4 address of RADIUS server

X:X::X:X	IPv6 address of RADIUS server
HOSTNAME	DNS host name of RADIUS server
auth-port	UDP port to use for RADIUS accounting messages
<0-65535>	Range of UDP port numbers
acct-port	UDP port to use for RADIUS accounting messages
<0-65535>	Range of UDP port numbers
timeout	How long to wait for a response from the RADIUS server before declaring a timeout failure
<1-60>	Range of timeout period in seconds
vrf	Virtual Routing and Forwarding
management	Management VRF

Default

By default, radius-server login host acct-port is 1812

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#radius-server login host 203.0.113.15  vrf management auth-port 23255
```

radius-server login host key

Use this command to set per-server shared key (“shared secret”) which is a text string shared between the device and RADIUS servers.

Use the no form of this command to remove a server shared key.

Command Syntax

```
radius-server login host (A.B.C.D | X:X::X:X | HOSTNAME) (vrf management|) (|(key
  ((0 WORD) | (7 WORD) | (WORD)) (|(auth-port <0-65535> (|(acct-port <0-65535>
  (|(timeout <1-60>)))))))) no radius-server login host (A.B.C.D | X:X::X:X |
HOSTNAME) (vrf management|) (key

  ((0 WORD) | (7 WORD) | (WORD)) (|(auth-port <0-65535> (|(acct-port
  (|(timeout)))))))
```

Parameters

login	Remote login
A.B.C.D	IPv4 address of RADIUS server
X:X::X:X	IPv6 address of RADIUS server
HOSTNAME	DNS host name of RADIUS server
0	Unencrypted (clear text) shared key

WORD	Unencrypted key value; maximum length 63 characters
7	Hidden shared key
WORD	Hidden key value; maximum length 63 characters
WORD	Unencrypted (clear text) shared key value; maximum length 63 characters
auth-port	UDP port to use for RADIUS accounting messages
<0-65535>	Range of UDP port numbers
acct-port	UDP port to use for RADIUS accounting messages
<0-65535>	Range of UDP port numbers
timeout	How long to wait for a response from the RADIUS server before declaring a timeout failure
<1-60>	Range of timeout period in seconds
vrf	Virtual Routing and Forwarding
management	Management VRF

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced SWMRE version 1.3.2.

Examples

```
#configure terminal
(config)#radius-server login host 203.0.113.15 vrf management key 0
testing auth-port 23255
```

radius-server login key

Use this command to set a global preshared key (“shared secret”) which is a text string shared between the device and RADIUS servers.

Use the `no` form of this command to remove a global preshared key.

Command Syntax `radius-server login key ((0 WORD) | (7 WORD) | (WORD)) (vrf management|) no radius-server login key ((0 WORD) | (7 WORD) | (WORD)) (vrf management|)`

Parameters

`login`	Remote login
`0`	Unencrypted (clear text) shared key
`WORD`	Unencrypted key value; maximum length 63 characters
`7`	Hidden shared key
`WORD`	Hidden key value; maximum length 63 characters
`WORD`	Unencrypted (clear text) shared key value; maximum length 63 characters `vrf`
	Virtual Routing and Forwarding `management` Management VRF

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#radius-server login key 7 p2AcxlQA vrf management

#configure terminal
(config)#no radius-server login key 7 p2AcxlQA vrf management
```

radius-server login timeout

Use this command to set the global timeout which is how long the device waits for a response from a RADIUS server before declaring a timeout failure.

Use the `no` form of this command to set the global timeout to its default (1 second).

Command Syntax `radius-server login timeout <1-60> (vrf management|) no radius-server login timeout (vrf management|)`

Parameters

`login`	Remote login
`<1-1000>`	Range of timeout period in seconds
`vrf`	Virtual Routing and Forwarding
`management`	Management VRF

Default

By default, radius-server login timeout is 5 seconds

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#radius-server login timeout 15 vrf management

#configure terminal
(config)#no radius-server login timeout 15 vrf management
```

show debug radius

Use this command to display debugging information.

Command Syntax `show debug radius`

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show debug radius
```

show radius-server

Use this command to display the RADIUS server configuration.

Command Syntax `show radius-server (|vrf(management|all))((WORD)|(groups (GROUP|))|)|sorted`

Parameters

`WORD`	DNS host name or IP address
`groups`	RADIUS server group
`GROUP`	Group name; if this parameter is not specified, display all groups
`sorted`	Sort by RADIUS server name
`vrf`	management or all VRFs

Command Mode

Executive mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show radius-server
        VRF: default timeout value:
5

Total number of servers:1
```

Table 2-23 explains the output fields.

Table 2-23: show radius-server fields

Entry	Description
VRF	Virtual Routing and Forwarding (VRF) default support.
Timeout Value	Period the local router waits to receive a response from a RADIUS accounting server before retransmitting the message
Total number of servers	Number of authentication requests received by the authentication server.

show running-config radius

Use this command to display RADIUS configuration settings in the running configuration.

Command Syntax `show running-config radius`

Parameters

None

Command Mode

Executive mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show running-config radius
```

CHAPTER 3 TACACS+

Terminal Access Controller Access-Control System Plus (TACACS+, usually pronounced like tack-axe) is an access control network protocol for network devices.

The differences between RADIUS and TACACS+ can be summarized as follows:

- RADIUS combines authentication and authorization in a user profile, while TACACS+ provides separate authentication.
- RADIUS encrypts only the password in the access-request packet sent from the client to the server. The remainder of the packet is unencrypted. TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header.
- RADIUS uses UDP, while TACACS+ uses TCP.
- RADIUS is based on an open standard (RFC 2865). TACACS+ is proprietary to Cisco, although it is an open, publicly documented protocol (there is no RFC protocol specification for TACACS+).

Note: Only network administrators can execute these commands. For more, see the username command.

Note: The commands below are supported only on the “management” VRF. This chapter contains these commands:

- add policy
- debug tacacs+
- default
- deny
- feature dynamic-rbac enable
- feature tacacs+
- permit
- policy
- role
- show debug tacacs+
- show policy
- show rbac-role
- show running-config tacacs+
- show tacacs-server
- tacacs-server login host
- tacacs-server login key

add policy

Use this command to add a policy to a TACACS+ role-based authorization (RBAC) role.

Use the `no` form of this command to remove a policy from an RBAC role.

Command Syntax `add policy POLICY-NAME no add policy`

`POLICY-NAME`

Parameters

`POLICY-NAME` Name of the policy

Default

None

Command Mode

RBAC role mode

Applicability

This command was introduced in SWMRE version 1.3.5.

Examples

```
(config)#role myRole
(config-role)#default permit-all
(config-role)#add policy myPolicy1
(config-role)#no add policy myPolicy2
```

debug tacacs+

Use this command to display TACACS+ debugging information.

Use the `no` form of this command stop displaying TACACS+ debugging information.

Command Syntax `debug tacacs+ no debug tacacs+`

Parameters

None

Default

Disabled

Command Mode

Executive mode and configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#debug tacacs+
```

default

Use this command to set the default rule for a TACACS+ role-based authorization (RBAC) role.

Command Syntax `default (permit-all | deny-all)`

Parameters `permit-all` Permit all commands `deny-all`

Deny all commands

Default

Unless you explicitly give this command, the default rule for a role is `deny-all`.

Command Mode

RBAC role mode

Applicability

This command was introduced in SWMRE version 1.3.5.

Examples

```
(config)#role myRole
(config-role)#default permit-all
(config-role)#add policy myPolicy1
(config-role)#add policy myPolicy2
```

deny

Use this command to add a deny rule to a TACACS+ role-based authorization (RBAC) policy.

Use the `no` form of this command to remove a deny rule from an RBAC policy.

Command Syntax `deny RULE-STRING (mode MODE-NAME |) no deny RULE-STRING (mode MODE-NAME |)`

Parameters

`RULE-STRING`	Command string
`MODE-NAME`	Command prompt string such as “(config-router)” or “(config-if)’. Deny access to the command only in this mode.

Default

None

Command Mode

RBAC policy mode

Applicability

This command was introduced in SWMRE version 1.3.5.

Examples

```
#configure terminal
(config)#policy myPolicy
(config-policy)#deny "ip address" mode (config-if)
```

feature dynamic-rbac enable

Use this command to enable the TACACS+ role-based authorization (RBAC) feature.

Use the `no` form of this command to disable the RBAC feature.

Command Syntax `feature dynamic-rbac enable no feature dynamic-rbac enable`

Parameters

None

Default

By default, feature TACACS+ RBAC is disabled

Command Mode

Configure mode

Applicability

This command was introduced in SWMRE version 1.3.5.

Examples

```
#configure terminal
(config)#feature dynamic-rbac enable
```

feature tacacs+

Use this command to enable the TACACS+ feature.

Use the `no` form of this command to disable the TACACS+ feature.

Command Syntax `feature tacacs+ (vrf management|) no feature tacacs+ (vrf management|)`

Parameters `vrf` Virtual Routing and Forwarding `management` Management VRF

Default

By default, feature tacacs+ is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
                    (config)#feature tacacs+ vrf management
```

permit

Use this command to add a permit rule to a TACACS+ role-based authorization (RBAC) policy.

Use the `no` form of this command to remove a permit rule in an RBAC policy.

Command Syntax `permit RULE-STRING (mode MODE-NAME |) no permit RULE-STRING (mode MODE-NAME |)`

Parameters

`RULE-STRING`	Command string
`MODE-NAME`	Command prompt string such as “(config-router)” or “(config-if)”. Permit access to the command only in this mode.

Default

None

Command Mode

RBAC policy mode

Applicability

This command was introduced in SWMRE version 1.3.5.

Examples

```
#configure terminal
(config)#policy myPolicy
(config-policy)#permit “ip address” mode (config-if)
```

policy

Use this command to create a TACACS+ role-based authorization (RBAC) policy and enter RBAC policy mode.

Use the `no` form of this command to remove an RBAC policy.

Command Syntax `policy POLICY-NAME no policy POLICY-NAME`

Parameters

`POLICY-NAME` Policy name

Default

None

Command Mode

Configure mode

Applicability

This command was introduced in SWMRE version 1.3.5.

Examples

```
#configure terminal
(config)#policy myPolicy
(config-policy)#permit "ip address" mode (config-if)
```

role

Use this command to create a TACACS+ role-based authorization (RBAC) role and enter RBAC role mode.

Use the `no` form of this command to remove an RBAC role.

Command Syntax `role ROLE-NAME no role ROLE-NAME`

Parameters

`ROLE-NAME` Role name.

You *cannot* specify one of these roles already defined in SWMRE:

`network-admin network-user network-operator network-engineer`

For more about these built-in roles, see username.

Default

None

Command Mode

Configure mode

Applicability

This command was introduced in SWMRE version 1.3.5.

Examples

```
(config)#role myRole
(config-role)#default permit-all
(config-role)#add policy myPolicy1
(config-role)#add policy myPolicy2
```

show debug tacacs+

Use this command to display whether TACACS+ debugging is enabled.

Command Syntax `show debug tacacs+`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show debug tacacs+
```

show policy

Use this command to display TACACS+ role-based authorization (RBAC) policies.

Command Syntax `show policy (POLICY-NAME |)`

Parameters

`POLICY-NAME` Policy name

Default

None

Command Mode

Exec and privileged exec mode

Applicability

This command was introduced in SWMRE version 1.3.5.

Examples

```
#show policy myPolicy
```

show rbac-role

Use this command to display information about TACACS+ role-based authorization (RBAC) roles.

Command Syntax `show rbac-role (ROLE-NAME |)`

Parameters

`ROLE-NAME`	Role name

Default

None

Command Mode

Exec and privileged exec mode

Applicability

This command was introduced in SWMRE version 1.3.5.

Examples

```
#show rbac-role myRole
```

Table 3-24 explains the output fields.

Table 3-24: show rbac-role fields

Entry	Description
Role Name	Role name
Default rule	permit-all or deny-all
Attached Policies	Name of policies attached to this role

show running-config tacacs+

Use this command to display TACACS+ settings in the running configuration.

Command Syntax `show running-config tacacs+`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show running-config tacacs+ feature tacacs+ vrf management tacacs-server host
10.16.19.2 seq-num 1 vrf management key 7 "wawyanb"
```

Table 3-25 explains the output fields.

Table 3-25: show running-config fields

Entry	Description
TACAS server host	TACACS+ server Domain Name Server (DNS) name.
Seq-num	Sequence number of user authentication attempt with the TACACS+ server.
VRF Management	The management traffic using VPN Routing and Forwarding (VRFs).

show tacacs-server

Use this command to display the TACACS+ server configuration.

Command Syntax `show tacacs-server (|vrf (management|all))((WORD)|(groups (GROUP|))|(sorted)`

Parameters

WORD	DNS host name or IP address
groups	TACACS+ server group
GROUP	Group name; if this parameter is not specified, display all groups
sorted	Sort by TACACS+ server name
vrf	management or all VRFs

Command Mode

Executive mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show tacacs-server total
number of servers:1

 Tacacs+ Server                 : 192.168.10.215/49(*)
           Sequence Number      : 1
         Failed Auth Attempts   : 0
       Success Auth Attempts    : 14
     Failed Connect Attempts    : 0
  Last Successful authentication: 2017 December 18, 12:27:13 (*)

indicates last active.
```

Table 3-26 explains the output fields.

Table 3-26: show tacacs-server output fields

Field	Description
Sequence Number	Sequence number of user authentication attempt with the TACACS+ server.
Failed Auth Attempts	Number of times user authentication failed with the TACACS+ server. Increments for server key mismatches and password mismatches or wrong password for the user.
Success Auth Attempts	Number of times user authenticated with TACACS+ server. Increments for each successful login.

Table 3-26: show tacacs-server output fields

scription
mber of failed TCP socket connections to the TACACS+ server. rements for server connection failure cases such as server not-reachable, server port mismatches.
estamp when user successfully authenticated with the TACACS+ server.

tacacs-server login host

Use this command to set the TACACS+ server host name or IP address.

Use the `no` form of this command to remove an TACACS+ server (if only a host name or IP address is specified as a parameter) or to remove all of a TACACS+ server's configuration settings (if any other parameters are also specified).

Command Syntax

```
tacacs-server login host (HOSTNAME | X:X::X:X | A.B.C.D) (vrf management|) (seq-num
<1-8> |) (key ((0 WORD) | (7 WORD) | (WORD))|) (port <1025-65535> |) no tacacs-
server login host (HOSTNAME | A.B.C.D | X:X::X:X) (vrf management|) no tacacs-
server login host (HOSTNAME | X:X::X:X | A.B.C.D) (vrf management|) (key ((0 WORD)
| (7 WORD) | (WORD))|) (port <1025-65535> |)
```

Parameters

`HOSTNAME`	Host name
`X:X::X:X`	IPv6 address
`A.B.C.D`	IPv4 address
`vrf`	Virtual Routing and Forwarding
`management`	Management VRF
`seq-num`	Sequence Number / Priority index for tacacs-servers
`key`	Authentication and encryption key ("shared secret")
`0`	Unencrypted (clear text) shared key
`WORD`	Unencrypted key value; maximum length 63 characters
`7`	Hidden shared key
`WORD`	Hidden key value; maximum length 63 characters
`WORD`	Unencrypted (clear text) shared key value; maximum length 63 characters
`port`	TACACS+ server port
`<1205-65535>`	TACACS+ server port number; the default is 49

Default

Enable authentication for TACACS+ server configured. Authorization is also enabled by default. The default server port is 49.

There is no command to enable authorization. Authorization functionality is enabled by default when remote authentication is enabled with TACACS+.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
                        (config)#tacacs-server login host 203.0.113.31 vrf management
```

tacacs-server login key

Use this command to set a global preshared key (“shared secret”) which is a text string shared between the device and TACACS+ servers.

Use the `no` form of this command to remove a global preshared key.

Command Syntax `tacacs-server login key ((0 WORD) | (7 WORD) | (WORD)) (vrf management|) no tacacs-server login key ((0 WORD) | (7 WORD) | (WORD)) (vrf management|)`

Parameters

`0` Unencrypted (clear text) shared key

`WORD` Unencrypted key value; maximum length 63 characters

`7` Hidden shared key

`WORD` Hidden key value; maximum length 63 characters

`WORD` Unencrypted (clear text) shared key value; maximum length 63 characters `vrf` Virtual Routing and Forwarding `management` Management VRF

Default

Disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#tacacs-server login key 7 jvn05mlQH1 vrf management
```

CHAPTER 4 Lightweight Directory Access Protocol

This chapter describes Lightweight Directory Access Protocol (LDAP) commands.

LDAP is an protocol for accessing and maintaining distributed directory information services over an IP network. LDAP is specified is in RFC 4511.

For SWMRE, LDAP is used for authentication.

This chapter contains these commands:

- clear ldap-server statistics
- debug ldap
- feature ldap
- ldap-server deadtime
- ldap-server host
- ldap-server port
- ldap-server timeout
- show debug ldap
- show ldap-server
- show running-config ldap

clear ldap-server statistics

Use this command to reset the LDAP server statistics.

Command Syntax `clear ldap-server statistics (|HOST)`

Parameters

`HOST`	Server host name, IPv4 address, or IPv6 address; if not specified, all hosts are displayed

Command Mode

Exec mode

Examples

```
#clear ldap-server statistics
```

debug ldap

Use this command to display LDAP debugging information.

Use the `no` form of this command stop displaying LDAP debugging information.

Command Syntax

```
debug ldap (aaa-request | aaa-request-lowlevel | all | config | config-lowlevel |
  server-monitor | server-monitor-errors)

no debug ldap (aaa-request | aaa-request-lowlevel | all | config | config-lowlevel
  | server-monitor | server-monitor-errors)
```

Parameters `aaa-request` LDAP AAA requests `aaa-request-lowlevel` LDAP AAA low-level requests

`all` All

`config` LDAP configuration `config-lowlevel` LDAP low-level configuration

`server-monitor` LDAP server monitor `server-monitor-errors` LDAP server monitor errors

Command Mode

Executive mode and configure mode

Examples

```
#debug ldap
```

feature ldap

Use this command to enable LDAP on the device.

Use the `no` form of this command to disable LDAP.

Command Syntax `feature ldap no feature ldap`

Parameters

None

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#feature ldap
```

ldap-server deadtime

Use this command to set the LDAP server deadtime period which is the duration for which a non-reachable server is skipped.

Use the `no` form of this command to set the LDAP server deadtime period to zero.

Command Syntax `ldap-server deadtime`

```
<1-1440> no ldap-server deadtime
<1-1440>
```

Parameters

`<1-1440>`	LDAP server deadtime period in minutes

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#ldap-server deadtime 270
```

ldap-server host

Use this command to set the LDAP server host name or IP address.

Use the `no` form of this command to remove an LDAP server (if only a host name or IP address is specified as a parameter) or to remove all an LDAP server's configuration settings (if any other parameters are also specified).

Command Syntax `ldap-server host (HOSTNAME | A.B.C.D | X:X::X:X) ldap-server host (HOSTNAME | A.B.C.D | X:X::X:X) enable-ssl ldap-server host (HOSTNAME | A.B.C.D | X:X::X:X) timeout <1-60> ldap-server host (HOSTNAME | A.B.C.D | X:X::X:X) port <1-65535> (|timeout <1-60>) ldap-server host (HOSTNAME | A.B.C.D | X:X::X:X) rootDN ROOTDN (password WORD |)`

`(port <1-65535>|) (timeout <1-60>|) ldap-server host (HOSTNAME | A.B.C.D | X:X::X:X) test rootDN ROOTDN (username`

`WORD|) (password WORD |) (idle-time <1-1440> |) no ldap-server host (HOSTNAME | A.B.C.D | X:X::X:X) no ldap-server host (HOSTNAME | A.B.C.D | X:X::X:X) enable-ssl no ldap-server host (HOSTNAME | A.B.C.D | X:X::X:X) timeout <1-60> no ldap-server host (HOSTNAME | A.B.C.D | X:X::X:X) port <1-65535> (|timeout <1-`

`60>) no ldap-server host (HOSTNAME | A.B.C.D | X:X::X:X) rootDN ROOTDN (password WORD |)`

`(port <1-65535>|) (timeout <1-60>|) no ldap-server host (HOSTNAME | A.B.C.D | X:X::X:X) test rootDN (username WORD|) password WORD |) (idle-time <1-ROOTDN 1440> |)`

Parameters

`HOSTNAME` Host name

`A.B.C.D` IPv4 address `X:X::X:X` IPv6 address

`enable-ssl` Establish an SSL session before sending a bind or search request

`timeout` Period to wait for a response from the server before the client declares a timeout failure `<1-60>` Timeout value in seconds; the default is 5 seconds `port` LDAP server port `<1-65535>` LDAP server port number; the default is 389

`rootDN` Root Designated Name (DN) for the LDAP server database

`ROOTDN` Root Designated Name value; maximum length 128 characters `password` Bind password for root

WORD Password value; maximum length 32 characters test

Verify the LDAP server state username User name used in test packets

WORD	User name value; maximum length 32 characters
password	Password used in test packets
WORD	Password value; maximum length 32 characters
idle-time	If a response is not received after this time, the server is assumed dead
<1-1440>	Idle-time value; the default is 60

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#ldap-server host 203.0.113.132 timeout 10
```

ldap-server port

Use this command to set the port number on which the LDAP server listens for connections. The default port on which the LDAP server listens is 389.

You can only give this command when the LDAP server is enabled. See the feature ldap command.

USe the `no` form of this command to set the LDAP server port to its default value (389).

Command Syntax `ldap-server  port`

`<1-65535> no ldap-server port`

`<1-65535>`

Parameters

`<1-65535>`	Port number

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#ldap-server port 934
```

ldap-server timeout

Use this command to set the period to wait for a response from the server before the client declares a timeout failure. The default timeout value is 5 seconds.

You can only give this command when the LDAP feature is enabled. See the feature ldap command.

Use the `no` form of this command to set the timeout value to its default value (5 seconds).

Command Syntax `ldap-server timeout <1-60> no ldap-server timeout <1-60>`

Parameters

`<1-60>`	Timeout value in seconds

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#ldap-server timeout 35
```

show debug ldap

Use this command to display whether LDAP debugging is enabled.

You can only give this command when the LDAP server is enabled. See the feature ldap command.

Command Syntax `show debug ldap`

Parameters

None

Command Mode

Exec mode

Examples

```
#show debug ldap
```

show ldap-server

Use this command to display the LDAP server group configuration information.

Command Syntax `show ldap-server ((groups (GROUP|)|) | (statistics (HOST|)|))`

Parameters

`groups`	Groups
`GROUP`	Server group name; if not specified, all groups are displayed
`statistics`	Statistics
`HOST`	Server host name, IPv4 address, or IPv6 address; if not specified, all hosts are displayed

Command Mode

Exec mode

Examples

```
#show ldap-server groups
```

show running-config ldap

Use this command to display LDAP settings in the running configuration.

You can only give this command when the LDAP server is enabled. See the feature ldap command.

Command Syntax `show running-config ldap`

Parameters

None

Command Mode

Exec mode

Examples

```
#show running-config ldap
```

SECTION 3

Security Features

© Symanitron

Symanitron

Security Features Configuration Guide

Contents

This guide contains these chapters:

- Chapter 1, *DHCP Snooping*
- Chapter 2, *Proxy ARP and Local Proxy ARP*
- Chapter 3 *DHCP Snooping IP Source Guard*

CHAPTER 1 DHCP Snooping

Overview

DHCP snooping is a series of techniques applied to ensure the security of an existing DHCP infrastructure. It is a security feature that acts like a fire wall between untrusted hosts and trusted DHCP servers. It is a layer-2 security technology built into the operating system of a capable network switch that drops DHCP traffic determined to be unacceptable.

The fundamental use case of DHCP snooping is to prevent unauthorized (rogue) DHCP servers offering IP addresses to DHCP clients. Rogue DHCP servers are often used in 'man-in the middle' or 'Denial of Service' attacks from malicious purpose. Similarly DHCP clients (rogue) can also cause 'Denial of Service' attacks by continuously requesting for IP addresses causing address depletion in the DHCP server.

The DHCP snooping feature performs the following activities:

- Validates DHCP messages received from un-trusted sources and filters out invalid messages.
- Rate-limits DHCP traffic from trusted and un-trusted sources.
- Builds and maintains the DHCP snooping binding database, which contains information about un-trusted hosts with leased IP addresses.
- Utilizes the DHCP snooping binding database to validate subsequent requests from un-trusted hosts.

DHCP snooping is enabled on a per-VLAN basis. By default, the feature is inactive on all VLANs. You can enable the feature on a single VLAN or a range of VLANs.

Topology

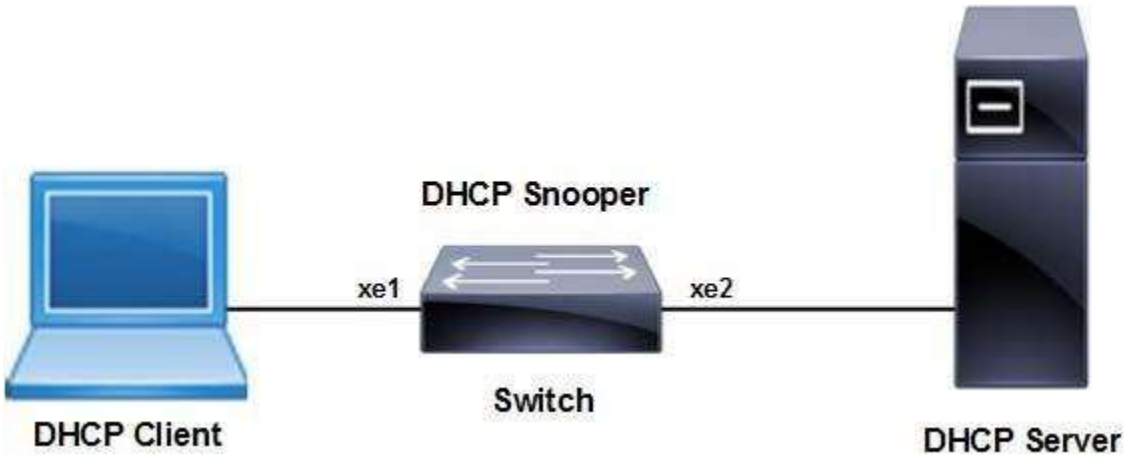


Figure 2-37: DHCP Snoop Topology

Configuration Guidelines

When configuring DHCP snooping, follow these guidelines:

DHCP Snooping

- DHCP snooping is not active until you enable the feature on at least one VLAN, and enable DHCP snooping globally on the switch.
- Before globally enabling DHCP snooping on the switch, make sure that the device acting as the DHCP server is configured and enabled.
- If a Layer 2 LAN port is connected to a DHCP server, configure the port as trusted by entering the `ip dhcp snooping trust interface` configuration command.
- If a Layer 2 LAN port is connected to a DHCP client, configure the port as un-trusted by entering the `no ip dhcp snooping trust interface` configuration command.

Procedures

The following subsections provide examples of how to enable and configure DHCP Snooping.

Enable DHCP Snooping Globally

`#configure terminal`	Enter Configure mode.
`(config)#bridge 1 protocol mstp`	Create mstp or ieee vlan-bridge.
`(config)#ip dhcp snooping bridge 1`	Enable DHCP Snooping on the bridge

Enable DHCP Snooping on a VLAN

`configure terminal`	Enter Configure mode.
`(config)#vlan 2 bridge 1`	Configure a vlan for the bridge.
`(config)#ip dhcp snooping vlan 2 bridge 1`	Enable DHCP Snooping on the vlan 2

Configuring the ports connected to DHCP server and DHCP client

`#configure terminal`	Enter the configure mode
`(config)#interface xe1`	Specify the interface xe1 to be configured, and enter the `Interface` mode
`(config-if)#switchport`	Configure the interface as a switch port.
`(config-if)#bridge-group 1`	Associate the interface `xe1` with bridge-group `1`.
`(config-if)#switchport mode access`	Configure the port as an access port
`(config-if)#switchport access vlan 2`	Bind the interface vlan 2 to the port.
`(config-if)#exit`	Exit the `Interface` mode.

(config)#interface xe2	Specify interface xe2 to be configured connected to server.
(config-if)#switchport	Configure the interface as a switch port.
(config-if)#bridge-group 1	Associate interface xe2 with bridge-group 1.

(config-if)#switchport mode access	Configure the port as an access port.
(config-if)#switchport access vlan 2	Bind the interface vlan 2 to the port.
(config-if)#exit	Exit the Interface mode.
(config)#exit	Exit the config mode.

Configuring Trusted and Un-trusted Ports

Usually the port connected to server is configured as trusted port and the ports connected to client is configured as untrusted port

In this example, xe1 is connected to the DHCP client and xe2 is connected to the DHCP server.

- Configure xe1 connected to DHCP client as un-trusted port.
- Configure xe2 connected to the DHCP server as trusted port.

#configure terminal	Enter Configure mode.
(config)#interface xe1	Specify the interface to be configured
(config-if)#no ip dhcp snooping trust	Disable the port as trusted.

DHCP Snooping Operation

1. Configure DHCP server that is connected to DHCP Snooper through trusted port.
2. Request an ip address from the DHCP client connected through the un-trusted port.
3. DHCP client broadcast the DHCP DISCOVER message to the switch.
4. DHCP server responds to the DHCP DISCOVER message with DHCP offer message to the client.
5. Once the DHCP OFFER is received by the client, it sends an DHCP REQUEST to the server.
6. DHCP server validates the request from the client and sends DHCP ACK with the offered ip address to the client with the lease time.
7. DHCP Snooper creates an entry for the above operation into the binding table which includes the MAC address of the host, the leased IP address, the lease time, the binding type, and the VLAN number and interface information associated with the host.
8. DHCP Snooper clears the entry in the binding table once the client sends the DHCP RELEASE query.

Validation

The show running-config ip dhcp snooping command displays the DHCP snooping commands configured on the device in question.

```
#show running-config ip dhcp snooping !
!
```

DHCP Snooping

```
ip dhcp snooping bridge 1 ip dhcp
snooping vlan 2 bridge 1 interface
xe2  ip dhcp snooping trust !
```

The `show ip dhcp snooping bridge 1` command displays the configured information about DHCP Snooping. `#show ip dhcp snooping bridge 1`

```
Bridge Group                                          : 1
DHCP snooping is                                      : Enabled
DHCP snooping option82 is                             : Disabled
Verification of hwaddr field is                       : Disabled
Rate limit(pps)                                       : 100
DHCP snooping is configured on following VLANs        : 2
DHCP snooping is operational on following VLANs       : 2
```

DHCP snooping trust is configured on the following Interfaces

```
Interface               Trusted --
-------------          ------xe1
No xe2                      Yes
```

The `show ip dhcp snooping binding bridge 1` command displays the binding table entries associated with un-trusted interfaces.

```
#show ip dhcp snooping binding bridge 1

Total number of static IPV4 entries : 1
Total number of dynamic IPV4 entries : 0
Total number of static IPV6 entries : 0
Total number of dynamic IPV6 entries : 0
MacAddress     IpAddress    Lease(sec)     Type                  VLAN    Interface
------------------  ---------------   ---------------- ---------------------  ---------
-  -------------

0002.a54e.c279    3.4.5.1        300           dhcp-snooping      1           xe1
```

CHAPTER 2 Proxy ARP and Local Proxy ARP

Overview

Proxy ARP (RFC 1027) is a technique by which a device on a given network answers the ARP queries for a network address that is not on that network. The Proxy ARP is aware of the location of the traffic's destination, and offers its own MAC address as destination. The captured traffic is then typically routed by the Proxy to the intended destination via another interface. Proxy ARP can help machines on a subnet reach remote subnets without the need to configure routing or a default gateway.

Use `no ip proxy-arp` to disable Proxy ARP, Proxy ARP is disabled by default.

Topology

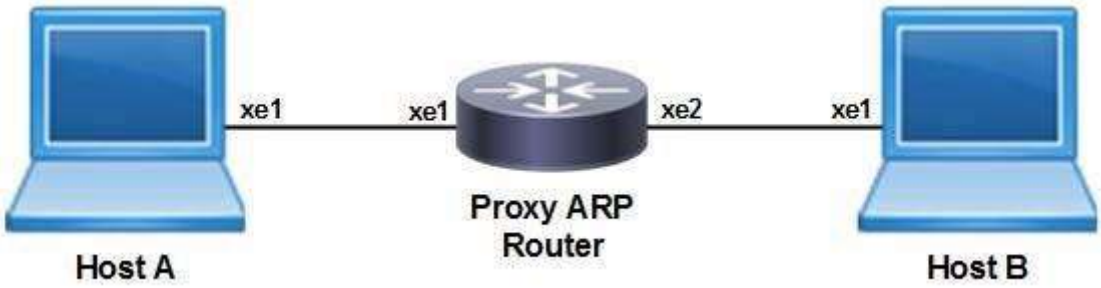


Figure 3-38: Sample topology

Host A:

`#configure terminal`	Enter Configure mode.
`(config)#interface xe1`	Specify the interface to be configured on Host A
`(config-if)#ip address 20.20.0.2/16`	Configure the ip address on the interface
`(config)#end`	Exit interface and configure mode

Host B:

`#configure terminal`	Enter Configure mode
`(config)#interface xe1`	Specify the interface to be configured on Host B
`(config-if)#ip address 20.20.1.2/24`	Configure the ip address on the interface
`(config)#end`	Exit interface and configure mode

Enable Proxy ARP:

`#configure terminal`	Enter Configure mode.
`(config)#interface xe1`	Specify the interface connected to Host A
`(config-if)#ip address 20.20.0.1/24`	Configure the ip address on the interface
`(config-if)#interface xe2`	Specify the interface connected to Host B
`(config-if)#ip address 20.20.1.1/24`	Configure the ip address on the interface

(config-if)#interface xe1	Specify the interface to configure Proxy ARP
(config-if)#ip proxy-arp	Enable Proxy ARP
(config)#end	Exit interface and configure mode

Validation

```
#show running-config arp
! interface xe1
ip proxy-arp !
```

The `show arp` command on the hosts shows the arp table entries to reach different subnets. Ping Host B from Host A.Host A. The ARP table should have Router's xe1 interface MAC address to reach Host B. Execute the below command at Host A.

```
#show arp

Flags: D - Static Adjacencies attached to down interface

IP ARP Table for context default
Total number of entries: 2
Address          Age          MAC Address     Interface    State
20.20.0.3       00:02:39     ecf4.bbc0.3d71       xe1       STALE.
```

Local Proxy ARP Overview

Local Proxy ARP feature is used to enable local proxy support for ARP requests per interface level. Activation will make the router answer all ARP requests on configured subnet, even for clients that should not normally need routing. Local proxy ARP means that the traffic comes in and goes out the same interface.

The local proxy ARP feature allows responding to ARP requests for IP addresses within a subnet where normally no routing is required. With the local proxy ARP feature enabled, ARP responds to all ARP requests for IP addresses within the subnet and forwards all traffic between hosts in the subnet. Use this feature only on subnets where hosts are intentionally prevented from communicating directly.

Topology

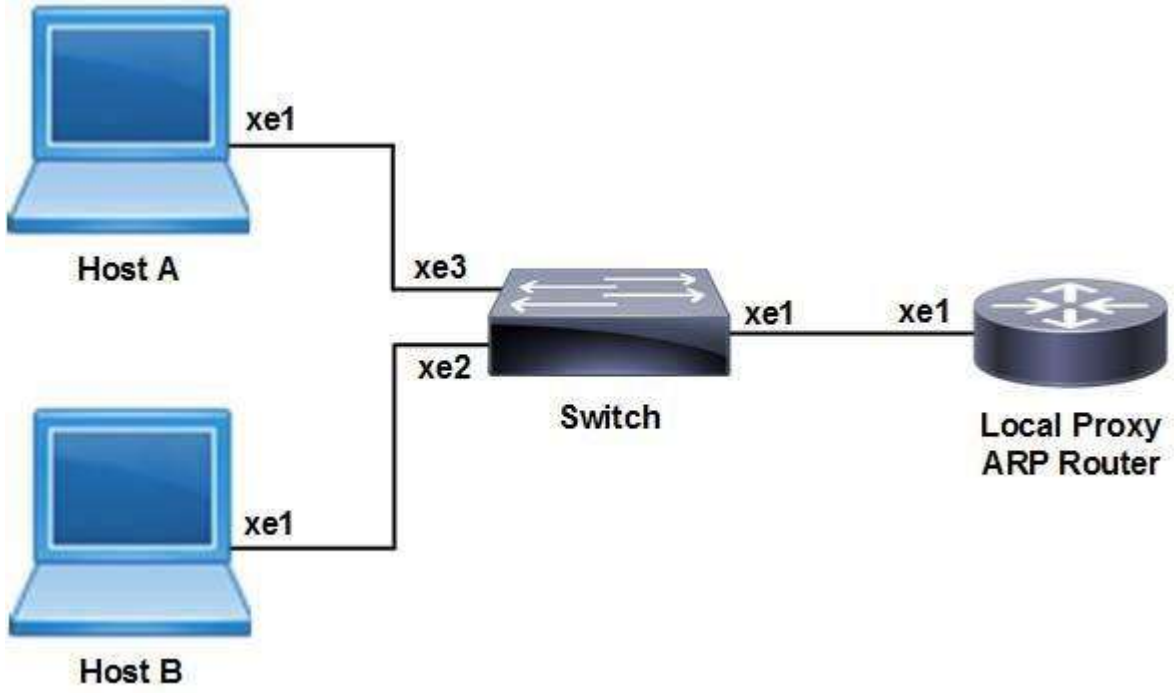


Figure 3-39: Sample topology

Host A:

`#configure terminal`	Enter Configure mode.
`(config)#interface xe1`	Specify the interface to be configured on Host A
`(config-if)#ip address 20.20.0.2/16`	Configure the ip address on the interface
`(config)#end`	Exit interface and configure mode

Host B:

`#configure terminal`	Enter Configure mode
`(config)#interface xe1`	Specify the interface to be configured on Host B
`(config-if)#ip address 20.20.0.3/24`	Configure the ip address on the interface
`(config)#end`	Exit interface and configure mode

Private Vlan Configuration on Switch:

`#configure terminal`	Enter Configure mode.
`(config)# bridge 1 protocol ieee vlan-bridge`	Create ieee vlan-bridge on switch for pvlan configuration
`(config)# vlan database`	Enter into the vlan database
`(config-vlan)# vlan 100-101 bridge 1 state enable`	Create vlans 100 and 101 as part of bridge 1
`(config-vlan)# private-vlan 100 primary bridge 1`	Configure vlan 100 as a primary vlan
`(config-vlan)# private-vlan 101 isolated bridge 1`	Configure vlan 101 as a isolated vlan
`(config-vlan)# private-vlan 100 association add 101 bridge 1`	Associate secondary vlan 101 to primary vlan 100

(config-vlan)#exit	Exit from the vlan database
(config)#interface xe1	Specify the interface to be configured
(config-if)#switchport	Configure xe1 as a layer2 interface.
(config-if)#bridge-group 1	Associate the interface to the bridge
(config-if)#switchport access vlan 100	Associate primary vlan to the interface
(config-if)#switchport mode private-vlan promiscuous	Configure xe1 interface as a promiscuous port
(config-if)# switchport private-vlan mapping 100 add 101	Associate primary vlan 100 and secondary vlan 101 to a promiscuous port
(config-if)# exit	Exit interface mode
(config)#interface xe2	Specify the interface to be configured
(config-if)#switchport	Configure xe2 as a layer2 interface.
(config-if)#bridge-group 1	Associate the interface to the bridge
(config-if)#switchport access vlan 100	Associate primary vlan to the interface
(config-if)#switchport mode private-vlan promiscuous	Configure xe2 interface as a promiscuous port
(config-if)# switchport private-vlan mapping 100 add 101	Associate primary vlan 100 and secondary vlan 101 to a promiscuous port
(config-if)# exit	Exit interface mode
(config)#interface xe3	Specify the interface to be configured
(config-if)#switchport	Configure xe3 as a layer2 interface.
(config-if)#bridge-group 1	Associate the interface to the bridge
(config-if)#switchport access vlan 100	Associate primary vlan to the interface
(config-if)#switchport mode private-vlan promiscuous	Configure xe2 interface as a promiscuous port
(config-if)# switchport private-vlan mapping 100 add 101	Associate primary vlan 100 and secondary vlan 101 to a promiscuous port
(config-if)# exit	Exit interface mode

Enable Local Proxy ARP on Router:

#configure terminal	Enter Configure mode
(config)#interface xe1	Specify the interface to be configured on Host B
(config-if)#ip address 20.20.0.3/24	Configure the ip address on the interface
(config-if)#ip local-proxy-arp	Enable Local Proxy ARP
(config)#end	Exit interface and configure mode

Validation

ARP cache on Host A and Host B

The show arp command on hosts shows the arp table entries to reach different subnets. Ping Host B from Host A.Host A ARP table should have Router's xe1 interface MAC address to reach Host B. Execute the below command at Host A.

```
#show arp

Flags: D - Static Adjacencies attached to down interface

IP ARP Table for context default
Total number of entries: 2
Address          Age          MAC Address     Interface    State 20.20.0.3
00:02:39      ecf4.bbc0.3d71      xe1       STALE.
```

CHAPTER 3 DHCP Snooping IP Source Guard

Overview

IPSG is a security feature that restricts IP traffic on non-routed, Layer 2 interfaces by filtering traffic based on the DHCP snooping binding database and on manually configured IP source bindings. Use IP source guard to prevent traffic attacks if a host tries to use the IP address of its neighbor.

Enable IP source guard when DHCP snooping is enabled on an untrusted interface. After IPSG is enabled on an interface, the switch blocks all IP traffic received on the interface except for DHCP packets allowed by DHCP snooping. A port access control list (ACL) is applied to the interface. The port ACL allows only IP traffic with a source IP address in the IP source binding table and denies all other traffic.

Topology

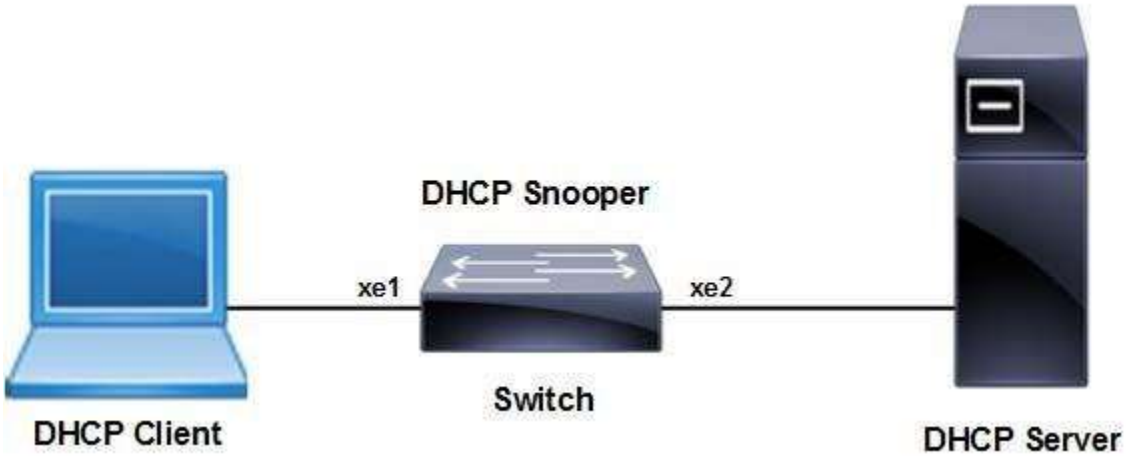


Figure 4-40: IP Source Guard Topology

Configuring the Switch

`#configure terminal`	Enter the configure mode
`(config)#bridge 1 protocol ieee vlan-bridge`	Create IEEE VLAN bridge 1.
`(config)#vlan 2 bridge 1 state enable`	Create VLAN 2.
`(config)# ip dhcp snooping bridge 1`	Configure DHCP snooping for bridge 1
`(config)# ip dhcp snooping information option bridge 1`	Configure DHCP snooping information option 82
`(config)# ip dhcp snooping ratelimit 0`	Configure DHCP snooping ratelimit. Default value is 100
`(config)# ip dhcp snooping vlan 2 bridge 1`	Configure DHCP snooping for vlan 2 for bridge 1

(config)# ip dhcp snooping verify macaddress bridge 1	Configure DHCP snooping verify mac-address
(config)#interface xe2	Enter Interface Mode
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode access	Set the Layer2 interface as Access. (It can be Trunk mode also)
(config-if)#switchport access vlan 2	Set the default VLAN for the interface
(config-if)#ip dhcp snooping trust	Configuring the interface as Trust. Basically this is configured on the interface which is connected to Server Side.
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter Interface Mode
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode access	Set the Layer2 interface as Access. (It can be Trunk mode also)
(config-if)#switchport access vlan 2	Set the default VLAN for the interface
(config-if)#ip verify source dhcp-snoopingvlan	Configuring IP source guard at Interface level and configured on the interface which is connected to client side
(config-if)#ip verify source access-group mode merge	Merge IPSG policy with other ACL
(config-if)#exit	Exit interface mode
(config)#ip dhcp snooping binding bridge 1 0011.1111.2222 2 ipv4 1.1.1.1 xe1	Configure Ipv4 Static Entry For DHCP snooping with MAC address and Source Address for an interface and vlan configured
(config)#ip dhcp snooping binding bridge 1 0022.2222.3333 2 ipv6 3ffe::1 xe1	Configure Ipv6 Static Entry For DHCP snooping with MAC address and Source Address for an interface and vlan configured
(config)#ip source binding ipv4 1.1.1.1 0011.1111.2222 vlan 2 interface xe1 bridge 1	Configure static IP source guard entry for ipv4 entries
(config)#ip source binding ipv6 3ffe::2 0022.2222.3333 vlan 2 interface xe1 bridge 1	Configure static IP source guard entry for ipv6 entries
(config)#exit	Exit config mode
#clear ip dhcp snooping binding bridge 1	Clear DHCP binding tables which are learned dynamically

Configuring Trusted and Un-trusted Ports

Usually the port connected to server is configured as trusted port and the ports connected to client is configured as untrusted port

In this example, xe1 is connected to the DHCP client and xe2 is connected to the DHCP server.

- Configure xe1 connected to DHCP client as un-trusted port.
- Configure xe2 connected to the DHCP server as trusted port.

#configure terminal	Enter Configure mode.
(config)#interface xe1	Specify the interface to be configured
(config-if)#no ip dhcp snooping trust	Disable the port as trusted.
(config-if)#exit	Exit interface mode
(config)#interface xe2	Specify the interface to be configured
(config-if)#ip dhcp snooping trust	Enable the port as trusted.
(config-if)#exit	Exit interface mode

Configuring IP Source Guard on LAG Port

#configure terminal	Enter the configure mode
(config)#interface xe2	Enter Interface Mode
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode access	Set the Layer2 interface as Access. (It can be Trunk mode also)
(config-if)#switchport access vlan 2	Set the default VLAN for the interface
(config-if)#ip dhcp snooping trust	Configuring the interface as Trust. Basically this is configured on the interface which is connected to Server Side.
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter Interface Mode
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode access	Set the Layer2 interface as Access. (It can be Trunk mode also)
(config-if)#switchport access vlan 2	Set the default VLAN for the interface
(config-if)#static-channel-group 2	Configure Static Channel lag on the interface
(config-if)#exit	Exit interface mode
(config)#interface sa1	Enter Interface Mode
(config-if)#ip verify source dhcp-snoopingvlan	Configuring IP source guard at Interface level and configured on the interface which is connected to client side
(config-if)#ip verify source access-group mode merge	Merge IPSG policy with other ACL
(config-if)#exit	Exit interface mode
(config)#ip dhcp snooping binding bridge 1 0011.1111.2222 2 ipv4 1.1.1.1 sa1	Configure Ipv4 Static Entry For DHCP snooping with MAC address and Source Address for lag interface and vlan configured
(config)#ip dhcp snooping binding bridge 1 0022.2222.3333 2 ipv6 3ffe::1 sa1	Configure Ipv6 Static Entry For DHCP snooping with MAC address and Source Address for lag interface and vlan configured

(config)#ip source binding ipv4 1.1.1.1 0011.1111.2222 vlan 2 interface sa1 bridge 1	Configure static IP source guard entry for ipv4 entries with lag interface
(config)#ip source binding ipv6 3ffe::2 0022.2222.3333 vlan 2 interface sa1 bridge 1	Configure static IP source guard entry for ipv6 entries with lag interface
(config)#exit	Exit config mode
#clear ip dhcp snooping binding bridge 1	Clear DHCP binding tables which are learned dynamically

Validation

Verify the dhcp snooping is enabled on the bridge

```
#sh ip dhcp snooping bridge 1
Bridge Group                                          : 1
DHCP snooping is                                      : Enabled
DHCP snooping option82 is                             : Enabled
Verification of hwaddr field is                       : Enabled
Rate limit (pps)                                      : 0
DHCP snooping is configured on following VLANs        : 2
DHCP snooping is operational on following VLANs       : 2
DHCP snooping trust is configured on the following Interfaces
Interface               Trusted -----
----------          ------xe2
Yes
DHCP snooping IP Source Guard is configured on the following Interfaces
Interface               Source Guard -----
----------          -----------xe1
Yes
```

Verify the static dhcp snooping entries configured for the bridge

```
#sh ip dhcp snooping binding bridge 1
Total number of static IPV4 entries                    : 1
Total number of dynamic IPV4 entries                   : 0
Total number of static IPV6 entries                    : 1
Total number of dynamic IPV6 entries                   : 0

MacAddress           IpAddress         Lease(sec) Type            VLAN   Interface
------------------   ---------------   ---------- -------------   ----   ---------------
0011.1111.2222       1.1.1.1           0          static          2      xe1
0022.2222.3333       3ffe::1           0          static          2      xe1
```

Verify the static IP dhcp snooping source guard entries configured for the bridge

```
#sh ip dhcp snooping source binding bridge 1
Total number of static source IPV4 entries             : 1
Total number of static source IPV6 entries             : 1
MacAddress           IpAddress         Lease (sec) Type            VLAN   Interface ------
------------   ---------------   ---------- -------------   ----   --------------
----
```

```
 0011.1111.2222       1.1.1.1           0         static           2     xe1
 0022.2222.3333       3ffe::2           0         static           2     xe1
```

Verify the dhcp snooping is enabled on the bridge with static lag interface

```
#sh ip dhcp snooping bridge 1
Bridge Group                                          : 1
DHCP snooping is                                      : Enabled
DHCP snooping option82 is                             : Enabled
Verification of hwaddr field is                       : Enabled
Rate limit(pps)                                       : 0
DHCP snooping is configured on following VLANs        : 2
DHCP snooping is operational on following VLANs       : 2
DHCP snooping trust is configured on the following Interfaces
Interface                Trusted
---------------          -------
Xe2                     Yes
DHCP snooping IP Source Guard is configured on the following Interfaces
Interface                Source Guard -----
----------          -----------sa2
Yes
```

Verify the static dhcp snooping or source guard entries configured for the bridge with lag interface

```
#sh ip dhcp snooping binding bridge 1
Total number of static IPV4 entries                   : 1
Total number of dynamic IPV4 entries                  : 0
Total number of static IPV6 entries                   : 1
Total number of dynamic IPV6 entries                  : 0
MacAddress           IpAddress         Lease(sec) Type            VLAN   Interface -------
-----------    ---------------   ---------- -------------   ----   --------------
----
0011.1111.2222       1.1.1.1           0          static          2      sa2
0022.2222.3333       3ffe::1           0          static          2      sa2

#sh ip dhcp snooping source binding bridge 1
Total number of static source IPV4 entries            : 1
Total number of static source IPV6 entries            : 1
MacAddress           IpAddress         Lease(sec) Type            VLAN   Interface -------
-----------    ---------------   ---------- -------------   ----   --------------
----
0011.1111.2222       1.1.1.1           0          static          2      sa2 0022.2222.3333
3ffe::2           0         static           2     sa2
```

SECTION 4 System Configuration

Hybrid Switch Router Configuration Guide

Contents

This guide contains these chapters:

- Chapter 1, *Hybrid Switching Overview*
- Chapter 2, *Hybrid Switch Router Configuration*

CHAPTER 1 Hybrid Switching Overview

An SWMRE Hybrid Switch Router offers Layer 3 forwarding found in routers with the high-speed performance associated with traditional Layer 2 switches. The following are some advantages of Hybrid Switch Routers:

- Reduced system cost and infrastructure. Traditionally you would require a separate box for switching and one for routing.
- Off-loading IP traffic from backbone routers, thus making them more efficient for firewalls and WAN connectivity.
- Simplified network design and maintenance.

Routing and Switching

Layer 2 and Layer 3 switches are similar at a high-level, both look at the packet headers, and steer the packets toward their destination port. Therefore, after being passed through a switch or router, the packet is closer to its destination.

Layer 2 Switching

Layer 2 switches are typically used to provide connectivity within high bandwidth local area networks (LANs). A Layer 2 switch makes forwarding decisions based on the MAC or the Layer 2 header. It extracts the Layer 2 header from the packet, finds a matching destination address in the forwarding table, and transmits the packet out to the port associated with the specific destination address in the forwarding table. The forwarding table is populated through a self-learning process, whereby each arriving packet is used to update the entries in the table. Typically, the Layer 2 switch implements the switching function in the hardware, as that requires stripping of the packet only in two layers (the physical and data link layer) to get to the useful part of the packet header. This allows switches to steer packets at wirespeed rates without slowing down arriving streams of packets to process them.

Layer 3 Routing

Layer 3 (L3) routers are typically used to provide connectivity between different LANs. A Layer 3 router discards MAC headers, and indexes further into the packet–making decisions based on the IP or Layer 3 header. It extracts the Layer-3 header from the packet, finds a matching destination address in a routing table, identifies a new MAC address for the packet from an ARP cache, wraps the IP packet in a new MAC header, and then transmits the packet out to the port associated with that destination address in the routing table.

The routing table is populated through statically configured command line interface entries or through routing protocol messages from neighboring routers. A Layer 3 router must strip through 3 layers (physical, data link, and network) which is more complicated than a Layer 2 switch. Layer 3 routers historically implement the routing function in software. This often results in limited packet-forwarding rates. However, improvements in VLSI circuit technology have allowed Layer 3 routing functions to be implemented rapidly in hardware, enabling wire-speed performance similar to the performance of Layer 2 switches. As a result, along with the complexity of next-generation Layer 3 routers, the throughput of these routers has also been increasing.

An architecture is required that is flexible enough to accommodate the demands of different customers, and accommodate the changing demands of a single customer whose requirements may change over time. Typical Layer 2 switches and Layer 3 routers fail to provide this flexibility.

An optimal configuration can be an integrated solution, a Layer 3 router with Layer 2 bridge groups around it. The SWMRE Hybrid Switch Router implementation allows easy configuration of different combinations of routers and switches. SWMRE can be configured as an absolute Layer 3 router, absolute Layer 2 switch (Figure 1-41) or a hybrid Layer 2/Layer 3 switch router, (Figure 1-42) that can easily change modes with the use of a single command.

Hybrid Switching Overview

System Configuration

- SWMRE stack will bring up all the ports of the board as routed ports by default.
- However SWMRE provides flexibility to create a Layer 2 bridge, and ports can be converted to switch ports and added to the bridge.
- SWMRE also supports VLAN interfaces and routing between VLANs.

Thus it can work as a router, a switch, or as a hybrid switch.

Hybrid Switch Router Possibilities

With only Layer 2 protocols configured, the SWMRE Hybrid Switch Router can become an absolute Layer 2 switch.

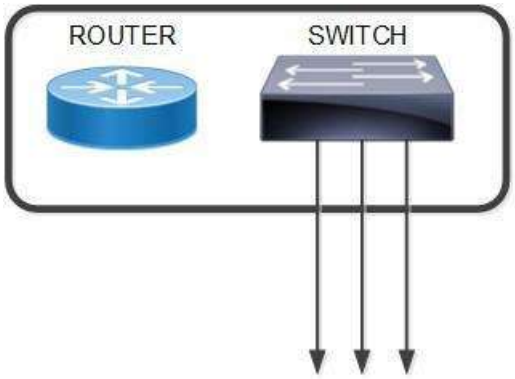


Figure 1-41: Layer 2 Switch

With Layer 2 and Layer 3 protocols configured, the SWMRE Hybrid Switch Router can become a Switch and/or a Router.

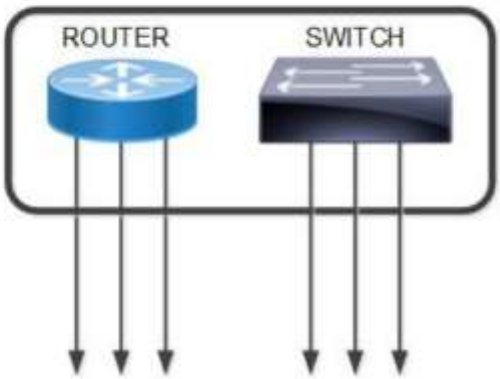


Figure 1-42: Working as a Router or a Switch

Hybrid Switching Overview

With only Layer 3 protocols enabled, the SWMRE Hybrid Switch Router can become an absolute router.

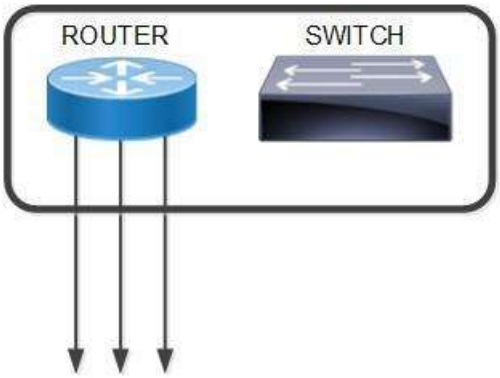


Figure 1-43: Working as Layer 3

Router On switch ports, VLANs can be created for different broadcast domains.

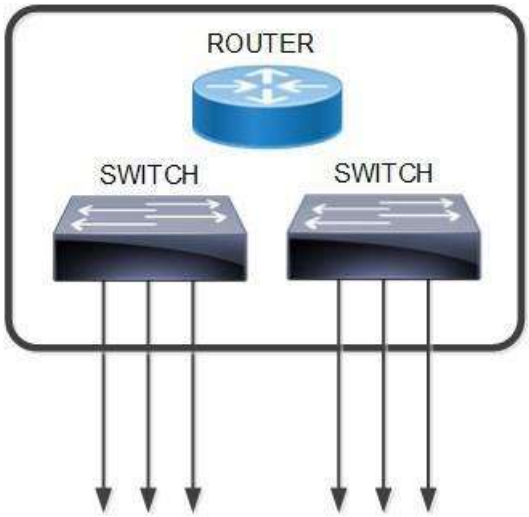


Figure 1-44: Port- or Policy-based VLANs

For routing between VLANs, the SWMRE routing protocols or static routing via NSM can be utilized.

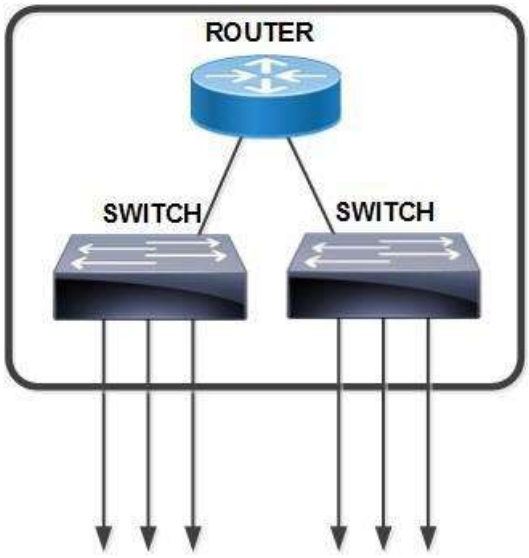


Figure 1-45: Routing between VLANs

For routing between VLANs and other routing ports, SWMRE routing protocols or static routing via NSM can be utilized.

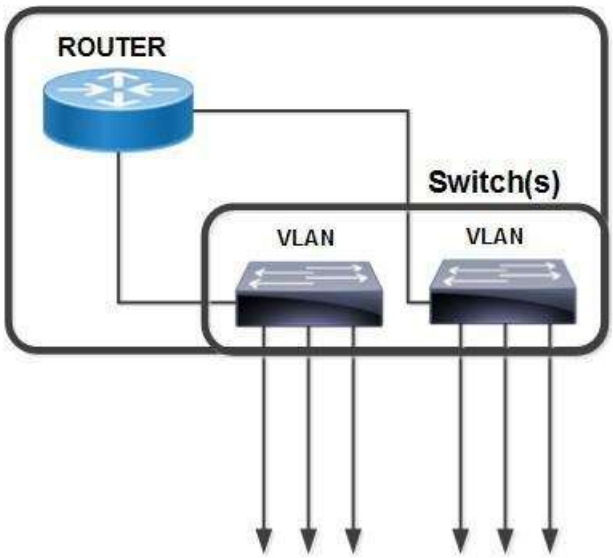


Figure 1-46: Routing between VLANs and Routing Ports

CHAPTER 2 Hybrid Switch Router Configuration

This chapter describes various configurations that can be done with the Hybrid Switch Router solution. SWMRE can be configured as a Layer 2 switch, a Layer 3 router or a Hybrid Switch Router.

Configuring a Hybrid Switch Router

When a port changes from a switched port to a routed port, an `Interface Delete` message is sent to the Layer 2 protocols and an `Interface Add` message is sent to the Layer 3 protocols. The following figure shows the port, changing from a switched port to routed port:

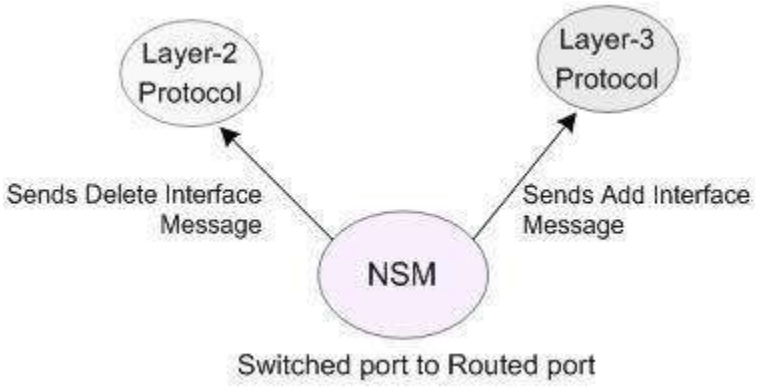


Figure 2-47: Switched Port to Routed Port

When a port changes from a routed port to a switched port, an `Interface Delete` message is sent to the Layer 3 protocols and an `Interface Add` message is sent to the Layer 2 protocols. In this case, all properties of the Layer 3 interfaces are deleted: for instance, this interface is deleted from all Layer 3 management, all routes pointing to this interface are invalidated, and IP addresses are deleted.

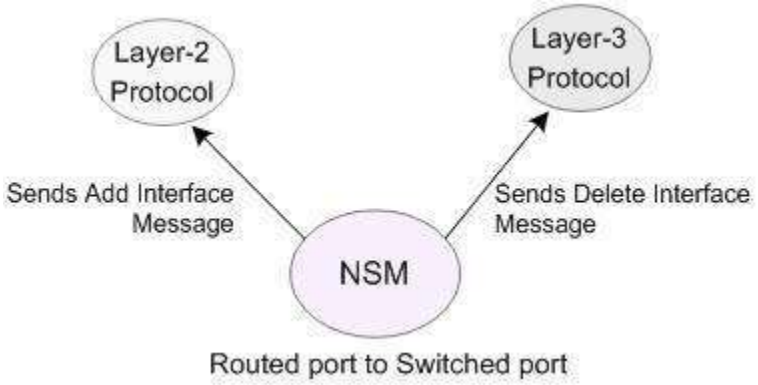


Figure 2-48: Routed Port to Switched Port

Configuring Layer 2 Interfaces

For the Hybrid Switch Router, it is important to understand that by default, all interfaces are configured as routed interfaces. To configure a Layer 2 interface (switched interface), you must explicitly configure this using the `switchport` command in the interface mode. For example:

Hybrid Switch Router Configuration

`#configure terminal`	Enter the Configure mode.
`(config)#bridge 1 protocol mstp`	Create a MSTP bridge.

(config)#interface eth2	Specify an interface to configure and enter the Interface mode.
(config-if)#switchport	Configure eth2 as a Layer 2 port.
(config-if)#bridge-group 1	Associate interface to bridge 1.
(config-if)#no shutdown	Start interface.eth2

Configuring Layer 3 Interfaces

For the Hybrid Switch Router, it is important to understand that by default, all interfaces in SWMRE are L3 ports. If a port has been configured as L2, then use the `no switchport` command to make it a L3 port.

For example:

#configure terminal	Enter the Configure mode.
(config)#interface eth3	Specify an interface to configure and enter the Interface mode.
(config-if)#no switchport	Configure eth3 as a Layer 3 port.

In the Hybrid Switch Router mode, if a VLAN is configured, a Layer 3 interface based on the bridge-group number and VLAN ID is created. This Layer 3 interface is advertised to all the Layer 3 protocols. For example:

#configure terminal	Enter the Configure mode.
(config)#bridge 1 protocol mstp	Creating bridge.
(config)#vlan database	Enter the VLAN configuration mode.
(config-vlan)#vlan 2 bridge 1	Enable VLAN 2 on bridge 1.

The last step in the example above show an interface given a name with the following format:

```
vlanXX.YYYY
```

Where `XX` is the bridge ID, and `YYYY` is the VLAN ID,

For example, the name, `vlan1.3` indicates that VLAN IP's interface is in VLAN 3, and bridge-group 1.

Integrated Management Interface Command Reference

Contents

This document contains these chapters:

- Chapter 1, *Common IMI Commands*
- Chapter 2, *IMI Shell Commands*
- Chapter 3, *VLOG Commands*
- Chapter 4, *System Commands*
- Chapter 5, *Licensing and Upgrade Commands*

© Symanitron

CHAPTER 1 Common IMI Commands

This chapter describes common Integration Management Interface (IMI) commands.

- banner motd
- configure terminal
- configure terminal force
- copy running-config startup-config
- disable
- enable
- enable password
- end
- exec-timeout
- exit
- help
- history
- hostname
- line console
- line vty
- logging cli
- logout • quit
- reload
- service advanced-vty
- service password-encryption
- service terminal-length
- show clock
- show cli history
- show logging cli
- show process
- show running-config
- show running-config access-list
- show running-config as-path access-list
- show running-config community-list
- show running-config interface igmp
- show running-config interface multicast
- show running-config prefix-list
- show running-config vrf
- show tcp

- show users
- terminal length
- terminal monitor
- write

© Symanitron Proprietary

banner motd

Use this command to set the message of the day (motd) at login.

After giving this command, you must write to memory using the write command. If you do not write to memory, the new message of the day is not available after the device reboots. Use the `no` parameter to not display a banner message at login.

Command Syntax `banner`

```
motd LINE banner motd
default no banner motd
```

Parameters

`LINE` Custom message of the day. `default` Default message of the day.

Default

By default, the following banner is displayed after logging in:

```
SWMRE version 1.3.4.268-DC-MPLS-ZEBM 09/27/2018 13:44:22
```

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#banner motd default

#configure terminal
(config)#no banner motd
```

configure terminal

Use this command to enter configure mode.

Command Syntax `configure terminal`

Parameters

None

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following example shows entering configure mode (note the change in the command prompt).

```
#configure terminal
(config)#
```

configure terminal force

Use the configure terminal force command to kick out the configure command mode to privileged EXEC mode, iff there is any session already in configure command mode.

Note: Configure terminal force with option 0 or without any option indicates immediate kick out the session which is locked to configure command mode. similarly, configure terminal force with option of any value indicates session locked to configure command mode will be exited to privileged Exec mode after the specified number of seconds completed.

Command Syntax `configure terminal force <0-600|>`

Parameters

`<0-600>`	Timeout value in seconds for the session in config mode to exit to Privileged

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal force 0
(config)#
```

copy running-config startup-config

Use this command to a write the configuration to the file used at startup. This is the same as the write command.

Command Syntax `copy running-config startup-config`

Parameters

None

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#copy running-config startup-config
Building configuration...
[OK]
#
```

disable

Use this command from to exit privileged exec mode and return to exec mode. This is the only command that allows you to go back to exec mode. The exit or quit commands in privileged exec mode end the session without returning to exec mode.

Command Syntax `disable`

Parameters

None

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#disable
>
```

enable

Use this command to enter privileged exec command mode.

Command Syntax `enable`

Parameters

None

Default

No default value is specified

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following example shows entering the Privileged Exec mode (note the change in the command prompt).

```
>enable
#
```

enable password

Use this command to change or create a password to use when entering enable mode.

Note: Only network administrators can execute this command. For more, see the username command.

There are three methods to enable a password:

Plain Password

The plain password is a clear text string that appears in the configuration file as configured.

Encrypted Password

An encrypted password encrypts a password. First, use this command to create a password. Then, use the service password-encryption command to encrypt the password. An encrypted password does not display in the configuration file; instead, it displays the encrypted string.

Hidden Password

A hidden password also encrypts a password; however, you do not need the service password-encryption command for this method. Use this method if you know the encrypted string of the plain text string that you want to use as a password. The output in the configuration file displays only the encrypted string and not the text string.

Use the `no` parameter to disable the password.

Command Syntax `enable password`

```
(8|) LINE no enable password
no enable password LINE
```

Parameters

`8`	Hidden password.
`line`	Password string, up to 80-characters, including spaces. The string cannot begin with a number.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#enable password mypasswd
```

end

Use this command to return to privileged exec command mode from any other advanced command mode.

Command Syntax `end`

Parameters

None

Default

No default value is specified

Command Mode

All command modes

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following example shows returning to privileged exec mode directly from interface mode.

```
#configure terminal
(config)#interface eth0
(config-if)#end
#
```

exec-timeout

Use this command to set the interval the command interpreter waits for user input detected. That is, this sets the time a telnet session waits for an idle VTY session before it times out. A value of zero minutes and zero seconds (0 and 0) causes the session to wait indefinitely.

Use the `no` parameter to disable the wait interval.

Command Syntax `exec-timeout <0-35791> (<0-2147483>|) no exec-timeout`

Parameters

`<0-35791>`	Timeout value in minutes.

<0-2147483>Timeout value in seconds.

Default

No default value is specified

Command Mode

Line mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

In the following example, the telnet session will timeout after 2 minutes, 30 seconds if there is no response from the user.

```
Router#configure terminal
Router(config)#line vty 23 66
Router(config-line)#exec-timeout 2 30
```

exit

Use this command to exit the current mode and return to the previous mode. When used in exec mode or privileged exec mode, this command terminates the session.

Command Syntax `exit`

Parameters

None

Default

No default value is specified

Command Mode

All command modes

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows exiting interface mode and returning to configure mode.

```
#configure terminal
(config)#interface eth0
(config-if)#exit
(config)#
```

help

Use this command to display help for the SWMRE command line interface.

Command Syntax `help`

Parameters

None

Default

No default value is specified

Command Mode

All command modes

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#help
CLI provides advanced help feature. When you need help, anytime at
the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1.     Full help is available when you are ready to enter a   command argument
(e.g. 'show ?') and describes each possible    argument.
2.     Partial help is provided when an abbreviated argument is entered   and
you want to know what arguments match the input    (e.g. 'show ve?'.)
```

history

Use this command to set the maximum number of commands stored in the command history.

Use the `no` parameter to remove the configuration.

Command Syntax `history max <0-2147483647> no history max`

Parameters

`<0-2147483647>` Number of commands.

Default

No default value is specified

Command Mode

Line mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#line vty 12 77
(config-line)#history max 123

(config-line)#no history max
```

hostname

Use this command to set the network name for the device. SWMRE uses this name in system prompts and default configuration filenames.

Setting a host name using this command also sets the host name in the kernel.

Note: After giving the `hostname` command, you must write to memory using the write command. If you do not write to memory, the change made by this command (the new host name) is not set after the device reboots.

Use the `no` parameter to disable this function.

Command Syntax `hostname`

```
WORD    no    hostname
(WORD|)
```

Parameter

`WORD`	Network name for a system. Per RFC 952 and RFC 1123, a host name string can contain only the special characters period (“.”) and hyphen (“-”). These special characters cannot be at the start or end of a host name.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#hostname ABC
(config)#

(config)#no hostname
(config)#exit
```

line console

Use the this command to move or change to the line console mode.

Command Syntax `line console <0-0>`

Parameters

<0-0>	First line number.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

This example enters line mode (note the change in the prompt).

```
#configure terminal
(config)#line console 0
(config-line)#
```

line vty

Use this command to move or change to VTY mode. This command is used to connect to a protocol daemon. This configuration is necessary for any session. This configuration should be in the daemon's config file before starting the daemon.

Use the `no` parameter to disable this command.

Command Syntax `line vty <0-871> (<0-871>|) no line vty <0-871> (<0-871>|)`

Parameters

<0-871>	Specify the first line number.
<0-871>	Specify the last line number.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following example shows entering line mode (note the change in the prompt).

```
#configure terminal
(config)#line vty 9
```

```
(config-line)#exit
(config)no line vty 9
```

logging cli

Use this command to enable logging commands entered by all users.

Use the `no` parameter to disable logging commands entered by all users.

Command Syntax `logging cli no logging cli`

Parameter

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced in SWMRE version 1.3.

Example

```
#configure terminal
(config)#logging cli
(config)#no logging cli
```

logout

Use this command to exit from the shell from any exec mode.

Command Syntax `logout`

Parameters

None

Default

No default value is specified

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following examples show the use of `logout` command.

```
>logout SWMRE login:
```

```
>enable en#logout >
```

quit

Use this command to exit the current mode and return to the previous mode. When this command is executed in one of the exec modes, it closes the shell and logs you out.

Command Syntax `quit`

Parameters

None

Default

No default value is specified

Command Mode

All modes

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#quit
(config)#

>enable
#quit
[root@TSUP-123 sbin]#
```

reload

Use this command to shut down the device and perform a cold restart. You call this command when:

- You detect a configuration issue such as `show running-config` displaying a configuration but when you try to remove that configuration, you get a message that it is not configured.
- You have replaced the start-up configuration file (in this case you specify the `flush-db` parameter).

Command Syntax `reload`

```
(flush-db|)
```

Parameters

`flush-db`	Delete the database file and recreate it from the start-up configuration file.

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced in SWMRE version 1.3.4.

Example

This example shows replacing a start-up configuration file and then synchronizing it to the configuration database:

```
#copy file /home/TEST.conf startup-config
Copy Success
#
#reload flush-db
The system has unsaved changes.
Would you like to save them now? (y/n): n

Configuration Not Saved!
Are you sure you would like to reset the system? (y/n): y
```

For both of these prompts, you must specify whether to save or discard the changes. Abnormal termination of the session without these inputs can impact the system behavior.

For the `unsaved changes` prompt:

`Would you like to save them now?`

You should always say “no” to this prompt because otherwise the command takes the current *running configuration* and applies it to the current start-up configuration.

service advanced-vty

Use this command to set multiple options to list when the tab key is pressed while entering a command. This feature applies to commands with more than one option.

Use the `no` parameter to not list options when the tab key is pressed while entering a command.

Command Syntax		
`service advanced-vty`	`no`	`service advanced-vty`

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#service advanced-vty
(config)#no service advanced-vty
```

service password-encryption

Use this command to encrypt passwords created with the enable password command. Encryption helps prevent observers from reading passwords.

Use the `no` parameter to disable this feature.

Command Syntax `service password-encryption` `no service password-encryption`

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#enable password mypasswd
(config)#service password-encryption
```

service terminal-length

Use this command to set the number of lines that display at one time on the screen for the current terminal session.

Use the `no` parameter to disable this feature.

Command Syntax `service terminal-length <0-512> no service terminal-length (<0-512>|)`

Parameters

`<0-512>`	Number of lines to display. A value of 0 prevents pauses between screens of output.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#service terminal-length 60
```

show clock

Use this command to display the current system time.

Command Syntax `show clock`

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show clock
12:54:02 IST Fri Apr 29 2016
```

show cli history

Use this command to list the commands entered in the current session. The history buffer is cleared automatically upon reboot.

Command Syntax `show cli history`

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show cli history
1 en
2 show ru
3 con t
4 show spanning-tree
5 exit
```

show logging cli

Use this command to display command history for all users.

Command Syntax `show logging cli ((logfile LOGFILENAME)|) (match-pattern WORD |) show logging cli last <1-9999> show logging logfile list`

Parameters

`LOGFILENAME` Name of a saved command history log file. The default path is `/var/log/messages`, but you can specify a full path to override the default.

`WORD` Display only lines with this search pattern.

`<1-9999>` Number of lines to display from the end of the command history. `logfile list`

Display a list of command history files.

Default

LOGFILENAME Name of a saved command history log file. The default path is /var/log/messages, but you can specify a full path to override the default.

Command Mode

Exec mode

Applicability

This command was introduced in SWMRE version 1.3.

Example

```
#sh logging cli
2017 Mar 01 16:30:59 : SWMRE : User root@/dev/pts/1 : CLI : exit
2017 Mar 01 16:31:03 : SWMRE : User root@/dev/pts/1 : CLI : sh logging logfile
lo *Failed*
2017 Mar 01 16:31:06 : SWMRE : User root@/dev/pts/1 : CLI : sh logging logfile
list

#sh logging cli logfile abc
2017 Mar 01 16:30:59 : SWMRE : User root@/dev/pts/1 : CLI : exit
2017 Mar 01 16:31:03 : SWMRE : User root@/dev/pts/1 : CLI : sh logging logfile
lo *Failed*
2017 Mar 01 16:31:06 : SWMRE : User root@/dev/pts/1 : CLI : sh logging logfile
list

#sh logging cli match-pattern root
2017 Mar 01 16:30:59 : SWMRE : User root@/dev/pts/1 : CLI : exit
2017 Mar 01 16:31:03 : SWMRE : User root@/dev/pts/1 : CLI : sh logging logfile
lo *Failed*
2017 Mar 01 16:31:06 : SWMRE : User root@/dev/pts/1 : CLI : sh logging logfile
list

#sh logging cli logfile abc match-pattern root
2017 Mar 01 16:30:59 : SWMRE : User root@/dev/pts/1 : CLI : exit
```

```
2017 Mar 01 16:31:03 : SWMRE : User root@/dev/pts/1 : CLI : sh logging logfile lo
*Failed*
2017 Mar 01 16:31:06 : SWMRE : User root@/dev/pts/1 : CLI : sh logging logfile
list

#show logging cli last 2
2017 Mar  1 16:34:26.302 : SWMRE : User root@/dev/pts/1 : CLI : sh logging info
2017 Mar 1 16:34:37.317 : SWMRE : User root@/dev/pts/1 : CLI : sh logging cli
last 2


#show logging logfile list
file1 file2
```


© Symanitron Proprietary

show process

Use this command to display the SWMRE daemon processes that are running.

Command Syntax `show process`

Parameters

None

Command Mode

Exec modes

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show process
 PID NAME             TIME    FD
1 nsm          00:56:29    7
2 ripd         00:56:29    11
3 ripngd       00:56:29    12
4 ospfd        00:56:29    9
5 ospf6d       00:56:29    10
6 bgpd         00:56:29    14
   9 isisd        00:56:29    8
#
```

Table 1-27 explains the output fields.

Table 1-27: show process fields

Entry	Description
PID Name	Process identifier name.
TIME	(S)—Number of system and user CPU seconds that the process has used. (None, D, and E)—Total amount of time that the command has been running.
FD	The Flexible Data-Rates (FD) of the interface.

show running-config

Use this command to show the running system status and configuration.

Command Syntax `show running-config show running-config full`

Parameters `full` Display the full configuration information.

Command Mode

Privileged exec mode and configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
    (config)#show running-config no service password-encryption
    ! no service dhcp ip domain-lookup
!
    mpls propagate-ttl
    ! vrrp vmac enable spanning-tree mode provider-rstp no data-
    center-bridging enable
    ! interface lo  ip address 127.0.0.1/8  ipv6 address
    ::1/128  no shutdown
    ! interface eth0  ip address 10.1.2.173/24  no shutdown
    ! interface eth1  shutdown

    ! line con 0  login
    ! end (config)#
```

show running-config access-list

Use this command to show the running system status and configuration details for access lists.

Command Syntax `show running-config access-list`

Parameters

None

Command Mode

Privileged exec mode, configure mode, router-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
    (config)#show running-config access-list
    ! access-list abc remark annai access-list
    abc deny any access-list abd deny any
!
```

#

show running-config as-path access-list

Use this command to show the running system status and configuration details for access lists based on autonomous system paths.

Command Syntax `show running-config as-path access-list`

Parameters

None

Command Mode

Privileged exec mode, configure mode, router-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
(config)#show running-config as-path access-list
!
ip as-path access-list wer permit knsmk
!
(config)#
```

show running-config community-list

Use this command to show the running system status and configuration details for community lists.

Command Syntax `show running-config community-list`

Parameters

None

Command Mode

Privileged exec mode, configure mode, router-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
>enable
(config)#show running-config community-list
! ip community-list standard aspd permit internet ip
community-list expanded cspd deny ljj ip community-list
expanded cspd permit dcv ip community-list expanded wde
permit njhd ip community-list expanded wer deny sde
(config)#
```

show running-config interface igmp

Use this command to show the running system status and configuration for IGMP.

Command Syntax `show running-config interface IFNAME ip igmp`

Parameters

`IFNAME`	Interface name.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show running-config interface eth1 ip igmp
!
interface eth1 !
```

show running-config interface multicast

Use this command to show the running system status and configuration for a multicast interface.

Command Syntax `show running-config interface IFNAME ip multicast`

Parameters

`IFNAME`	Interface name.

Command Mode

Privileged exec mode and configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show running-config interface eth1 ip multicast
!
interface eth1 !
```

show running-config prefix-list

Use this command to display the running system status and configuration details for prefix lists.

Command Syntax `show running-config prefix-list`

Parameters

None

Command Mode

Privileged exec mode, configure mode, router-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
>enable
#show running-config prefix-list
! ip prefix-list abc seq 5 permit any ip prefix-
list as description annai ip prefix-list wer seq 45
permit any !
```

show running-config vrf

Use this command to show the running system status and configuration details for a specified VRF instance name.

Command Syntax `show running-config`

`vrf WORD`

Parameters

`WORD`	Virtual Routing and Forwarding name

Command Mode

Privileged exec mode, configure mode, router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
>enable
#show running-config vrf xyz
! ip vrf xyz
description vrf  router-
id 11.11.11.11
```

show tcp

Use this command to display the Transmission Control Protocol (TCP) connections details.

Command Syntax `show`

`tcp`

Parameters

None

Command Mode

Exec mode and privileged exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show tcp
Proto Recv-Q Send-Q Local Address               Foreign Address         State  tcp
0       0 0.0.0.0:22              0.0.0.0:*               LISTEN tcp        0      0
127.0.0.1:25              0.0.0.0:*                  LISTEN tcp         0       1
10.12.44.1:57740        127.0.0.1:705             CLOSE_WAIT tcp        52      0
10.12.44.21:22          10.12.7.89:705            ESTABLISHED tcp       85      0
10.12.44.21:57742      10.12.44.21:57738      ESTABLISHED
```

Table 1-28: Show tcp output

Entry	Description
Proto	Protocol – TCP
Recv-Q	Number of TCP packets in the Receive Queue.
Send-Q	Number of TCP packets in the Send-Q.
Local Address and port number	Local IP address and the port number.

Table 1-28: Show tcp output (Continued)

	Description
number	Foreign (received) IP address and the port number.
	Current state of TCP connections: ESTABLISHED SYN_SENT SYN_RECV FIN_WAIT1 FIN_WAIT2 TIME_WAIT CLOSE CLOSE_WAIT LAST_ACK LISTEN CLOSING UNKNOWN

show users

Use this command to display information about current users.

Command Syntax `show`

```
users
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show users
Current user          : (*).  Lock acquired by user : (#).
CLI user              : [C].  Netconf users         : [N].
Location : Applicable to CLI users.
Session  : Applicable to NETCONF users.

      Line      User      Idle     Location/Session       PID     TYPE         Role
(*) 130 vty 0 [C]root    00:00:36     pts/0             20872    Local     network-admin
(#)    NA      [N]root      NA           1                 NA      NA       network-admin
NA       [N]root     NA           2                 NA       NA       network-admin
131 vty 1 [C]joyce   00:00:26    pts/1             17593     Remote     network-admin
```

Table 1-29 explains the output fields.

Table 1-29: show users fields

Entry	Description
Current users	
CLI user	
Location	
Session	
Lock acquired by user	

Netconf users	
Line	
User	User name.

Table 1-29: show users fields

	Description
	How long the user has been idle.
	Process identifier name.

terminal length

Use this command to set the number of lines displayed on the screen.

Use the `no` option to unset the number of lines on a screen.

Command Syntax `terminal length <0-511> terminal no length`

`<0-511>`

Parameters

`<0-511>`	Number of lines on screen. Specify 0 for no pausing.

Default

By default, terminal length is 25 lines.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
>enable
#terminal length 0
```

The following example sets the terminal length to 30 lines.

```
#terminal length 30
```

terminal monitor

Use this command to display debugging output on a terminal.

Use one of the optional parameters to display debugging output for the Privileged Virtual Router (PVR) or VR user. When the command is used without a parameter, it can be used by a PVR user or non-PVR user to display the debug output on the terminal for the user local VR. When used with a parameter, it may be used only by a PVR user.

The `no` form of the command terminates the debug output on the terminal. Both the PVR and VR user can use this command. In addition, the PVR user can cancel a debug output from a specific VR or all VRs.

Command Syntax `terminal monitor`

`terminal monitor (all|WORD|)`

`terminal no monitor terminal`

`no monitor (WORD|)`

Parameters

`WORD`	Used in the PVR context, and contains the VR name to be included in the debugging session.
`all`	Used the PVR context to include all VR in a PVR debugging session.

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
>Enable
#terminal monitor
#terminal no monitor
```

write

Use this command to a write the configuration to the file used at startup or to a specified file. This is the same as the copy running-config startup-config command.

Command Syntax

```
write  file  FILE
write    memory
write WORD
```

Parameters

`FILE` Write to a given path and file. If you do not give a file path, the file is added to `/root`. `memory`

Write to non-volatile memory. `WORD` Write to running configuration file path.

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

This example shows writing the configuration to the startup configuration file:

```
#write
Building configuration...
[OK]
```

This example shows writing the configuration to a specified file:

```
#write file /home/test.txt
Building configuration...
[OK]
```

CHAPTER 2 IMI Shell Commands

This chapter describes IMI shell commands.

- do
- login local
- logout
- ping
- interactive ping
- privilege level
- show privilege
- telnet
- traceroute
- write terminal

do

Use this command to run several exec mode or privileged exec mode commands from configure mode. The commands that can be run from configure mode using `do` are: `show`, `clear`, `debug`, `ping`, `traceroute`, `write`, and `no debug`.

Note: The `do` command supports only the following CLI commands only

Command Syntax `do`

```
LINE
```

Parameters

`LINE`	Command and its parameters.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
#(config)#do show interface
Interface lo
  Hardware is Loopback index 1 metric 1 mtu 16436 duplex-half arp ageing timeout
25
  <UP,LOOPBACK,RUNNING>
  VRF Binding: Not bound
  Label switching is disabled
  No Virtual Circuit configured
  Administrative Group(s): None   DSTE
Bandwidth Constraint Mode is MAM   inet
4.4.4.40/32 secondary   inet 127.0.0.1/8
inet6 ::1/128   Interface Gifindex: 3
  Number of Data Links: 0
  GMPLS Switching Capability Type:
    Packet-Switch Capable-1 (PSC-1)
  GMPLS Encoding Type: Packet
Minimum LSP Bandwidth 0
    input packets 10026, bytes 730660, dropped 0, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 10026, bytes 730660, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window
0 collisions 0
#
```

login local

Use this command to set a password prompt before entering the configuration mode and to enable password checking.

Use the `no login` command to allow users to connect directly to privileged exec mode skipping the password verification prompt. After using the `no login` command, if the user gives to the `login` command again, the system uses the password used earlier, unless the user specifies a password in configure mode.

Command Syntax `login`

```
local  no  login
local
```

Parameters

None

Default

By default, login local is enabled

Command Mode

Line mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following examples shows setting a password `pass` (in configure mode) before giving the `login` command.

```
#configure terminal
(config)#enable password pass
(config)#line vty 1
(config-line)#login local
```

```
#configure terminal
(config)#line vty 1
(config-line)#no login
```

logout

Use this command to exit the SWMRE shell.

Command Syntax `logout`

Parameters

None

Default

No default value is specified

Command Mode

Exec mode and privileged exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
>logout
[root@TSUP40 sbin]#
```

ping

Use this command to send echo messages to another host.

Command Syntax `ping WORD (vrf (NAME|management)|) ping ip WORD (vrf (NAME|management)|) ping ipv6 WORD (|IFNAME) ping ipv6 WORD (|IFNAME) (vrf (NAME|management)|)`

Parameters

`WORD`	Destination address (in A.B.C.D format for IPv4 or X:X::X:X for IPv6) or host name.
`vrf`	Virtual Routing and Forwarding instance.
`NAME`	Virtual Routing and Forwarding name.
`management`	Virtual Routing and Forwarding name.
`ip`	IPv4 echo.
`WORD`	Destination address in A.B.C.D format or host name.
`ipv6`	IPv6 echo.
`WORD`	Destination address in X:X::X:X format or host name.
`IFNAME`	Name of the interface.

Default

No default value is specified

Command Mode

Privileged exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
>enable
#ping 20.20.20.1 vrf management
Press CTRL+C to exit
PING 20.20.20.1 (20.20.20.1) 56(84) bytes of data.
64 bytes from 20.20.20.1: icmp_seq=1 ttl=64 time=0.032 ms
64 bytes from 20.20.20.1: icmp_seq=2 ttl=64 time=0.035 ms
64 bytes from 20.20.20.1: icmp_seq=3 ttl=64 time=0.033 ms
64 bytes from 20.20.20.1: icmp_seq=4 ttl=64 time=0.034 ms
64 bytes from 20.20.20.1: icmp_seq=5 ttl=64 time=0.034 ms
64 bytes from 20.20.20.1: icmp_seq=6 ttl=64 time=0.036 ms
64 bytes from 20.20.20.1: icmp_seq=7 ttl=64 time=0.036 ms
64 bytes from 20.20.20.1: icmp_seq=8 ttl=64 time=0.036 ms

--- 20.20.20.1 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 6999ms
```

```
rtt min/avg/max/mdev = 0.032/0.034/0.036/0.006 ms

#ping ipv6 3001:db8:0:1::129 vrf management
Press CTRL+C to exit
PING 3001:db8:0:1::129(3001:db8:0:1::129) 56 data bytes
64 bytes from 3001:db8:0:1::129: icmp_seq=1 ttl=64 time=0.038 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=2 ttl=64 time=0.047 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=3 ttl=64 time=0.047 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=4 ttl=64 time=0.049 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=5 ttl=64 time=0.044 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=6 ttl=64 time=0.048 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=7 ttl=64 time=0.046 ms
64 bytes from 3001:db8:0:1::129: icmp_seq=8 ttl=64 time=0.048 ms

--- 3001:db8:0:1::129 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 6999ms
```

interactive ping

Use this command to send echo messages to another host interactively. You are prompted with options supported by the command.

Command Syntax `ping`

Parameters

None

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
>enable
#ping
Protocol [ip]:
Target IP address: 20.20.20.1
Name of the VRF : management
Repeat count [5]: 6
Time Interval in Sec [1]: 2.2
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Ping Broadcast? Then -b [n]:
PING 20.20.20.1 (20.20.20.1) 100(128) bytes of data.
108 bytes from 20.20.20.1: icmp_seq=1 ttl=64 time=0.038 ms
108 bytes from 20.20.20.1: icmp_seq=2 ttl=64 time=0.038 ms
108 bytes from 20.20.20.1: icmp_seq=3 ttl=64 time=0.038 ms
108 bytes from 20.20.20.1: icmp_seq=4 ttl=64 time=0.036 ms
108 bytes from 20.20.20.1: icmp_seq=5 ttl=64 time=0.037 ms
108 bytes from 20.20.20.1: icmp_seq=6 ttl=64 time=0.034 ms

--- 20.20.20.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 11000ms rtt
min/avg/max/mdev = 0.034/0.036/0.038/0.007 ms

#ping
Protocol [ip]: ipv6
Target IP address: 3001:db8:0:1::129 Name
of the VRF : management
Repeat count [5]:
```

```
Time Interval in Sec [1]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
PING 3001:db8:0:1::129(3001:db8:0:1::129) 100 data bytes
108 bytes from 3001:db8:0:1::129: icmp_seq=1 ttl=64 time=0.050 ms
108 bytes from 3001:db8:0:1::129: icmp_seq=2 ttl=64 time=0.047 ms
108 bytes from 3001:db8:0:1::129: icmp_seq=3 ttl=64 time=0.042 ms
108 bytes from 3001:db8:0:1::129: icmp_seq=4 ttl=64 time=0.048 ms
108 bytes from 3001:db8:0:1::129: icmp_seq=5 ttl=64 time=0.051 ms

--- 3001:db8:0:1::129 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.042/0.047/0.051/0.008 ms
```

The input prompts are described in Table 2-30:

Table 2-30: ping output fields

Protocol [ip]	IPv4 or IPv6. The default is IPv4 if not specified.
Target IP address	IPv4 or IPv6 address or host name.
Name of the VRF	Name of the Virtual Routing and Forwarding instance.
Repeat count [5]	Number of ping packets to send. The default is 5 if not specified.
Time Interval in Sec [1]	Time interval between two ping packets. The default is 1 second if not specified.
Datagram size [100]	Ping packet size. The default is 100 bytes if not specified.
Timeout in seconds [2]	Time to wait for ping reply. The default is 2 seconds if not specified.
Extended commands [n]	Options for extended ping. The default is “no”.
Source address or interface	Source address or interface.
Type of service [0]	Types of service. The default is 0 if not specified.
Set DF bit in IP header? [no]	Do not fragment bit. The default value is “no” if not specified.
Data pattern [0xABCD]	Specify a pattern.
Ping Broadcast? Then -b [n]	Broadcast ping. The default is “no”. For a broadcast address, the value should be “y”.

privilege level

Use this command to set the command privilege level.

Note: Privilege levels 2-14 are undefined.

Use the `no` parameter with this command to disable the command privilege level.

Command Syntax `privilege level <1-15> privilege level (16) no privilege level (<1-15>|) no privilege level (16)`

Parameters

`16`	Maximum privilege level for a line.
`<1-15>`	Default privilege level for a line.

Default

No default value is specified

Command Mode

Line mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#line vty 0 5
(config-line)#privilege level 15
```

show privilege

Use this command to display the current privilege level. The privilege level range is 1-15.

Command Syntax `show privilege`

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show privilege
```

```
Current privilege level is 15
#
```

telnet

Use this command to open a telnet session.

Command Syntax `telnet WORD vrf management|) telnet WORD PORT`

Parameters

`WORD`	IP address or hostname of a remote system.
`PORT`	TCP port number.
`vrf`	Virtual Routing and Forwarding
`management`	Management VRF

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#telnet 2.2.2.2 2602 trying telnet 2.2.2.2 2602...
```

traceroute

Use this command to trace an IPv4/v6 route to its destination.

Command Syntax `traceroute WORD traceroute WORD (vrf (NAME|management)|) traceroute ipv6 WORD traceroute ipv6 WORD (vrf (NAME|management)|)`

Parameters

`WORD` Destination address (in A.B.C.D format for IPv4 or X:X::X:X for IPv6) or host name.

`vrf` Virtual Routing and Forwarding instance.

`NAME` Virtual Routing and Forwarding name. `management` Virtual Routing and Forwarding name. `ip` IPv4 echo.

`WORD` Destination address in A.B.C.D format or host name. `ipv6` IPv6 echo.

`WORD` Destination address in X:X::X:X format or host name.

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#traceroute ip 10.10.100.126 vrf management
traceroute to 10.10.100.126 (10.10.100.126), 30 hops max, 38 byte packets
1 10.1.2.1 (10.1.2.1) 0.386 ms 0.315 ms 0.293 ms
2  10.10.100.126 (10.10.100.126)  1.944 ms  1.497 ms  1.296 ms#
```

write terminal

Use this command to display the current configuration.

Command Syntax `write terminal`

Parameters

None

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example `#write terminal`

```
Current configuration:
!
hostname ripd password zebra log stdout
! debug rip events debug rip packet
!
interface lo
!
interface eth0  ip rip send version  1 2  ip rip receive version 1 2
!
interface eth1  ip rip send version  1 2  ip rip receive version 1 2
! !
router rip network 10.10.10.0/24 network 10.10.11.0/24
redistribute connected
```

```
! line vty  exec-timeout 0 0
```

CHAPTER 3 VLOG Commands

This chapter describes virtual router log (VLOG) commands.

- show vlog all
- show vlog clients
- show vlog terminals
- show vlog virtual-routers

show vlog all

Use this command to display the output of all virtual router log `show` commands. For column descriptions, refer to descriptions of the individual commands.

Command Syntax `show`

```
vlog all
```

Parameters

None

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
>enable
#show vlog all

Type       Name      FD  UserVR   AllVrs  VRCnt
tty    /dev/pts/8   12  vr222     ---        1
tty    /dev/pts/4   13 <PVR>     ---       1

VR-Name  VR-Id  PVR-Terms  VR-Terms                    LogFile
CurSize
<PVR>         0          1         0        /var/local/SWMRE/log/pvr/my-log
1624320
vr111         1          0         0        n/a
n/a
vr222         2          0         1
/var/local/SWMRE/log/vr222/logvr222           0
vr333         3          0         0
/var/local/SWMRE/log/vr333/logvr333           0

Name   Id   MsgCnt        ConTime              ReadTime
NSM     1        1  Fri May-15 21:05:04 Fri May-15 21:05:04
```

```
IMI    19        1   Fri May-15 21:05:02  Fri May-15 21:05:02
```

show vlog clients

Use this command to display all attached virtual router log clients (protocol modules).

Command Syntax `show vlog clients`

Parameters

None

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
>enable
#show vlog clients

Name    Id  MsgCnt          ConTime                ReadTime
NSM      1        1     Fri May-15  21:05:04  Fri May-15 21:05:04
IMI     19        1     Fri May-15  21:05:02  Fri May-15 21:05:02
```

Table 3-31 explains the output:

Table 3-31: Virtual router log clients

Name	Name of protocol module
Id	Protocol module identifier
MsgCnt	Number of log messages received from protocol module
ConTime	Time the connection was established
ReadTime	Time the last log message was received

show vlog terminals

Use this command to display all active connections where VLOGD is forwarding log output.

Command Syntax `show vlog terminals`

Parameters

None

Default

None

Command Mode

Privileged exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
>enable
#show vlog terminals

Type     Name     FD  UserVR  AllVrs  VRCnt tty    /dev/pts/8  12
vr222    ---        1 tty   /dev/pts/4   13  <PVR>     ---       1
```

Table 3-32 explains the output:

Table 3-32: Virtual router log terminals

Type	Type of terminal
Name	Device name
FD	File descriptor
UserVR	Name of the Virtual Router where in which the user is logged in
AllVRs	Whether the PVR user requested debug output from all VRs
VRCnt	Number of VRs to which a terminal is attached

show vlog virtual-routers

Use this command to display virtual router statistics such as the number of terminals attached.

Command Syntax `show vlog virtual-routers`

Parameters

None

Default

None

Command Mode

Privileged exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
>enable
#show vlog virtual-routers

VR-Name  VR-Id  PVR-Terms  VR-Terms LogFile
CurSize
<PVR>          0 1           0        /var/local/SWMRE/log/pvr/my-log
1624320
vr111          1 0           0        n/a                                    n/a
vr222          2 0           1        /var/local/SWMRE/log/vr222/log-vr222    0
vr333          3 0           0        /var/local/SWMRE/log/vr333/log-vr333    0
```

Table 3-33 explains the output:

Table 3-33: Virtual router statistics

VR-Name	Virtual router name
VR-Id	Virtual router identifier
PVR-Terms	Number of attached PVR terminals
VR-Terms	Number of attached VR terminals

LogFile	Name of VR log file (this column is empty if writing to a log file is disabled)
CurSize	Log file current size

CHAPTER 4 System Commands

This chapter is a reference for system commands.

- mv
- pwd

mv

Use this command to rename (move) a file.

Command Syntax `mv LINE`

Parameters

`LINE`	Source and destination file names

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#mv old-name new-name
```

pwd

Use this command to print the working directory.

Command Syntax `pwd`

Parameters

None

Default

No default value is specified

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#pwd
```

CHAPTER 5 Licensing and Upgrade Commands

This chapter is a reference for license and upgrade commands.

- license get
- show license
- show sys-update details
- sys-update commit
- sys-update install
- sys-update list-version
- sys-update rollback

license get

Use this command to fetch the license for this device from a network path or a USB mount path. This command validates the license against the device identifier.

Note: You can provide license file in `.bin` or `.tar` format. If you specify a license file with the extension `.tar`, then this command extracts the file and loads it.

For HTTP, FTP, or TFTP, ensure that the IP address is reachable from the SWMRE device and that the file location is correct.

If you install a license from a USB stick, insert it, and the contents of the USB are available as `//mnt/usb/`. For example:

```
>license get file://mnt/usb/license-FM5RX42-P-20160213.tar
```

After running the `license get` command, you can immediately use the switch without rebooting.

To verify, run the show license command after giving this command.

Command Syntax `license get (|(source-interface IFNAME)) WORD`

Parameters

`IFNAME`	The interface used to download the license. If not specified, `eth0` is used. If the management interface of the switch is in the “management” VRF, then this command uses the “management” VRF to get the license from the specified path. You do need not to know if the management port is in the default VRF or the “management” VRF.
`WORD`	Where to get the license: http://your-server-ip/path/to/file/DeviceId-license.tar ftp://your-server-ip/path/to/file/DeviceId-license.tar tftp://your-server-ip/path/to/file/DeviceId-license.tar file://mnt-point/usb/path/to/file/DeviceId-license.tar

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
>license get http://myServer/license-FM5RX42-P-20160213.tar
```

Specify the `source-interface` parameter to set the interface to use:

```
>license get source-interface xe2 license get http://myServer/license-FM5RX42P-20160213.tar
```

show license

Use this command to display the current license details and errors. The licenses are device locked, which means that a separate license is required for each device. If the License Type is "Limited Edition", then you cannot enter privileged exec mode and execute configuration commands.

Command Syntax

```
show license
```

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
>show license
License Type: Device Locked, Full edition
License Validity: Permanent
Service Tag: 0030AB30D60C
Service End Date: May 13 2017
```

show sys-update details

Use this command to display upgrade details. The output indicates whether the current version is committed or rolled back.

Command Syntax `show sys-`

```
update details
```

Parameters

None

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show sys-update details
Previous_version EC_AS5812_54X-SWMRE-1.3.4.265-DC_MPLS_ZEBM-S0-P0
Current_version EC_AS5812_54X-SWMRE-1.3.4.266-DC_MPLS_ZEBM-S0-P0-installer
(committed)
Last_upgraded Wed Sep 26 14:40:06 UTC 2018
Auto Rollback end time NA
```

sys-update commit

Use this command to accept a new version. After a commit, you cannot roll back to a previous version. Until you commit a new version, you cannot save the configuration. Upgrading with an installer file is auto committed.

Command Syntax `sys-update`

```
commit
```

Parameters

None

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#sys-update commit
```

sys-update install

Use this command to upgrade the current software to a newer version. You can do two types of installation:

- If a `.deb` file is provided, the board is loaded with new binaries.
- If an installer file is provided, the board is completely installed with a new kernel and binaries.

Command Syntax `sys-update install (|(source-interface IFNAME)) URL (verbose|)`

Parameters

`IFNAME`	The interface used to download the new version. If not specified, `eth0` is used.
`URL`	Where to get the new version: `http://your-server-ip/path/to/file/<abc-updater.deb or abcinstaller> ftp://your-server-ip/path/to/file/<abc-updater.deb or abcinstaller> tftp://your-server-ip/path/to/file/<abc-updater.deb or abcinstaller> file://mnt/usb/path/to/file/<abc-updater.deb or abc-installer>`
`verbose`	Include upgrade logs in the output.

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#sys-update install source-interface eth2 http://10.12.52.150/myServer/
EC_AS5812_54X-SWMRE-1.3.4.266-DC_MPLS_ZEBM-S0-P0-installer verbose

#sys-update install http://10.12.52.150/myServer/EC_AS5812_54X-
SWMRE1.3.4.266-DC_MPLS_ZEBM-S0-P0-installer verbose

#sys-update install http://10.12.52.150/myServer/EC_AS5812_54X-
SWMRE1.3.4.266-DC_MPLS_ZEBM-S0-P0-installer

#sys-update install http://10.12.52.150/myServer/EC_AS5812_54X-
SWMRE1.3.4.266-DC_MPLS_ZEBM-S0-P0-updater.deb
```

sys-update list-version

Use this command to display files and folders. This command supports only FTP and the local file system.

Command Syntax `sys-update list-version ((source-interface IFNAME)|) URL`

Parameters

`IFNAME`	The interface used to download the list. If not specified, `eth0` is used.

`URL`	Where to get the list:
	`ftp://(username@|)serverIP/path/to/file/`
	`file://mnt/usb/path/to/file/`

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#sys-update list-version ftp://10.12.52.150/
```

sys-update rollback

Use this command to roll back to the previous version. After a commit, you cannot roll back. Upgrading with an installer file does not support roll back.

Command Syntax `sys-update rollback (verbose|)`

Parameters `verbose` Include details in the output.

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#sys-update rollback
#sys-update rollback verbose
```

Network Services Module Command Reference

Contents

This document contains these chapters:

- Chapter 1, *Common Exec Mode Commands*
- Chapter 2, *Common Configure Mode Commands*
- Chapter 3, *Common Route-Map Mode Commands*
- Chapter 4, *Interface Commands*
- Chapter 5, *Access Control List Commands*
- Chapter 6, *Traffic Engineering Commands*
- Chapter 7, *Control Channel Mode Commands*
- Chapter 8, *Control Adjacency Commands*
- Chapter 9, *Tunneling Commands*
- Chapter 10, *Remote Monitoring Commands*
- Chapter 11, *Unicast Reverse Path Forwarding Check*
- Chapter 12, *Internet Protocol Security Commands*

© Symanitron

CHAPTER 1 Common Exec Mode Commands

This chapter is a reference for Exec and Privileged mode commands. All commands are common to multipleprotocols. This chapter includes the following commands:

- clear interface fec
- copy empty-config startup-config
- debug nsm all
- debug nsm bfd
- debug nsm events • debug nsm hal
- debug nsm packet
- show cli
- show debugging nsm
- show dot1X
- show interface fec
- show ipv6 rpf
- show list
- show nsm client
- show process
- show running-config router
- show running-config switch
- show running-config urpf
- show startup-config
- show version

clear interface fec

Use this command to clear FEC (forward error correction) statistics on a specified interface or on all interfaces.

Note: This command is not supported on loop-back interfaces or the out-of-band (OOB) management interface.

Command Syntax `clear interface (IFNAME|) fec`

Parameters

`IFNAME`	Physical Interface name.

Default

None

Command Mode

Exec mode and Privileged exec mode

Applicability

This command was introduced before SWMRE version 1.3.4.

Example

```
#clear interface ce1/1 fec
```

copy empty-config startup-config

Use this command to clear the contents of the startup configuration.

Command Syntax `copy empty-config startup-config`

Parameters

None

Default

None

Command Mode

Privileged exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#copy empty-config startup-config
#
```

debug nsm all

Use this command to enable NSM debugging.

Use the `no` parameter with this command or the `undebug` command to disable NSM debugging.

Command Syntax `debug nsm (all|) no`

`debug nsm (all|) undebug nsm (all|)`

Parameters

`all`	Enable all debugging.

Default

By default, debug command is disabled.

Command Mode

Exec mode, privileged exec mode, and configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#debug nsm all
#
```

debug nsm bfd

Use this command to enable debugging BFD (Bidirectional Forwarding Detection) events.

Use the `no` parameter with this command or the `undebug` command to disable BFD debugging.

Command Syntax `debug nsm bfd no`

`debug nsm bfd undebug nsm bfd`

Parameters

None

Default

By default, debug command is disabled.

Command Mode

Exec mode, privileged exec mode, and configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#debug nsm bfd
#
```

debug nsm events

Use this command to enable debugging of NSM events.

Use the `no` parameter with this command or the `undebug` command to disable event debugging.

Command Syntax `debug nsm events no`

`debug nsm events undebug nsm events`

Parameters

None

Default

By default, debug command is disabled.

Command Mode

Exec mode, privileged exec mode, and configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#debug nsm events
#
```

debug nsm hal

Use this command to enable debugging of NSM HAL (hardware abstraction layer) events.

Use the `no` parameter with this command or the `undebug` command to disable HAL debugging.

Command Syntax `debug nsm hal (all|) debug`

`debug nsm hal events no debug nsm hal (all|) no debug nsm hal events undebug nsm hal events`

Parameters

`all`	Enable all HAL debugging.
`events`	Enable debugging of only NSM HAL events.

Default

By default, debug command is disabled.

Command Mode

Exec mode, privileged exec mode, and configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#debug nsm hal all
#
```

debug nsm packet

Use this command to enable debugging of NSM packet events.

Use the `no` parameter with this command or the undebug command to disable packet debugging.

Command Syntax `debug nsm packet (recv|send|) (detail|) no`

`debug nsm packet (recv|send|) (detail|) undebug nsm packet (recv|send|) (detail|)`

Parameters

`recv`	Specify the debug option-set for receive packet.
`send`	Specify the debug option-set for send packet.
`detail`	Sets the debug option to provide detailed information.

Default

By default, debug command is disabled.

Command Mode

Privileged exec mode, and configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#debug nsm packet
#debug nsm packet recv detail
#
```

show cli

Use this command to display the command tree of the current mode.

Command Syntax

`show cli`

Parameters

None

Default

None

Command Mode

All command modes

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show cli
Exec mode:
+-clear
  +-arp-cache [clear arp-cache]
  +-ethernet
    +-cfm
      +-errors
        +-domain
          +-DOMAIN_NAME [clear ethernet cfm errors
(domain DOMAIN_NAME|level LEVEL_ID) (bridge <1-32>|)]
            +-bridge
              +-<1-32> [clear ethernet cfm errors (domain
DOMAIN_NAME|level LEVEL_ID) (bridge <1-32>|)]
        +-level
          +-LEVEL_ID [clear ethernet cfm errors (domain
DOMAIN_NAME|level LEVEL_ID) (bridge <1-32>|)]
            +-bridge
              +-<1-32> [clear ethernet cfm errors (domain DOMAIN_NAME|level
LEVEL_ID) (bridge <1-32>|)]
      +-maintenance-points
        +-remote
          +-domain
            +-DOMAIN_NAME [clear ethernet cfm maintenance-points
remote(domain
D
--More--
```

show debugging nsm

Use this command to display debugging information.

Command Syntax `show debugging nsm`

Parameters

None

Default

None

Command Mode

Exec mode and privileged exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show debugging nsm
NSM debugging status:
  NSM event debugging is on
  NSM packet debugging is on
  NSM kernel debugging is on
#
```

show dot1X

Use this command to display IEEE 802.1x port-based access control information.

Command Syntax `show dot1x show dot1x all show dot1x diagnostics interface IFNAME show dot1x interface IFNAME show dot1x sessionstatistics interface IFNAME show dot1x statistics interface IFNAME`

Parameters `all` Display all IEEE 802.1x port-based access control information. `diagnostics` Display diagnostics information.

`IFNAME` Interface name.

`sessionstatistics` Display the statistics for a session.

`statistics` Display the statistics.

Default

None

Command Mode

Exec mode and privileged exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show dot1x all
802.1X Port-Based Authentication Disabled
  RADIUS client address: not configured
#
```

Table 1-34 explains the output fields.

Table 1-34: port variables

Field	Description
port Enabled	Interface operational status (Up-true/down-false).
port Control	Current control status of the port for 802.1x control.
port Status	802.1x status of the port (authorized/unauthorized).

Table 1-34: port variables

Field	Description
reAuthenticate	Reauthentication enabled/disabled status on port
reAuthPeriod	Value holds meaning only if reAuthentication is enabled

Table 1-35 explains the output fields.

Table 1-35: supplicant pae related global variables

Field	Description
abort	Authentication should be aborted when set to true.
fail	Failed authentication attempt when set to false.
start	Authentication should be started when set to true.
timeout	Authentication attempt timed out when set to true.
success	Authentication successful when set to true.

Table 1-36 explains the output fields.

Table 1-36: 802.1x operational state of interface

Field	Description
mode	Configured 802.1x mode
reAuthCount	Number of reauthentication count in the interface.
quietperiod	Time between reauthentication attempts in transmit.
reAuthMax	Maximum reauthentication attempts in the interface.

Table 1-37 explains the output fields.

Table 1-37: backend authentication state machine variables and constants

© Symanitron Proprietary

Field	Description
state	State of the port.
reqCount	Count of requests sent to server
suppTimeout	The number of seconds the port waits for a response when relaying a request from the authentication server to the supplicant before resending the request.

Table 1-37: backend authentication state machine variables and constants

Field	Description
serverTimeout	The number of seconds the port waits for a reply when relaying a response from the supplicant to the authentication server before timing out.
maxReq	The maximum number of times a request packet is retransmitted to the supplicant before the authentication session times out.

Table 1-38 explains the output fields.

Table 1-38: controlled directions state machine

Field	Description
adminControlledDirections	Administrative value (Both/In)
operControlledDirections	Operational Value (Both/In)

Table 1-39 explains the output fields.

Table 1-39: kr -- key receive state machine

Field	Description
rxKey	True when EAPOL-Key message is received by supplicant or authenticator. false when key is transmitted

Table 1-40 explains the output fields.

Table 1-40: key transmit state machine

Field	Description
keyAvailable	False when key has been transmitted by authenticator, true when new key is available for key exchange
keyTxEnabled	Key transmission enabled/disabled status

show interface fec

Use this command to display the FEC (forward error correction) statistics for an interface.

Note: You can only display FEC statistics for physical interfaces and not for management or logical interfaces.

Command Syntax `show interface (IFNAME|) fec`

Parameters

`IFNAME`	Physical Interface name.

Default

None

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.4.

Example

```
#show interface ce1/1 fec

    +----------------+--------+-------------------------------------------------+
|  Interface   | FEC   | CORRECTED BLOCK COUNT | UNCORRECTED BLOCK COUNT | +----
------------+--------+-----------------------------------------------+    ce1/1
off         0                           0
```

show ip rpf

Use this command to display reverse path forwarding (RPF) information for the specified source address.

Command Syntax `show ip rpf A.B.C.D show ip rpf (vrf NAME|) A.B.C.D`

Parameters

`A.B.C.D`	IP address of multicast source.
`NAME`	Virtual Routing and Forwarding name.

Default

None

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip rpf 10.10.10.50

RPF information for 10.10.10.50
  RPF interface: eth0
  RPF neighbor: 10.1.2.1
  RPF route: 0.0.0.0/0
  RPF type: unicast (kernel)
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
  Distance: 0
  Metric: 0
#
```

show ipv6 rpf

Use this command to display reverse path forwarding (RPF) information for the specified source address.

Command Syntax `show ipv6 rpf X:X::X:X show ipv6 rpf (vrf NAME|) X:X::X:X`

Parameters

`X:X::X:X`	IP address of multicast source.
`NAME`	Virtual Routing and Forwarding name.

Default

None

Command Mode

Exec and privileged exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ipv6 rpf 10:10::10:50

RPF information for 10.10.10.50
  RPF interface: eth0
```

```
  RPF neighbor: 10.1.2.1
  RPF route: 0.0.0.0/0
  RPF type: unicast (kernel)
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
  Distance: 0
  Metric: 0
#
```

Table 1-41 Explains the show commands output fields.

Table 1-41: Show ipv6 rpf output fields

Field	Description
RPF Interface	Name of the RPF interface.
RPF neighbor	Upstream RPF neighbor.
RPF route	Route table in which the logical interface address is located.
RPF type	Different type of RPF like multicast, unicast, MBGP, DVMRP, or static mroutes.

Field	Description
RPF recursion count	Number of times that the router lookups its routing table more than once to find out the immediate nexthop and exiting interface.
Distance	IPv6 address of the remote side of the connection. Doing distance-preferred lookups across tables.
Metric	Metrics are informational units that can be measured and compared.

show list

Use this command to display the commands relevant to the current mode.

Command Syntax `show list`

Parameters

None

Default

None

Command Mode

All command modes except IPv4 access-list and IPv6 access-list mode.

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
>show list  clear arp-cache   clear bgp *    clear bgp * in   clear bgp * in
prefix-filter   clear bgp * out   clear bgp * soft    clear bgp * soft in
clear bgp * soft out   clear bgp <1-4294967295>   clear bgp <1-4294967295> in
clear bgp <1-4294967295> in prefix-filter    clear bgp <1-4294967295> out
clear bgp <1-4294967295> soft   clear bgp <1-4294967295> soft in    clear bgp
<1-4294967295> soft out    clear bgp (A.B.C.D|X:X::X:X)   clear bgp
(A.B.C.D|X:X::X:X) in   clear bgp (A.B.C.D|X:X::X:X) in prefix-filter   clear
bgp (A.B.C.D|X:X::X:X) out   clear bgp (A.B.C.D|X:X::X:X) soft    clear bgp
(A.B.C.D|X:X::X:X) soft in   clear bgp X:X::X:X soft out

--more--
```

show nsm client

Use this command to display NSM client information including the services requested by the protocols, statistics and the connection time

Command Syntax `show`

```
nsm client
```

Parameters

None

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show nsm client
NSM client ID: 1

NSM client ID: 19
 IMI, socket 23
  Service: Interface Service, Router ID Service, VRF Service
  Messsage received 1, sent 58
  Connection time: Thu Jul 22 11:03:12 2010
  Last message read: Service Request
  Last message write: Link Up
NSM client ID: 25
 ONMD, socket 24
  Service: Interface Service, Bridge service, VLAN service
  Messsage received 2, sent 74
  Connection time: Thu Jul 22 11:03:15 2010
  Last message read: OAM  LLDP msg
  Last message write: Link Up
#
```

show process

Use this command to display a process ID, the name of the process, how long the process has been running and any faults detected on the process.

Command Syntax

```
show process
```

Parameters

None

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show process
 PID NAME             TIME FD
   1 nsm          01:49:24 6

#
```

show running-config router

Use this command to display the running system router configuration.

Command Syntax `show running-config router bgp show running-config router isis show running-config router ldp show running-config router ospf show running-config router rip show running-config router rsvp show running-config router vrrp`

Parameters

`bgp`	Display Border Gateway Protocol (BGP) information.
`isis`	Display Intermediate System to Intermediate System (IS-IS) information.
`ldp`	Display Label Distribution Protocol (LDP) information.
`ospf`	Display Open Shortest Path First (OSPF) information.
`rip`	Display Routing Information Protocol (RIP) information.
`rsvp`	Display Resource Reservation Protocol (RSVP) information.
`vrrp`	Display Virtual Router Redundancy Protocol (VRRP) information.

Default

None

Command Mode

Privileged exec mode, configure mode, router-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
>enable
#show running-config router vrrp
!
router-id 3.3.3.3 !
```

show running-config switch

Use this command to display the running system switch configuration.

Command Syntax `show running-config switch bridge show running-config switch dot1x show running-config switch gmrp show running-config switch gvrp show running-config switch lacp show running-config switch lmi show running-config switch mstp show running-config switch radius-server show running-config switch rpsvt+ show running-config switch rstp show running-config switch ptp show running-config`

```
switch stp show running-config switch synce show
running-config switch vlan
```

Parameters `bridge` Display Bridge group information. `dot1x` Display 802.1x port-based authentication information. `gmrp` Display GARP Multicast Registration Protocol (GMRP) information. `gvrp` Display GARP VLAN Registration Protocol (GVRP) information. `lacp` Display Link Aggregation Control Protocol (LACP) information.

`lmi` Display Ethernet Local Management Interface Protocol (LMI) information. `mstp` Display Multiple Spanning Tree Protocol (MSTP) information.

`radius-server` Display RADIUS server information. `rpvst+` Display Rapid Per-VLAN Spanning Tree (rpvst+) information. `rstp` Display Rapid Spanning Tree Protocol (RSTP) information.

`ptp` Display Precision time Protocol (PTP) `stp` Display Spanning Tree Protocol (STP) information.

`synce` Display synce information. `vlan` Display values associated with a single VLAN.

Default None **Command**

Mode

Privileged exec mode, configure mode, router-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
                                        (config)#show running-config switch stp
! bridge 6 ageing-time 45 bridge 6 priority 4096 bridge 6
max-age 7
```

show running-config urpf

Use this command to check uRPF status for this system.

Command Syntax `show running-config urpf`

Parameters

None

Default

None

Command Mode

Exec mode and Privileged exec mode

Applicability

This command was introduced in SWMRE version 1.3.2.

Example

```
    #show running-config urpf ip urpf enable

    (config)#show running-config urpf ip urpf enable
```

show startup-config

Use this command to display the startup configuration.

Command Syntax `show startup-config`

Parameters

None

Default

None

Command Mode

Privileged exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
    #show startup-config
    !   2001/04/21 11:38:52
!
    hostname ripd password zebra log stdout
    ! debug rip events debug rip packet
    !
```

```
interface lo
!
interface eth0  ip rip send version 1 2  ip rip receive version 1 2
!
interface eth1  ip rip send version 1 2  ip rip receive version 1 2
!
router rip redistribute connected network 10.10.10.0/24
network 10.10.11.0/24
! line vty  exec-timeout 0 0
```

show version

Use this command to display SWMRE version information.

Command Syntax

```
show version
```

Parameters

None

Default

None

Command Mode

Exec mode and privileged exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show version
Software version: EC_AS5812-54X-SWMRE-1.3.4.268-DC_MPLS_ZEBM-S0-P0
09/27/2018 13:44:22
 Copyright (C) 2018 Coriant. All rights reserved

 Software Product: SWMRE, Version: 1.3.4.268
 Hardware Model: Edgecore 5812-54X-O-AC-F
 Software Feature Code: DC-MPLS-ZEBM
 System Configuration Code: S0
 Package Configuration Code: P0
Software Baseline Version: 1.3.4.208

Installation Information:
 Image Filename: EC_AS5812_54X-SWMRE-1.3.4.268-DC_MPLS_ZEBM-S0-P0-installer
 Install method: http
 ONIE SysInfo: x86_64-accton_as5812_54x-r0
#
```

Table 1-42: Show version output

Entry	Description
Software version	The software version including hardware device name and date.
Software Product	Product name and version.
Hardware Model	Hardware platform.
Software Feature Code	SKU that specifies the capabilities of this version of the software.
System Configuration Code	System configuration number.

Table 1-42: Show version output (Continued)

	Description
	ONIE package installer versions.
	Version from which this release branch is created.
	Information about the installation.
	The file name of the installed image.
	The type of server (or USB stick) from which the software was installed.
	ONIE version.

© Symanitron Proprietary

CHAPTER 2 Common Configure Mode Commands

This chapter provides a reference for the configure mode commands.

- automatic-router-id-selection enable
- clear router-id
- clock timezone
- errdisable cause
- errdisable link-flap-setting
- errdisable timeout
- forwarding custom-profile
- forwarding profile
- hardware-profile filter
- hardware-profile filter (Qumran)
- hardware-profile statistics (Qumran)
- ip urpf enable
- ip urpf allow-default
- ip mroute
- ipv6 mroute
- load-balance rtag7
- load-balance rtag7 hash
- load-balance rtag7 macro-flow
- router-id
- show errdisable details
- show forwarding profile limit
- show hardware-profile filters
- show interface errdisable status
- show router-id
- show running-config router-id

- snmp restart
- watch static-mac-movement

automatic-router-id-selection enable

Use this command to assure that SWMRE selects the loopback IP address as the router-id each time the device is rebooted.

Use the `no` form of this command to remove this constraint.

Command Syntax `automatic-router-id-selection enable no automatic-router-id-selection enable`

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced in SWMRE version 1.3.4.

Examples

```
#configure terminal
(config)#automatic-router-id-selection enable (config)#
```

clear router-id

Use this command to clear the current Router-Id and trigger the Router-Id calculation again. The new Router-id is sent to all protocol modules.

- To clear only the router-id for the default VRF, enter `clear router-id`.
- To clear the router-id for a particular VRF, enter `clear router-id vrf VRFNAME`.
- To clear the router-id for all VRFs, enter `clear router-id vrf`.

Command Syntax `clear router-id (vrf (VRFNAME|))`

Parameters

`VRFNAME`	VPN routing/forwarding instance name.

Command Mode

Configure mode

Applicability

This command was introduced in SWMRE version 1.3.4.

Examples

```
#configure terminal
(config)#clear router-id
(config)#


#configure terminal
(config)#clear router-id vrf
(config)#
```

clock timezone

Use this command to set the system time zone.

Use `no` form of this command to set the default system time zone (UTC).

Command Syntax `clock timezone (WORD) no clock timezone`

Parameters

`WORD`	Timezone name such as Los_Angeles or Hong_Kong

Default

By default, system time zone is UTC

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clock timezone Los_Angeles
```

errdisable cause

Use this command to globally shut down a port when certain errors happen:

- BPDU guard puts an interface configured for Spanning Tree Protocol (STP) Port Fast into the ErrDisable state upon receipt of a STP BPDU to avoid a potential bridging loop.
- If one side of a link-access group (LAG) is configured as a static LAG and the other side as a dynamic LAG, the ports on the side receiving LACP BPDUs go into the ErrDisable state

Note: When link-flap ErrDisable is enabled globally, then all interfaces are enabled. Link-flap ErrDisable can be enabled globally, but disabled for a specific interface with the `no link-flap errdisable` command.

Use `no` form of this command to not shut down a port when certain errors happen.

Command Syntax `errdisable cause {stp-bpdu-guard|lag-mismatch|link-flap}` `no errdisable cause {stp-bpdu-guard|lag-mismatch|link-flap}`

Parameters `stp-bpdu-guard` ErrDisable on stp-bpdu-guard `lag-mismatch` ErrDisable on lag-mismatch `link-flap` ErrDisable on link-flap

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#errdisable cause lag-mismatch
```

errdisable link-flap-setting

Use this command to configure the link-flap errdisable feature.

Note: Any previous flapping accumulated is flushed when you execute this command.

Command Syntax `errdisable link-flap-setting max-flaps <1-100> time <1-1800>`

Parameters

`<1-100>`	Maximum link-flap range
`<1-1800>`	Timer interval in seconds

Default

Five flaps in ten seconds:

max-flaps: 5 time: 10 seconds

Command Mode

Configure mode

Applicability

This command was introduced in SWMRE version 1.3.2.

Examples

```
#configure terminal
                        (config)#errdisable link-flap-setting max-flaps 5 time 20
```

errdisable timeout

Use this command to:

- Enable or disable ErrDisable timeout
- Set the ErrDisable timeout interval

Command Syntax `errdisable timeout (enable|disable) errdisable timeout interval <10-1000000>`

Parameters

`enable`	Enable timeout `disable` Disable timeout
`<10-1000000>`	Timeout interval in seconds

Default

By default, zero: timer is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#errdisable timeout enable
                                    (config)#errdisable timeout interval 1000
```

forwarding custom-profile

Use this command to configure forwarding table sizes.

Note: You must reboot after any profile change, except a change to the default profile. The configuration is applied only after a reboot.

Use `show-running configuration` or show forwarding profile limit to verify the selected profile.

Use the `forwarding custom-profile default` command (with no parameters) to set the forwarding table size to its default.

Command Syntax

Tomahawk platform:

```
forwarding custom-profile {l2-banks <1-4>|l3-banks <1-4>|lpm-banks 2}
```

Helix4 platform:

```
forwarding custom-profile {l2-banks <1-24>|l3-banks <1-23>|vlan-xlate-banks
  <123>|ep-vlan-xlate-banks <1-23>}
```

Tomahawk and Helix4 platforms:

```
forwarding custom-profile default
```

Parameters

`l2-banks` L2 banks. Unspecified banks are used as L2 banks.

`<1-4>` Number of L2 banks. Each bank size is 32k entries and each entry is 105 bits.

`<1-24>` Number of L2 banks. Each bank size is 1k entries and each entry is 420 bits.

`l3-banks` L3 banks. Unspecified banks are used as L2 banks.

`<1-4>` Number of L3 banks. Each bank size is 32k entries and each entry is 105 bits.

`<1-23>` Number of L3 banks. Each bank size is 1k entries and each entry is 420 bits.

`lpm-banks` Longest-prefix match banks. Unspecified banks are used as L2 banks.

`2` Two LPM banks per entry. The remaining banks can be used by any.

`vlan-xlate-banks`

VLAN translate banks. Unspecified banks are used as L2 banks.

`<1-23>` Number of VLAN translate banks. Each bank size is 1k entries and each entry is 420 bits. `ep-vlan-xlate-banks`

Egress VLAN translate banks. Unspecified banks are used as L2 banks.

<1-23>	Number of EP VLAN translate banks. Each bank size is 1k entries and each entry is 420 bits.
default	Use L2 profile Three; the size of the l2 table (MAC address table) and L3 table (host table) is almost equal.

Default

By default, forwarding table size is L2 profile Three.

Command Mode

Configure mode

Applicability

This command was introduced in SWMRE version 1.3.

This command only applies to Tomahawk and Helix4 platforms.

Examples

```
#configure terminal
                                        (config)#forwarding custom-profile l3-banks 4
```

forwarding profile

Use this command to configure forwarding table sizes.

Note: You must reboot after any profile change, except a change to the default profile. The configuration is applied only after a reboot.

Use `show-running configuration` or show forwarding profile limit to verify the selected profile.

Use this `no` command to set the forwarding table size to the default.

Command Syntax

```
forwarding profile (l2-profile-one | l2-profile-two | l2-profile-three |
                                                              l3-profile
| l3-128bit-profile | lpm-profile | lpm-128bit-profile)
no forwarding profile
```

Parameters

For details about these profiles, see show forwarding profile limit.

`l2-profile-one` L2 profile One `l2-profile-two` L2 profile Two `l2-profile-three`

L2 profile Three (default); the size of the l2 table (Mac address table) and l3 table (Host table) is almost equal

`l3-profile` L3 profile `l3-128bit-profile`

L3 profile with IPv6 prefix >64 support

`lpm-profile` Longest-prefix match profile `lpm-128bit-profile`

LPM profile with IPv6 prefix >64 support

Default

The default forwarding table size is L2 profile Three.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#forwarding profile l2-profile-one
```

hardware-profile filter

Use this command to enable or disable ingress IPv4 or IPv6 and egress IPv6 filter groups. Disabling filter groups increases the configurable filter entries.

Command Syntax `hardware-profile filter (ingress-ipv4|ingress-ipv6|egress-ipv6) (enable|disable)`

Parameter `ingress-ipv4` IPv4 filter ingress group. `ingress-ipv6` IPv6 filter ingress group. `egress-ipv6` IPv6 filter egress group. `enable` Enable filter group. `disable` Disable filter group.

Default

By default, all filter groups are enabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

This form of the `hardware-profile filter` command is *not* available on Qumran platforms. See hardware-profile filter (Qumran).

Examples

```
#configure terminal
(config)#hardware-profile filter ingress-ipv4 disable
(config)#hardware-profile filter ingress-ipv4 enable
```

hardware-profile filter (Qumran)

Use this command to enable or disable ingress and egress filter groups. Disabling filter groups increases the configurable filter entries.

Command Syntax

```
hardware-profile filter (ingress-l2-group|ingress-ipv4|qos-group|egress-ipv4|egress-ipv6|egress-l2-group) (enable|disable)
```

Parameter `ingress-l2-group` Layer 2 (MAC) filter ingress group. `ingress-ipv4` IPv4 filter ingress group. `qos-group` QoS filter group. `egress-ipv4` IPv4 filter egress group. `egress-ipv6` IPv6 filter egress group. `egress-l2-group` Layer 2 (MAC) filter egress group.

`enable`	Enable filter group. `disable` Disable filter group.

Default

By default, all filter groups are enabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

This command was only available on Qumran platforms. For other platforms, see hardware-profile filter.

Examples

```
#configure terminal
(config)#hardware-profile filter ingress-ipv4 disable
(config)#hardware-profile filter ingress-ipv4 enable
```

hardware-profile statistics (Qumran)

Use this command to enable or disable filter statistics in hardware.

Note: You must reboot the switch after giving this command for the changes to take effect.

Command Syntax

```
hardware-profile statistics (ingress-acl|mpls-ac|mpls-lsp|mpls-pwe)
  (enable|disable)
```

Parameter

`ingress-acl`	Ingress ACL statistics.
`mpls-ac`	Attachment circuit statistics.
`mpls-lsp`	LSP statistics.
`mpls-pwe`	Pseudowire logical interfaces statistics.
`enable`	Enable statistics.
`disable`	Disable statistics.

Default

By default, filter statistics are disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

This command is only available on Qumran platforms.

Examples

```
#configure terminal
(config)#hardware-profile statistics mpls-lsp enable
```

ip urpf enable

Use this command to enable uRPF mode on the system.

Use the `no` form of the command to disable uRPF mode on this system.

Note:The configuration is applied only after a reboot.

Command Syntax `ip urpf enable`

```
no ip urpf enable
```

Parameter

None

Default

By default, uRPF mode on the system is disabled.

Command Mode

Configure mode

Applicability

This command was introduced in SWMRE version 1.3.2.

Examples

```
#configure terminal
(config)#ip urpf enable
% System Reboot is required for new URPF configurations to take effect

(config)#no ip urpf enable
% System Reboot is required for new URPF configurations to take effect
```

ip urpf allow-default

Use this command to enable default route check for uRPF mode.

Use `no` form of this command to disable default route check for uRPF mode.

Command Syntax

This command applies only to Qumran platforms. `ip urpf allow-default no ip`

```
urpf allow-default
```

Parameter

None

Default

By default, uRPF mode on the system is disabled.

Command Mode

Configure mode

Applicability

This command was introduced in SWMRE version 1.3.2.

Examples

```
#configure terminal
(config)#ip urpf allow-default

(config)#no ip urpf allow-default
```

ip mroute

Use this command to create a multicast static route.

Multicast static routes are unicast routes which allow multicast and unicast topologies to be incongruous. These routes are used by multicast routing protocols to perform Reverse Path Forwarding (RPF) checks.

Use the `no` form of this command to clear a multicast static route.

Command Syntax `ip mroute (vrf NAME|) A.B.C.D/M (static|rip|ospf|bgp|isis|) (A.B.C.D|INTERFACE)`

`ip mroute (vrf NAME|) A.B.C.D/M (static|rip|ospf|bgp|isis|) (A.B.C.D|INTERFACE) <1-255>`

`no ip mroute (vrf NAME|) A.B.C.D/M (static|rip|ospf|bgp|isis|)`

Parameters

`NAME`	Virtual Routing and Forwarding name
`A.B.C.D/M`	Multicast source IP address and mask of the source
`static`	Static routes.
`rip`	Routing Information Protocol.
`ospf`	Open Shortest Patch First protocol.
`bgp`	Border Gateway Protocol.
`isis`	Intermediate System to Intermediate System protocol.
`A.B.C.D`	IP address to use as the RPF address. A host IP address can be a directly connected system or a remote system. For remote systems, a recursive lookup is done from the unicast routing table to find a directly connected system. Recursive lookup is done up to one level.
`INTERFACE`	Incoming interface name or pseudo interface null. Only specify for non-broadcast interfaces.
`<1-255>`	Administrative distance for the multicast static route. This value determines whether a unicast route or multicast static route is used for the RPF lookup. Lower distances have preference. If the multicast static route has the same distance as the other RPF sources, the multicast static route takes precedence.

Default

The default administrative distance for the multicast static route is 0.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip mroute 10.10.10.50/24 10.10.10.20 1
```

```
#configure terminal
(config)#ip mroute vrf VRF_A 10.10.10.50/1 10.10.10.20 1
```

ipv6 mroute

Use this command to create a multicast static route.

Multicast static routes are unicast routes that allow multicast and unicast topologies to be incongruous. These routes are used by multicast routing protocols to perform Reverse Path Forwarding (RPF) checks.

Use the `no` form of this command to clear a multicast static route.

Command Syntax `ipv6 mroute (vrf NAME|) X:X::X:X/M (static|rip|ospf|bgp|isis|) X:X::X:X INTERFACE`

`ipv6 mroute (vrf NAME|) X:X::X:X/M (static|rip|ospf|bgp|isis|) (X:X::X:X|INTERFACE)`

`ipv6 mroute (vrf NAME|) X:X::X:X/M (static|rip|ospf|bgp|isis|) X:X::X:X INTERFACE <1-255>`

`ipv6 mroute (vrf NAME|) X:X::X:X/M (static|rip|ospf|bgp|isis|) (X:X::X:X|INTERFACE)`

`<1-255> no ipv6 mroute (vrf NAME|) X:X::X:X/M (static|rip|ospf|bgp|isis|)`

Parameters

`NAME`	Virtual Routing and Forwarding name
`X:X::X:X/M`	Specify multicast source IP address and mask
`static`	Static routes.
`rip`	Routing Information Protocol.
`bgp`	Border Gateway Protocol.
`ospf`	Open Shortest Path First.
`isis`	Intermediate System to Intermediate System.
`X:X::X:X`	RPF address for the multicast route. A host IP address can be a directly connected system or a remote system. For remote systems, a recursive lookup is done from the unicast routing table to find a directly connected system. Recursive lookup is done up one level.
`INTERFACE`	Incoming interface name. Can only be specified for non-broadcast interfaces.
`<1-255>`	Administrative distance for the multicast static route. This value determines whether a unicast route or multicast static route is used for the RPF lookup. Lower distances have preference. If the multicast static route has the same distance as the other RPF sources, the multicast static route takes precedence.

Default

The default administrative distance for the multicast static route is 0.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
(config)#ipv6 mroute 10:10::10:10/64 10:10::10:12 1
```

load-balance rtag7

Use this command to configure rtag7 load balancing.

Use the `no` option to disable the rtag7 load balancing.

Command Syntax

This form enables or disables rtag7 load balancing globally:

```
load-balance rtag7 no load-balance rtag7
```

By default, load balancing is enabled for ECMP, LAG, and TRILL.

This form sets rtag7 hashing for ECMP and L3 LAG based on IPv4 fields:

```
load-balance rtag7 (ipv4 {src-ipv4|dest-ipv4|srcl4-port|destl4-port|protocol-id})
no load-balance rtag7 (ipv4 {src-ipv4|dest-ipv4|srcl4-port|destl4-port|protocol-
id})
```

By default, IPv4 ECMP is configured with the fields `src-ipv4`, `dest-ipv4`, `srcl4-port`, and `dest-l4port`.

By default, L3 LAG is configured with the fields `src-ipv4` and `dest-ipv4`.

This form sets rtag7 hashing for ECMP based on IPv6 fields:

```
load-balance rtag7 (ipv6 {src-ipv6|dest-ipv6|srcl4-port|destl4-port|next-hdr}) no
load-balance rtag7 (ipv6 {src-ipv6|dest-ipv6|srcl4-port|destl4-port|next-hdr})
```

By default, IPv6 ECMP is configured with the fields `src-ipv6`, `dest-ipv6`, `srcl4-port`, and `dest-l4port`.

This form sets rtag7 hashing for L2 LAG based on L2 fields:

```
load-balance rtag7 (l2 {dest-mac|src-mac|ether-type|vlan}) no
load-balance rtag7 (l2 {dest-mac|src-mac|ether-type|vlan})
```

By default, L2 LAG is configured with the fields `src-mac` and `dest-mac`.

This form sets rtag7 hashing on an MPLS egress LER node based on L2/L3 fields:

```
load-balance rtag7 (mpls-ler ((inner-l2 ({dest-mac|src-mac|ether-type|vlan})) |
  (inner-l3 ({src-ip|dest-ip|srcl4-port|destl4-port|protocol-id})))) no load-
balance rtag7 (mpls-ler ((inner-l2 ({dest-mac|src-mac|ether-type|vlan})) | (inner-
l3 ({src-ip|dest-ip|srcl4-port|destl4-port|protocol-id}))))
```

Please note the following:

- For ingress LER nodes, hashing is done on L2 fields, L3 fields (outer IPx), or inner IP fields (only for IPx-over-IPx or IPx-over-GRE-IPx).
- For egress LER nodes, hashing is done based on only L2 and L3 fields immediately after the MPLS header which is popped. Any other fields are not supported.

This form sets rtag7 hashing based on TRILL fields:

```
load-balance rtag7 (trill (outer-l2|inner-l2|inner-l3)) no
load-balance rtag7 (trill (outer-l2|inner-l2|inner-l3))
```

By default, TRILL is configured with the inner-l2 header's inner SMAC and DMAC.

This form sets rtag7 hashing based on the outer IP address:

```
load-balance rtag7 (tunnel outer-l3-header) no
load-balance rtag7 (tunnel outer-l3-header)
```

Parameters `ipv4` Load balance IPv4 packets

`src-ipv4` Source IPv4 based load balancing `dest-ipv4` Destination IPv4 based load balancing `srcl4-port` Source L4 port based load balancing `destl4-port` Destination L4 port based load balancing `protocol-id` Protocol ID based load balancing

`ipv6` Load balance IPv6 packets

`src-ipv6` Source IPV6 based load balancing `dest-ipv6` Destination IPv6 based load balancing `srcl4-port` Source L4 port based load balancing `destl4-port` Destination L4 port based load balancing `next-hdr` Next header field for IPv6

`l2` Load balance L2 packets

`dest-mac` Destination MAC address based load balancing `src-mac` Source MAC address based load balancing `ether-type` Ether-type based load balancing `vlan` VLAN-based load balancing

`trill` Load balance TRILL packets

`outer-l2` TRILL outer l2 header (outer SMAC, outer DMAC, outer VLAN) `inner-l2` TRILL inner l2 header (inner SMAC, inner DMAC, inner VLAN, TRILL tunnel) `inner-l3` TRILL inner l3 header (inner SIP, inner DIP, L4 src/dest port)

`tunnel` Load balance tunneled packets based on outer header (default uses the inner-header)

`outer-l3-header`

Use outer header for hashing (ip-over-ip, ipv6-over-ip, ip-over-gre-ip, ipv6-over-gre-ip, ipv6-over-ipv6, ip-over-ipv6, ip-over-gre-ipv6, ipv6-over-gre-ipv6)

`mpls-ler` Load balance LER packets `inner-l2` Load balance Inner l2 header `dest-mac` Destination MAC address load balancing `src-mac` Source MAC address

`ether-type`

Ether-type based load balancing

`vlan` VLAN tag id

`inner-l3` Inner l3 header `dest-ip` Destination IP address `src-ip` Source IP address

`srcl4-port`

Source L4 port based load balancing

`protocol ID`

Protocol (IPv4), nxt-hdr (IPv6)

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#load-balance rtag7
                                    (config)#load-balance rtag7 ipv4 src-ipv4
```

load-balance rtag7 hash

Use this command to set the rtag7 hash computation method.

Use the `no` parameter to set the rtag7 hash computation method to its default.

Command Syntax `load-balance rtag7 hash (crc16-bisync|crc16-ccitt|crc32-lo|crc32-hi) no load-balance rtag7 hash`

Parameters

`crc16-bisync`	16-bit CRC16 using the binary synchronous polynomial.
`crc16-ccitt`	16-bit CRC16 using the CCITT polynomial.
`crc16-hi`	16 most significant bits of computed CRC32.
`crc16-lo`	16 least significant bits of computed CRC32

Default

The default rtag7 hash computation method is 16-bit CRC16 using the binary synchronous polynomial `(crc16bisync)`.

Command Mode

Configure mode

Default settings `load-balance rtag7 hash`

`crc16-bisync`

Applicability

This command was introduced in version SWMRE version 1.3.1.

Example

```
#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
(config)#load-balance rtag7
(config)#load-balance rtag7 hash crc16-ccit (config)#show
running-config | inc rtag7
!
load-balance rtag7
load-balance rtag7 hash crc16-ccitt
!
(config)#no load-balance rtag7 hash
(config)#
```

load-balance rtag7 macro-flow

Use this command to enable rtag7 macro-flow based hashing.

When macro-flow is enabled, a hash function is chosen dynamically based on corresponding macro flow. It is useful when hash polarization is observed in the topology.

Use the `no` parameter to disable rtag7 macro-flow based hashing.

Command Syntax `load-balance rtag7 macro-flow no load-balance rtag7 macro-flow`

Parameters

None

Default

By default, rtag7 macro-flow based hashing is disabled.

Command Mode

Configure mode

Applicability

This command was introduced in version SWMRE version 1.3.1.

Example

```
#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
(config)#load-balance rtag7
(config)#load-balance rtag7 macro-flow
(config)#show running-config | inc rtag7
!
load-balance rtag7 load-
balance rtag7 macro-flow
!
(config)#no load-balance rtag7 macro-flow
```

router-id

Use this command to add a router identifier for this system.

Use the `no` form of this command to disable this function.

Command Syntax `router-id A.B.C.D no router-id (A.B.C.D)`

Parameters

`A.B.C.D`	Router identifier in IP address format for this system.

Default

None

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router-id 123.12.3.123
(config)#
```

show errdisable details

Use this command to display ErrDisable settings.

Command Syntax `show errdisable details`

Parameters

None

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show errdisable details
```

show forwarding profile limit

Use this command to show all the forwarding table sizes.

Command Syntax `show forwarding profile limit`

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show forwarding profile limit
Current profile : l2-profile-three

=========================================================================
                              Forwarding Profile Table                  |
-------------------------------------------------------------------------|
Profile Name        | MAC-Table Size |Host-Table Size| Prefix-Table Size |
                    | ------------------------------------------------|
                    |   MAC ADDR     |IPV4 UC IPV6 UC|    IPV4    IPV6   | ---
-------------------------------------------------------------------------| l2-
profile-one           288K          16K     8K          8k     4k      | l2-
profile-two           224K          80K     40K         8k     4k      | l2-
profile-three                                                          |
(default)        160K          144K    72K         8k     4k     | l3-profile
96K           208K    104K        8k     4k     | lpm-profile             32K
16K     8K          128k   16k    |
========================================================================= #
```

Table 2-43 explains the show command output fields.

Table 2-43: show forwarding profile limit output

Entry	Description
Profile Name	Names of the forwarding profiles.

MAC-Table Sizes	The MAC address tables
Host-Table Sizes	Size of host tables.

Table 2-43: show forwarding profile limit output (Continued)

	Description
	Size of the prefix tables.
	Number of kilobytes available for MAC for each forwarding table.
	Number of kilobytes available for IPv4 unicast host for each forwarding table.
	Number of kilobytes available for IPv6 unicast hosts for each forwarding table.
	Number of kilobytes available for IPv4 addresses for each forwarding table.
	Number of kilobytes available for IPv6 prefixes that are less than or equal to 64 for each forwarding table.
	Number of kilobytes available for IPv6 prefixes that are greater than or equal 65 for each forwarding table.

show hardware-profile filters

Command Syntax `show hardware-profile filters`

Parameters

None

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

This command is *not* available on Qumran platforms.

Examples

```
#show hardware-profile filters
INGRESS:
+--------------------+---------+---------+-------------------------+
|                    | Free    | Used    |       Total Entries     |
| TCAMS              | Entries | Entries |-------------------------|
|                    |         |         | Total | Dedicated | shared |
+--------------------+---------+---------+-------+-----------+--------+
 QOS                  1012      12        1024    512         512
 L2-ACL               1021      3         1024    512         512
 IPV4-ACL             768       0         768     256         512
 IPV6-ACL             766       2         768     256         512
EGRESS:
+--------------------+---------+---------+-------------------------+
|                    | Free    | Used    |       Total Entries     |
| TCAMS              | Entries | Entries |-------------------------|
|                    |         |         | Total | Dedicated | shared |
+--------------------+---------+---------+-------+-----------+--------+
 L2-ACL/IPV4-ACL/QOS  256       0         256     256         0
 IPV6-ACL             256       0         256     256         0
```

show interface errdisable status

Use this command to display ErrDisable conditions for an interface.

Command Syntax `show interface errdisable status`

Parameters

None

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show interface errdisable status ge1 lag-mismatch-errdisable ge2 stp-
bpdu-guard-errdisable
```

show router-id

Use this command to display the Router ID of the current system.

Command Syntax `show router-id`

Parameters

None

Default

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show router-id
Router ID: 10.55.0.2 (automatic)
```

show running-config router-id

Use this command to show the running system global router ID configuration.

Command Syntax `show running-config router-id`

Parameters

None

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
>enable
#show running-config router-id
!
router-id 3.3.3.3 !
```

snmp restart

Use this command to restart SNMP for a given process.

Command Syntax

```
snmp restart (auth | bfd | bgp | cfm | efm | isis | ldp | lldp | mrib | mstp | nsm |
  ospf | ospf6 | pim | rib| rip | rmon | rsvp | trill | vrrp)
```

Parameters

None

Default

By default, SNMP resart is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#snmp restart nsm
```

watch static-mac-movement

Use this command to watch any MAC movement is detected over static MAC entry for a time period. Notification will be displaying if static MAC movement happens till timer expires.

Command Syntax `watch static-mac-movement`

`(<1-300>|)`

Parameters

`<1-300>`	Timer value in second.

Default

By default, timer is 10 seconds

Command Mode

Exec mode

Applicability

This command was introduced in SWMRE version 1.3.2.

Examples

```
#watch static-mac-movement
```

CHAPTER 3 Common Route-Map Mode Commands

This chapter is a reference for route-map commands. These commands are common to multiple protocols

This chapter includes the following commands:

- continue
- match as-path
- match community
- match extcommunity
- match interface
- match ip address
- match ip address prefix-list
- match ip next-hop
- match ip next-hop prefix-list
- match ip peer
- match ipv6 address
- match ipv6 address prefix-list
- match ipv6 next-hop
- match ipv6 next-hop prefix-list
- match ipv6 peer
- match metric
- match origin
- match route-type
- match tag
- route-map
- set aggregator
- set as-path
- set atomic-aggregate
- set comm-list
- set community
- set dampening
- set extcommunity
- set interface null0
- set ip next-hop
- set ipv6 next-hop
- set level
- set local-preference
- set metric

- set metric-type
- set origin
- set originator-id
- set tag
- set vpnv4 next-hop
- set weight
- show route-map
- show running-config route-map

continue

The continue clause provides the capability to execute additional entries in a route map after an entry is executed with a successful match and set clauses (i.e), the continue command allows multiple entries to be evaluated within a single route-map. Continue commands can be assigned optional sequence numbers that indicate the order in which clauses are to be evaluated.

Use the no form of the command (specifying a particular sequence number if desired), to remove individual or all continue clauses from a route-map.

Continue clause with match Clauses

When a match clause exists in a route map with continue clause, then the continue clause is executed only when a successful match occurs. If a match clause does not exist in the route-map and if a continue clause does exist, the continue clause will be evaluated and then go to the specified route-map entry. When a successful match occurs and we have a continue clause, the route-map executes the set clauses and then goes to the specified route-map entry. If continue clause does not exist in the next route map, then the route-map will behave normally. If a continue clause exists in the next route-map but a match is not successful, the route-map will not continue and will *fall through* to the next sequence number if one exists.

Continue clause with set Clauses

Set clauses are executed after the route-map evaluation is done. The set clauses are evaluated and executed in the order in which they were configured. Set clauses are only executed after a successful match occurs. The continue statement proceeds to the specified route-map entry only after configured set actions are performed. If a set action is configured in the first route-map and then the same set action occurs again, but with a different value in a subsequent route-map entry, then the last set action will override the previous set actions, which were configured with the same set command.

Command Syntax continue

```
<2-65535>|) no continue
<2-65535>|)
```

Parameter

<2-65535>	Continue sequence number.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced in SWMRE version 1.3.5.

Example

```
(config)#route-map Rmap1
(config-route-map)#continue ?
```

```
      <2-65535>  Route-map entry sequence number
                                                                  <cr>
    (config-route-map)#continue 10
(config-route-map)#continue 30
```

match as-path

Use this command to match an autonomous system path access list. This command specifies the autonomous system path to be matched. If there is a match for the specified AS path, and `permit` is specified, the route is redistributed or controlled, as specified by the set action. If the match criteria are met, and `deny` is specified, the route is not redistributed or controlled. If the match criteria are `not` met then the route is neither accepted nor forwarded, irrespective of `permit` or `deny` specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes, depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Note: This command is valid only for BGP.

Use the `no` parameter with this command to remove a path list entry.

Command Syntax `match as-path WORD no match as-path (WORD|)`

Parameter

`WORD`	Autonomous system path access list name.

Default

Enabled

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#route-map myroute deny 34
(config-route-map)#match as-path myaccesslist
```

match community

Use this command to specify the community to be matched.

Communities are used to group and filter routes. They are designed to provide the ability to apply policies to large numbers of routes by using match and set commands. Community lists are used to identify and filter routes by their common attributes. This command allows the matching based on community lists.

The values set by the `match community` command overrides the global values. The route that does not match at least one match clause is ignored.

Note: This command is valid only for BGP.

Use the `no` parameter with this command to remove the community list entry.

Command Syntax `match community (<1-99>|<100-199>|WORD) (exact-match|) no match community (<1-99>|<100-199>|WORD|) (exact-match|)`

Parameters

`<1-99>`	Community-list number (standard).
`<100-199>`	Community-list number (expanded).
`WORD`	Community-list name.
`exact-match`	Do exact matching of communities.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#route-map myroute permit 3
(config-route-map)#match community mylist
```

match extcommunity

Use this command to match BGP external community list

Communities are used to group and filter routes. They are designed to provide the ability to apply policies to large numbers of routes by using match and set commands. Community lists are used to identify and filter routes by their common attributes. This command allows the matching based on community lists.

The values set by this command overrides the global values. The route that does not match at least one match clause is ignored.

Note: This command is valid only for BGP.

Use the no parameter with this command to remove the community list entry.

Command Syntax match extcommunity (<1-99>|<100-199>|WORD) (exact-match|) no match extcommunity (<1-99>|<100-199>|WORD|) (exact-match|)

Parameters

<1-99>	Community-list number (standard).
<100-199>	Community-list number (expanded).
WORD	Name of the community-list.
exact-match	Do exact matching of communities.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#route-map myroute permit 3
(config-route-map)#match extcommunity mylist
```

match interface

Use this command to define the interface match criterion. This command specifies the next-hop interface name of a route to be matched.

Use the no parameter with this command to remove the specified match criterion.

Command Syntax match interface IFNAME no match interface (IFNAME|)

Parameter

IFNAME	Interface name.

Default

By default, match interface is disabled

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#route-map mymap1 permit 10
(config-route-map)#match interface eth0
```

match ip address

Use this command to specify the match address of route. If there is a match for the specified IP address, and `permit` is specified, the route is redistributed or controlled, as specified by the set action. If the match criteria are met, and `deny` is specified then the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of `permit` or `deny` specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes, depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Use the `no` parameter with this command to remove the `match ip address` entry.

Command Syntax `match ip address (<1-199>|<1300-2699>|WORD)` `no match ip address (<1-199>|<1300-2699>|WORD|)`

Parameters

`WORD`	IP access-list name.
`<1-199>`	IP access-list number (standard range).
`<1300-2699>`	IP access-list number (expanded range).

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#route-map myroute permit 3
(config-route-map)#match ip address List1
```

match ip address prefix-list

Use this command to match entries of a prefix-list. The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or

content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables. Use the `no` parameter with this command too disable this function

Command Syntax `match ip address prefix-list WORD no match ip address prefix-list (WORD|)`

Parameter

`WORD`	IP prefix list name.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#match ip address prefix-list mylist
```

match ip next-hop

Use this command to specify a next-hop address to be matched in a route-map. The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Use the `no` parameter with this command to disable this function.

Command Syntax `match ip next-hop (<1-199>|<1300-2699>|WORD) no match ip next-hop (<1-199>|<1300-2699>|WORD|)`

Parameters

`WORD`	Specify the IP access-list name.
`<1-199>`	Specify the IP access-list number (standard range).
`<1300-2699>`	Specify the IP access-list number (expanded range).

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#match ip next-hop mylist
```

match ip next-hop prefix-list

Use this command to specify the next-hop IP address match criterion using the prefix-list. This command matches the next-hop IP address of a route.

Use the `no` parameter with this command to remove the specified match criterion.

Command Syntax `match ip next-hop prefix-list WORD no match ip next-hop prefix-list (WORD|)`

Parameter

`WORD`	Prefix-list name.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#route-map mymap permit 3
(config-route-map)#match ip next-hop prefix-list list1
```

match ip peer

Use this command to specify the match peer IPv4 address of a route.

Use the `no` parameter with this command to remove the specified match criterion.

Command Syntax `match ip peer (<1-199>|<1300-2699>|WORD) no match ip peer (<1-199>|<1300-2699>|WORD|)`

Parameter

WORD	IP access-list name.
<1-199>	IP access-list number (standard range).
<1300-2699>	IP access-list number (expanded range).

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#route-map mymap permit 3
(config-route-map)#match ip peer 123

(config-route-map)#no match ip peer 123
```

match ipv6 address

Use this command to specify the match address of route. The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Use the `no` parameter with this command to remove the `match ip address` entry.

Note: This command is valid for BGP, OSPFv3, and RIPng only.

Command Syntax `match ipv6 address WORD no match ipv6 address (WORD|)`

Parameter

WORD	IPv6 access list name.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#route-map myRM deny 1
(config-route-map)#match ipv6 address myRM
```

match ipv6 address prefix-list

Use this command to match entries of a prefix-list. The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes, depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Note: This command is valid for BGP, OSPFv3, and RIPng only.

Use the `no` parameter with this command to disable this function

Command Syntax `match ipv6 address prefix-list WORD no match ipv6 address prefix-list (WORD|)`

Parameter

`WORD`	IPv6 access list name.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#match ipv6 address prefix-list mylist
```

match ipv6 next-hop

Use this command to specify the next-hop address to be matched. The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Note: This command is valid for BGP and IS-IS only.

Use the `no` parameter with this command to disable this function

Command Syntax `match ipv6 next-hop (X:X::X:X|WORD) no match ipv6 next-hop (X:X::X:X|WORD|)`

Parameters

X:X::X:X	IPv6 address of the next-hop.
WORD	IPv6 access list name.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#match ipv6 next-hop 3ffe::1
```

match ipv6 next-hop prefix-list

Use this command to match entries of a prefix-list. The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Note: This command is valid for BGP and IS-IS only.

Use the `no` parameter with this command to disable this function

Command Syntax `match ipv6 next-hop prefix-list WORD no match ipv6 next-hop prefix-list WORD`

Parameters

WORD	IPv6 access list name.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
```

```
(config-route-map)#match ipv6 next-hop prefix-list new
```

match ipv6 peer

Use this command to specify the match peer IPv6 address of a route.

Use the `no` parameter with this command to remove the specified match criterion.

Command Syntax `match ipv6 peer (<1-199>|<1300-2699>|WORD) no match ipv6 peer (<1-199>|<1300-2699>|WORD|)`

Parameter

`WORD`	IP access-list name.
`<1-199>`	IP access-list number (standard range).
`<1300-2699>`	IP access-list number (expanded range).

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#route-map mymap permit 3
(config-route-map)#match ipv6 peer 123

(config-route-map)#no match ipv6 peer 123
```

match metric

Use this command to match a metric of a route. The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Note: This command is valid for BGP, OSPF, RIP, and IS-IS only.

Use the `no` parameter with this command to disable this function

Command Syntax `match metric <0-4294967295> no match metric (<0-4294967295>|)`

Parameters

`<0-4261412864>`	Metric value.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#route-map myroute permit 3
(config-route-map)#match metric 888999
```

match origin

Use this command to match origin code. The origin attribute defines the origin of the path information. The `egp` parameter is indicated as an `e` in the routing table, and it indicates that the origin of the information is learned via EGP (Exterior Gateway Protocol). The `igp` parameter is indicated as an `i` in the routing table, and it indicates the origin of the path information is interior to the originating AS. The `incomplete` parameter is indicated as a `?` in the routing table, and indicates that the origin of the path information is unknown or learned through other means. If a static route is redistributed into BGP, the origin of the route is incomplete.

This command specifies the origin to be matched. If there is a match for the specified origin, and `permit` is specified when you created the route-map, the route is redistributed or controlled as specified by the set action. If the match criteria are met, and `deny` is specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of `permit` or `deny` specifications.

The route specified by the policies might not be the same as specified by the routing protocols. Setting policies enable packets to take different routes depending on their length or content. Packet forwarding based on configured policies overrides packet forwarding specified in routing tables.

Note: This command is valid only for BGP.

Use the `no` parameter with this command to disable this matching.

Command Syntax `match origin`

```
(egp|igp|incomplete) no match origin
(egp|igp|incomplete|)
```

Parameters `egp` Remote exterior gateway protocol.

`igp` Local internal gateway protocol.

`incomplete` Unknown heritage.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#route-map myroute deny 34
(config-route-map)#match origin egp
```

match route-type

Use this command to match an external route type. AS-external LSA is either Type-1 or Type-2. External type-1 matches only Type 1 external routes and external type-2 matches only Type 2 external routes.

Use the `no` parameter with this command to turn off the matching.

Command Syntax `match route-type external (type-1|type-2) no match route-type external (type-1|type-2|)`

Parameters

`type-1`	Match OSPF External Type 1 metric.
`type-2`	Match OSPF External Type 2 metric.

Default

By default, match route type external is disabled

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#route-map mymap1 permit 10
(config-route-map)#match route-type external type-1
```

match tag

Use this command to match the specified tag value.

Use the `no` parameter with this command to turn off the declaration.

Command Syntax `match tag <0-4294967295> no match tag (<0-4294967295>|)`

Parameters

`<0-4294967295>`	Tag value.

Default

By default, match tag is disabled

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#route-map mymap1 permit 10
(config-route-map)#match tag 100
```

route-map

Use this command to enter route-map mode and to permit or deny match/set operations.

This command controls and modifies routing information to allow redistribution of routes. It has a list of `match` and `set` commands associated with it. The `match` commands specify the conditions under which redistribution is allowed, and the `set` commands specify the particular redistribution actions to be performed if the criteria enforced by match commands are met. Route maps are used for detailed control over route distribution between routing processes.

Route maps also allow policy routing, and might route packets to a different route than the obvious shortest path.

Use the `no` parameter with this command to turn off the declaration.

Command Syntax `route-map WORD (deny|permit) <1-65535> no route-map WORD ((deny|permit) <1-65535>|)`

Parameters

`WORD`	Route-map name (maximum size 63 characters).
`deny`	Route map deny set operations. If this parameter is specified, and the match criteria are met, the route is not redistributed, and any other route maps with the same map tag are not examined.
`permit`	Route map permit set operations. If this parameter is specified, and the match criteria are met, the route is redistributed as specified by the set actions. If the `match` criteria are not met, the next route map with the same tag is tested.
`<1-65535>`	Sequence to insert into or delete from an existing route-map.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#route-map route1 permit 1
(config-route-map)#
```

set aggregator

Use this command to set the AS number for the route map and router ID. An Autonomous System (AS) is a collection of networks under a common administration sharing a common routing strategy. It is subdivided by areas, and is assigned a unique 16-bit number. Use the `set aggregator` command to assign an AS number for the aggregator.

To use the `set aggregator` command, you must first have a match clause. `Match` and `set` commands set the conditions for redistributing routes from one routing protocol to another. The `match` command specifies the match criteria under which redistribution is allowed for the current route-map. The `set` command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Use the `no` parameter with this command to disable this function

Command Syntax `set aggregator as <1-65535>`

`A.B.C.D no set aggregator as (<1-65535>`

`A.B.C.D|)`

Parameters

`<1-65535>` AS number of aggregator. `A.B.C.D`

IP address of aggregator.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#route-map myroute permit 3
(config-route-map)#set aggregator as 43 10.10.0.3
```

set as-path

Use this command to modify an autonomous system path for a route. By specifying the length of the AS-Path, the router influences the best path selection by a neighbor. Use this command to prepend an AS path string to routes increasing the AS path length.

To use this command, you must first give the match and set commands configure the conditions for redistributing routes from one routing protocol to another:

- The match command specifies the match criteria under which redistribution is allowed for the current route-map.
- The set command specifies the set redistribution actions to be performed if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Use the no parameter with this command to disable this function.

Command Syntax set as-path prepend .<1-65535>

set as-path prepend .<1-4294967295> no set as-path prepend (.<1-65535>|) no set as-path prepend (.<1-4294967295>|)

Parameters

<1-65535> SWMRE prepends this number to the AS path.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#route-map myroute permit 3
(config-route-map)#set as-path prepend 8 24
```

set atomic-aggregate

Use this command to set an atomic aggregate attribute.

To use this command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Use the no parameter with this command to disable this function

Command Syntax set atomic-aggregate no set atomic-aggregate

Parameters

No default value is specified

Default

None

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set atomic-aggregate
```

set comm-list

Use this command to delete the matched communities from the community attribute of an inbound or outbound update when applying route-map.

Use the `no` parameter with this command to disable this feature.

Command Syntax `set comm-list (<1-99>|<100-199>|WORD) delete no set comm-list (<1-99>|<100-199>|WORD) delete`

Parameters

`<1-99>`	Standard community-list number.
`<100-199>`	Expanded community-list number.
`WORD`	Name of the community-list.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#route-map myRM permit 3
(config-route-map)#set comm-list 34 delete
```

set community

Use this command to set the communities attribute. and group destinations in a certain community, as well as apply routing decisions according to those communities.

To use this command, you must first have a match clause. `Match` and `set` commands set the conditions for redistributing routes from one routing protocol to another. The `match` command specifies the match criteria under which redistribution is allowed for the current route-map. The `set` command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Use the `no` parameter with this command to delete the entry.

Command Syntax

```
set community [<65536-4294901759>|AA:NN|internet|local-AS|no-advertise|no-
  export|none] (additive|)
no set community [AA:NN|internet|local-AS|no-advertise|no-export|none] (additive|)
```

Parameters

`<65536-4294901759>`	Community number
`AA:NN`	The community number in aa:nn format.
`internet`	Internet.
`local-AS`	Do not send outside the local AS (well-known community).
`no-advertise`	Do not advertise this route to eBGP peers
`no-export`	Do not advertise this route to any peer.
`none`	Remove the community attribute from the prefixes that pass the route-map.
`additive`	Add to the existing community.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following examples show the use of the `set community` command with different parameters.

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set community no-export no-advertise
```

```
#configure terminal
(config)#route-map rmap1 permit 3
```

```
(config-route-map)#set community no-advertise
```

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set community 10:01 23:34 12:14 no-export
```

set dampening

Use this command to enable route-flap dampening and set parameters. Set the unreachability half-life time to be equal to, or greater than, reachability half-life time. The suppress-limit value must be greater than or equal to the reuse limit value.

Use the `no` parameter with this command to delete the entry.

Command Syntax `set dampening <1-45> <1-20000> <1-20000> <1-255>`

`(<1-45>|) no set dampening <1-45> <1-20000> <1-20000> <1-255>`

`(<1-45>|)`

Parameters

`<1-45>`	Reachability half-life time in minutes. The time for the penalty to decrease to one-half of its current value.
`<1-20000>`	Reuse-limit value. When the penalty for a suppressed route decays below the reuse value, the routes become unsuppressed.
`<1-20000>`	Suppress-limit value. When the penalty for a route exceeds the suppress value, the route is suppressed.
`<1-255>`	Max-suppress-time. Maximum time that a dampened route is suppressed.
`<1-45>`	Unreachability half-life time for penalty, in minutes.

Default

Default reachability half-life time: 15 minutes

Default reuse limit value: 750

Default suppress limit value: 2000

Default max-suppress value is 4 times the half-life time (60 minutes)

Default unreachability half-life time value: 15 minutes

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#route-map R1 permit 24
(config-route-map)#set dampening 20 333 534 30
```

set extcommunity

Use this command to set an extended community attribute.

To use this command you must first have a match clause. The `match` and `set` commands define the conditions for redistributing routes from one routing protocol to another:

- The `match` command defines the match criteria under which redistribution is allowed for the current route-map.

- The `set` command defines the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Use the `no` parameter with this command to disable this function.

Command Syntax `set extcommunity rt .AA:NN (additive|) set extcommunity soo .AA:NN set extcommunity cost (igp|pre-bestpath|) <0-255> <0-4294967295> no set extcommunity rt (.AA:NN|) (additive|) no set extcommunity soo (.AA:NN|)`

`no set extcommunity cost (igp|pre-bestpath|) <0-255> <0-4294967295>`

Parameters

`rt`	Route target extended community.
`.AA:NN`	VPN extended community
`additive`	Add to the exsisting community.
`soo`	Site-of-origin extended community.
`cost`	Extended cost community.
`igp`	Compare following IGP cost comparison.
`pre-bestpath`	Compare following IGP cost comparison.
`<0-255>`	Community ID.
`<0-4294967295>`	Cost.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
```

```
(config)#route-map rmap1 permit 3 (config-
route-map)#set extcommunity rt 06:01

#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set extcommunity rt 0.0.0.6:01

#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set extcommunity soo 06:01

#configure terminal
(config-route-map)#route-map rmap1 permit 3
(config-route-map)#set extcommunity soo 0.0.0.6:01
```


© Symanitron Proprietary

set interface null0

Use this command to discard routes based on policy/rules configured for a route map.

Route maps can be applied to BGP neighbors. When this command is given for a route map and that route map is applied to a BGP neighbor, the discard route entries are added by BGP for the prefix permitted by the route map.

Use the `no` form of this command to not discard routes based on policy/rules configured for a route map.

Command Syntax `set interface null0 no set interface null0`

Parameters

None

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced in SWMRE version 1.3.4.

Example

To discard 1.1.1.1/24 from BGP neighbor 30.1.1.1:

```
#configure terminal
(config)#ip prefix-list myPrefixList seq 5 permit 1.1.1.1/24 eq
24 (config)#route-map myRM permit 1
(config-route-map)#match ip address prefix-list
myPrefixList (config-route-map)#set interface null0
(config-route-map)#exit (config)#router bgp
200
(config-router)#neighbor 30.1.1.1 remote-as 200
(config-router)#neighbor 30.1.1.1 route-map myRM in
```

set ip next-hop

Use this command to set the specified next-hop value.

Use the `no` parameter with this command to turn off the setting.

Note: This command is valid for BGP, OSPF, and RIP only.

Command Syntax `set ip next-hop A.B.C.D no set ip next-hop (A.B.C.D|)`

Parameter

`A.B.C.D`	IP address of the next-hop.

Default

By default, set ip next hop A.B.C.D is disabled

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#route-map mymap permit 3
                                        (config-route-map)#set ip next-hop 10.10.0.67
```

set ipv6 next-hop

Use this command to set a next hop-address.

Use the `no` parameter with this command to delete an entry.

Note: This command is valid for BGP and OSPFv3 only.

Command Syntax `set ipv6 next-hop X:X::X:X set ipv6 next-hop local X:X::X:X no set ipv6 next-hop (X:X::X:X|) no set ipv6 next-hop local (X:X::X:X|)`

Parameters

`X:X::X:X` Global IPv6 address of the nexthop. `local` Local IPv6 address of the nexthop.

Default

By default, set ipv6 next hop X:X::X:X is disabled

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
               (config-route-map)#set ipv6 next-hop local fe80::203:47ff:fe97:66dc
```

set level

Use this command to set the IS-IS level to export a route.

Use the `no` parameter with this command to disable this function.

Command Syntax `set level (level-1|level-2|level-1-2) no set level (level-1|level-2|level-1-2|)`

Parameters

`level-1`	Export into a level-1 area.
`level-2`	Export into a level-2 sub-domain.
`level-1-2`	Export into level-1 and level-2.

Default

By default, set level is disabled

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set level level-1
```

set local-preference

Use this command to set the BGP local preference path attribute.

Use the `no` parameter with this command to disable this function.

Command Syntax `set local-preference <0-4294967295> no set local-preference (<0-4294967295>|)`

Parameters

`<0-4294967295>` Tag value for destination routing protocol.

Default

By default, set local preference is disabled

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#route-map rmap1 permit 3
                  (config-route-map)#set local-preference 12
```

set metric

Use this command to set a metric value for a route and influence external neighbors about the preferred path into an Autonomous System (AS). The preferred path is the one with a lower metric value. A router compares metrics for paths from neighbors in the same ASs. To compare metrics from neighbors coming from different ASs, use the `bgp always-compare-med` command.

To use this command, you must first have a match clause. `Match` and `set` commands set the conditions for redistributing routes from one routing protocol to another. The `match` command specifies the match criteria under which redistribution is allowed for the current route-map. The `set` command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Use the `no` parameter with this command to disable this function.

Command Syntax `set metric`

`WORD no set metric`

`(WORD|)`

Parameters

`WORD`	Metric value [+/-] <1-4294967295>

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set metric 600
```

set metric-type

Use this command to set the metric type for the destination routing protocol. Select a type to be either Type-1 or Type2 in the AS-external-LSA when the route-map matches the condition.

Note: This command is for OSPF, OSPFv3, or IS-IS only.

Use the `no` parameter with this command to return to the default.

Command Syntax `set metric-type (internal|external)` `set metric-type (type-1|type-2)` `no set metric-type (internal|external|)` `no set metric-type (type-1|type-2|)`

Parameters

`external`	IS-IS external metric type.
`internal`	IS-IS internal metric type.
`type-1`	OSPF external type 1 metric.
`type-2`	OSPF external type 2 metric

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

In this example the metric type of the destination protocol is set to OSPF external Type 1.

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set metric-type 1
```

set origin

Use this command to set the BGP origin code. The origin attribute defines the origin of the path information.

To use this command, you must first have a match clause. `Match` and `set` commands set the conditions for redistributing routes from one routing protocol to another. The `match` command specifies the match criteria under which redistribution is allowed for the current route-map. The `set` command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Use the `no` parameter with this command to delete an entry.

Command Syntax `set origin (egp|igp|incomplete)` `no set origin (egp|igp|incomplete|)`

Parameters `egp` Learned through an Exterior Gateway Protocol.

`igp` Interior to the originating AS. This happens when an Internal Gateway Protocol is redistributed into BGP.

`incomplete` Unknown or learned through some other means. This happens when a static route is redistributed in BGP and the origin of the route is incomplete.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set origin egp
```

set originator-id

Use this command to set the originator ID attribute.

To use this command, you must first have a match clause. `Match` and `set` commands set the conditions for redistributing routes from one routing protocol to another. The `match` command specifies the match criteria under which redistribution is allowed for the current route-map. The `set` command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process. Use the `no` parameter with this command to disable this function

Command Syntax `set originator-id A.B.C.D`

`no set originator-id (A.B.C.D|)`

Parameter

`A.B.C.D`	IP address of originator.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set originator-id 1.1.1.1
```

set tag

Use this command to set a tag value. The parameter is the route tag that is labeled by another routing protocol (BGP or other IGP when redistributing), because AS-external-LSA has a route-tag field in its LSAs. In addition, when using route-

map, SWMRE can tag the LSAs with the appropriate tag value. Sometimes the tag matches with using route-map, and sometimes, the value may be used by another application.

Use the `no` parameter with this command to unset a tag value.

Command Syntax `set tag <0-4294967295> no set tag (<0-4294967295>|)`

Parameter

`<0-4294967295>` Tag value for destination routing protocol.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

In the following example the tag value of the destination routing protocol is set to 6:

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set tag 6
```

set vpnv4 next-hop

Use this command to set a VPNv4 next-hop address.

To use this command, you must first have a match clause. `Match` and `set` commands set the conditions for redistributing routes from one routing protocol to another. The `match` command specifies the match criteria under which redistribution is allowed for the current route-map. The `set` command specifies the set redistribution actions to be performed, if the match criteria are met.

If the packets do not match any of the defined criteria, they are routed through the normal routing process.

Note: This command is valid for BGP only.

Use the no parameter with this command to disable this function

Command Syntax set vpnv4 next-hop A.B.C.D
no set vpnv4 next-hop (A.B.C.D|)

Parameter

A.B.C.D IP address of originator.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#set vpnv4 next-hop 6.6.6.6
```

set weight

Use this command to set weights for the routing table.

The weight value is used to assist in best path selection. It is assigned locally to a router. When there are several routes with a common destination, the routes with a higher weight value are preferred.

To use this command, you must first have a match clause. Match and set commands set the conditions for redistributing routes from one routing protocol to another. The match command specifies the match criteria under which redistribution is allowed for the current route-map. The set command specifies the set redistribution actions to be performed, if the match criteria are met.

Note: This command is valid only for BGP.

Use the no parameter with this command to delete an entry.

Command Syntax `set weight <0-4294967295> no set weight (<0-4294967295>|)`

Parameter

`<0-4294967295>` Weight value.

Default

No default value is specified

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

In the following configuration, all routes that apply to access-list 10 will have the weight set at 400. If the packets do not match any of the defined criteria, they are routed through the normal routing process.

```
#configure terminal
(config)#route-map rmap1 permit 3
(config-route-map)#match as-path 10
(config-route-map)#set weight 400
```

show route-map

Use this command to display route-map information.

Command Syntax `show route-map (|WORD)`

Parameters

`WORD`	Route-map name (maximum size 63 characters)

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following is a sample output of the `show route-map` command.

```
#show route-map route-map myRM, permit, sequence 1
  Match clauses:     metric 200   Set clauses:
metric 60
#
```

show running-config route-map

Use this command to display the running system status and configuration details for route-maps.

Command Syntax `show running-config route-map`

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
>enable
#show running-config route-map
! route-map abc deny 2 match
community 2
! route-map abc permit 3 match route-type
external type-2 set metric-type type-1 !
```

CHAPTER 4 Interface Commands

This chapter is a reference for each of the interface commands.

- admin-group
- bandwidth
- clear interface counters
- clear interface cpu counters
- clear ip prefix-list
- clear ipv6 neighbors
- clear ipv6 prefix-list
- description
- duplex
- fec
- hardware-profile portmode
- hardware-profile portmode bundle
- if-arbiter
- interface
- ip address A.B.C.D/M
- ip address dhcp
- ip forwarding
- ip local-proxy-arp
- ip prefix-list
- ip proxy-arp
- ip remote-address
- ip unnumbered
- ip vrf forwarding
- ipv6 address
- ipv6 forwarding
- ipv6 nd current-hoplimit
- ipv6 nd link-mtu
- ipv6 nd managed-config-flag
- ipv6 nd minimum-ra-interval
- ipv6 nd other-config-flag
- ipv6 nd prefix
- ipv6 nd ra-interval
- ipv6 nd ra-lifetime

- ipv6 nd reachable-time
- ipv6 nd retransmission-time
- ipv6 nd suppress-ra
- ipv6 prefix-list
- ipv6 unnumbered
- link-flap errdisable
- load interval
- mtu
- multicast
- port breakout enable
- port bundle enable
- show interface
- show interface counters
- show interface counters drop-stats
- show interface counters error-stats
- show interface counters (indiscard-stats|outdiscard-stats)
- show interface counters protocol
- show interface counters queue-drop-stats
- show interface counters queue-stats
- show interface counters rate
- show interface counters summary
- show ip forwarding
- show ip interface
- show ip prefix-list
- show ip route
- show ip vrf
- show ipv6 forwarding
- show ipv6 interface brief
- show ipv6 route
- show ipv6 prefix-list
- show hosts
- show running-config interface
- show running-config interface ip
- show running-config interface ipv6
- show running-config ip
- show running-config ipv6

- shutdown
- speed
- switchport
- switchport allowed ethertype

admin-group

Use this command to create an administrative group to be used for links. Each link can be a member of one or more, or no administrative groups.

When used in the interface mode, this command adds a link between an interface and a group. The name is the name of the group previously configured. There can be multiple groups per interface. The group is created in configure mode, then interfaces are added to the group in interface mode.

Use the `no` parameter with this command to disable this command.

Command Syntax `admin-group NAME no admin-group NAME`

Parameters

`NAME`	Name of the admin group to add.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

In the following example, the `eth3` interface is added to the group `myGroup`:

```
#configure terminal
(config)#interface eth3
(config-if)#admin-group myGroup
```

bandwidth

Use this command to specify a discrete, maximum bandwidth value for the interface.

Use the `no` parameter resets the interface's bandwidth to the default value.

Command Syntax

```
bandwidth BANDWIDTH
no bandwidth
```

Parameter

BANDWIDTH	<1-999>k for 1 to 999 kilobits/s
	<1-999>m for 1 to 999 megabits/s
	<1-100>g for 1 to 100 gigabits/s

Default

Default bandwidth will be default speed of the interface. For LAG, default bandwidth will be collective bandwidth of its member ports. For VLAN interface, default bandwidth is 1 gigabits/sec.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface xe4
(config-if)#bandwidth 100m
```

clear interface counters

Use this command to clear the statistics on a specified interface or on all interfaces.

Note: This command is not supported on loopback interfaces or the out-of-band management (OOB) management interface.

Command Syntax `clear interface`

```
(IFNAME|) counters
```

Parameter

IFNAME	Interface name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear interface xe0 counters
```

clear interface cpu counters

Use this command to clear the CPU queue counters.

Command Syntax `clear interface cpu counters`

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in SWMRE version 1.3.1.

This command is not available on Qumran platforms.

Example

```
#clear interface cpu counters
```

clear ip prefix-list

Use this command to reset the hit count to zero in the prefix-list entries for an IPv4 interface.

Command Syntax `clear ip prefix-list clear ip prefix-list`

`WORD clear ip prefix-list WORD A.B.C.D/M`

Parameters

`WORD`	Name of the prefix-list.
`A.B.C.D/M`	IP prefix and length.

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear ip prefix-list List1
```

clear ipv6 neighbors

Use this command to clear all dynamic IPv6 neighbor entries.

Command Syntax `clear ipv6 neighbors`

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear ipv6 neighbors
```

clear ipv6 prefix-list

Use this command to reset the hit count to zero in the prefix-list entries for an IPv6 interface.

Command Syntax `clear ipv6 prefix-list clear ipv6 prefix-list`

`WORD clear ipv6 prefix-list WORD X:X::X:X/M`

Parameters

`WORD`	Name of the prefix-list.
`X:X::X:X/M`	IP prefix and length.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear ipv6 prefix-list List1
```

description

Use this command to assign an description to an interface.

Use the `no` parameter to remove an interface description.

Command Syntax `description LINE no description`

Parameter

`LINE` Interface description.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example provides information about the connecting router for interface `eth1`.

```
Router#configure terminal
Router(config)#interface eth1
Router(config-if)#description Connected to Zenith's fas2/0
```

duplex

Use this command to set the duplex mode for each interface.

Use the `no` parameter to remove the duplex mode.

Command Syntax `duplex (half|full) no duplex`

Parameter

`half` Half-duplex mode. `full` Full-duplex mode.

Default

By default, duplex mode is full duplex.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#duplex full

(config-if)#no duplex
```

fec

Use this command to configure forward error correction (FEC) on a physical port.

Use no parameter to un-configure FEC.

Command Syntax `fec (on|auto) no fec`

Parameter

`on`	Enable FEC. `auto` Enable FEC with autonegotiation.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#fec on

(config-if)#no fec
```

hardware-profile portmode

Use this command to set the global port mode.

Command Syntax `hardware-profile portmode (4X10g|40g)`

Parameter

`4X10g`	Split all the 40G flex ports on the system
`40g`	Disable splitting on all flex ports and make all ports 40G

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#hardware-profile portmode 40g
```

hardware-profile portmode bundle

Use this command to set the global port mode to bundle.

Command Syntax `hardware-profile portmode bundle (40g|4X10g)`

Parameter

`40g`	Bundle four 10G ports to a single 40G port
`4x10g`	Unbundle ports

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#hardware-profile portmode bundle 40g
(config)#exit
(config)#hardware-profile portmode bundle 4x10g
(config)#exit
```

if-arbiter

Use this command to discover new interfaces recently added to the kernel and add them to the SWMRE database.

This command starts the arbiter to check interface information periodically. SWMRE dynamically finds any new interfaces added to the kernel. If an interface is loaded dynamically into the kernel when SWMRE is already running, this command polls and updates the kernel information periodically.

Use the `no` parameter with this command to revert to default.

Command syntax `if-arbiter (interval <1-65535>|) no if-arbiter`

Parameter `interval` Interval (in seconds) after which NSM sends a query to the kernel.

Default

By default, `if-arbiter` is disabled. When interface-related operations are performed outside of SWMRE (such as when using the `ifconfig` command), enable `if-arbiter` for a transient time to complete synchronization. When synchronization is complete, disable it by giving the `noif-arbiter` command.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#if-arbiter interval 5
```

interface

Use this command to select an interface to configure, and to enter the `Interface` command mode.

Use the `no` parameter with this command to remove this configuration.

Command Syntax		
`IFNAME`	`no`	`interface IFNAME`

Parameter

`IFNAME`	Name of the interface.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

This example shows the use of this command to enter the `Interface` mode (note the change in the prompt).

```
#configure terminal
(config)#interface eth3
(config-if)#
```

ip address A.B.C.D/M

Use this command to specify that an IP address and prefix length will be used by this interface. If the `secondary` parameter is not specified, this command overwrites the primary IP address. If the `secondary` parameter is specified, this command adds a new IP address to the interface. The secondary address cannot be configured in the absence of a primary IP address. The primary address cannot be removed when a secondary address is present.

Use the `no` parameter with this command to remove the IP address from an interface.

Command Syntax `ip address A.B.C.D/M label LINE`

```
ip address A.B.C.D/M (secondary|) ip address
A.B.C.D/M secondary label LINE no ip address
A.B.C.D/M label LINE no ip address A.B.C.D/M
secondary label LINE no ip address (A.B.C.D/M
(secondary|)|)
```

Parameters

`LINE`	Label of this address.
`secondary`	Make the IP address secondary.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#interface eth3
(config-if)#ip address 10.10.10.50/24
(config-if)#ip address 10.10.11.50/24 secondary
```

ip address dhcp

Use this command to specify that a DHCP client will be used to obtain an IP address for an interface.

Use the `no` parameter with this command to remove the IP address from an interface.

Command Syntax `ip address dhcp no`

```
ip address dhcp
```

Parameters

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#interface eth3
(config-if)#ip address 10.10.10.50/24 (config-
if)#ip address 10.10.11.50/24 secondary
(config-if)#ip address dhcp
```

ip forwarding

Use this command to turn on IP forwarding.

Use the `no` parameter with this command to turn off IP forwarding.

Command Syntax `ip forwarding ip forwarding vrf NAME no ip forwarding`

```
no ip forwarding vrf NAME
```

Parameters

`NAME`	Virtual Routing and Forwarding name

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip forwarding
```

ip local-proxy-arp

Use this command to enable local proxying of ARP requests at the interface level.

After giving this command, the device answers all ARP requests on a configured subnet, even for clients that normally do not need routing. Local proxy ARP implies a proxy ARP that occurs on the same interface, that is, the traffic comes in and goes out the same interface.

With local proxy ARP, ARP responds to all ARP requests for IP addresses within the subnet and forwards all traffic between hosts in the subnet. Use this feature only on subnets where hosts are intentionally prevented from communicating directly.

Use the `no` parameter to disable the local proxy ARP feature on an interface.

Command Syntax `ip local-proxy-arp` `no ip local-proxy-arp`

Parameters

None

Default

By default, local proxy ARP is disabled

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth3
(config-if)#ip local-proxy-arp
```

ip prefix-list

Use this command to create an entry for a prefix list.

A router starts to match prefixes from the top of the prefix list and stops whenever a match or deny occurs. To promote efficiency, use the `seq` parameter and place common matches or denials towards the top of the list. The sequence values are generated in the sequence of 5.

Use the parameters `ge` and `le` specify the range of the prefix length to be matched. When setting these parameters, set `le` to be less than 32 and `ge` to be less than `le` value.

Use the `no` parameter with this command to delete the prefix-list entry.

Command Syntax `ip prefix-list WORD (deny|permit) (A.B.C.D/M|any) ip prefix-list WORD (deny|permit) A.B.C.D/M eq <0-32> ip prefix-list WORD (deny|permit) A.B.C.D/M ge <0-32> ip prefix-list WORD (deny|permit) A.B.C.D/M ge <0-32> le <0-32> ip prefix-list WORD (deny|permit) A.B.C.D/M le <0-32> ip prefix-list WORD (deny|permit) A.B.C.D/M le <0-32> ge <0-32> ip prefix-list WORD seq <1-4294967295> (deny|permit) (A.B.C.D/M|any) ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M eq <0-32> ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M ge <0-32> ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M ge <0-32> le <0-32> ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M le <0-32> ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M le <0-32> ge <0-32> no ip prefix-list WORD no ip prefix-list WORD (deny|permit) (A.B.C.D/M|any) no ip prefix-list WORD (deny|permit) A.B.C.D/M eq <0-32> no ip prefix-list WORD (deny|permit)`

A.B.C.D/M ge <0-32> no ip prefix-list WORD (deny|permit) A.B.C.D/M ge <0-32> le <0-32> no ip prefix-list WORD (deny|permit) A.B.C.D/M le <0-32> no ip prefix-list WORD (deny|permit) A.B.C.D/M le <0-32> ge <0-32> no ip prefix-list WORD seq <1-4294967295> (deny|permit) (A.B.C.D/M|any) no ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M eq <0-32> no ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M ge <0-32> no ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M ge <0-32> le <0-

32> no ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M le <0-32> no ip prefix-list WORD seq <1-4294967295> (deny|permit) A.B.C.D/M le <0-32> ge <0-

32> ip prefix-list sequence-number no ip prefix-list sequence-number

```
ip prefix-list WORD description LINE
no ip prefix-list WORD description
LINE no ip prefix-list WORD
description
```

Parameters

WORD	Name of the prefix list.
deny	Reject packets.
permit	Accept packets.
A.B.C.D/M	IP address mask and length of the prefix list mask.
eg	Exact prefix length match
le	Maximum prefix length match
ge	Minimum prefix length match
<0-32>	Prefix length to match
<1-4294967295>	Sequence number of the prefix list.
any	Take all packets of any length. This parameter is the same as using 0.0.0.0/0 le 32 for A.B.C.D/M.
sequence-number	To suppress sequence number generation, give the `no ip prefix-list sequencenumber` command. If you disable the generating sequence numbers, you must specify the sequence number for each entry using the sequence number parameter in the `ip prefix-list` command. To enable sequence number generation, give the `ip prefix-list sequencenumber` command.
LINE	Up to 80 characters describing this prefix-list.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

In this configuration, the `ip prefix-list` command matches all, but denies the IP address range, 76.2.2.0.

```
#conf t
(config)#router bgp 100
(config-router)#network 172.1.1.0
(config-router)#network 172.1.2.0
(config-router)#
(config-router)#neighbor 10.6.5.3 remote-as 300
```


© Symanitron Proprietary

```
    (config-router)#neighbor 10.6.5.3 prefix-list mylist out
    (config-router)#exit
    (config)#ip prefix-list mylist seq 5 deny 76.2.2.0/24
(config)#ip prefix-list mylist seq 10 permit 0.0.0.0/0
```

ip proxy-arp

Use this command to enable the proxy ARP feature on an interface.

Use the `no` parameter to disable the proxy ARP feature on an interface.

Command Syntax `ip proxy-arp no ip proxy-arp`

Parameters

None

Default

By default, the ip proxy-arp is disabled

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth3
(config-if)#ip proxy-arp
```

ip remote-address

Use this command to set the remote address (far end) on a point-to-point non multi-access link. This command can be used only on unnumbered interfaces. When a new remote-address is configured, the old address gets overwritten.

Use the `no` parameter to disable this function.

Command Syntax `ip remote-address A.B.C.D/M`

`no ip remote-address`

Parameter

`A.B.C.D/M`	IP address and prefix length of the link remote address.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
(config)#interface ppp0
(config-if)#ip unnumbered eth1
(config-if)#ip remote-address 1.1.1.1/32
```

ip unnumbered

Use this command to enable IP processing without an explicit address on a point-to-point non multi-access link.

This command lets an interface borrow the IP address of a specified interface to enable IP processing on a point-topoint interface without assigning it an explicit IP address. In this way, the IP unnumbered interface can borrow the IP address of another interface already configured on the router to conserve network and address space.

Use the `no` parameter with this command to remove this feature on an interface.

Command Syntax `ip unnumbered IFNAME`

`no ip unnumbered`

Parameter

`IFNAME`	Interface name.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example creates a tunnel on `eth1`.

```
(config)#interface lo
(config-if)#ip address 127.0.0.1/8
(config-if)#ip address 33.33.33.33/32 secondary
(config-if)#exit
(config)#interface eth1
(config-if)#ip address 10.10.10.145/24
(config-if)#exit
(config)#interface Tunnel0
(config-if)#tunnel source 10.70.0.145
(config-if)#tunnel destination 10.70.0.77
(config-if)#tunnel ttl 255
(config-if)#tunnel path-mtu-discovery
(config-if)#tunnel mode gre
(config-if)#ip unnumbered eth1
(config-if)#exit
(config)#router ospf
(config-router)#network 10.10.10.0/24 area 0
```

ip vrf forwarding

This command associates an interface with a VRF.

Use the `no` parameter with this command to unbind an interface.

Note: When you give this command in interface configuration or subinterface configuration mode of the parent VR, the IP address and other attributes of the interface are deleted from the interface. After giving this command, the IP attributes must then be configured in the context of the VRF.

Note: The Out Of Band (OOB) management port is part of the “management” VRF. Also, this port cannot be moved out of “management” VRF.

Command Syntax `ip vrf forwarding WORD no ip vrf forwarding WORD`

Parameter

`WORD`	Name of the VRF.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ip vrf myVRF
(config-vrf)#exit
(config)#interface eth1
(config-if)#ip vrf forwarding myVRF
```

ipv6 address

Use this command to set the IPv6 address of an interface.

Use the `no` form of this command to disable this function.

Command Syntax `ipv6 address X:X::X:X/M ipv6 address X:X::X:X/M anycast no ipv6 address X:X::X:X/M`

Parameters

`X:X::X:X/M`	IP destination prefix and a mask length.
`anycast`	Make an anycast address which is assigned to a set of interfaces that belong to different devices. A packet sent to an anycast address is delivered to the closest interface (as defined by the routing protocols in use) identified by the anycast address

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 address 3ffe:506::1/64
```

ipv6 forwarding

Use this command to turn on IPv6 forwarding.

Use the `no` parameter with this command to turn off IPv6 forwarding.

Command Syntax `ipv6 forwarding ipv6 forwarding vrf NAME no ipv6 forwarding no ipv6 forwarding vrf NAME`

Parameters

NAME	Virtual Routing or Forwarding name

Default

No default value is specified

Command Mode

Command mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ipv6 forwarding
```

ipv6 nd current-hoplimit

Use this command to set an ND (Neighbor Discovery) advertised hop limit for an interface.

Use the `no` option of this command to set the current hop limit to its default value.

Command Syntax `ipv6 nd current-hoplimit <0-255> no ipv6 nd current-hoplimit`

Parameter

<0-255>	Hop limit.

Default

By default, hop limit is 64

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 nd current-hoplimit 10
(config-if)#no ipv6 nd current-hoplimit
```

ipv6 nd link-mtu

Use this command to set an advertised maximum transmission unit (MTU).

Use the `no` option with the command to reset the MTU to the default statute.

Command Syntax `ipv6 nd link-mtu (<1280-65535>) no ipv6 nd link-mtu`

Parameters

`<1280-65535>` Link MTU value.

Default

By default, link MTU value is 1500

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 nd link-mtu 1600
(config-if)#no ipv6 nd link-mtu
```

ipv6 nd managed-config-flag

Use this command to set the managed address configuration flag in the Router Advertisement to be used for the IPv6 address auto-configuration.

Use the `no` parameter with this command to reset the value to default.

Command Syntax `ipv6 nd managed-config-flag no ipv6 nd managed-config-flag`

Parameters

None

Default

The managed address configuration flag is not set.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
```

```
(config)#interface eth3 (config-if)#ipv6
nd managed-config-flag (config-if)#no ipv6
nd managed-config-flag
```

ipv6 nd minimum-ra-interval

Use this command to set a minimum Router Advertisement (RA) interval for the interface.

Use the `no` option with the command to set the RA interval to its default value.

Command Syntax `ipv6 nd minimum-ra-interval <3-1350> no ipv6 nd minimum-ra-interval (<3-1350>|)`

Parameter

`<3-1350>`	Minimum RA interval (in seconds).

Default

By default, RA interval is 180 seconds

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 nd minimum-ra-interval 400
(config-if)#no ipv6 nd minimum-ra-interval
```

ipv6 nd other-config-flag

Use this command to set the other stateful configuration flag in Router Advertisement to be used for IPv6 address autoconfiguration.

Use `no` parameter with this command to reset the value to default.

Command Syntax `ipv6 nd other-config-flag no ipv6 nd other-config-flag`

Parameters

None

Default

Other stateful configuration flag is not set.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 nd other-config-flag
(config-if)#no ipv6 nd suppress-ra
```

ipv6 nd prefix

Use this command to set IPv6 prefix information that is advertised for address auto-configuration.

Use `no` parameter with this command to remove an IPv6 prefix.

Command Syntax

```
          ipv6 nd prefix X:X::X:X/M <0-4294967295> <0-4294967295> (off-link|) (no-
  autoconfig|)
ipv6 nd prefix X:X::X:X/M ipv6 nd prefix valid-lifetime <0-
4294967295> ipv6 nd prefix preferred-lifetime <0-4294967295>
ipv6 nd prefix offlink ipv6 nd prefix no-autoconf no ipv6 nd
prefix X:X::X:X/M no ipv6 nd prefix valid-lifetime (<0-
4294967295>|) no ipv6 nd prefix preferred-lifetime (<0-
4294967295>|) no ipv6 nd prefix offlink no ipv6 nd prefix
no-autoconf
```

Parameters

`X:X::X:X/M` IPv6 prefix.

`<0-4294967295>` Valid lifetime in seconds. `<0-4294967295>` Preferred lifetime in seconds. `off-link` Do not use prefix for onlink determination. `no-autoconfig` Do not use prefix for autoconfiguration.

Default

By default, valid life time is 2592000 seconds and preferred life time is 604800 seconds

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Defaults

The default valid lifetime is 2592000 seconds.

The default preferred lifetime is 604800 seconds.

Examples

```
(config)#interface eth3
(config-if)#ipv6 nd prefix 2001:ffff::/64
```

```
(config)#interface eth3
(config-if)#ipv6 nd prefix no-autoconf

(config)#interface eth3
(config-if)#ipv6 nd prefix preferred-lifetime 550000
```


© Symanitron Proprietary

ipv6 nd ra-interval

Use this command to specify the interval between IPv6 Router Advertisements (RA).

Use `no` parameter with this command to set the value to its default.

Command Syntax `ipv6 nd ra-interval <4-1800> no ipv6 nd ra-interval`

Parameter

`<4-1800>`	RA interval in milliseconds.

Default

By default, RA interval is 600 milliseconds.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 nd ra-interval 60
(config-if)#ipv6 nd prefix 3ffe:ffff:ffff::/64

(config-if)#no ipv6 nd ra-interval
```

ipv6 nd ra-lifetime

Use this command to specify the Router Advertisement (RA) lifetime for this device to act as a default gateway for the network.

Use `no` parameter with this command to reset the value to default.

Command Syntax `ipv6 nd ra-lifetime <0-9000> no ipv6 nd ra-lifetime`

Parameter

`<0-9000>`	RA lifetime duration in seconds.

Default

The default RA lifetime is 1800 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 nd ra-lifetime 9000 (config-if)#no
ipv6 ra-lifetime 9000
```

ipv6 nd reachable-time

Use this command to specify the reachable time in the Router Advertisement to be used for detecting unreachability of the IPv6 neighbor.

Use the `no` parameter with this command to set the value to its default.

Command Syntax `ipv6 nd reachable-time <0-3600000> no ipv6 nd reachable-time`

Parameter

`<0-3600000>`	Reachable time in milliseconds.

Default

By default, reachable time is zero (0) milliseconds.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 nd reachable-time 1800000
(config-if)#no ipv6 nd reachable-time 1800000
```

ipv6 nd retransmission-time

Use this command to set an IPv6 advertised retransmission time for the current interface.

Use the `no` form of the command to set the retransmission time to its default value.

Command Syntax `ipv6 nd retransmission-time (0-4294967295) no ipv6 nd retransmission-time`

Parameter

`<0-4294967295>` Retransmission time in milliseconds

Default

By default, retransmission time is zero (0) milliseconds.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth3
(config-if)#ipv6 nd retransmission-time 1200
(config-if)#no ipv6 nd retransmission-time
```

ipv6 nd suppress-ra

Use this command to suppress IPv6 Router Advertisement (RA) transmission for the current interface. Router Advertisement is used for IPv6 stateless auto-configuration.

Use the `no` parameter with this command to enable Router Advertisement transmission.

Command Syntax `ipv6 nd suppress-ra (mtu |) no ipv6 nd suppress-ra (mtu |)`

Parameters `mtu` Do not send maximum transmission unit (MTU) in Router Advertisement messages

Default

By default, ipv6 nd suppress-ra is suppressed

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth3
```

```
(config-if)#ipv6 nd suppress-ra
```

ipv6 prefix-list

Use this command to create an entry for an ipv6 prefix-list.

Router starts to match prefixes from the top of the prefix list, and stops whenever a match or deny occurs. To promote efficiency, use the `seq` parameter and place common matches or denials towards the top of the list. The sequence values are generated in the sequence of 5.

The parameters `ge` and `le` specify the range of the prefix length to be matched.

Use the `no` parameter with this command to delete the prefix-list entry.

Command Syntax `ipv6 prefix-list WORD (deny|permit) (X:X::X:X/M|any) ipv6 prefix-list WORD (deny|permit) X:X::X:X/M ge <0-128> ipv6 prefix-list WORD (deny|permit) X:X::X:X/M ge <0-128> le <0-128> ipv6 prefix-list WORD (deny|permit) X:X::X:X/M le <0-128> ipv6 prefix-list WORD (deny|permit) X:X::X:X/M le <0-128> ge <0-128> ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) (X:X::X:X/M|any) ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) X:X::X:X/M ge <0-128> ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) X:X::X:X/M ge <0-128> le <0-128> ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) X:X::X:X/M le <0-128> ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) X:X::X:X/M le <0-128> ge <0-128> no ipv6 prefix-list WORD no ipv6 prefix-list WORD (deny|permit) (X:X::X:X/M|any) no ipv6 prefix-list WORD (deny|permit) X:X::X:X/M ge <0-128> no ipv6 prefix-list WORD (deny|permit) X:X::X:X/M ge <0-128> le <0-128> no ipv6 prefix-list WORD (deny|permit) X:X::X:X/M le <0-128> no ipv6 prefix-list WORD (deny|permit) X:X::X:X/M le <0-128> ge <0-128> no ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) (X:X::X:X/M|any) no ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) X:X::X:X/M ge <0-128> no ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) X:X::X:X/M ge <0-128> le <0-128> no ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) X:X::X:X/M le <0-128> no ipv6 prefix-list WORD seq <1-4294967295> (deny|permit) X:X::X:X/M le <0-128> ge <0-128> ipv6 prefix-list sequence-number no ipv6 prefix-list sequence-number ipv6 prefix-list WORD description LINE no ipv6 prefix-list WORD description`

Parameters

WORD	Name of the prefix list.
deny	Reject packets.
permit	Accept packets.
X:X::X:X/M	IP address mask and length of the prefix list mask.
any	Take all packets of any length. This is the same as specifying ::/0 for X:X::X:X/M.
eg	Exact prefix length match
le	Maximum prefix length match
ge	Minimum prefix length match
<0-128>	Prefix length to match
<1-4294967295>	Sequence number of the prefix list.
sequence-number	To suppress sequence number generation, give the no ipv6 prefix-list sequence-number command. If you disable the generating sequence numbers, you must specify the sequence number for each entry using the sequence number parameter in the ipv6 prefix-list command. To enable sequence number generation, give the ipv6 prefix-list sequencenumber command.
LINE	Up to 80 characters describing this prefix-list.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ipv6 prefix-list mylist seq 12345 deny 3ffe:345::/16 le 22 ge 14
```

ipv6 unnumbered

Use this command to enable IPv6 processing without an explicit address, on a point-to-point non multi-access link.

This command lets an interface borrow the IPv6 address of a specified interface to enable IPv6 processing on a pointto-point interface without assigning it an explicit IPv6 address. In this way, the IPv6 unnumbered interface can borrow the IPv6 address of another interface already configured on the router to conserve network and address space.

Use the no parameter with this command to remove this feature on an interface.

Command Syntax `ipv6 unnumbered IFNAME no ipv6 unnumbered`

Parameter

`IFNAME` Interface name.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following example creates a tunnel on eth1:

```
#configure terminal
(config)#interface lo
(config-if)#ipv6 address::1/128
(config-if)#exit
(config)#interface eth1
(config-if)#ipv6 address fe80::20e:cff:fe6e:56dd/64
(config-if)#exit
(config)#interface Tunnel0
(config-if)#tunnel source 10.70.0.145
(config-if)#tunnel destination 10.70.0.77
(config-if)#tunnel ttl 255
(config-if)#tunnel path-mtu-discovery
(config-if)#tunnel mode gre
(config-if)#ipv6 unnumbered eth1
(config-if)#ipv6 router ospf area 0 tag 1
(config-if)#exit
(config)#router ipv6 ospf 1
(config-router)#router-id 10.70.0.145
```

link-flap errdisable

Use this command to shut down the interface when it continually goes up and down.

The link-flap ErrDisable feature must be enabled globally with the errdisable cause command.

Note: When link-flap ErrDisable is enabled globally, then all interfaces are enabled. Link-flap ErrDisable can be enabled globally, but disabled for a specific interface with the `no link-flap errdisable` command.

Note: This feature is supported only on physical ports.

Use the `no` form of this command to disable this behavior.

Command Syntax `link-flap errdisable no link-flap errdisable`

Parameter

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced in SWMRE version 1.3.4.

Example

```
#configure terminal
(config)#interface xe1/1
(config-if)#link-flap errdisable
```

load interval

Use this command to configure the interval for which average traffic rate need to be shown. Intervals can be configured in steps of 30 seconds.

Use the no parameter with this command to set the load interval to its default.

Command Syntax `load-interval <30-300> no load-interval`

Parameter

`<30-300>`	Load period in multiples of 30 seconds.

Default

By default, load interval is 300 seconds

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
```

```
(config)#interface xe1/1
(config-if)#load-interval 30
(config-if)#no load-interval
```

mtu

Use this command to set the Maximum Transmission Unit (MTU) for an interface.

Use the `no` parameter with this command to set the MTU to its default.

Command Syntax `mtu <64-65536> no mtu`

Parameter

`<64-65536>` Specify the size of MTU in bytes:

`<64-16338>` for L2 packet

`<576-9216>` for L3 IPv4 packet

`<1280-9216>` for L3 IPv6 packet

`<576-65536>` for IPv4 packet

`<1280-65536>` for IPv6 packet on loopback interface

Default

By default, MTU is 1500 bytes

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth3
(config-if)#mtu 120
```

multicast

Use this command to set the multicast flag for the interface.

Use the `no` form of this command to disable this function.

Command Syntax `multicast no multicast`

Parameters

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth3
(config-if)#multicast
```

port breakout enable

Use this command to split a 40G interface to four 10G interfaces or 100G interface to four 10G or four 25G or two 50G interfaces without restarting the device.

You can only break out controlling ports. For example, in the group that contains the `xe1/1`, `xe1/2`, `xe1/3`, and `xe1/ 4` interfaces, the `xe1/1` interface is the controlling port (first port in the group) and `xe1/2`, `xe1/3`, and `xe1/4` are subsidiary ports (non control ports).

Ports that support the breakout feature display with a "/" in their name. By default, only control ports are active (/1) and remaining ports (/2, /3, and /4) are inactive.

Use the `show interface brief` command to verify if a port is controlling or subsidiary. You can also use the `show interface` command to check the flexport status. The status would be one of the below:

```
Flexport: Control Port (Active): Break Out disabled
Flexport: Control Port (Active): Break Out Enabled
Flexport: Non Control Port (InActive)
Flexport: Non Control Port (Active)
```

The output from commands such as `show running-config` reflect the split port configuration.

The bandwidth of a controlling port is reset to its maximum allowed speed after a split is enabled or disabled.

Any pre-configuration of the subsidiary port is applied directly once it becomes active.

Use the `no` form of this command to return the interface to single-port, 40G/100G operation.

Note: There are some configuration restrictions for Subsidiary ports such as:

1. Port breakout enable/disable is not allowed on Subsidiary ports.
2. Speed, Duplex configurations are not allowed on InActive Subsidiary ports.

Command Syntax

40G port:

```
port breakout enable
no port breakout
```

100G port:

```
port breakout enable (4x10g|4x25g|2x50g)
no port breakout
```

Parameters

`<4x10g>`	Split 100G to 4X10g
`<4x25g>`	Split 100G to 4X25g
`<2x50g>`	Split 100G to 2X50g

Default

By default, only control ports are active (/1) and remaining ports (/2, /3, and /4) are inactive.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

This example shows how to split a 40G port:

```
#configure terminal
(config)#interface xe1/1 (config-if)#port breakout enable (config-if)#end

#show running-config
!
no service password-encryption
!
logging monitor 7
!
ip vrf management
! forwarding profile l2-profile-two ip domain-lookup bridge 1 protocol rstp
vlan-bridge data-center-bridging enable bridge 1 ethernet cfm enable !

! interface xe1/1 port breakout enable switchport bridge-group 1
switchport mode access channel-group 1 mode active
! interface xe1/2  speed 1g
! interface xe1/3  speed 1g  switchport  bridge-group 2
switchport mode trunk
!
interface xe1/4 !
```

This example shows how to split a 100G port:

```
#configure terminal
(config)#interface ce1/1
(config-if)#port breakout enable ?
  2X50g  split to 2X50g
  4X10g  split to 4X10g
  4X25g  split to 4X25g
(config-if)#port breakout enable 4X25g
(config-if)#end
#show running-config
!
no service password-encryption
!
logging monitor 7
!
ip vrf management
! forwarding profile l2-profile-two ip domain-lookup bridge 1 protocol
rstp vlan-bridge data-center-bridging enable bridge 1

ethernet cfm enable
! interface ce1/1 port breakout enable 4X25g
```

Similarly, a 100G port can be split into 4x10G ports or 2x50G ports.

 © Symanitron Proprietary

port bundle enable

Use this command to bundle four 10G SFP+ interfaces into a single 40G interface without restarting the device. You can use this command only on bundle control ports.

For example, if the xe1 interface is bundle control port then this command can be used and following three ports xe2, xe3, and 4 would be subsidiary ports (non control ports) and would become inactive.

Use the show interface brief command to verify if a port is bundle controlling or subsidiary. You can also use the show interface command to check the flexport status. The status would be one of the below:

Flexport: Bundle Control Port (Active): Bundle disabled

Flexport: Bundle Control Port (Active): Bundle Enabled

Flexport: Non Control Port (InActive)

Flexport: Non Control Port (Active)

The output from commands such as show running-config reflect the bundle port configuration.

Use the `no` form of this command to revert to four 10G ports.

Note: There are some configuration restrictions for Subsidiary ports such as:

1. Port breakout enable/disable is not allowed on Subsidiary ports.
2. Speed, Duplex configurations are not allowed on InActive Subsidiary ports.

Command Syntax `port`

```
bundle enable no
port bundle
```

Parameters

None

Default

By default, ports are not bundled and all the ports are active (xe1, xe2, xe3, and xe4).

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

This example shows how to split a 40G port:

```
#show running-config
!
no service password-encryption
!
logging monitor 7
! ip vrf
management !
```

```
    forwarding
    profile l2-
    profile-two ip
    domain-lookup
    bridge 1
    protocol rstp
    vlan-bridge
    data-center-
    bridging enable
    bridge 1
    ethernet cfm
    enable
! !
interface xe1 port bundle enable
!
interface xe2
!
interface xe3
!
interface xe4 !
```

show interface

Use this command to display interface configuration and status information.

Command Syntax `show interface (IFNAME|)`

Parameter

IFNAME	Interface name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show interface xe1/1
Interface xe1/1
  Scope: both
  Flexport: Breakout Control Port (Active): Break Out Enabled
  Hardware is ETH  Current HW addr: ecf4.bb6e.934b
  Physical:ecf4.bb6e.934b  Logical:(not set)
  Port Mode is access
  Interface index: 5001
  Metric 1 mtu 1500 duplex-full(auto) link-speed 1g(auto)
  <UP,BROADCAST,RUNNING,MULTICAST>
  VRF Binding: Not bound
  Label switching is disabled   No
Virtual Circuit configured
DHCP client is disabled.
  Last Flapped: 2016 Nov 05 22:40:23 (00:19:25 ago)
  Statistics last cleared: 2016 Nov 05 04:49:55 (18:09:53 ago)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 256 bits/sec, 0 packets/sec   RX
    unicast packets 39215813 multicast packets 0 broadcast packets 0     input
packets 39215813 bytes 2666662432     jumbo packets 0
    runts 0 giants 0 CRC 0 fragments 0 jabbers 0     input
error 0
    input with dribble 0 input discard 0
    Rx pause 0   TX
    unicast packets 38902 multicast packets 437 broadcast packets 0
output packets 437 bytes 28018     jumbo packets 0
    output errors 0 collision 0 deferred 0 late collision 0     output
discard 0
    Tx pause 0
```

Table 4-44 explains the output fields.

Table 4-44: show interface output details

Field	Description
Scope	Interface can be used for communication within the device and outside the device (Both).
Flexport	Specifies whether the ports has Breakout capabilities or is a Non-Control Port.
Breakout Control Port (Active)	Specifies whether Breakout is active or disabled.
Hardware is ETH Current HW addr	The MAC address of the interface.
Physical	Displays the physical MAC address of the interface.
Logical	Displays the logical MAC address (if any) of the interface.
Port Mode	Displays the port mode: Router, VLAN access, switch, or trunk.
Interface index	Index number, Metric, MTU size, duplex-full (auto) or half-duplex, minimum link speed in gigabits, and if the interface is up, broadcasting, and multicasting.
VRF Binding	Show whether the interface is VRF bound and (if bound) with what VRF, if Label Switching is enabled or disabled, and if a virtual circuit is configured.
DHCP client	The state of the DHCP client – whether this interface is connected to a DHCP server.
Last Flapped	Date and time when the interface last flapped.
Statistics last cleared	Date and time when the interface's statistics were cleared.
5 minute input rate	Input rate in bits/second and packets/second
5 minute output rate	Output rate in bits/second and packets/second
RX	Counters for unicast packets, multicast packets, broadcast packets, input packets, bytes, jumbo packets, runts, giants, CRC errors, fragments, jabbers, input errors, input with dribble input discards, and receive pause.
TX	Counters for unicast packets, multicast packets, broadcast packets, output packets, bytes, jumbo packets, output errors, collisions, differed packets, input late collisions, output discards, and transmit pause.

show interface counters

Use this command to display the ingress and egress traffic counters on the interface.

Note: Counters are meant for debugging purpose and the accuracy of the transmit discard counter is not guaranteed in all scenarios.

Command Syntax `show interface (IFNAME|) counters (active|)` `show interface cpu counters`

Parameter

`IFNAME`	Interface name.
`active`	Statistics for link-up interfaces.
`cpu`	CPU interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

This command is not available on Qumran platforms.

Example

```
#show interface xe1/1 counters
Interface xe1/1
  Scope: both
  Rx Packets: 1000
  Rx Bytes: 1000000
  Rx Unicast Packets: 1000
  Rx Packets from 512 to 1023 bytes: 1000
  Tx Packets: 3897
  Tx Bytes: 249408
  Tx Multicast Packets: 3897
  Tx Packets with 64 bytes: 3897
  Tx Packet rate: 1 pps
Tx Bit rate: 255 bps

#show interface cpu counters
CPU Interface
  Tx Packets: 104508
  Tx Bytes: 7106272
  Tx Discard Packets: 89613672
  Tx Discard Bytes: 5735237844
Rx Discard Packets: 11938
```

Table 4-45 explains the output fields.

Table 4-45: show interface counters output details

	Description
	Rx Packets Rx Bytes Rx Unicast Packets Rx Packets from 128 to 255 bytes Rx Discard Packet
	Tx Packets Tx Bytes Tx Multicast Packets Tx Packets from 65 to 127 bytes Tx Packets from 128 to 255 bytes
	Tx Packets Tx Bytes Tx Discard Packets Tx Discard Bytes Rx Discard Packets

show interface counters drop-stats

Use this command to display the ingress and egress traffic discard reason counters on the interface.

Note: You can only display statistics for physical ports and cpu ports, but not for the out-of-band management (OOB) management port or logical interfaces.

Note: Drops in the CPU queue are listed under `Tx Multicast Queue Drops`, whether the packet is unicast or multicast

Command Syntax `show interface (IFNAME|) counters drop-stats show interface cpu counters drop-stats`

Parameter

`IFNAME` Physical interface name `cpu`

CPU interface

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.1.

This command is not available on Qumran platforms.

Example

```
#show interface xe32/2 counters drop-stats
+---------------------+----------------+---------------- +--------------------+
| Counter Description | Count          | Last Increment | Last Increment Time
|
+---------------------+----------------+---------------- +--------------------+
 Rx Bad CRC errors     0                0
 Rx Undersize errors   0                0
 Rx Oversize errors    0                0
 Rx Fragments errors   0                0
 Rx Jabbers errors     0                0
 Rx Port Block Drops   6                1               2016 Nov 09 08:59:33
 Rx Vlan Discards      0                0
 Rx ACL/QOS Drops      0                0
 Rx Policy Discards    0                0
 Rx EGR Port Unavail   38784            5               2016 Nov 09 18:19:31
 Rx IBP Discards       0                0
 Tx Port Block Drops   359              1               2016 Nov 09 08:59:33
 Tx Vlan Discards      0                0
 Tx TTL Discards       0                0
 Tx Unknown Discards   359              1               2016 Nov 09 08:59:33
 Tx Ucast Queue Drops  0                0
 Tx Mcast Queue Drops  0                0
+---------------------+----------------+---------------- +--------------------+
```

Table 4-46 explains the output fields.

Table 4-46: show interface counters drop-stats output details

	Description
n	Shows the type of packet and/or the reason why the packet was dropped.
	The number of packets dropped for each reason.
	Number of packets dropped since this command was last entered.
me	Date and time when the last packet was dropped.
s	Received packets dropped because they didn't pass the cyclic Redundancy Check (CRC).
rs	Number of received runt packets dropped.
s	Number of received giant packets dropped
rs	Number of received packet fragments dropped
	Received packets dropped because of jabber – long packet error.
ps	Received packets dropped because port blocking is enabled.
	VLAN received packets dropped because there is no VLAN configured on the port.
ps	Received packets match a field processing entry with a drop or color drop action, such as: User-configured ACL that denies traffic Service policy with a police action that drops the traffic received at a rate higher than the configured limit.
s	Received packets dropped because of device policies violated, such as a storm control rate violation.

vail	No output port can be determined for these received packets. This counter increments along with other counter types in this table because it is a “catchall” for multiple types of discards as shown below: VLAN check failed MTU check failed ACL/QoS drops Policy discards Source MAC is null Destination IP/source IP address is null Source MAC address and destination MAC address are the same Forwarding lookup failure
	Ingress Back Pressure (ingress congestion) when the ingress packets buffer is full for an interface.
ps	Transmitted packets dropped because port blocking is enabled.
	Transmitted VLAN packets dropped because there is no VLAN configured on the port.
	Transmitted packets discarded because their Time To Live (TTL) has ended.

Table 4-46: show interface counters drop-stats output details (Continued)

	Description
n Discards	Transmitted packets dropped for unknown reason. May have something to do with the condition/configuration of the port at the other end of the connection.
ueue Drops	Transmitted packets dropped as a result of Unicast buffer overflow.
ueue Drops	Transmitted packets dropped as a result of Multicast buffer overflow.

show interface counters error-stats

Use this command to display the ingress error traffic counters on the interface.

Command Syntax `show interface (IFNAME|) counters error-stats`

Parameter

`IFNAME`	Interface name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show interface xe1/1 counters error-stats
   +----------+-------------+--------+----------+---------+-----------+---------+
|Interface |Total errors |Bad CRC |Undersize |Oversize | Fragments | Jabbers | +-
---------+-------------+--------+----------+---------+-----------+---------+
xe1/1      120           8        100        10        2           0
```

Table 4-47 explains the columns in the output.

Table 4-47: error traffic counters

Column	Description	Causes
Interface	Name of the interface	Point of interconnection in network.
Total errors	Total number of all types of errors	Number of errors in network.
Bad CRC	Number of packets received by the port from the network, where the packets have no CRC or a bad CRC.	Packet data modified making the CRC invalid.
Undersize	Total number of packets received that are less than 64 octets long (which exclude framing bits, but include the FCS) and have a good FCS value.	Bad frame generated by the connected device.
Oversize	Number of packets received by the port from the network, where the packets were more than maximum transmission unit size.	Faulty hardware, dot1q, or ISL trunking configuration issues.

Fragments	Total number of frames whose length is less than 64 octets (which exclude framing bits, but which include the FCS) and have a bad FCS value.	Ports are configured at half-duplex. Change the setting to full-duplex.
Jabbers	Total number of frames whose length is more than the maximum MTU size. (which exclude framing bits, but which include FCS) and have a bad FCS value.	Ports are configured at half-duplex. Change the setting to full-duplex.

show interface counters (indiscard-stats|outdiscard-stats)

Use this command to display the ingress and egress traffic discard reason counters on the interface.

Note: You can only display statistics for data ports and CPU ports, not for the out-of-band management (OOB) management port or logical interfaces.

Command Syntax `show interface (IFNAME|) counters (indiscard-stats|outdiscard-stats) show interface cpu counters (indiscard-stats|outdiscard-stats)`

Parameter

`IFNAME` Physical Interface name.

`indiscard-stats`

Discard reasons for ingress dropped packets.

`outdiscard-stats`

Discard reasons for egress dropped packets.

`cpu` CPU Interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

This command is not available on Qumran platforms.

Examples

```
#show interface xe1/3 counters indiscard-stats
+-------------------- +----------------   +---------------- +--------------------- + |
Counter Description | Count          | Last Increment | Last Increment Time | +---
------------------+---------------- +---------------+--------------------                + STP
Discards          0                 0  Vlan Discards          0                0
ACL Drops             0                 0  Policy Discards        0                0
 EGR Port Unavail      1092867          1092867          2016 Oct 25 19:54:58
 IBP Discards          0                0
+-------------------- +----------------   +---------------- +--------------------- +

#show interface counters indiscard-stats
+------------ +------------------ +---------------+---------------+------------------+------------------+--------------+ ------
-------------- +
|  Interface  | Port Block Drops | Vlan Discards | ACL/QOS Drops | Policy Discards | EGR Port Unavail | IBP Discards |   Total
Discards    |
+------------ +------------------ +---------------+---------------+------------------+------------------+--------------+ ------
```

```
-------------- +
xe1            0                   0                 35703           0                  11                  0              35714 xe2
0                   0                 295744           0                  13604              0                309348 xe3           0
0                9501             0                  20405               0              29906 xe5            0                   0
0                0                  13602               0              13602 xe49/1         0                   0               0
0                  0                   20658           20658 xe52/1         0                   3                856029          10
13613              0              869642 xe54/1         0                  5371            0                 0                 5371
0              5371 cpu            0                   0                 0                 0                  6                   0
N/A

#show interface counters outdiscard-stats +------------- +-----------------            +---------------+-------------    +------------------  +--
-------------- +----------------  +------
-------------- +
|  Interface  | Port Block Drops | Vlan Discards | TTL Discards | Unknown Discards |  UcastQ Drops   |  McastQ Drops |   Total
Discards   |
+------------- +-----------------   +--------------- +-------------- +-----------------        +----------------+---------------- +------
-------------- +
xe1            0                   0                 0              204338              0                0                204338 xe2
0                   0                 0              1094368             0                 0               1094368 xe3           0
0                0               818672             0                0                818672  xe52/1        0                  0
0              1275156             0                 0               1275156 xe54/1         0                   0               0
13575              0                 0                13575 cpu           0                   0                 0               0
N/A              1014224          N/A
```

Table 4-48 explain the fields in the command output.

Table 4-48: indiscard statistic output details

Statistic	Description
STP Discards	Packets received when the ingress interface is not in STP forwarding state.
Port Block Drops	Packets discarded on an ingress interface where port blocking is configured.
VLAN Discards	VLAN tagged packets received on a port which is not a member of the VLAN or untagged packets received on a trunk port.
ACL/QoS Drops	Incoming packets match a field processing entry with a drop or color drop action, such as: • User-configured ACL that denies traffic • Service policy with a police action that drops the traffic received at a rate higher than the configured limit
Policy Discards	Device policies violated, such as a storm control rate violation, source or destination discards when L2 tagged traffic received on router interface.
EGR (Egress) Port Unavail	No output port can be determined for this packet. This counter increments along with other counter types in this table because it is a “catchall” for multiple types of discards as shown below: • VLAN check failed • MTU check failed • ACL/QoS drops • Policy discards • Source MAC is null • Destination IP/source IP address is null • Source MAC address and destination MAC address are the same• Forwarding lookup failure

IBP Drops	Ingress Back Pressure (ingress congestion) when the ingress packet buffer is full for an interface.
Total Discards	Total number of ingress dropped packets.

Table 4-49 explain the fields in the command output.

Table 4-49: outdiscard statistics

Statistics	Description
Port Block Drops	Packets discarded on an egress interface where port blocking is configured.
VLAN Discards	Packets discarded because an invalid VLAN tag is encountered at an egress interface.

Table 4-49: outdiscard statistics

n
scarded because the Time-To Live (TTL) of the outgoing packet has passed.
scarded for other possible reasons like ACL drop in egress or a policer drop in egress. aused by congestion at queues and drops at queues are not counted under unknown
opped in the unicast queues because of congestion.
opped in the multicast queues because of congestion.
er of egress dropped packets.

show interface counters protocol

Use this command to display protocol packets received at the CPU by the control plane.

Command Syntax `show interface (IFNAME|) counters protocol`

Parameters

`IFNAME`	Interface name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.1.

This command is not available on Qumran platforms.

Example

```
#show interface counters protocol Interface ce1/1
lacp                 : 4   icmp6                :
5
```

Table 4-50 explain the fields in the command output.

Table 4-50: show interface counters protocol output details

Field	Description
Interface	Name of the configured interface.
lacp	Total number of lacp protocol in the interface.
icmp6	Total number of icmp6 protocol in the interface.

show interface counters queue-drop-stats

Use this command to display dropped packets in the CPU queue and the last increment time.

Command Syntax `show interface cpu counters queue-drop-stats`

Parameters

`cpu`	CPU interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in SWMRE version 1.3.2.

This command is not available on Qumran platforms.

Example `show interface cpu counters queue-drop-stats`

```
+-------------------+---------------+---------------+---------------------+      |
Queue Name     |     Count      | Last Increment | Last Increment Time | +----------
---------+----------------+----------------+---------------------+               arp
169735545        9145653          2017 Oct 23 14:33:54
```

Table 4-51 explain the fields in the command output.

Table 4-51: show interface counters queue-drop-stats output details

Field	Description
Queue Name	Name of the protocol.
Count	Number of arp protocols in the interface.
Last Increment	Final increment number in the protocol.
Last Increment time	Time of the last increment in the protocol.

show interface counters queue-stats

Use this command to display transmitted and dropped packet and byte counts of individual queues.

Command Syntax `show interface (IFNAME|) counters queue-stats show interface cpu counters queue-stats`

Parameters

`IFNAME`	Interface name.
`cpu`	CPU interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in SWMRE version 1.3.1.

This command is not available on Qumran platforms.

Example

```
#show interface counters queue-stats
D - Default Queue, U - User-defined Queue
+--------+---------------+------+-----------+-----------+-----------+---------------+
|Interface|Queue/Class-map|Q-Size|Output pkts|Output bytes|Dropped pkts|Dropped bytes  | +--------+-
```

```
                +------+-----------+------------+------------+---------------+ xe1/1     q1
(D) 0       12           1368        0            0 xe1/1     mc-q7         (D) 0       1            82
0              0 xe25      q1          (D) 0       6           684           0             0

#show interface xe1/1 counters queue-stats
D - Default Queue, U - User-defined Queue
                +------ +-------+-  -------+----------- +-------------           +
|Queue/Class-map|Q-Size|Tx pkts| Tx bytes |Dropped pkts|Dropped bytes | +----------
-----+------ + -------+----------+------------+-------------  + q0            (D) 0
0       0           0           0 q1            (D) 0     12      1368        0
0 q2             (D) 0     0      0           0            0 q3            (D) 0
0       0           0           0 q4            (D) 0     0       0           0
0 q5             (D) 0     0      0           0            0 q6            (D) 0
0       0           0           0 q7            (D) 0     0       0           0
0 mc-q0          (D) 0     0      0           0            0  mc-q1        (D) 0
0       0           0           0  mc-q2        (D) 0     0       0           0
0 mc-q3          (D) 0     0      0           0            0  mc-q4        (D) 0
0       0           0           0  mc-q5        (D) 0     0       0           0
0 mc-q6          (D) 0     0      0           0            0  mc-q7        (D) 0
1       82          0           0

#show interface cpu counters queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
              +--------        +----------------    +------------------        +-----------------     +------------------     +            |
Queue/Class-map  | Q-Size |      Tx pkts     |     Tx bytes        | Dropped pkts    |  Dropped bytes    | +---------------
-----+-------- +----------------- +------------------    +----------------        +------------------          +
igmp                (E) 800592  14519              987292              1304163            88683084 arp
(E) 1250496   1008785           68597380             0                  0
```

Table 4-52 explain the fields in the command output.

Table 4-52: queue flags detail

Flag	Meaning
D	Default queue of the port.
U	User defined queue of the port.
E	Outgoing hello packet's queue in the port.
I	Incoming hello packet's queue in the port.
Q	Hello packet's queue size in bytes.

Table 4-53 explain the fields in the command output.

Table 4-53: show interface counters queue-stats output details

Field	Description
Interface	A defined physical interface to which the queue is associated.

Queue/Class-map	Queues associated with a QoS class-map.
Q-Size	The size of a specified queue in bytes.
Output pkts	The number of out bound packets residing in the queues.
Output Bytes	The number of bytes in the outbound queue.
Dropped pkts	The number of packets dropped because of queue overflow.
Dropped bytes	The number of bytes dropped because of queue overflow.
Tx pkts	The number of transmit packets contained in the out bound queue.
Tx bytes	The number of transmit bytes contained in the out bound queue.

show interface counters rate

Use this command to display the average traffic rate over the load interval of the interface.

Command Syntax `show interface (IFNAME|) counters rate (kbps|mbps|gbps|) show interface cpu counters rate (kbps|mbps|gbps|)`

Parameter

`IFNAME`	Interface name.
`kbps`	Kilobits per second.
`mbps`	Megabits per second.
`gbps`	Gigabits per second.
`cpu`	CPU interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

This command is not available on Qumran platforms.

Example

```
#show interface counters rate
+-------------+--------------------------+-------------------------------+ |
|              Rx           |               Tx               | |  Interface  |---
-----------------------+-------------------------------| |             |
```

```
bps       |      pps     |       bps       |      pps      | +------------        +----------
                  +-----------------------------                +    xe1/1          548439552
1008160      544400            1000

#show interface cpu counters rate
Load interval: 30 second
                     +--------------+-------------+-------------    +------------        + |
CPU Queue(%)    |     Rx bps     |    Rx pps    |     Tx bps      |    Tx pps    | +-------
            +--------------+-------------+-------------+------------        +  isis
(   0%) -              -              742            0   arp           (   0%) -
-              6              0
```

Table 4-54 explain the fields in the command output.

Table 4-54: show interface counters rate output details

scription
e particular interface.
mber of hello packets received from the neighbor.
mber hello packets transmitted to the neighbor.
tes per second.
ckets per second.
U Queues used for various functions. In the example the CPU is maintaining queues for ARP and the S routing facilities.
e length of time for which data is used to compute load statistics.
mber of hello packets received from the neighbor in bytes per second.
mber of hello packets received from the neighbor in packets per second.
mber hello packets transmitted to the neighbor in bytes per second.
mber hello packets transmitted to the neighbor in packets per second.

show interface counters summary

Use this command to display the summary of traffic counters on a specific interface or all interfaces.

Note: This command is supported for the out-of-band management (OOB) management interface.

Command Syntax `show interface (IFNAME|) counters summary`

Parameter

`IFNAME`	Interface name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show interface xe1/1 counters summary
+----------- +-------------------------------                  +-------------------------------                        + |             |
Rx                  |                Tx                  | | Interface |---------------------------
.............................                                | |             |     packets     |     bytes       |
packets     |      bytes     | +-----------+---------------  +---------------  +---------------     +--
------------     +   xe1/1        11032977        11032960000      61                3904


#show interface counters summary
+------------ +-------------------             +-------------------  +-------------------  +-------------------             + |  Interface  |
Rx packets      |       Rx bytes       |      Tx packets      |       Tx bytes       | +------------- +-------------------
-+-------------------             +-------------------           +-------------------           +
 eth0              206222                  13756391                  235123                  337010937   po1
809121               72989094              825221               90605534  xe1/1          0                   0
1                     114  xe3/1        43                     4730                  21                  2298
xe5/1           29                     3178                    21                     2298  xe8            10
1076                  14                   1532  xe9/1          16                    1760                 21
2298    xe11/1          0                        0                      7                        766   xe19/1
12426292              1298526692          6                     620 xe21/1          13                  1386
14                   1532   xe28/1       3144                  202370               21                  2298
xe30/1          3161                  202304                 7                     766  xe32/1         694067
61687838                 710274                 79315093  xe32/2          115054                  11301256
114947                    11290441  xe32/3          603759                   51208946                620502
68865557   xe32/4          7                     766                    7                     766
```

Table 4-55 explain the fields in the command output.

Table 4-55: show interface counters summary output details

Description
The particular interface.
Number of hello packets received from the neighbor.

Number hello packets transmitted to the neighbor.
Bytes per second.
Packets per second.
Number of hello packets received from the neighbor in bytes per second.
Number of hello packets received from the neighbor in packets per second.
Number hello packets transmitted to the neighbor in bytes per second.
Number hello packets transmitted to the neighbor in packets per second.

show ip forwarding

Use this command to display the IP forwarding status.

Command Syntax `show ip forwarding`

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following is a sample output of the `show ip forwarding` command displaying the IP forwarding status.

```
#show ip forwarding
vrf (management) :IP forwarding is on
vrf (default) :IP forwarding is on #
```

show ip interface

Use this command to display brief information about interfaces and the IP addresses assigned to them. To display information about a specific interface, specify the interface name with the command.

Command Syntax `show ip interface`

`brief show ip interface IFNAME`

`brief`

Parameters

`IFNAME` Interface name. `brief` Brief summary of IP status and configuration.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following is a sample output from the `show ip interface brief` command:

```
#show ip interface brief

'*' - address is assigned by dhcp client

Interface             IP-Address      Admin-Status          Link-
Status eth0                  *10.10.26.101   up                    up
lo                    127.0.0.1       up                    up
lo.management         127.0.0.1       up                    up xe1/1
10.1.1.1        up                     up xe1/2
unassigned      down                   down xe1/3
unassigned      down                   down xe1/4
unassigned      down                   down xe2
unassigned      up                     down xe3/1
unassigned      up                     up xe3/2
unassigned      down                   down xe3/3
unassigned      down                   down
```

Table 4-56 explain the fields in the command output.

Table 4-56: show ip interface output details

Field	Description

Interface	Interface name, also specifies interface type (eth0, lo, xe1/1, and xe1/2).
IP-Address	The IP address assigned to the interface. An asterisks indicates that the IP address was provided by DHCP.

Table 4-56: show ip interface output details (Continued)

	Description
	Interface is up and functioning or down.
	Interface is connected and passing traffic.

show ip prefix-list

Use this command to display the prefix list entries for IPv4 interfaces.

Syntax Description `show ip prefix-list show ip prefix-list WORD show ip prefix-list WORD seq <1-4294967295> show ip prefix-list WORD A.B.C.D/M show ip prefix-list WORD A.B.C.D/M longer show ip prefix-list WORD A.B.C.D/M first-match show ip prefix-list summary show ip prefix-list summary WORD show ip prefix-list detail show ip prefix-list detail WORD`

Parameters

`WORD` Name of a prefix list.

`A.B.C.D/M` IP prefix <network>/<length> (for example, 35.0.0.0/8).

`first-match` First matched prefix. `longer` Lookup longer prefix.

`<1-4294967295>` Sequence number. `detail` Detail of prefix lists. `summary` Summary of prefix lists.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following is a sample output of the `show ip prefix-list` command showing prefix-list entries.

```
#show ip prefix-list
ip prefix-list myPrefixList: 3 entries    seq
5 permit 172.1.1.0/16    seq     10 permit
173.1.1.0/16    seq     15 permit 174.1.1.0/16
```

show ip route

Use this command to display the IP routing table for a protocol or from a particular table.

When multiple entries are available for the same prefix, NSM uses an internal route selection mechanism based on protocol administrative distance and metric values to choose the best route. All best routes are entered into the FIB and can be viewed using this command. To display *all* routes (selected and not selected), use the `show ip route database` command.

Command Syntax `show ip route A.B.C.D show ip route A.B.C.D/M`

`show ip route (database|) show ip route (database|)`

`(bgp|connected|database|isis|fast-`

`reroute|interface|isis|kernel|mbgp|mstatic|next-hop|ospf|rip|static)`

`show ip route summary show ip route`

`vrf WORD (database|)`

`show ip route vrf WORD (database|) (bgp|connected|isis|kernel|ospf|rip|static)`

Parameters

`A.B.C.D`	Network in the IP routing table.
`A.B.C.D/M`	IP prefix <network>/<length>, for example, 35.0.0.0/8.
`bgp`	Border Gateway Protocol.
`connected`	Connected.
`database`	Routing table database.
`fast-reroute`	Fast reroute repair paths.
`interface`	Interface.
`isis`	IS-IS.
`kernel`	Kernel.
`mbgp`	Multiprotocol BGP routes.
`mstatic`	Multicast static routes.
`next-hop`	Next hop address.
`ospf`	Open Shortest Path First.
`rip`	Routing Information Protocol.
`static`	Static routes.
`summary`	Summarize all routes.
`WORD`	Routes for a Virtual Routing/Forwarding instance.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example: Display FIB Routes

The following shows output for the best routes.

```
#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       area * - candidate default
Gateway of last resort is 10.30.0.11 to network 0.0.0.0
```

```
K*      0.0.0.0/0 via 10.30.0.11, eth0
O       9.9.9.9/32 [110/31] via 10.10.31.16, eth2, 00:18:56
K10.10.0.0/24 via 10.30.0.11, eth0
C10.10.31.0/24 is directly connected, eth2
S10.10.34.0/24 [1/0] via 10.10.31.16, eth2
O10.10.37.0/24 [110/11] via 10.10.31.16, eth2, 00:20:54
C10.30.0.0/24 is directly connected, eth0
S11.22.11.0/24 [1/0] via 10.10.31.16, eth2
O E214.5.1.0/24 [110/20] via 10.10.31.16, eth2, 00:18:56
S16.16.16.16/32 [1/0] via 10.10.31.16, eth2
O17.17.17.17/32 [110/31] via 10.10.31.16, eth2, 00:20:54
C45.45.45.45/32 is directly connected, lo
O55.55.55.55/32 [110/21] via 10.10.31.16, eth2, 00:20:54
C127.0.0.0/8 is directly connected, lo
```

Header

Each entry in this table has a code preceding it, indicating the source of the routing entry. For example, O indicates OSPF as the origin of the route and K indicates that the route has been learned from the kernel. Table 4-57 shows these codes and modifiers.

Table 4-57 explain the fields in the command output.

Table 4-57: route codes and modifiers

Code	Meaning	Description
K	kernel	Routes added through means other than by using the CLI; for example by using the operating system route command. Static routes added using kernel commands and static routes added using SWMRE commands are different. The kernel static routes are not redistributed when you give the `redistribute static` command in a protocol. However, the kernel static routes can be redistributed using the `redistribute kernel` command.
C	connected	Routes directly connected to the local device that were not distributed via IGP. The device inherently knows of these networks, so there is no need to learn about these from another device. Connected routes are preferred over routes for the same network learned from other routing protocols. Routes for connected networks always exist in the kernel routing table but as an exception are not marked as kernel routes because SWMRE always calculates entries for these routes upon learning interface information from the kernel.
S	static	Routes manually configured via CLI which are not updated dynamically by IGPs.
The codes below are for routes received and dynamically learned via IGP neighbors. These networks are not directly connected to this device and were announced by some other device on the network. IGPs update these routes as the network topology changes.		
R	RIP	

B	BGP	
O	OSPF	Modifiers for OSPF: IA - OSPF inter area N1 - OSPF NSSA external type 1 N2 - OSPF NSSA external type 2 E1 - OSPF external type 1 E2 - OSPF external type 2
i	IS-IS	Modifiers for IS-IS: L1 - IS-IS level-1 L2 - IS-IS level-2 ia - IS-IS inter area
Other modifiers:		
v	vrf leaked	The device has two or more VRFs configured and each has at least one interface bound to it. While each VRF will have its own routing table, the VRFs can learn each other's routes.
*	candidate default	Route has been added to the FIB. With equal cost paths to a destination, the router does per-packet or per-destination load sharing. An asterisk ("*") means that the route is being used at that instant for forwarding packets. If you run the same `show ip route x.x.x.x` command over and over, you might see the * moving between the route entries.
>	selected route	When multiple routes are available for the same prefix, the best route. When multiple entries are available for the same prefix, SWMRE uses an internal route selection mechanism based on protocol administrative distance and metric values to choose the best route. SWMRE populates the FIB with the *best* route to each destination
p	stale info	

After the codes, the header has default gateway information:

```
Gateway of last resort is 10.12.4.1 to network 0.0.0.0
```

The "gateway of last resort", also called the default gateway, is a static route that routes IP address 0.0.0.0 (all destinations) through a single host (the gateway). The effect of setting a gateway is that if no routing table entry exists for a destination address, packets to that address will be forwarded to the gateway router.

Route Entry Fields

Table 4-58 explains the each route entry fields.

Table 4-58: route entry output details

Field	Description
Codes and modifiers	As explained in Table 4-57.

IP address	IP address of the remote network.
Administrative distance and metric	The administrative distance determines how trustworthy this route is. If there is a similar route but with a smaller administrative distance, it is used instead, because it is more “trustworthy”. The smaller the administrative distance, the more trustworthy the route. Directly connected routes have an administrative distance of 0, which makes them the most trustworthy type of route.The metric varies from protocol to protocol, and for OSPF the metric is cost, which indicates the best quality path to use to forward packets. Other protocols, like RIP, use hop count as a metric. For neighboring routers, the metric value is 1.
Next hop router IP address	This route is available through the next hop router located at this IP address. This identifies exactly where packets go when they match this route.
Outgoing interface name	Interface used to get to the next-hop address for this route.
Duration	Length of time that this route has been present in the routing table. This is also the length of time this route has existed without an update. If the route were removed and then re-added (if the cable was disconnected, for instance), this timer would begin again at 00:00:00.

Route Entry Examples

```
O       10.10.37.0/24 [110/11] via 10.10.31.16, eth2, 00:20:54
```

- This route in the network 10.10.37.0/24 was added by OSPF.
- This route has an administrative distance of 110 and metric/cost of 11.
- This route is reachable via nexthop 10.10.31.16.
- The outgoing local interface for this route is eth2.
- This route was added 20 minutes and 54 seconds ago.

```
O E2    14.5.1.0/24 [110/20] via 10.10.31.16, eth2, 00:18:56
```

- This route is the same as the other OSPF route above; the only difference is that it is a Type 2 External OSPF route.

```
C       10.10.31.0/24 is directly connected, eth2
```

- This route is directly connected.
- Route entries for network 10.10.31.0/24 are derived from the IP address of local interface eth2.

```
K10.10.0.0/24 via 10.30.0.11, eth0
```

- This route in the network 10.10.0.0/24 was learned from the kernel routing table (route was statically added using kernel commands).
- This route is reachable via nexthop 10.30.0.11.
- The outgoing local interface for this route is eth0.

```
K*      0.0.0.0/0 via 10.30.0.11, eth0
```

- This is a default route that was learned from the kernel (route was statically added using kernel commands).
- This route is reachable via nexthop 10.30.0.11.
- The local interface for this route is eth0.

Example: Display OSPF Routes

The following is the output with the `ospf` parameter:

```
#show ip route ospf
O       1.1.1.0/24 [110/20] via  2.2.2.1, eth2, 00:00:44
O IA    4.4.4.0/24 [110/21] via  2.2.2.1, eth2, 00:00:44 #
```

Example: Display Route Summary

The following is the output with the `summary` parameter.

```
#show ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 4
Route Source    Networks
kernel          1
connected       5 ospf
2 Total           8
FIB             2
```

Example: Display RIB Routes

The following shows displaying database routes.

```
#show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF  NSSA  external  type 1, N2  -  OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       area > - selected route, * - FIB route, p - stale info

K    *> 0.0.0.0/0 via 10.30.0.11, eth0
O    *> 9.9.9.9/32 [110/31] via 10.10.31.16, eth2, 00:19:21
K*> 10.10.0.0/24 via 10.30.0.11, eth0
O10.10.31.0/24 [110/1] is directly connected, eth2, 00:28:20
C*> 10.10.31.0/24 is directly connected, eth2
S*> 10.10.34.0/24 [1/0] via 10.10.31.16, eth2
O10.10.34.0/24 [110/31] via 10.10.31.16, eth2, 00:21:19
O*> 10.10.37.0/24 [110/11] via 10.10.31.16, eth2, 00:21:19
K*  10.30.0.0/24 is directly connected, eth0
C*> 10.30.0.0/24 is directly connected, eth0
S*> 11.22.11.0/24 [1/0] via 10.10.31.16, eth2
O E2 *> 14.5.1.0/24 [110/20] via 10.10.31.16, eth2, 00:19:21
O16.16.16.16/32 [110/11] via 10.10.31.16, eth2, 00:21:19
S*> 16.16.16.16/32 [1/0] via 10.10.31.16, eth2
O*> 17.17.17.17/32 [110/31] via 10.10.31.16, eth2, 00:21:19
C*> 45.45.45.45/32 is directly connected, lo
O*> 55.55.55.55/32 [110/21] via 10.10.31.16, eth2, 00:21:19
K*  127.0.0.0/8 is directly connected, lo
C*> 127.0.0.0/8 is directly connected, lo
```

The codes and modifier at the start of each route entry are explained in Table 4-57.

Routes in the FIB are marked with a *. When multiple routes are available for the same prefix, the best route is indicated with the > symbol. Unselected routes have neither the * nor the > symbol.

Route Database Entry Examples

This example shows 2 entries in the route database; one learned from the kernel and the other derived from interface information.

```
K    * 10.30.0.0/24 is directly connected, eth0
C *> 10.30.0.0/24 is directly connected, eth0
```

- Both these routes are in the same network 10.30.0.0/24.
- The first route has originated from the kernel. The * indicates that it has been added to the FIB.
- The second route is derived from the IP address of local interface eth0. It is marked as a connected route. Since a connected route has the lowest administrative distance, it is the selected route.

```
S    *> 10.10.34.0/24 [1/0] via 10.10.31.16, eth2
O       10.10.34.0/24 [110/31] via 10.10.31.16, eth2, 00:21:19
```

- The same prefix was learned from OSPF and from static route configuration.
- Static routes are preferred over OSPF routes, so the static route is selected and installed in the FIB.

  Note: If the static route becomes unavailable, SWMRE automatically selects the OSPF route and installs it in the FIB.

show ip vrf

This command displays routing information about VRFs.

Command Syntax `show ip vrf show ip vrf WORD`

Parameter

`WORD`	Virtual Routing and Forwarding name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip forwarding vrf (management) :IP forwarding is on vrf (default)
:IP forwarding is on
```

show ipv6 forwarding

Use this command to display the IPv6 forwarding status.

Command Syntax `show ipv6 forwarding`

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following is a sample output of the `show ipv6 forwarding` command displaying the IPv6 forwarding status.

```
#show ipv6 forwarding
 vrf (management) :IPv6 forwarding is on vrf
(default) :IPv6 forwarding is on#
```

show ipv6 interface brief

Use this command to display information about interfaces. To display information about a specific interface, include the interface name.

Command Syntax `show ipv6 interface brief show ipv6 interface IFNAME brief`

Parameters

`IFNAME`	Name of the interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ipv6 interface brief
Interface           IPv6-Address                Admin-Status lo

::1                          [up/up] gre0                unassigned

[admin down/down]

eth3                3ffe:abcd:104::1            [up/up]
                    3ffe:abcd:103::1

fe80::2e0:29ff:fe6f:cf0 eth1               fe80::260:97ff:fe20:f257

[up/up] eth2                  unassigned                       [admin

down/down] eth3                 unassigned                     [admin

down/down] sit0                 unassigned                     [admin

down/down] tun24                unassigned                     [admin

down/down]

tun10               unassigned                  [admin down/down]
```

Table 4-59 explains the each interface brief entry.

Table 4-59: show interface brief output details

scription

me of the interface.
v6 address. An asterisk (“*”) means the address was assigned by the DHCPv6 client.
atus of the interface: e first part of the field indicates if the interface is up. e second part indicates if the interface is running.

show ipv6 route

Use this command to display the IP routing table for a protocol or from a particular table, including database entries known by NSM. When multiple entries are available for the same prefix, NSM uses an internal route selection mechanism based on protocol administrative distance and metric values to choose the best route. The best routes in the FIB can be viewed using `show ipv6 route`.

Command Syntax `show ipv6 route vrf WORD (database|) show ipv6 route vrf WORD (database|) (bgp|connected|isis|kernel|ospf|rip|static) show ipv6 route (database) show ipv6 route (database) (bgp|connected|isis|kernel|ospf|rip|static) show ipv6 route X:X::X:X show ipv6 route X:X::X:X/M show ipv6 route summary`

Parameters

`X:X::X:X`	Network in the IP routing table.
`X:X::X:X/M`	Prefix <network>/<length>, e.g., 35.0.0.0/8
`all`	All IPv6 routes
`bgp`	Border Gateway Protocol.
`connected`	Connected.
`database`	IPv6 routing table database.
`isis`	IS-IS.
`IFNAME`	Interface name
`kernel`	Kernel.
`ospf`	Open Shortest Path First.
`rip`	Routing Information Protocol.
`static`	Static routes.
`summary`	Summarize all routes
`WORD`	Routes from a Virtual Routing and Forwarding instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

See Table 4-57 and Table 4-58 for an explanation of the codes and fields in the output.

```
    #show ipv6 route
      Codes: K - kernel route, C - connected, S - static, R - RIPng, O - OSPFv3,
        I - IS-IS, B - BGP, > - selected route, * - FIB route, p - stale info.
C> * ::1/128 is directly connected, lo
C> * 3ffe:1::/48 is directly connected, eth1
C> * 3ffe:2:2::/48 is directly connected, eth2 #
```

show ipv6 prefix-list

Use this command to display the prefix list entries for IPv6 interfaces.

Syntax Description `show ipv6 prefix-list show ipv6 prefix-list WORD show ipv6 prefix-list WORD seq <1-4294967295> show ipv6 prefix-list WORD X:X::X:X/M show ipv6 prefix-list WORD X:X::X:X/M longer show ipv6 prefix-list WORD X:X::X:X/M first-match show ipv6 prefix-list summary show ipv6 prefix-list summary WORD show ipv6 prefix-list detail show ipv6 prefix-list detail WORD`

Parameters

`WORD` Name of prefix list.

`X:X::X:X/M` IP prefix <network>/<length> (for example, 35.0.0.0/8). `first-match` First matched prefix. `longer` Look up longer prefix.

`<1-4294967295>`

Sequence number of an entry.

`detail` Detail of prefix lists. `summary` Summary of prefix lists.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following is a sample output of the `show ip prefix-list` command showing prefix-list entries.

```
#show ip prefix-list
ip prefix-list myPrefixList: 3 entries    seq
5 permit 172.1.1.0/16    seq     10 permit
173.1.1.0/16    seq     15 permit 174.1.1.0/16
```

show hosts

Use this command to display the IP domain-name, lookup style and any name server.

Command Syntax `show hosts`

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show hosts
```

show running-config interface

Use this command to show the running system status and configuration for a specified interface, or a specified interface for a specified protocol.

Command Syntax `show running-config interface IFNAME show running-config interface IFNAME bridge show running-config interface IFNAME dot1x show running-config interface IFNAME ip igmp show running-config interface IFNAME ip multicast show running-config interface IFNAME ip pim show running-config interface IFNAME ipv6 ospf show running-config interface IFNAME ipv6 rip show running-config interface IFNAME ipv6 pim show running-config interface IFNAME isis show running-config interface IFNAME lacp show running-config interface IFNAME ldp show running-config interface IFNAME mpls show running-config interface IFNAME mstp show running-config interface IFNAME ospf show running-config interface IFNAME ptp show running-config interface IFNAME rip show running-config interface IFNAME rstp show running-config interface IFNAME rsvp show running-config interface IFNAME stp show running-config interface IFNAME synce show running-config interface IFNAME trill`

Parameters

`bridge`	Bridge.
`dot1x`	IEEE 802.1X port-based access control.
`ip`	IPv4 (see also show running-config interface ip).
`ipv6`	IPv6 (see also show running-config interface ipv6).
`isis`	Intermediate System to Intermediate System.
`lacp`	Link Aggregation Control Protocol.
`ldp`	Label Distribution Protocol.
`mpls`	Multi-Protocol Label Switching.
`mstp`	Multiple Spanning Tree Protocol.

`ospf` Open Shortest Path First. `ptp` Precision Time Protocol. `rip` Routing Information Protocol. `rstp` Rapid Spanning Tree Protocol. `rsvp` Resource Reservation Protocol. `stp` Spanning Tree Protocol. `synce` Synchronous Ethernet. `trill` Transparent Interconnection of Lots of Links.

Command Mode

Privileged Exec mode and Config Mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show running-config interface eth1 bridge
! interface eth1
switchport bridge-group 1
switchport mode access
user-priority 3
 traffic-class-table user-priority 2 num-traffic-classes 3 value 3 trafficclass-
table user-priority 7 num-traffic-classes 1 value 2 traffic-class-table user-
priority 7 num-traffic-classes 2 value 0 traffic-class-table userpriority 7 num-
traffic-classes 3 value 0 traffic-class-table user-priority 7 num-traffic-
classes 4 value 0 traffic-class-table user-priority 7 num-trafficclasses 5 value
0 traffic-class-table user-priority 7 num-traffic-classes 6
```

show running-config interface ip

Use this command to show the running system status and configuration for a specified IP.

Command Syntax `show running-config interface IFNAME ip (igmp|multicast|pim|)`

Parameters

`IFNAME`	Interface name.
`igmp`	Internet Group Management Protocol.
`multicast`	Multicast.
`pim`	Protocol Independent Multicast.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show running-config interface eth1 ip igmp
! interface eth1 switchport
```

show running-config interface ipv6

Use this command to show the running system status and configuration for a specified IPv6 protocol.

Command Syntax `show running-config interface IFNAME ipv6 (mld|multicast|ospf|pim|rip|)`

Parameters

`IFNAME`	Interface name.
`mld`	Multicast Listener Discovery
`multicast`	Multicast
`ospf`	Open Shortest Path First
`pim`	Protocol Independent Multicast
`rip`	Routing Information Protocol

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show running-config interface eth1 ipv6 rip
! interface
eth1 switchport
```

show running-config ip

Use this command to show the running system of IP configurations.

Command Syntax `show running-config ip (dhcp|mroute|route)`

Parameters

`dhcp`	Dynamic Host Configuration Protocol.
`mroute`	Static IP multicast route.
`route`	Static IP route.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
>enable
#show running-config ip route
! ip route 3.3.3.3/32 eth3 ip route 3.3.3.3/32 eth2 ip
route 200.0.0.0/16 lo !
```

show running-config ipv6

Use this command to show the running system status and configuration for IPv6.

Command Syntax `show running-config ipv6 (access-list|mroute|neighbor|prefix-list|route|)`

Parameters

`access-list`	Access list.
`mroute`	Static IPv6 Multicast route.
`neighbor`	Static IPv6 neighbor entry.
`prefix-list`	IPv6 prefix-list.
`route`	Static IPv6 route.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
>enable
#show running-config ipv6 access-list
!
ipv6 access-list abc permit any
!
#show running-config ipv6 prefix-list
!
ipv6 prefix-list sde seq 5 permit any
!
#show running-config ipv6 route
!
ipv6 route 3e11::/64 lo ipv6 route
3e11::/64 eth2 ipv6 route
fe80::/64 eth2 !
```

shutdown

Use this command to shut down an interface.

Use the `no` form of this command to bring up an interface.

Command Syntax `shutdown`

`no shutdown`

Parameters

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows the use of the `shutdown` command to shut down the interface called `eth3`.

```
#configure terminal
(config)#interface eth3
(config-if)#shutdown
```

speed

Use this command to set the link speed of the interface.

Use the `no` parameter to set the speed to its default value.

On Trident2 and Trident2+ switches, even if a fiber port is running at a variable 10M/100M/1G auto-negotiated speed, if you give this command to manually set the speed to less than 1G, the speed is always set to 1G. However, the show interface command displays the speed of such ports as set by you.

If a switch has copper ports and you set the speed using this command, the link goes down. For these switches, only use auto-negotiated port speeds.

Note: If a 1G copper SFP is inserted, auto-negotiation should be disabled and the port speed should be configured as 1G by using the command: `speed 1g`. This is necessary because even if auto-negotiation is disabled on the board, the external PHYs on 1G copper SFPs will still auto-negotiate with their peers for 1G port speed.

Command Syntax

```
speed (10m | 100m | 1g | 2.5g | 10g | 20g | 25g | 40g | 50g | 100g |
  (auto (1g | 10g | 20g | 25g | 40g | 50g | 100g |)))
no speed
```

Parameter

`10m`	10 megabits
`100m`	100 megabits
`1g`	1 gigabit
`2.5g`	2.5 gigabits
`10g`	10 gigabits
`20g`	20 gigabits
`25g`	25 gigabits
`40g`	40 gigabits

`50g`	50 gigabits
`100g`	100 gigabits
`auto`	Negotiate the speed with a connected port

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

Configure forced speed to 10G:

```
#configure terminal
(config)#interface xe0
(config-if)#speed 10g
```

Enable auto-negotiation:

```
#configure terminal
(config)#interface xe0
(config-if)#speed auto
```

Enable auto-negotiation up to 10G:

```
#configure terminal
(config)#interface xe0
(config-if)#speed auto 10g
```

switchport

Use this command to set the mode of an interface to switched.

All interfaces are configured `routed` by default. To change the behavior of an interface from switched to routed, you must explicitly give the `no switchport` command.

Note: When you change the mode of an interface from switched to routed and vice-versa, all configurations for that interface are erased.

User should be prompted for confirmation, while executing `switchport/no switchport` command. To support this requirement, please refer the command `enable/disable confirmation-dialog.`

Use the `no` form of this command to set the mode to routed.

Command Syntax

```
switchport
no
switchport
```

Parameters

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0 (config-
if)#switchport

(config)#interface eth0
(config-if)#no switchport

#configure terminal
(config)#enable confirmation-dialog
(config)#interface xe5
(config-if)#switchport
Are you sure? (y/n): y
(config-if)#
(config-if)#exit

(config)#disable confirmation-dialog
(config)#
```

```
(config)#interface xe5
(config-if)#switchport
(config-if)#
```

switchport allowed ethertype

Use this command to indicate which types of traffic will be allowed on the switchport.

Note: A maximum of 5 Ethertype values can be assigned on an interface.

Command Syntax `switchport allowed ethertype {arp|ipv4|ipv6|mpls|ETHTYPE|log}`

Parameters

`arp`	ARP traffic
`ipv4`	IPv4 traffic
`ipv6`	IPv6 traffic
`mpls`	MPLS traffic
`ETHTYPE`	Traffic of any Ethertype value (0x600 - 0xFFFF).
`log`	Log unwanted ethertype packets.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
(config)#interface xe32/1

(config-if)#switchport
(config-if)#switchport allowed ethertype ipv4
(config-if)#switchport allowed ethertype 0x800
```

© Symanitron Proprietary

CHAPTER 5 Access Control List Commands

This chapter is a reference for the Access Control List (ACL) commands:

- access-list logging cache-size
- access-list logging rate-limit
- clear access-list log-cache
- clear access-list
- clear ip access-list
- clear ipv6 access-list
- clear mac access-list
- ip access-group
- ip access-list default
- ip access-list icmp
- ip access-list filter
- ip access-list fragments
- ip access-list remark
- ip access-list resequence
- ip access-list tcp|udp
- ip access-list WORD
- ipv6 access-list default
- ipv6 access-list filter
- ipv6 access-list fragments
- ipv6 access-group
- ipv6 access-list icmpv6
- ipv6 access-list remark
- ipv6 access-list resequence
- ipv6 access-list sctp
- ipv6 access-list tcp|udp
- ipv6 access-list WORD
- mac access-group
- ip access-list default
- mac access-list filter
- mac access-list remark
- mac access-list resequence
- mac access-list WORD
- show access-lists

- show access-list log-cache
- show ip access-lists
- show ipv6 access-lists
- show mac access-lists
- show running-config aclmgr
- show running-config access-list
- show running-config ipv6 access-list

access-list logging cache-size

Use this command to set the ACL logging table size.

Use no command to set the table size to its default.

Command Syntax `access-list logging cache-size <1000-10000> no access-list logging cache-size`

Parameters

`<1000-10000>` Maximum number of cache entries

Default

By default, logging table size is 1000.

Command Mode

Configuration mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#access-list logging cache-size 2000
(config)#end
```

access-list logging rate-limit

Use this command to set the rate limit for logging ACL denied packets.

Use no command to reset the rate to default.

Command Syntax `access-list logging rate-limit <0-1000> no access-list logging rate-limit`

Parameters

`<0-1000>` Packets per second

Default

By default, rate is 200 packets per second.

Command Mode

Configuration mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#access-list logging rate-limit 500
(config)#end
```

clear access-list log-cache

Use this command to clear the access-list logging table.

Command Syntax `clear access-list log-cache`

Parameters

None

Command Mode

Exec mode and Privilege exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear access-list log-cache
```

clear access-list

Use this command to clear the access-list counters.

Command Syntax `clear access-list (WORD|) counters`

Parameters

`WORD`	Access-list name.

Command Mode

Exec mode and Privilege exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear access-list counters
```

clear ip access-list

Use this command to clear the IP access-list counters.

Command Syntax `clear ip access-list (WORD|) counters`

Parameters

`WORD`	Access-list name.

Command Mode

Exec mode and Privilege exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear ip access-list counters
```

clear ipv6 access-list

Use this command to clear the IPv6 access-list counters.

Command Syntax `clear ipv6 access-list (WORD|) counters`

Parameters

`WORD`	Access-list name.

Command Mode

Exec mode Privilege exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear ipv6 access-list counters
```

clear mac access-list

Use this command to clear the MAC access-list counters.

Command Syntax `clear mac access-list (WORD|) counters`

Parameters

`WORD`	Access-list name.

Command Mode

Exec mode Privilege exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear mac access-list counters
```

ip access-group

Use this command to attach IP access list to an interface to filter incoming or outgoing packets.

When you attach an access list to a VLAN interface or LAG interface as well as to a physical interface that is a member of that LAG and/or VLAN interface, the priority order is:

1. VLAN interface
2. LAG interface
3. Physical interface

For example, if you attach access lists to both a LAG interface and a physical interface that is a member of that LAG, matching traffic rules are applied to the LAG interface, but not to the physical interface.

Use the `no` parameter with this command to detach an IP access group.

Note: Access-group on egress direction uses the TCAM group used by QoS output service policy. Hence, actions will be unpredictable when conflicting matches are configured on same interface. It is recommended to avoid such configuration. Otherwise user need to configure priority (in QoS) / sequence number (in ACL) carefully to tackle such cases.

C

o

m

m

a

n

d

S

y

n

t

a

x

`i`

`p`

`a`

```
c
c
e
s
s
-
g
r
o
u
p
W
O
R
D
(
i
n
|
o
u
t
)
n
o
i
p
a
c
c
e
s
s
-
g
r
o
```

```
u
p
W
O
R
D
(
i
n
|
o
u
t
)
```

Parameters

WORD	Access list name.
in	Filter incoming packets (not supported on Qumran platform)
out	Filter outgoing packets.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip access-list mylist
(config-ip-acl)#permit ip any any
(config-ip-acl)#exit

(config)#interface eth3
(config-if)#ip access-group mylist in
(config-if)#exit

(config)#interface eth3
```

```
(config-if)#no ip access-group mylist in
(config-if)#exit
```

ip access-list default

Use this command to modify the default rule action of access-list. Default rule is applicable only when access-list is attached to interface. Default rule will have the lowest priority and only the packets not matching any of the user defined rules match default rule.

Command Syntax `default (deny-all|permit-all) (log|) (sample|)`

Parameters

`deny-all`	Drop all packets.
`permit-all`	Accept all packets.
`log`	Log the packets matching the filter (in-direction only).
`Sample`	Sample the packets matching the filter (in-direction only).

Default

No default value is specified

Command Mode

IP access-list mode

Applicability

This command was introduced before SWMRE version 1.3.

Log feature is supported only with deny rules. Sample feature is supported only with permit rules. Feature is not supported on Qumran platforms.

Examples

```
#configure terminal
(config)#ip access-list ip-acl-01
(config-ip-acl)#default permit-all sample
```

ip access-list icmp

Use this command to permit or deny ICMP packets based on the given source and destination IP address. Even DSCP, precedence and fragment number can be configured to permit or deny with the given values.

Use the no form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Command Syntax

```
(<1-268435453>|)(deny|permit) (icmp) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
  (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any) (administratively-prohibited|
   alternate-address| conversion-error|dod-host-prohibited| dod-net-prohibited| echo|
echo-reply|general-parameter-problem| host-isolated| host-precedence-
unreachable|host-redirect| host-tos-redirect| host-tos-unreachable| host-unknown|host-
unreachable| information-reply| information-request| mask- reply|mask-request| mobile-
redirect| net-redirect| net-tos-redirect|net-tos- unreachable| net-
```

```
  unreachable| network-unknown| no-room-for-option|option-missing| packet-too-big|
  parameter-problem| port-unreachable|precedence-unreachable| protocol-unreachable|
  reassembly-timeout| redirect|router-advertisement| router- solicitation| source-
  quench|source-route-failed|time-exceeded| timestamp-reply| timestamp-request|
  traceroute|ttl-exceeded|unreachable|(<0-255> (<0-255>|))|) ((dscp (<0-63>|af11|
  af12| af13| af21| af22| af23| af31|af32| af33| af41| af42| af43| cs1| cs2| cs3|
  cs4| cs5|cs6| cs7| default| ef ))| (precedence (<0-7>| critical| flash |
  flashoverride|immediate| internet| network| priority| routine))|) (fragments|)
  (log|) (sample|)

no (<1-268435453>|)(deny|permit) (icmp) (A.B.C.D/M|A.B.C.D A.B.C.D|host
  A.B.C.D|any) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any) (administratively-
  prohibited| alternate-address| conversion-error|dod-host-prohibited| dod-net-
  prohibited| echo| echo-reply|general-parameter-problem| host-isolated| host-
  precedence-unreachable|host-redirect| host-tos-redirect| host-tos-unreachable|
  host-unknown|host-unreachable| information-reply| information-request| mask-
  reply|mask-request| mobile-redirect| net-redirect| net-tos-redirect|net-tos-
  unreachable| net-unreachable| network-unknown| no-room-for-option|option-missing|
  packet-too-big| parameter-problem| port-unreachable|precedence-unreachable|
  protocol-unreachable| reassembly-timeout| redirect|router-advertisement| router-
  solicitation| source-quench|source-route-failed|time-exceeded| timestamp-reply|
  timestamp-request| traceroute|ttl-exceeded|unreachable|(<0-255> (<0-255>|))|)
  ("dscp (<0-63>|af11| af12| af13| af21| af22| af23| af31|af32| af33| af41| af42|
  af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7| default| ef ))| (precedence (<0-7>|
  critical| flash | flashoverride|immediate| internet| network| priority|
  routine))|) (fragments|) (log|) (sample|)
```

Parameters

`<1-268435453>` IPv4 ACL sequence number. `deny` Drop the packet. `permit` Accept the packet. `icmp` Internet Control Message Protocol packet. `A.B.C.D/M` Source IP prefix and length.

`A.B.C.D A.B.C.D`

Source IP address and mask. `host A.B.C.D` A single source host IP address. `any` Match any source IP address.

`A.B.C.D/M` Destination IP prefix and length.

`A.B.C.D A.B.C.D`

Destination IP address and mask. `host A.B.C.D` A single destination host IP address. `any` Match any destination IP address.

`administratively-prohibited`

Administratively prohibited.

`alternate-address`

Alternate address.

`conversion-error`

Datagram conversion.

`dod-host-prohibited`

Host prohibited.

`dod-net-prohibited`

Net prohibited. `echo` Echo (ping). `echo-reply` Echo reply. `general-parameter-problem`

Parameter problem. `host-isolated` Host isolated. `host-precedence-unreachable`

Host unreachable for precedence. `host-redirect` Host redirect.

`host-tos-redirect`

Host redirect for ToS.

`host-tos-unreachable`

Host unreachable for ToS. `host-unknown` Host unknown.

`host-unreachable`

Host unreachable.

`information-reply`

Information replies.

`information-request`

Information requests. `mask-reply` Mask replies. `mask-request` Mask requests.

`mobile-redirect`

Mobile host redirect. `net-redirect` Network redirect.

`net-tos-redirect`

Net redirect for ToS.

`net-tos-unreachable`

Network unreachable for ToS.

`net-unreachable`

Net unreachable.

`network-unknown`

Network unknown.

`no-room-for-option`

Parameter required but no room. `option-missing` Parameter required but not present. `packet-too-big` Fragmentation needed and DF set.

`parameter-problem`

All parameter problems.

`port-unreachable`

Port unreachable.

`precedence-unreachable`

Precedence cutoff.

`protocol-unreachable`

Protocol unreachable.

`reassembly-timeout`

Reassembly timeout. `redirect` All redirects. `router-advertisement`

Router discovery advertisements.

`router-solicitation`

Router discovery solicitations. `source-quench` Source quenches.

`source-route-failed`

Source route failed. `time-exceeded` All time-exceeded messages.

`timestamp-reply`

Time-stamp replies.

`timestamp-request`

Time-stamp requests.

`traceroute`	Traceroute.
`ttl-exceeded`	TTL exceeded.
`unreachable`	All unreachables.
`<0-255>`	ICMP type.
`<0-255>`	ICMP code.
`dscp`	Match packets with given DSCP value.
`<0-63>`	Enter DSCP value between 0-63.
`af11`	AF11 DSCP (001010) decimal value 10.
`af12`	AF12 DSCP (001100) decimal value 12.
`af13`	AF13 DSCP (001110) decimal value 14.

af21	AF21 DSCP (010010) decimal value 18.
af22	AF22 DSCP (010100) decimal value
af23	AF23 DSCP (010110) decimal value 22.
af31	AF31 DSCP (011010) decimal value 26.
af32	AF32 DSCP (011100) decimal value 28.
af33	AF33 DSCP (011110) decimal value 30.
af41	AF41 DSCP (100010) decimal value 34
af42	AF42 DSCP (100100) decimal value 36.
af43	AF43 DSCP (100110) decimal value 38.
cs1	CS1 (precedence 1) DSCP (001000) decimal value 8.
cs2	CS2 (precedence 2) DSCP (010000) decimal value 16.
cs3	CS3 (precedence 3) DSCP (011000) decimal value 24.
cs4	CS4 (precedence 4) DSCP (100000) decimal value 32.
cs5	CS5 (precedence 5) DSCP (101000) decimal value 40.
cs6	CS6 (precedence 6) DSCP (110000) decimal value 48.
cs7	CS7 (precedence 7) DSCP (111000) decimal value 56.
default	Default DSCP (000000) decimal value 0.
ef	EF DSCP (101110) decimal value 46.
precedence	Match packets with given precedence value.
<0-7>	Enter precedence value 0-7.
critical	Match packets with critical precedence (5).
flash	Match packets with flash precedence
flashoverride	(3).
	Match packets with flash override precedence (4).
immediate	Match packets with immediate precedence (2).
internet	Match packets with internetwork control precedence (6).
network	Match packets with network control precedence (7).
priority	Match packets with priority precedence (1).
routine	Match packets with routine precedence (0).

`fragments`	Check non-initial fragments.
`log`	Log the packets matching the filter (in-direction only). (Only supported with deny rules)
`sample`	Sample the packets matching the filter (in-direction only). (Only supported with permit rules)

Default

No default value is specified

Command Mode

IP access-list mode

Applicability

This command was introduced before SWMRE version 1.3.

This command is not supported on Qumran platforms.

Examples

```
#configure terminal
(config)#ip access-list ip-icmp
(config-ip-acl)#200 permit icmp any any
```

ip access-list filter

Use this command to configure access control entry in an access control list (ACL).

This determines whether to accept or drop a packet based on the configured match criteria. Use the no form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Command Syntax

```
(<1-268435453>|) (deny|permit) (<0-255>|ahp|any|eigrp|esp|gre|ipip|ipcomp|ipv6ip
  |ospf|pim|rsvp|vrrp) (A.B.C.D/ M|A.B.C.D A.B.C.D|host A.B.C.D|any) (A.B.C.D/
  M|A.B.C.D A.B.C.D|host A.B.C.D|any) (dscp (<0-63>|af11| af12| af13| af21| af22|
  af23| af31|af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7|
  default| ef )|) (flow-label <0-1048575>|) (fragments|) (log|) (sample|)

no (<1-268435453>|)(deny|permit)(<0-255> |ahp | any | eigrp | esp | gre | ipip |
  ipcomp | ipv6ip | ospf | pim | rsvp| vrrp) (A.B.C.D/ M|A.B.C.D A.B.C.D | host
  A.B.C.D|any) (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any) (dscp (<0-63> |af11|
  af12| af13| af21| af22| af23| af31|af32| af33| af41| af42| af43| cs1| cs2| cs3|
  cs4| cs5|cs6| cs7| default| ef )|) (flow-label <0-1048575>|) (fragments|) (log|)
  (sample|)
```

Parameters

`<1-268435453>`	IPv4 ACL sequence number.
`deny`	Drop the packet.
`permit`	Accept the packet.
`<0-255>`	IANA assigned protocol number.
`any`	Any protocol packet.
`ahp`	Authentication Header packet.
`eigrp`	Enhanced Interior Gateway Routing Protocol packet.
`esp`	Encapsulating Security Payload packet.
`gre`	Generic Routing Encapsulation packet.
`ipip`	IPv4 over IPv4 encapsulation packet.
`ipcomp`	IP Payload Compression Protocol packet.
`ipv6ip`	IPv6 over IPv4 encapsulation packet.
`ospf`	Open Shortest Path First packet.
`pim`	Protocol Independent Multicast packet
`rsvp`	Resource Reservation Protocol packet.
`vrrp`	Virtual Router Redundancy Protocol packet.
`A.B.C.D/M`	Source IP prefix and length.
`A.B.C.D A.B.C.D`	Source IP address and mask.
`host A.B.C.D`	A single source host IP address.

any	Match any source IP address.
A.B.C.D/M	Destination IP prefix and length.

A.B.C.D A.B.C.D

Destination IP address and mask.

host A.B.C.D	A single destination host IP address.
any	Any destination address
any	Match any destination IP address.
log	Log the packets matching the filter (in-direction only).
sample	Sample the packets matching the filter (in-direction only).
dscp	Match packets with given DSCP value.
<0-63>	Enter DSCP value between 0-63.
af11	AF11 DSCP (001010) decimal value 10.
af12	AF12 DSCP (001100) decimal value 12.
af13	AF13 DSCP (001110) decimal value 14.
af21	AF21 DSCP (010010) decimal value 18.
af22	AF22 DSCP (010100) decimal value
af23	AF23 DSCP (010110) decimal value 22.
af31	AF31 DSCP (011010) decimal value 26.
af32	AF32 DSCP (011100) decimal value 28.
af33	AF33 DSCP (011110) decimal value 30.
af41	AF41 DSCP (100010) decimal value 34
af42	AF42 DSCP (100100) decimal value 36.
af43	AF43 DSCP (100110) decimal value 38.
cs1	CS1 (precedence 1) DSCP (001000) decimal value 8.
cs2	CS2 (precedence 2) DSCP (010000) decimal value 16.
cs3	CS3 (precedence 3) DSCP (011000) decimal value 24.
cs4	CS4 (precedence 4) DSCP (100000) decimal value 32.
cs5	CS5 (precedence 5) DSCP (101000) decimal value 40.
cs6	CS6 (precedence 6) DSCP (110000) decimal value 48.
cs7	CS7 (precedence 7) DSCP (111000) decimal value 56.
default	Default DSCP (000000) decimal value 0.
ef	EF DSCP (101110) decimal value 46.
precedence	Match packets with given precedence value.
<0-7>	Enter precedence value 0-7.
critical	Match packets with critical precedence (5).

`flash` Match packets with flash precedence (3).
`flashoverride`

Match packets with flash override precedence (4).

`immediate` Match packets with immediate precedence (2).

`internet`	Match packets with internetwork control precedence (6).
`network`	Match packets with network control precedence (7).
`priority`	Match packets with priority precedence (1).
`routine`	Match packets with routine precedence (0).
`fragments`	Check non-initial fragments.
`log`	Log the packets matching the filter (in-direction only).
`sample`	Sample the packets matching the filter (in-direction only).

Default

No default value is specified

Command Mode

IP access-list mode

Applicability

This command was introduced before SWMRE version 1.3.

Log feature is supported only with deny rules. Sample feature is supported only with permit rules. Feature is not supported on Qumran platforms.

Examples

```
#configure terminal
(config)#ip access-list ip-acl-01
(config-ip-acl)#11 permit any 30.0.0.1 0.0.0.255 172.124.0.2 0.0.0.255
(config-ip-acl)#no 11
```

ip access-list fragments

Use this command to configure access list to deny or permit all the IP fragmented.

Use the `no` form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Command Syntax

`(<1-268435453>|) fragments (deny-all|permit-all) (log|) (sample|) no (<1-268435453>|) fragments (deny-all|permit-all) (log|) (sample|)` **Parameters**

`deny-all`	Drop the packet.
`permit-all`	Accept the packet.
`<1-268435453>`	IPv4 ACL sequence number.

`fragments`	Check non-initial.
`log`	Log the packets matching the filter (in-direction only.
`Sample`	Sample the packets matching the filter (in-direction only.

Default

No default value is specified

Command Mode

IP access-list mode

Applicability

This command was introduced before SWMRE version 1.3.

Log feature is supported only with deny rules. Sample feature is supported only with permit rules. Feature is not supported on Qumran platforms.

Examples

```
#configure terminal
(config)#ip access-list mylist
(config-ip-acl)#fragments deny-all
(config-ip-acl)#end
```

ip access-list remark

Use this command to add a description to a named IPv4 access control list (ACL).

Use the `no` form of this command to remove an ACL description.

Command Syntax `remark LINE no remark`

Parameters

`LINE`	ACL description up to 100 characters.

Default

No default value is specified

Command Mode

IP access-list mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip access-list mylist (config-ip-acl)#remark
permit the inside admin address (config-ip-acl)#exit


(config)#ip access-list mylist
```

```
(config-ip-acl)#no remark
(config-ip-acl)#exit
```

ip access-list resequence

Use this command to re-sequence the IP access list.

Note: Use a non-overlapping sequence space for new sequence number sets to avoid possible unexpected rule matches during transition.

Note: Re-sequencing an ACL attached to a management interface clears the ACL counters associated to it.

Command Syntax `resequence <1-268435453> INCREMENT`

Parameters

`<1-268435453>` Starting sequence number.

`INCREMENT` Sequence number increment steps.

Default

None

Command Mode

IP access-list mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip access-list mylist (config-ip-acl)#resequence 5 5
(config-ip-acl)#end
```

ip access-list tcp|udp

Use this command to define a named access control list (ACL) that determines whether to accept or drop an incoming packet based on the criteria that you specify.

This form of this command filters packets based on source and destination IP address along with protocol (TCP or UDP) and port.

This command has these main parts:

- The source that you can specify as a prefix and length, an address and mask, a host address, or `any`. Optionally, you can specify a port.
- The destination that you specify the same as the source.

An ACL is made up of one or more ACL specifications. You can repeat this command and add multiple specifications. Each time you give this command, the specification is added to the end of the list.

Each packet that arrives at the device is compared to each specification in each ACL in the order that they are defined. The device continues to look until it has a match. If no match is found and the device reaches the end of the list, the

packet is denied. For this reason, place the most frequently occurring specifications at the top of the list. The device stops checking the specifications after a match occurs.

There is an implied `deny` specification for traffic that is not permitted. A single-entry ACL with only one `deny` specification is the same as denying all traffic. You must have at least one `permit` specification in an ACL or all traffic is blocked.

Use the `no` form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Command Syntax

```
(<1-268435453>|) (deny|permit) tcp (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
 ((eq|gt|lt|neq) (<0-65535>|bgp|chargen|cmd|daytime|discard|domain|drip|echo
 |exec|finger|ftp |ftp- data|gopher|hostname|ident|irc|klogin|kshell|login
 |lpd|nntp|pim-auto- rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet|time|
 uucp|whois|www)| range <0-65535> <0-65535>|) (A.B.C.D/M|A.B.C.D A.B.C.D|host
 A.B.C.D|any) ((eq|gt|lt|neq) (<0-65535>|bgp|chargen|cmd|daytime|discard|domain|
 drip|echo|exec|finger|ftp|ftp-data|gopher|hostname|ident|irc|klogin|kshell|login
 |lpd|nntp|pim-auto- rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet
 |time|uucp|whois|www) | range <0-65535> <0-65535>|) ((dscp (<0-63>| af11| af12|
 af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4|
 cs5| cs6| cs7| default| ef)) |(precedence (<0-7>| critical| flash | flashoverride|
 immediate| internet| network| priority| routine)) |)
 ({ack|established|fin|psh|rst|syn|urg}|) (log|) (sample|)

(<1-268435453>|) (deny|permit) udp (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
 ((eq|gt|lt|neq)                (<0-65535>|biff|bootpc|bootps|discard|dnsix|domain|
 echo|isakmp|mobile-ip  |nameserver  |  netbios-dgm  |  netbios-ns|  netbios-
 ss|non500isakmp                          |ntp                          |pim-auto-
 rp|rip|snmp|snmptrap|sunrpc|syslog|tacacs|talk|tftp |time|who|xdmcp) | range <0-
 65535>  <0-65535>|)  (A.B.C.D/M|A.B.C.D  A.B.C.D|host  A.B.C.D|any)  ((eq|gt
 |lt|neq)(<0-65535>  |biff  |bootpc  |bootps|  discard|  dnsix|  domain|  echo|
 isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|netbiosss|non500-isakmp
 |ntp|pim-auto- rp| rip| snmp| snmptrap| sunrpc| syslog| tacacs| talk| tftp| time|
 who| xdmcp) | range <0-65535> <0-65535>|) ((dscp (<0-63>| af11| af12| af13| af21|
 af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7|
 default| ef)) | (precedence (<0-7>| critical| flash | flashoverride| immediate|
 internet| network| priority| routine))|) (log|)
 (sample|) no (<1-268435453>|) (deny|permit) tcp (A.B.C.D/M|A.B.C.D
A.B.C.D|host
 A.B.C.D|any)((eq|gt|lt|neq) (<0-65535>| bgp| chargen| cmd| daytime| discard|
 domain| drip| echo|exec|finger|ftp |ftp- data |gopher |hostname| ident| irc|
 klogin| kshell|login|lpd|nntp|pim-auto- rp |pop2 |pop3 |smtp| ssh| sunrpc| tacacs
 |talk|telnet|time|uucp|whois|www)  |  range  <0-65535>  <0-65535>|)  (A.B.C.D/
 M|A.B.C.D A.B.C.D|host A.B.C.D|any)((eq|gt|lt|neq) (<0-65535> |bgp |chargen |cmd
 |daytime|discard|domain|drip|echo|exec|finger|ftp|ftp-data|  gopher|  hostname|
 ident| irc| klogin| kshell| login| lpd| nntp| pim-auto-rp | pop2| pop3| smtp |ssh
 |sunrpc|tacacs|talk|telnet|time|uucp|whois|www)  |  range  <0-65535>  <0-65535>|)
 ((dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42|
 af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef)) | (precedence (<0-7>|
 critical| flash | flashoverride| immediate| internet| network| priority|
 routine)) |) ({ack|established|fin|psh|rst|syn|urg}|) (log|) (sample|)
```

```
no (<1-268435453>|)(deny|permit) udp (A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D|any)
  ((eq|gt|lt|neq) (<0-65535> |biff| bootpc| bootps| discard| dnsix| domain| echo|
  isakmp|mobile-ip|nameserver|netbios-dgm|netbios-ns|netbios-ss|non500-isakmp|
  ntp|pim-auto- rp|rip|snmp|snmptrap|sunrpc|syslog|tacacs|talk|tftp|time|who|xdmcp)
  | range <0-65535> <0-65535>|)(A.B.C.D/M|A.B.C.D A.B.C.D|host A.B.C.D| any)
  ((eq|gt|lt|neq) (<0-65535> |biff| bootpc| bootps| discard| dnsix| domain|echo|
  isakmp|mobile-       ip|nameserver|netbios-dgm|netbios-ns|netbios-ss|non500-isakmp|
  ntp|pim-auto-  rp|rip|snmp|snmptrap|sunrpc|syslog|tacacs|talk|tftp|time|who|xdmcp)
  | range <0-65535> <0-65535>|) ((dscp (<0-63>| af11| af12| af13| af21| af22| af23|
  af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default|
  ef)) | (precedence (<0-7>| critical| flash | flashoverride| immediate| internet|
  network| priority| routine)) |) (log|) (sample|)
```

Parameters

`<1-268435453>` IPv4 ACL sequence number.

`deny` Drop the packet. `permit` Accept the packet.

`tcp` Transmission Control Protocol. `udp` User Datagram Protocol.

`A.B.C.D/M` Source or destination IP prefix and length.

`A.B.C.D A.B.C.D` Source or destination IP address and mask.

`host A.B.C.D` Source or destination host IP address.

`any` Any source or destination IP address.

`eq` Source or destination port equal to.

`gt` Source or destination port greater than.

`lt` Source or destination port less than.

`neq` Source or destination port not equal to.

`<0-65535>` Source or destination port number.

`range` Range of source or destination port numbers:

`<0-65535>` Lowest value in the range. `<0-65535>` Highest value in the range. `bgp` Border Gateway Protocol. `chargen` Character generator. `cmd` Remote commands. `daytime` Daytime. `discard` Discard. `domain` Domain Name Service. `drip` Dynamic Routing Information Protocol.

`echo` Echo.

`exec` EXEC.

finger	Finger.
ftp	File Transfer Protocol.
ftp-data	FTP data connections.
gopher	Gopher.
hostname	NIC hostname server.
ident	Ident Protocol.
irc	Internet Relay Chat.
klogin	Kerberos login.
kshell	Kerberos shell.
login	Login.
lpd	Printer service.
nntp	Network News Transport Protocol.
pim-auto-rp	PIM Auto-RP.
pop2	Post Office Protocol v2.
pop3	Post Office Protocol v3.
smtp	Simple Mail Transport Protocol.
ssh	Secure Shell.
sunrpc	Sun Remote Procedure Call.
tacacs	TAC Access Control System.
talk	Talk.
telnet	Telnet.
time	Time.
uucp	UNIX-to-UNIX Copy Program.
whois	WHOIS/NICNAME
www	World Wide Web.
nntp	Range of source or destination port numbers:
dscp	Match packets with given DSCP value.
<0-63>	Enter DSCP value between 0-63.
af11	AF11 DSCP (001010) decimal value 10.
af12	AF12 DSCP (001100) decimal value 12.
af13	AF13 DSCP (001110) decimal value 14.
af21	AF21 DSCP (010010) decimal value 18.
af22	AF22 DSCP (010100) decimal value
af23	AF23 DSCP (010110) decimal value 22.
af31	AF31 DSCP (011010) decimal value 26.
af32	AF32 DSCP (011100) decimal value 28.
af33	AF33 DSCP (011110) decimal value 30.
af41	AF41 DSCP (100010) decimal value 34

af42	AF42 DSCP (100100) decimal value 36.
af43	AF43 DSCP (100110) decimal value 38.
cs1	CS1 (precedence 1) DSCP (001000) decimal value 8.
cs2	CS2 (precedence 2) DSCP (010000) decimal value 16.
cs3	CS3 (precedence 3) DSCP (011000) decimal value 24.
cs4	CS4 (precedence 4) DSCP (100000) decimal value 32.
cs5	CS5 (precedence 5) DSCP (101000) decimal value 40.
cs6	CS6 (precedence 6) DSCP (110000) decimal value 48.
cs7	CS7 (precedence 7) DSCP (111000) decimal value 56.
default	Default DSCP (000000) decimal value 0.
ef	EF DSCP (101110) decimal value 46.
precedence	Match packets with given precedence value.
<0-7>	Enter precedence value 0-7.
critical	Match packets with critical precedence (5).
flash	Match packets with flash precedence (3).
flashoverride	Match packets with flash override precedence (4).
immediate	Match packets with immediate precedence (2).
internet	Match packets with internetwork control precedence (6).
network	Match packets with network control precedence (7).
priority	Match packets with priority precedence (1).
routine	Match packets with routine precedence (0).
ack	Match on the Acknowledgment (ack) bit.
established	Matches only packets that belong to an established TCP connection.
fin	Match on the Finish (fin) bit.
psh	Match on the Push (psh) bit.
rst	Match on the Reset (rst) bit.
syn	Match on the Synchronize (syn) bit.
urg	Match on the Urgent (urg) bit.
biff	Biff.
bootpc	Bootstrap Protocol (BOOTP) client.
bootps	Bootstrap Protocol (BOOTP) server.
discard	Discard.
dnsix	DNSIX security protocol auditing.
domain	Domain Name Service.
echo	Echo.
isakmp	Internet Security Association and Key Management Protocol.

mobile-ip	Mobile IP registration.
nameserver	IEN116 name service.
netbios-dgm	Net BIOS datagram service.
netbios-ns	Net BIOS name service.
netbios-ss	Net BIOS session service.
non500-isakmp	Non500-Internet Security Association and Key Management Protocol.
ntp	Network Time Protocol.
pim-auto-rp	PIM Auto-RP.
rip	Routing Information Protocol.
snmp	Simple Network Management Protocol.
snmptrap	SNMP Traps.
sunrpc	Sun Remote Procedure Call.
syslog	System Logger.
tacacs	TAC Access Control System.
talk	Talk.
tftp	Trivial File Transfer Protocol.
time	Time.
who	Who service.
xdmcp	X Display Manager Control Protocol.
Log	Log the packets matching the filter (in-direction only.
Sample	Sample the packets matching the filter (in-direction only.

Default

No default value is specified

Command Mode

IP access-list mode

Applicability

This command was introduced before SWMRE version 1.3.

Log feature is supported only with deny rules. Sample feature is supported only with permit rules. Feature is not supported on Qumran platforms.

Examples

```
#configure terminal
(config)#ip access-list ip-acl-02
(config-ip-acl)#deny udp any any eq tftp
(config-ip-acl)#deny tcp any any eq ssh
(config-ip-acl)#end
```

ip access-list WORD

Use this command to define a named access control list (ACL) that determines whether to accept or drop an incoming packet based on the source IP address, either an exact match or a range of prefixes.

An ACL is made up of one or more ACL specifications. You can repeat this command and add multiple specifications. Each time you give this command, the specification is added to the end of the list.

Each packet that arrives at the device is compared to each specification in each ACL in the order that they are defined. The device continues to look until it has a match. If no match is found and the device reaches the end of the list, the packet is denied. For this reason, place the most frequently occurring specifications at the top of the list.

The device stops checking the specifications after a match occurs.

There is an implied `deny` specification for traffic that is not permitted. A single-entry ACL with only one `deny` specification is the same as denying all traffic. You must have at least one `permit` specification in an ACL or all traffic is blocked.

Use the `no` form of this command to remove an ACL specification.

Command Syntax `ip access-list WORD no ip access-list WORD`

Parameters

`WORD`	Access-list name.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip access-list ip-acl-01
```

ipv6 access-list default

Use this command to modify the default rule action of access-list. Default rule is applicable only when access-list is attached to interface. Default rule will have the lowest priority and only the packets not matching any of the user defined rules match default rule.

Command Syntax `default (deny-all|permit-all) (log|) (sample|)`

Parameters

`deny-all`	Drop all packets.

permit-all	Accept all packets.
log	Log the packets matching the filter (in-direction only).
Sample	Sample the packets matching the filter (in-direction only).

Default

No default value is specified

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before SWMRE version 1.3.

Log feature is supported only with deny rules. Sample feature is supported only with permit rules. Feature is not supported on Qumran platforms.

Examples

```
#configure terminal
(config)#ip access-list ipv6-acl-01
(config-ipv6-acl)#default permit-all sample
```

ipv6 access-list filter

Use this command to define an access-control entry in an access control list (ACL) that determines whether to accept or drop a packet based on the criteria specified. This form of this command filters packets based on:

- Protocol
- Source IP address
- Destination IP address

Use the no form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Command Syntax

```
(<1-268435453>|) (deny|permit)(<0-255>|ahp|any|eigrp|esp|gre|ipipv6|ipcomp
  |ipv6ipv6|ospf|pim|rsvp|vrrp) (X:X::X:X/ M|X:X::X:X X:X::X:X|host X:X::X:X|any)
  (X:X::X:X/M|X:X::X:X X:X::X:X|host X:X::X:X|any) (dscp (<0-63>|af11| af12| af13|
  af21| af22| af23| af31|af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6|
  cs7| default| ef )|) (flow-label<0-1048575>|) (fragments|) (log|) (sample|)

no (<1-268435453>|)(deny|permit)(<0-255>|ahp|any|eigrp|esp|gre|ipipv6|ipcomp
  |ipv6ipv6|ospf|pim|rsvp|vrrp) (X:X::X:X/ M|X:X::X:X X:X::X:X|host X:X::X:X|any)
  (X:X::X:X/M|X:X::X:X X:X::X:X|host X:X::X:X|any) (dscp (<0-63>|af11| af12| af13|
  af21| af22| af23| af31|af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6|
  cs7| default| ef )|) (flow-label<0-1048575>|) (fragments|) (log|) (sample|)
```

Parameters

<1-268435453>	IPv4 ACL sequence number.
deny	Drop the packet.

permit Accept the packet.
<0-255> IANA assigned protocol number.
any Any protocol packet.
ahp Authentication Header packet.
eigrp Enhanced Interior Gateway Routing Protocol packet.
esp Encapsulating Security Payload packet.
gre Generic Routing Encapsulation packet.
ipipv6 IPv4 over IPv6 Encapsulation packet.
ipcomp IP Payload Compression Protocol packet.
ipv6ipv6 IPv6 over IPv6 Encapsulation packet.
ospf Open Shortest Path First packet.
pim Protocol Independent Multicast packet
rsvp Resource Reservation Protocol packet. v
rrp Virtual Router Redundancy Protocol packet.
X:X::X:X/M Source Address with network mask length.
X:X::X:X X:X::X:X
Source Address with wild card mask.
host X:X::X:X Source Address's wild card mask (ignored bits). any Any source address.
X:X::X:X/M Destination address with network mask length.
X:X::X:X X:X::X:X
Destination address with wild card mask.
host X:X::X:X Destination address's wild card mask (ignored bits).
any Any destination address any Match any destination IP address. log Log the packets matching the filter (in-direction only). sample Sample the packets matching the filter (in-direction only).
dscp Match packets with given DSCP value.
<0-63> Enter DSCP value between 0-63. af11 AF11 DSCP (001010) decimal value 10. af12 AF12 DSCP (001100) decimal value 12. af13 AF13 DSCP (001110) decimal value 14. af21 AF21 DSCP (010010) decimal value 18. af22 AF22 DSCP (010100) decimal value af23 AF23 DSCP (010110) decimal value 22. af31 AF31 DSCP (011010) decimal value 26. af32 AF32 DSCP (011100) decimal value 28. af33 AF33 DSCP (011110) decimal value 30. af41 AF41 DSCP (100010) decimal value 34 af42 AF42 DSCP (100100) decimal value 36. af43 AF43 DSCP (100110) decimal value 38. cs1 CS1 (precedence 1) DSCP (001000) decimal value 8. cs2 CS2 (precedence 2) DSCP (010000) decimal value 16. cs3 CS3 (precedence 3) DSCP (011000) decimal value 24. cs4 CS4 (precedence 4) DSCP (100000) decimal value 32. cs5 CS5 (precedence 5) DSCP (101000) decimal value 40. cs6 CS6 (precedence 6) DSCP (110000) decimal value 48. cs7 CS7 (precedence 7) DSCP (111000) decimal value 56. default Default DSCP (000000) decimal value 0. ef EF DSCP (101110) decimal value 46.

Default

No default value is specified

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before SWMRE version 1.3.

Log feature is supported only with deny rules. Sample feature is supported only with permit rules. Feature is not supported on Qumran platforms.

Examples

```
#configure terminal
(config)#ipv6 access-list ipv6-acl-01
(config-ip-acl)#permit ipipv6 any any
(config-ip-acl)#end
```

ipv6 access-list fragments

Use this command to permit or deny all the IPv6 fragments.

Use the no form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Command Syntax

```
    (<1-268435453>|) fragments (deny-all|permit-all) (log|) (sample|) no (<1-
268435453>|) fragments (deny-all|permit-all) (log|) (sample|)
```

Parameters

`<1-268435453>`	IPv6 ACL sequence number.
`fragments`	Check non-initial fragments.
`deny-all`	Specify packets to reject.
`permit-all`	Specify packets to forward.
`log`	Log the packets matching the filter (in-direction only).
`sample`	Sample the packets matching the filter (in-direction only).

Default

No default value is specified

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before SWMRE version 1.3.

Log feature is supported only with deny rules. Sample feature is supported only with permit rules. Feature is not supported on Qumran platforms.

Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)#fragments deny-all
```

ipv6 access-group

Use this command to attach an IPv6 access list to an interface to filter incoming or outgoing packets.

When you attach an access list to a VLAN interface or LAG interface as well as to a physical interface that is a member of that LAG and/or VLAN interface, the priority order is:

1. VLAN interface
2. LAG interface
3. Physical interface

For example, if you attach access lists to both a LAG interface and a physical interface that is a member of that LAG, matching traffic rules are applied to the LAG interface, but not to the physical interface.

Use the `no` parameter with this command to detach an IPv6 access list.

Command Syntax `ipv6 access-group WORD (in|out) no ipv6 access-group WORD (in|out)`

Parameters

`WORD`	Access list name.
`in`	Filter incoming packets.
`out`	Filter outgoing packets (not supported on Qumran platform).

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)#permit ipv6 any any
(config-ipv6-acl)#exit

(config)#interface eth3
(config-if)#ipv6 access-group mylist in

(config)#interface eth3
(config-if)#no ipv6 access-group mylist in
```

ipv6 access-list icmpv6

Use this command to permit or deny packets with the given source and destination IPv6 address, DSCP value, fragments and flow label.

Use the no form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Command Syntax

```
(<1-268435453>|)(deny|permit) (icmpv6) (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  (X:X::X:X/ M|X:X::X:X X:X::X:X|any) (beyond-scope| destination-unreachable| echo-
  reply| echo-request| header| hop-limit| mld-query| mld-reduction| mld-report| nd-
  na| nd-ns| nextheader| no-admin| no-route| packet-too-big| parameter-option|
  parameter-problem| portunreachable| reassembly-timeout| redirect| renum-command|
  renum-result| renum-seq-number| router-advertisement| router-renumbering| router-
  solicitation| time-exceeded| unreachable | (<0-255> (<0-255>|)|)) (dscp (<0-
```

63>|af11| af12| af13| af21| af22| af23| af31|af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7| default| ef)|) (flowlabel <0-1048575>|) (fragments|) (log|) (sample|)

no (<1-268435453>|)(deny|permit) (icmpv6) (X:X::X:X/M|X:X::X:X X:X::X:X|any) (X:X::X:X/M|X:X::X:X X:X::X:X|any) (beyond-scope| destination-unreachable| echo-reply| echo-request| header| hop-limit| mld-query| mld-reduction| mld-report| nd-na| nd-ns| nextheader| no-admin| no-route| packet-too-big| parameter-option| parameter-problem| portunreachable| reassembly-timeout| redirect| renum-command| renum-result| renum-seq-number| router-advertisement| router-renumbering| router-solicitation| time-exceeded| unreachable | (<0-255> (<0-255>|)|)) (dscp (<0-63>|af11| af12| af13| af21| af22| af23| af31|af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5|cs6| cs7| default| ef)|) (flowlabel <0-1048575>|) (fragments|) (log|) (sample|)

Parameters

<1-268435453> IPv6 ACL sequence number. deny Drop the packet. permit Accept the packet. icmpv6 Internet Control Message Protocol packet. X:X::X:X/M Source Address with network mask length.

X:X::X:X X:X::X:X

Source Address with wild card mask.

host X:X::X:X Source Address's wild card mask (ignored bits).

any Any source address.

X:X::X:X/M Destination address with network mask length.

X:X::X:X X:X::X:X

Destination address with wild card mask.

host X:X::X:X Destination address's wild card mask (ignored bits).

any Any destination address

beyond-scope Destination beyond scope

destination-unreachable Destination address is unreachable

echo-reply Echo reply

echo-request Echo request (ping) Parameter header

header hop-limit problems Hop limit exceeded in transit

mld-query Multicast Listener Discovery Query Multicast

mld-reduction Listener Discovery Reduction Multicast

mld-report Listener Discovery Report Neighbor

nd-na discovery neighbor advertisements Neighbor

nd-ns discovery neighbor solicitations Parameter

next-header problems Administration

no-admin prohibited destination

no-route No route to destination
packet-too-big Packet too big parameter-option
Parameter option problems
parameter-problem
All parameter problems
port-unreachable
Port unreachable
reassembly-timeout
Reassembly timeout
redirect Neighbor redirect renum-command Router renumbering command renum-
result Router renumbering result renum-seq-
number Router renumbering sequence number reset
router-advertisement
Neighbor discovery router advertisements
router-renumbering
All router renumbering
router-solicitation
Neighbor discovery router solicitations
time-exceeded All time exceeded messages unreachable All unreachable
<0-255> ICMPv6 message type <0-255> ICMPv6 message code dscp Match packets with given DSCP value.

<0-63>	Enter DSCP value between 0-63.
af11	AF11 DSCP (001010) decimal value 10.
af12	AF12 DSCP (001100) decimal value 12.
af13	AF13 DSCP (001110) decimal value 14.
af21	AF21 DSCP (010010) decimal value 18.
af22	AF22 DSCP (010100) decimal value
af23	AF23 DSCP (010110) decimal value 22.
af31	AF31 DSCP (011010) decimal value 26.
af32	AF32 DSCP (011100) decimal value 28.
af33	AF33 DSCP (011110) decimal value 30.
af41	AF41 DSCP (100010) decimal value 34
af42	AF42 DSCP (100100) decimal value 36.
af43	AF43 DSCP (100110) decimal value 38.
cs1	CS1 (precedence 1) DSCP (001000) decimal value 8.
cs2	CS2 (precedence 2) DSCP (010000) decimal value 16.
cs3	CS3 (precedence 3) DSCP (011000) decimal value 24.
cs4	CS4 (precedence 4) DSCP (100000) decimal value 32.

cs5	CS5 (precedence 5) DSCP (101000) decimal value 40.
cs6	CS6 (precedence 6) DSCP (110000) decimal value 48.
cs7	CS7 (precedence 7) DSCP (111000) decimal value 56.
default	Default DSCP (000000) decimal value 0.
ef	EF DSCP (101110) decimal value 46.
flow-label	IPv6 Flow-label.
<0-1048575>	IPv6 Flow-label value.
fragments	Check non-initial fragments.
log	Log the packets matching the filter (in-direction only).
sample	Sample the packets matching the filter (in-direction only).

Default

No default value is specified

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before SWMRE version 1.3.

Log feature is supported only with deny rules. Sample feature is supported only with permit rules. Feature is not supported on Qumran platforms.

Examples

```
    #configure terminal
    (config)#ipv6 access-list mylist
(config-ipv6-acl)#200 permit icmpv6 any any fragments
```

ipv6 access-list remark

Use this command to add a description to an IPv6 access control list (ACL). Use the `no` form of this command to remove an access control list description.

Command Syntax `remark LINE no remark`

Parameters

`LINE`	ACL description up to 100 characters.

Default

No default value is specified

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)# remark Permit the inside admin address
```

ipv6 access-list resequence

Use this command to re-sequence the IPv6 access list.

Note: Use a non-overlapping sequence space for new sequence number sets to avoid possible unexpected rule matches during transition.

Note: Re-sequencing an ACL attached to a management interface clears the ACL counters associated to it.

Command Syntax `resequence <1-268435453> INCREMENT`

Parameters

`<1-268435453>`	Starting Sequence number.
`INCREMENT`	Sequence number increment steps.

Default

No default value is specified

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)#resequence 15 15
```

ipv6 access-list sctp

Use this command to allow ACL to permit or deny SCTP packets based on the given source and destination IPV6 address. Even DSCP, flow label and fragment can be configured to permit or deny with the given values.

Use the `no` form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Command Syntax

```
(<1-268435453>|) (deny|permit) (sctp) (X:X::X:X/M|X:X::X:X X:X::X:X|any) (X:X::X:X/
  M|X:X::X:X X:X::X:X|any) {(eq|gt|lt|neq) (<0-65535>) | (range <0-65535> <065535>)|
  (fragments)| } (dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31| af32|
  af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef)|)
  ((flow-label   <0-1048575>)|)   (log|)   (sample|)   no   (<1-268435453>|)

(deny|permit) (sctp) (X:X::X:X/M|X:X::X:X X:X::X:X|any)

  (X:X::X:X/M|X:X::X:X X:X::X:X|any) {(eq|gt|lt|neq) (<0-65535>) | (range <0-65535>
  <0-65535>)| (fragments)| } (dscp (<0-63>| af11| af12| af13| af21| af22| af23|
  af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default|
  ef)|) ((flow-label <0-1048575>)|) (log|) (sample|)
```

Parameters

`<1-268435453>`	IPv6 ACL sequence number.
`deny`	Drop the packet.
`permit`	Accept the packet.
`sctp`	Stream Control Transmission Protocol packet.
`X:X::X:X/M`	Source address with network mask length.
`X:X::X:X`	Source address with wild card mask.
`X:X::X:X`	Source address's wild card mask (ignored bits).
`any`	Any source address.
`X:X::X:X/M`	Destination address with network mask length.
`X:X::X:X`	Destination address with wild card mask.
`X:X::X:X`	Destination address's wild card mask (ignored bits).
`any`	Any destination address.
`eq`	Source or destination port equal to.
`gt`	Source or destination port greater than.

lt	Source or destination port less than.
neq	Source or destination port not equal to.
<0-65535>	Source or destination port number.
range	Range of source or destination port numbers:
<0-65535>	Lowest value in the range.
<0-65535>	Highest value in the range.
dscp	Match packets with given DSCP value.
<0-63>	Enter DSCP value between 0-63.
af11	AF11 DSCP (001010) decimal value 10.
af12	AF12 DSCP (001100) decimal value 12.
af13	AF13 DSCP (001110) decimal value 14.
af21	AF21 DSCP (010010) decimal value 18.
af22	AF22 DSCP (010100) decimal value
af23	AF23 DSCP (010110) decimal value 22.
af31	AF31 DSCP (011010) decimal value 26.
af32	AF32 DSCP (011100) decimal value 28.
af33	AF33 DSCP (011110) decimal value 30.
af41	AF41 DSCP (100010) decimal value 34
af42	AF42 DSCP (100100) decimal value 36.
af43	AF43 DSCP (100110) decimal value 38.
cs1	CS1 (precedence 1) DSCP (001000) decimal value 8.
cs2	CS2 (precedence 2) DSCP (010000) decimal value 16.
cs3	CS3 (precedence 3) DSCP (011000) decimal value 24.
cs4	CS4 (precedence 4) DSCP (100000) decimal value 32.
cs5	CS5 (precedence 5) DSCP (101000) decimal value 40.
cs6	CS6 (precedence 6) DSCP (110000) decimal value 48.
cs7	CS7 (precedence 7) DSCP (111000) decimal value 56.
default	Default DSCP (000000) decimal value 0.
ef	EF DSCP (101110) decimal value 46.
flow-label	IPv6 Flow-label.
<0-1048575>	IPv6 Flow-label value.
fragments	Check non-initial fragments.
log	Log the packets matching the filter (in-direction only).
sample	Sample the packets matching the filter (in-direction only).

Default

No default value is specified

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before SWMRE version 1.3.

Log feature is supported only with deny rules. Sample feature is supported only with permit rules. Feature is not supported on Qumran platforms.

Examples

```
    #configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)#200 permit sctp any any fragments
```

ipv6 access-list tcp|udp

Use this command to define a named access control list (ACL) that determines whether to accept or drop an incoming packet based on the criteria that you specify. This form of this command filters packets based on source and destination IP address along with protocol (TCP or UDP) and port.

This command has these main parts:

- The source which you can specify as a prefix and length, an address and mask, a host address, or `any`. Optionally, you can specify a port.
- The destination which you specify the same as the source.

An ACL is made up of one or more ACL specifications. You can repeat this command and add multiple specifications. Each time you give this command, the specification is added to the end of the list.

Each packet that arrives at the device is compared to each specification in each ACL in the order that they are defined. The device continues to look until it has a match. If no match is found and the device reaches the end of the list, the packet is denied. For this reason, place the most frequently occurring specifications at the top of the list.

The device stops checking the specifications after a match occurs.

There is an implied `deny` specification for traffic that is not permitted. A single-entry ACL with only one `deny` specification is the same as denying all traffic. You must have at least one `permit` specification in an ACL or all traffic is blocked.

Use the `no` form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Command Syntax

```
(<1-268435453>|) (deny|permit) tcp (X:X::X:X/M|X:X::X:X X:X::X:X|any)
  ((eq|gt|lt|neq) <0-65535> |bgp|chargen|cmd|daytime|discard|domain|drip
  |echo|exec|finger|ftp |ftp- data|gopher|hostname|ident|irc|klogin|kshell
  |login|lpd|nntp|pim-auto- rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet
  |time|uucp|whois|www) | range <0-65535> <0-65535>|) | range <0-65535> <0-
  65535>|)(X:X::X:X/M|X:X::X:X      X:X::X:X|any)      ((eq|gt|lt|neq)      <0-65535>
  |bgp|chargen|cmd|daytime|discard|domain|drip|echo|exec|finger|ftp            |ftp-
  data|gopher|hostname|ident|irc|klogin|kshell|login|lpd|nntp|pim-auto-
  rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet|time|uucp|whois|www)     |     range
  <065535> <0-65535>|) | range <0-65535> <0-65535>|) ((dscp (<0-63>| af11| af12|
  af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4|
  cs5| cs6| cs7| default| ef)) | (precedence (<0-7>| critical| flash | flash-
  override| immediate| internet| network| priority| routine)) |)
  ({ack|established|fin|psh|rst|syn|urg}|) (<1-268435453>|) (deny|permit) udp
  (X:X::X:X/M|X:X::X:X X:X::X:X|any) ((eq|gt|lt|neq) <0-
  65535>|bgp|chargen|cmd|daytime|discard|domain|drip|echo|exec|finger|ftp|ftp-
  data|gopher|hostname|ident|irc|klogin|kshell|login|lpd|nntp|pim-auto-
  rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet|time|uucp|whois|www) | range <0-
  65535> <0-65535>|) | range <0-65535> (log|) (sample|)
<0-65535>|)(X:X::X:X/M|X:X::X:X      X:X::X:X|any)      ((eq|gt|lt|neq)      <0-65535>
  |bgp|chargen|cmd|daytime|discard|domain|drip|echo|exec|finger|ftp |ftp-
  data|gopher|hostname|ident|irc|klogin|kshell|login|lpd|nntp|pim-auto-
  rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet|time|uucp|whois|www) | range <065535>
  <0-65535>|) | range <0-65535> <0-65535>|) ((dscp (<0-63>| af11| af12| af13|
```

af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef)) | (precedence (<0-7>| critical| flash | flash- override| immediate| internet| network| priority| routine)) |)
({ack|established|fin|psh|rst|syn|urg}|) (log|) (sample|) no (<1-268435453>|) (deny|permit) tcp (X:X::X:X/M|X:X::X:X X:X::X:X|any)

((eq|gt|lt|neq) <0-65535> |bgp|chargen|cmd|daytime|discard|domain|drip |echo|exec|finger|ftp |ftp- data|gopher|hostname|ident|irc|klogin|kshell |login|lpd|nntp|pim-auto- rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet |time|uucp|whois|www) | range <0-65535> <0-65535>|) | range <0-65535> <0-65535>|)(X:X::X:X/M|X:X::X:X X:X::X:X|any) ((eq|gt|lt|neq) <0-65535> |bgp|chargen|cmd|daytime|discard|domain|drip|echo|exec|finger|ftp |ftp-data|gopher|hostname|ident|irc|klogin|kshell|login|lpd|nntp|pim-auto-rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet|time|uucp|whois|www) | range <0-65535> <0-65535>|) | range <0-65535> <0-65535>|) ((dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef)) | (precedence (<0-7>| critical| flash | flash- override| immediate| internet| network| priority| routine)) |)
({ack|established|fin|psh|rst|syn|urg}|) (log|) (sample|) no (<1-268435453>|) (deny|permit) udp (X:X::X:X/M|X:X::X:X X:X::X:X|any)

((eq|gt|lt|neq) <0-65535> |bgp|chargen|cmd|daytime|discard|domain|drip |echo|exec|finger|ftp |ftp- data|gopher|hostname|ident|irc|klogin|kshell |login|lpd|nntp|pim-auto- rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet |time|uucp|whois|www) | range <0-65535> <0-65535>|) | range <0-65535> <0-65535>|)(X:X::X:X/M|X:X::X:X X:X::X:X|any) ((eq|gt|lt|neq) <0-65535> |bgp|chargen|cmd|daytime|discard|domain|drip|echo|exec|finger|ftp |ftp-data|gopher|hostname|ident|irc|klogin|kshell|login|lpd|nntp|pim-auto-rp|pop2|pop3|smtp|ssh|sunrpc|tacacs|talk|telnet|time|uucp|whois|www) | range <065535> <0-65535>|) | range <0-65535> <0-65535>|) ((dscp (<0-63>| af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef)) | (precedence (<0-7>| critical| flash | flash-override| immediate| internet| network| priority| routine)) |)
({ack|established|fin|psh|rst|syn|urg}|) (log|) (sample|)

Parameters

<1-268435453> IPv6 ACL sequence number.

deny Drop the packet. permit Accept the packet.

tcp Transmission Control Protocol. udp User Datagram Protocol.

X:X::X:X/M Source or destination IPv6 prefix and length.

X:X::X:X X:X::X:X Source or destination IPv6 address and mask. host X:X::X:X A single source or destination host IPv6 address. any Any source or destination IPv6 address. eq Source or destination port equal to. gt Source or destination port greater than.

`lt` Source or destination port less than. `neq` Source or destination port not equal to.

`<0-65535>`	Source or destination port number.
`range`	Range of source or destination port numbers:
`<0-65535>`	Lowest value in the range.
`<0-65535>`	Highest value in the range.
`ftp`	File Transfer Protocol (21).
`ssh`	Secure Shell (22).
`telnet`	Telnet (23).
`www`	World Wide Web (HTTP 80).
`tftp`	Trivial File Transfer Protocol (69).
`bootp`	Bootstrap Protocol (BOOTP) client (67).
`bgp`	Border Gateway Protocol.
`chargen`	Character generator.
`cmd`	Remote commands.
`daytime`	Daytime.
`discard`	Discard.
`domain`	Domain Name Service.
`drip`	Dynamic Routing Information Protocol.
`echo`	Echo.
`exec`	EXEC.
`finger`	Finger.
`ftp`	File Transfer Protocol.
`ftp-data`	FTP data connections.
`gopher`	Gopher.
`hostname`	NIC hostname server.
`ident`	Ident Protocol.
`irc`	Internet Relay Chat.
`klogin`	Kerberos login.
`kshell`	Kerberos shell.
`login`	Login.
`lpd`	Printer service.
`nnt`	Network News Transport Protocol.
`pim-auto-rp`	PIM Auto-RP.
`pop2`	Post Office Protocol v2.
`pop3`	Post Office Protocol v3.
`smtp`	Simple Mail Transport Protocol.

ssh	Secure Shell.
sunrpc	Sun Remote Procedure Call.
tacacs	TAC Access Control System.
talk	Talk.
telnet	Telnet.
time	Time.
uucp	UNIX-to-UNIX Copy Program.
whois	WHOIS/NICNAME
www	World Wide Web.
nntp	Range of source or destination port numbers:
dscp	Match packets with given DSCP value.
<0-63>	Enter DSCP value between 0-63.
af11	AF11 DSCP (001010) decimal value 10.
af12	AF12 DSCP (001100) decimal value 12.
af13	AF13 DSCP (001110) decimal value 14.
af21	AF21 DSCP (010010) decimal value 18.
af22	AF22 DSCP (010100) decimal value
af23	AF23 DSCP (010110) decimal value 22.
af31	AF31 DSCP (011010) decimal value 26.
af32	AF32 DSCP (011100) decimal value 28.
af33	AF33 DSCP (011110) decimal value 30.
af41	AF41 DSCP (100010) decimal value 34
af42	AF42 DSCP (100100) decimal value 36.
af43	AF43 DSCP (100110) decimal value 38.
cs1	CS1 (precedence 1) DSCP (001000) decimal value 8.
cs2	CS2 (precedence 2) DSCP (010000) decimal value 16.
cs3	CS3 (precedence 3) DSCP (011000) decimal value 24.
cs4	CS4 (precedence 4) DSCP (100000) decimal value 32.
cs5	CS5 (precedence 5) DSCP (101000) decimal value 40.
cs6	CS6 (precedence 6) DSCP (110000) decimal value 48.
cs7	CS7 (precedence 7) DSCP (111000) decimal value 56.
default	Default DSCP (000000) decimal value 0.
ef	EF DSCP (101110) decimal value 46.
precedence	Match packets with given precedence value.
<0-7>	Enter precedence value 0-7.

`critical`	Match packets with critical precedence (5).
`flash`	Match packets with flash precedence (3).
`flashoverride`	Match packets with flash override precedence (4).
`immediate`	Match packets with immediate precedence (2).
`internet`	Match packets with internetwork control precedence (6).
`network`	Match packets with network control precedence (7).
`priority`	Match packets with priority precedence (1).
`routine`	Match packets with routine precedence (0).

`ack`	Match on the Acknowledgment (ack) bit.
`established`	Matches only packets that belong to an established TCP connection.
`fin`	Match on the Finish (fin) bit.
`psh`	Match on the Push (psh) bit.
`rst`	Match on the Reset (rst) bit.
`syn`	Match on the Synchronize (syn) bit.
`urg`	Match on the Urgent (urg) bit.
`biff`	Biff.
`bootpc`	Bootstrap Protocol (BOOTP) client.
`bootps`	Bootstrap Protocol (BOOTP) server.
`discard`	Discard.
`dnsix`	DNSIX security protocol auditing.
`domain`	Domain Name Service.
`echo`	Echo.
`isakmp`	Internet Security Association and Key Management Protocol.
`mobile-ip`	Mobile IP registration.
`nameserver`	IEN116 name service.
`netbios-dgm`	Net BIOS datagram service.
`netbios-ns`	Net BIOS name service.
`netbios-ss`	Net BIOS session service.
`non500-isakmp`	Non500-Internet Security Association and Key Management Protocol.
`ntp`	Network Time Protocol.
`pim-auto-rp`	PIM Auto-RP.
`rip`	Routing Information Protocol.
`snmp`	Simple Network Management Protocol.
`snmptrap`	SNMP Traps.
`sunrpc`	Sun Remote Procedure Call.

`syslog`	System Logger.
`tacacs`	TAC Access Control System.
`talk`	Talk.
`tftp`	Trivial File Transfer Protocol.
`time`	Time.
`who`	Who service.
`xdmcp`	X Display Manager Control Protocol.
`log`	Log the packets matching the filter (in-direction only).
`sample`	Sample the packets matching the filter (in-direction only).

Default

No default value is specified

Command Mode

IPv6 access-list mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ipv6 access-list mylist
(config-ipv6-acl)#deny udp any eq tftp
(config-ipv6-acl)#deny tcp fd22:bf66:78a4:10a2::/64 fdf2:860a:746a:e49c::/64
eq ssh
```

ipv6 access-list WORD

Use this command to define a named access control list (ACL) that determines whether to accept or drop an incoming packet based on the criteria that you specify. This form of this command filters packets based on:

- Protocol
- Source IP address
- Destination IP address.

An ACL is made up of one or more ACL specifications. You can repeat this command and add multiple specifications. Each time you give this command, the specification is added to the end of the list.

Each packet that arrives at the device is compared to each specification in each ACL in the order that they are defined. The device continues to look until it has a match. If no match is found and the device reaches the end of the list, the packet is denied. For this reason, place the most frequently occurring specifications at the top of the list.

The device stops checking the specifications after a match occurs.

There is an implied `deny` specification for traffic that is not permitted. A single-entry ACL with only one `deny` specification is the same as denying all traffic. You must have at least one `permit` specification in an ACL or all traffic is blocked.

Use the `no` form of this command to remove an ACL specification.

Command Syntax `ipv6 access-list WORD`

`no ipv6 access-list WORD`

Parameters

`WORD`	Access-list name.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ipv6 access-list ipv6-acl-01
(config-ipv6-acl)#exit
```

mac access-group

Use this command to attach a MAC access list to an interface to filter incoming packets.

When you attach an access list to a VLAN interface or LAG interface as well as to a physical interface that is a member of that LAG and/or VLAN interface, the priority order is:

1. VLAN interface
2. LAG interface
3. Physical interface

For example, if you attach access lists to both a LAG interface and a physical interface that is a member of that LAG, matching traffic rules are applied to the LAG interface, but not to the physical interface.

Use the no parameter with this command to detach a MAC access group.

Note: Access-group on egress direction uses the TCAM group used by QoS output service policy. Hence, actions will be unpredictable when conflicting matches are configured on same interface. It is recommended to avoid such configuration. Otherwise user need to configure priority (in QoS) / sequence number (in ACL) carefully to tackle such cases.

Command Syntax `mac access-group`

`WORD in no mac access-group`

`WORD in`

Parameters

`WORD`	Access list name.
`in`	Filter incoming packets.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#mac access-list mylist (config-mac-
acl)#permit any any
(config-mac-acl)#exit

(config)#interface eth3
(config-if)#mac access-group mylist in
(config-if)#exit

(config)#interface eth3
(config-if)#no mac access-group mylist in
(config-if)#exit
```

mac access-list default

Use this command to modify the default rule action of access-list. Default rule is applicable only when access-list is attached to interface. Default rule will have the lowest priority and only the packets not matching any of the user defined rules match default rule.

Command Syntax `default (deny-all|permit-all) (log|) (sample|)`

Parameters

`deny-all`	Drop all packets.
`permit-all`	Accept all packets.
`log`	Log the packets matching the filter (in-direction only).
`Sample`	Sample the packets matching the filter (in-direction only).

Default

No default value is specified

Command Mode

MAC access-list mode

Applicability

This command was introduced before SWMRE version 1.3.

Log feature is supported only with deny rules. Sample feature is supported only with permit rules. Feature is not supported on Qumran platforms.

Examples

```
#configure terminal
(config)#mac access-list mac-acl-01
(config-mac-acl)#default permit-all sample
```

mac access-list filter

Use this command to define an access control entry (ACE) in a named access control list (ACL) that determines whether to permit or deny Layer2 packets with the given source and destination MAC, ether type, cos and VLAN values.

Use the no form of this command to remove an ACL specification.

Note: Configuring same filter again with change of sequence number or change of action will result in update of sequence number or filter action.

Command Syntax

```
(<1-268435453>|)(deny|permit) (any | (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (any | (XX-XX-XX-XX-
  XX-XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (aarp|appletalk|decnet-
  iv|diagnostic|etype-6000|etype-8042 |ip4|ip6|mpls|lat|lavc-sca|mop-console|mop-
  dump|vines-echo|WORD|) (cos <0-7>|)(vlan <1-4094>|) (log|) (sample|)

no (<1-268435453>|)(deny|permit) (any | (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (any | (XX-XX-XX-XX-
  XX-XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX) | host (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)) (aarp|appletalk|decnet-
  iv|diagnostic|etype-6000|etype-8042 |ip4|ip6|mpls|lat|lavc-sca|mop-console|mop-
  dump|vines-echo|WORD|) (cos <0-7>|)(vlan <1-4094>|) (log|) (sample|)
```

Parameters

`deny` Drop the packet. `permit`

Accept the packet.

`<1-268435453>` IPv4 ACL sequence number.

`any` Source/Destination any.

`XX-XX-XX-XX-XX-XX`

Source/Destination MAC address (Option 1).

`XX:XX:XX:XX:XX:XX`

Source/Destination MAC address (Option 2).

`XXXX.XXXX.XXXX`

Source/Destination MAC address (Option 3).

`XX-XX-XX-XX-XX-XX`

Source/Destination wildcard (Option1).

`XX:XX:XX:XX:XX:XX`

Source/Destination wildcard (Option2).

XXXX.XXXX.XXXX	Source/Destination wildcard (Option3).
host	A single source/destination host.
aarp	Ethertype - 0x80f3.
appletalk	Ethertype - 0x809b.
decnet-iv	Ethertype - 0x6003.
diagnostic	Ethertype - 0x6005.
etype-6000	Ethertype - 0x6000.
etype-8042	Ethertype - 0x8042.
ip4	Ethertype - 0x0800.
ip6	Ethertype - 0x86dd.
mpls	Ethertype - 0x8847.
lat	Ethertype - 0x6004.
lavc-sca	Ethertype - 0x6007.
mop-console	Ethertype - 0x6002.
mop-dump	Ethertype - 0x6001.
vines-echo	Ethertype - 0x0baf.
WORD	Any Ethertype value.
cos <0-7>	Cos value.
vlan <1-4094>	VLAN value.
log	Log the packets matching the filter (in-direction only).
sample	Sample the packets matching the filter (in-direction only).

Default

No default value is specified

Command Mode

MAC access-list mode

Applicability

This command was introduced before SWMRE version 1.3.

Log feature is supported only with deny rules. Sample feature is supported only with permit rules. Feature is not supported on Qumran platforms.

Examples

```
#configure terminal
(config)#mac access-list mac-acl-01 (config-mac-acl)#permit
0000.1234.1234 0000.0000.0000 any sample
```

mac access-list remark

Use this command to add a description to an MAC access control list (ACL).

Use the `no` form of this command to remove an ACL description.

Command Syntax `remark LINE no remark`

Parameters

LINE	ACL description up to 100 characters.

Default

No default value is specified

Command Mode

MAC access-list mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#mac access-list mylist
                    (config-mac-acl)# remark Permit the inside admin address
```

mac access-list resequence

Use this command to re-sequence the mac access list.

Note: Use a non-overlapping sequence space for new sequence number sets to avoid possible unexpected rule matches during transition.

Note: Re-sequencing an ACL attached to a management interface clears the ACL counters associated to it.

Command Syntax `resequence <1-268435453>`

`INCREMENT`

Parameters

`<1-268435453>` Starting sequence number.

`INCREMENT` Sequence number increment steps.

Default

No default value is specified

Command Mode

MAC access-list mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#mac access-list mylist
(config-mac-acl)#resequence 15 15
```

mac access-list WORD

Use this command to define a named access control list (ACL) that determines whether to permit or deny packets with the given source and destination MAC, ether type, cos or VLAN values.

An ACL is made up of one or more ACL specifications. You can repeat this command and add multiple specifications. Each time you give this command, the specification is added to the end of the list.

Each packet that arrives at the device is compared to each specification in each ACL in the order that they are defined. The device continues to look until it has a match. If no match is found and the device reaches the end of the list, the packet is denied. For this reason, place the most frequently occurring specifications at the top of the list.

The device stops checking the specifications after a match occurs.

There is an implied `deny` specification for traffic that is not permitted. A single-entry ACL with only one `deny` specification is the same as denying all traffic. You must have at least one `permit` specification in an ACL or all traffic is blocked.

Use the `no` form of this command to remove an ACL specification.

Command Syntax `mac access-list WORD no mac access-list WORD`

Parameters

`WORD`	Access-list name.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#mac access-list mac-acl-01
(config-mac-acl)#exit
```

show access-lists

Use this command to display a list of access list

Command Syntax `show access-lists (WORD|) (expanded|summary|)`

Parameters

`WORD`	Access-list name.
`expanded`	Expanded access-list.
`summary`	Summary of access-list.

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show access-lists expanded
IP access list Iprule1
11 permit ip 30.0.0.1 0.0.0.255 172.124.0.2 0.0.0.255
```

```
default deny-all MAC access list Macrule1 10 permit host
0000.1234.1234 any default deny-all IPv6 access list ipv6-
acl-01 10 deny ahp 3ffe::/64 4ffe::/64 default deny-all

#show access-lists summary IPV4 ACL Iprule1
statistics enabled Total ACEs Configured: 1
Configured on interfaces: xe3/1 - egress
(Router ACL) Active on interfaces:
xe1/3 - ingress (Router ACL) MAC ACL Macrule1
statistics enabled
Total ACEs Configured: 0 Configured on interfaces:
Active on interfaces: IPV6 ACL ipv6-acl-01
statistics enabled
Total ACEs Configured: 2
Configured on interfaces:
```

```
xe7/1 - ingress (Router ACL) Active on interfaces:
```


© Symanitron Proprietary

show access-list log-cache

Use this command to show the ACL logging table entries

Command Syntax `show access-lists log-cache`

Parameters

None

Default

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show access-lists log-cache
2016 Oct 26 12:08:37:xe1/1: 0000.0100.0a00 -> 0000.0100.0b00, ethertype IP
(0x800), proto tcp, vlan 2, 0.0.0.0:0 -> 0.0.0.0:0 ...suppressed 11 times

  2016 Oct 26 12:07:51:xe1/1: 0000.0100.0a00 -> 0000.0100.0b00, ethertype IP
(0x800), proto 255, vlan 2, 0.0.0.0 -> 0.0.0.0 ...suppressed 10 times
```

show ip access-lists

Use this command to display IP access list

Command Syntax `show ip access-lists (WORD|) (expanded|summary|)`

Parameters

`WORD`	Access-list name.
`expanded`	Expanded access-list.
`summary`	Summary of access-list.

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip access-lists
IP access list Iprule2
11 permit ip 30.0.0.1 0.0.0.255 172.124.0.2 0.0.0.255 12 deny ip 30.0.0.2
0.0.0.255 182.124.0.3/24 default deny-all

#show ip access-lists summary IPV4 ACL Iprule3
statistics enabled Total ACEs Configured: 4
Configured on interfaces: sa1 - ingress (Port ACL)
sa3 - ingress (Router ACL) sa8 - ingress (Port ACL)
vlan1.3 - ingress (Router ACL) xe1/1 - ingress (Port
ACL) xe1/2 - ingress (Router ACL) xe1/3 - ingress
(Router ACL) xe3/1 - egress (Router ACL) Active on
interfaces: sa1 - ingress (Port ACL) xe1/1 - ingress
(Port ACL) xe1/2 - ingress (Router ACL) xe1/3 -
ingress (Router ACL)
```

show ipv6 access-lists

Use this command to display IPv6 access lists.

Command Syntax `show ipv6 access-lists (WORD|) (expanded|summary|)`

Parameters

`WORD`	Access-list name.
`expanded`	Expanded access-list.
`summary`	Summary of access-list.

Default

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ipv6 access-lists
IPv6 access list ipv6-acl-01
10 deny ahp 3ffe::/64 4ffe::/64
20 permit ahp 78fe::1/48 68fe::1/48
30 permit ahp 3333::1/64 4444::1/48 fragments 40 permit ahp 5555::1/64
4444::1/48 dscp af23 default deny-all
```

```
#show ipv6 access-lists summary IPV6 ACL ipv6-acl-01
statistics enabled Total ACEs Configured: 4 Configured
on interfaces: sa3 - ingress (Router ACL) vlan1.3 -
ingress (Router ACL) xe1/1 - ingress (Port ACL) xe1/2 -
ingress (Router ACL) xe1/3 - ingress (Router ACL) Active
on interfaces: xe1/1 - ingress (Port ACL) xe1/2 -
ingress (Router ACL) xe1/3 - ingress (Router ACL)
```

show mac access-lists

Use this command to display MAC access lists.

Command Syntax `show mac access-lists (WORD|) (expanded|summary|)`

Parameters

`WORD`	Access-list name.
`expanded`	Expanded access-list.
`summary`	Summary of access-list.

Default

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show mac access-lists MAC
access list Macrule2 default
deny-all MAC access list
Macrule3
10 permit host 0000.1234.1234 any
20 deny host 1111.1111.AAAA any 65535
30 permit host 2222.2222.AAAA any 65535
40 permit 0000.3333.3333 0000.0000.FFFF 4444.4444.4444
0000.0000.FFFF default deny-all [match=1126931077]

# show mac access-lists summary MAC ACL
Macrule3 statistics enabled Total ACEs
Configured: 4 Configured on interfaces:
sa3 - ingress (Router ACL) sa8 -
ingress (Port ACL) vlan1.3 - ingress
(Router ACL) xe1/1 - ingress (Port ACL)
xe1/2 - ingress (Router
```

```
ACL) xe1/3 - ingress (Router ACL)
Active on interfaces:
xe1/1 - ingress (Port ACL) xe1/2 -
ingress (Router ACL) xe1/3 - ingress
(Router ACL)
```

show running-config aclmgr

Use this command to display the entire access list configurations along with the attachment to interfaces.

Command Syntax `show running-config aclmgr`

Parameters

None

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
>enable
#show running-config aclmgr ip
access-list ip-acl-01
11 permit ip 30.0.0.1 0.0.0.255 172.124.0.2 0.0.0.255 12
deny ip 30.0.0.2 0.0.0.255 182.124.0.3/24 default deny-all
mac access-list mac-acl-01 10 permit host 0000.1234.1234
any 20 permit host 0000.1111.AAAA any ipv4 cos 3 vlan 3
default deny-all !
ipv6 access-list ipv6-acl-01
10 deny ipv6 3ffe::/64 4ffe::/64 dscp af43 20
permit ipv6 78fe::/64 68fe::/64 dscp cs3 default
deny-all ! interface xe1/1 ip access-group ip-
acl-01 in !
```

show running-config access-list

Use this command to show the running system status and configuration details for MAC and IP access lists.

Command Syntax `show running-config access-list`

Parameters

None

Default

None

Command Mode

Privileged Exec mode, Configure mode and Router-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show running-config access-list ip
access-list abd 10 deny any any any
! mac access-list abc
remark test
10 deny any any !
```

show running-config ipv6 access-list

Use this command to show the running system status and configuration details for IPv6 access lists.

Command Syntax `show running-config ipv6 access-list`

Parameters

None

Default

None

Command Mode

Privileged Exec mode, Configure mode and Router-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show running-config ipv6 access-list ipv6
access-list test 10 permit any any any !
```

© Symanitron Proprietary

CHAPTER 6 Traffic Engineering Commands

This chapter provides a reference of the NSM Traffic Engineering (TE) command. Most commands are executed in TE link mode.

This chapter includes the following commands:

- data-link
- description
- ip address
- label-switching
- remote ip address
- remote-link-id
- reservable-bandwidth
- show running-config te-link
- show te-link
- shutdown
- te-link

data-link

Use this command to associate data links with TE links. Only data-links can be associated to a TE link. Attempting to map multiple data links to the same TE link returns an error.

Use the `no` option with this command to remove an existing data link from a TE link.

Command Syntax `data-link IFNAME`

`no data-link IFNAME`

Parameter

`IFNAME`	Indicate the interface name.

Command Mode

TE Link mode

Examples

```
#configure terminal
(config)#te-link te1 local-link-id 172.1.1.1
(config-te)#data-link eth1

(config-te)#no data-link eth1
(config-te)#data-link eth2
```

description

Use this command to provide a TE Link-specific description.

Use the `no` option with this command to remove the description.

Command Syntax `description`

```
LINE no description
```

Parameters

`LINE`	Text describing the specific interface.

Command Mode

TE Link mode

Examples

```
#configure terminal
          (config)#te-link te1 local-link-id 172.1.1.1
          (config-te)#description This is for Testing
```

ip address

Use this command to set the IP address for an interface.

Use the `no` parameter with this command to remove the IP address from an interface.

Command Syntax `ip address`

```
A.B.C.D/M no ip address
(A.B.C.D/M |)
```

Parameters

`A.B.C.D/M`	Specify the IP address and prefix length of an interface.

Command Mode

Interface mode

Examples

```
(config)#interface eth0
(config-if)#ip address 10.10.10.50/24
```

label-switching

Use this command to enable label-switching on a TE link.

Use the no option with this command to disable label-switching on a TE link.

Command Syntax `label-switching` `no label-switching`

Parameters

None

Command Mode

TE Link mode

Example

```
#configure terminal
  (config)#te-link te1 local-link-id 172.1.1.1
(config-te)#label-switching
```

remote ip address

Use this command to set a remote IP address for an interface.

Use the `no` parameter with this command to remove the IP address from an interface.

Command Syntax `remote ip address`

`A.B.C.D/M no remote ip address`

`(A.B.C.D/M |)`

Parameters

`A.B.C.D/M`	Specify the IP address and prefix length of an interface.

Command Mode

Interface mode

Examples

```
(config)#interface eth0 (config-if)#remote
ip address 10.10.10.50/24
```

remote-link-id

Use this command to configure remote link id for each TE link.

Use the no option with this command to remove the remote link ID from a TE link.

Command Syntax `remote-link-id`

`A.B.C.D` `no` `remote-link-id`

`(A.B.C.D|)`

Parameters

`A.B.C.D`	Remote link ID in IPv4 address format.

Command Mode

TE Link mode

Examples

```
#configure terminal
(config)#te-link te1 local-link-id 172.1.1.1
(config-te)#remote-link-id 172.1.2.3
```

reservable-bandwidth

Use this command to specify the maximum reservable bandwidth per interface. This value can be a larger or smaller value than `max-bandwidth`. When no max-reservable-bandwidth is specified, the default is equal to the `maxbandwidth`. Use the `no` parameter to remove the maximum reservable, and use the maximum bandwidth.

Use the `no` parameter with this command to disable the configuration.

Comman

d

Syn

tax

```
res
erv
abl
e-
ban
dwi
dth
BAN
DWI
DTH
no
res
erv
abl
e-
ban
dwi
dth
```

Parameters

`BANDWIDTH`	<1-999>k for 1 to 999 kilobits/s
	<1-999>m for 1 to 999 megabits/s
	<1-100>g for 1 to 100 gigabits/s

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#reservable-bandwidth 100m
```

show running-config te-link

Use this command to show the running system status of TE-link configurations.

Command Syntax `show running-config te-link show running-config te-link TLNAME`

Parameters

`TLNAME`	Display the TE link name

Command Mode

Privileged Exec mode

Example

```
>enable
#show running-config te-link new-te-123 !
```

show te-link

This command is used to display the properties for a particular TE link.

Command Syntax `show te-link (TLNAME|)`

Parameter

`TLNAME`	Displays the name of a TE link.

Command Mode

Exec mode

Example

The following example is sample output for this command:

```
#show te-link te1 te-
link te1
        description test
  Data-link: eth1
  Local link-id: 2.3.4.5
  Remote-link-id: 3
        IP address: 10.10.10.50/24
  Remote IP address: 10.10.10.51/24
  Index 2 mtu 1500
    <UP,POINT-TO-POINT,RUNNING >
  Control Adjacency: Rtr2
         Link ID: 22.2.2.2
    Administrative Group(s): None
  TE Metric 20
  Bandwidth 100m
  Maximum reservable bandwidth 70m
  DSTE Bandwidth Constraint Mode is MAM
    Bandwidth Constraint for Class Type default is
70m
  Available b/w for TE-CLASS 0 {a2, 5} is 0
    Maximum LSP b/w at Priority 0 is 0
  Maximum LSP b/w at Priority 1 is 0
        Maximum LSP b/w at Priority 2 is 70m
        Maximum LSP b/w at Priority 3 is 70m
        Maximum LSP b/w at Priority 4 is 70m
        Maximum LSP b/w at Priority 5 is 70m
        Maximum LSP b/w at Priority 6 is 70m
        Maximum LSP b/w at Priority 7 is 70m
  Minimum LSP Bandwidth is 10m
```

```
  Switching Capability: PSC1
  Encoding Type:
Packet   Protection:
1:1   risk-group 2, 3
mtu: 1500
#
```

shutdown

Use this command to shut down the selected TE link.

Use the `no` form of this command to disable this function.

Command Syntax `shutdown`

```
no shutdown
```

Parameters

None

Command Mode

TE Link mode

Examples

```
#configure terminal
         (config)#te-link te1 local-link-id 172.1.1.1
(config-te)#shutdown
```

te-link

Use this command to create a TE (traffic engineering) link and set its local-link-id.

Use the `no` option with this command to delete an existing TE link.

Command Syntax `te-link TLNAME te-link TLNAME local-link-id A.B.C.D (numbered |) no te-link TLNAME ((local-link-id A.B.C.D (numbered |))|)`

Parameters

`TLNAME`	Name of the TE link. `local-link-id`
	Local link Identifier.
`A.B.C.D`	Local interface ID expressed in IPv4 address format.
`numbered`	The data link type is numbered.

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#te-link te1 local-link-id 172.1.1.1

#configure terminal
(config)#te-link te1 local-link-id 1.2.3.4

#configure terminal
(config)#te-link te1 local-link-id 1.2.3.4 numbered
```

CHAPTER 7 Control Channel Mode Commands

The commands in this chapter are issued in the NSM Control Channel mode. It includes the following commands:

- control-channel
- description
- local-address
- show control-channel
- show running-config control-channel
- shutdown

control-channel

Use this command to create a new Control Channel. It is also used to identify a control-channel ID (`cc-id`), and designate the local and remote addresses used by the control channel. Use the `no` option with this command to delete an existing Control Channel.

Command Syntax `control-channel CCNAME`

```
control-channel CCNAME cc-id <1-4294967295> local-address A.B.C.D peer-address
  A.B.C.D no control-channel CCNAME cc-id <1-4294967295> local-address A.B.C.D
peer-address A.B.C.D
```

Parameters

`CCNAME`	Control channel name.
`cc-id`	Control channel parameters.
`<1-4294967295>`	Control channel ID value in integer format.
`local-address`	Control channel local address.
`A.B.C.D`	Control channel local address in IPv4 address format.
`peer-address`	Control channel local address.
`A.B.C.D`	Control channel peer address in IPv4 address format.

Command Mode

Configure mode

Example

```
#configure terminal
(config)#control-channel cc1 cc-id 22 local-address 2.2.2.2 peer-address
4.4.4.4
(config-cc)#

(config-cc)#description This is for Testing
```

description

Use this command to provide an Control Channel-specific description.

Use the `no` parameter to remove the description.

Command Syntax

```
description
LINE          no
description
```

Parameter

`LINE`	Characters describing this control channel.

Command Mode

Control Channel mode

Examples

```
(config)#control-channel new cc-id 123 local-address 123.4.5.67 peer-address
123.4.5.68
(config-cc)#description Connected to eth1

(config-cc)#no description
```

local-address

Use this command to set a local IP address for an interface.

Use the `no` parameter with this command to remove the IP address from an interface.

Command Syntax `local-address A.B.C.D no local-address (A.B.C.D/M |)`

Parameters

`A.B.C.D/M`	Specify the IP address and prefix length of an interface.

Command Mode

Interface mode

Examples

```
(config)#interface eth0
(config-if)#local-address 10.10.10.50/24
```

show control-channel

Use this command to display information about a control channel.

Command Syntax `show control-channel (CCNAME|)`

Parameter

`CCNAME`	Specify name of the control channel.

Command Mode

Exec mode and Privileged Exec mode

Example

The following is a sample output of this command:

```
==============================
Control-Channel : newer
  Gifindex : 20
  Local-address : 1.2.3.4
  Peer-address : 1.2.3.5
  Control-Channel ID : 12345
  Interface binding: N/A
  Belong to Control-Adjacency : N/A
  Status DOWN : admin Up   operational Down   NSM Down
  Last UP Time : 00:00:00
  Last Down Time : 20:17:55
==============================
Control-Channel : new
  Description Control Channel specific description :
  Gifindex : 18
  Local-address : 1.2.3.4
  Peer-address : 1.2.3.4
  Control-Channel ID : 123
  Interface binding: N/A
  Belong to Control-Adjacency : N/A
  Status DOWN : admin Up   operational Down   NSM Down
  Last UP Time : 18:49:31
```

```
                                                                    Last Down
    Time : 18:49:27
    ================================
    #
```

show running-config control-channel

Use this command to show the complete status and configuration of a control channel configuration.

Command Syntax `show running-config control-channel show running-config control-channel CCNAME`

Parameters

`CC_NAME`	Specify name of the control-channel.

Command Mode

Privileged Exec mode, Configure mode, Router mode

Example

```
(config)#show running-config control-channel no
shutdown

 !
!
(config)#
```

shutdown

Use this command to shut down the selected control channel.

Use the `no` form of this command to disable this function.

Command

Syntax

```
shutdown
no
shutdown
```

Parameters

None

Command Mode

Control Channel mode

Examples

The following example shows the use of the `shutdown` command.

```
(config)#control-channel new cc-id 123 local-address 123.4.5.67 peer-
address 123.4.5.68
(config-cc)#shutdown

(config-cc)#no shutdown
```

© Symanitron Proprietary

CHAPTER 8 Control Adjacency Commands

The commands in this chapter are issued in the Control Adjacency mode. It includes the following commands:

- control-adjacency
- description
- show control-adjacency
- show running-config control-adjacency
- te-link

control-adjacency

Use this command to create a new Control Adjacency with a neighbor router. The command also configures a peer address for the control adjacency, and provides the option to specify whether it is statically configured or should be managed using LMP.

Use the `no` option with this command to remove an existing control adjacency.

Command Syntax `control-adjacency CADJNAME peer-address A.B.C.D (static |using-lmp |) no control-adjacency CADJNAME ((peer-address A.B.C.D (static |using-lmp|))|)` **Parameters**

`CADJNAME`	Control adjacency name in text format.
`A.B.C.D`	Control adjacency peer address in IPv4 address format.
`peer-address`	Control Adjacency Parameters.
`static`	Static configuration of control adjacency.
`using-lmp`	Control adjacency is managed using Link Management Protocol (LMP).

Command Mode

Configure mode

Example

```
#configure terminal
(config)#control-adjacency rtr2 peer-address 4.4.4.4
static (config-ca)#
```

description

Use this command to provide a control adjacency-specific description.

Use the `no` parameter to remove the description.

Command Syntax `description LINE no description`

Parameter

`LINE`	Characters describing this control adjacency.

Command Mode

Control Adjacency mode

Examples

```
                (config)#control-adjacency new peer-address 1.2.3.4 static
(config-ca)#description Connected to eth1

(config-ca)#no description
```

show control-adjacency

This command is used to display the properties for a particular Control Adjacency.

Command Syntax `show control-adjacency (CANAME|)`

Parameter

`CANAME`	Name of the control adjacency

Command Mode

Exec Mode

Example

The following example is sample output for this command:

```
#show control-adjacency ca2 Control-channel
Rtr2 description test Control Channels:
cc1, cc2
Primary Control Channel : cc1 TE Links: te1, te2
peer-address 3.3.3.3 index 2 <UP, RUNNING>
LMP is in USE
```

show running-config control-adjacency

Use this command to show the running system status and details for any control adjacency configuration.

Command Syntax `show running-config control-adjacency show running-config control-adjacency CANAME`

Parameter

`CANAME`	Indicate the control adjacency name.

Command Mode

Privileged Exec mode

Example

```
>enable
#show running-config control-adjacency !
```

te-link

Use this command to configure a TE link name.

Use the `no` parameter to remove a TE link name.

Command Syntax `te-link TELNAME no te-link TELNAME`

Parameters

None

Command Mode

Control Adjacency mode

Examples

```
#configure terminal
(config)#control-adjacency new peer-address 1.2.3.4 static (config-ca)#te-link new-link

                (config)#control-adjacency new peer-address 1.2.3.4 static (config-ca)#no te-link new-link
```

CHAPTER 9 Tunneling Commands

This chapter contains commands for IP tunneling.

- interface tunnel
- tunnel checksum
- tunnel destination
- tunnel dmac
- tunnel mode
- tunnel mode ipv6ip
- tunnel path-mtu-discovery
- tunnel source
- tunnel tos
- tunnel ttl

interface tunnel

Use this command to create a new tunnel interface.

Use the `no` parameter to destroy the tunnel interface.

Command Syntax `interface tunnel <0-2147483647> no interface tunnel <0-2147483647>`

Parameter

`<0-2147483647>` Specify a tunnel interface number.

Default

Disabled

Command Mode

Configure mode

Example

```
#configure terminal
(config)#interface tunnel 100
(config-if)#
```

tunnel checksum

Use this command to enable a checksum feature for the tunnel. When configuring the tunnel checksum, make sure to:

- configure the tunnel checksum feature before configuring the tunnel source and destination.
- configure the tunnel checksum on both ends of the tunnel.

Use the `no` parameter to disable the feature.

Command Syntax `tunnel`

```
checksum no tunnel
checksum
```

Parameters

None

Default

Disabled

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface tunnel 0
(config-if)#tunnel mode gre
(config-if)#tunnel checksum
(config-if)#tunnel source 192.168.1.1
```

```
(config-if)#tunnel destination 192.168.254.2
```

tunnel destination

Use this command to specify a tunnel destination address in an IPv4 portion.

Use the `no` parameter to undo the address.

Command Syntax `tunnel destination A.B.C.D no tunnel destination`

Parameter

`A.B.C.D`	Specify a tunnel destination IPv4 address.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface tunnel 200
(config-if)#tunnel mode ipip
(config-if)#tunnel source 10.10.0.1
(config-if)#tunnel destination 10.11.0.1
```

tunnel dmac

Use this command to set a destination MAC address for tunneled packets. This command supports IP-in-IP tunneling on Broadcom.

Use the `no` option with this command to remove the destination MAC address.

Command Syntax `tunnel`

`dmac/mac MAC no`

`tunnel dmac`

Parameter

`MAC`	Destination address in MAC format.

Default

If a specific MAC address is not set with this command, all tunneled packets are sent with a destination address of 0.

Command Mode

Interface mode

Examples

```
broadcom(config)#interface tunnel 7
broadcom(config-if)#tunnel dmac 1213.2322.123
```

tunnel mode

Use this command to configure an IPv4 tunnel mode. This command specifies a tunnel encapsulation mode for either GRE and IPIP mode The GRE tunnel mode is used for IPv4-to-IPv4 tunneling.

Use the `no` parameter to remove the configuration from a mode.

Command Syntax `tunnel mode (ipip|gre) no tunnel mode`

Parameters

`ipip` IPIP tunnel mode. `gre` Generic Routing Encapsulation (GRE)

tunnel mode.

Command Mode

Interface mode

Example

```
#configure terminal
(config)#interface tunnel 2
(config-if)#tunnel source 192.168.1.1
(config-if)#tunnel destination 192.168.2.1
(config-if)#tunnel mode gre
```

tunnel mode ipv6ip

Use this command to configure an IPv6 tunnel mode. This command specifies a tunnel encapsulation mode for either GRE and IPIP mode The GRE tunnel mode is used for IPv6-to-IPv6 tunneling.

Use the `no` parameter to remove the configuration from a mode.

Command Syntax `tunnel mode ipv6ip (6to4|isatap|) no tunnel mode`

Parameters

`6to4` IPv6 automatic tunnelling using 6to4. `isatap` IPv6 automatic tunnelling using ISATAP.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface tunnel 0
(config-if)#tunnel source 10.10.1.1
(config-if)#tunnel destination 10.10.2.1
(config-if)#tunnel mode ipv6ip 6to4
```

tunnel path-mtu-discovery

Use this command to enable path Maximum Transmission Unit (MTU) discovery in the underlying tunnel interface.

Use the `no` parameter to disable this feature.

Command Syntax `tunnel path-mtu-discovery` `no tunnel path-mtu-discovery`

Parameters

None

Default

Disabled

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface tunnel 0
(config-if)#tunnel mode gre
(config-if)#tunnel source 192.168.0.1
(config-if)#tunnel destination 10.0.0.1
(config-if)#tunnel path-mtu-discovery
```

tunnel source

Use this command to specify a tunnel source address in a IPv4 portion.

Use the `no` parameter to undo the tunnel source address.

Command Syntax `tunnel source A.B.C.D no tunnel source`

Parameter

A.B.C.D	IPv4 tunnel source address.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface tunnel 0
(config-if)#tunnel mode gre
(config-if)#tunnel destination 10.10.1.1
(config-if)#tunnel source 10.11.2.1
```

tunnel tos

Use this command to specify a value of Type of Service (TOS) in the tunnel IPv4 encapsulation header.

Use the `no` parameter to make `0` the default value.

Command Syntax `tunnel tos <0-255>`

`no tunnel tos`

Parameter

`<0-255>`	Specify a type of service integer.

Default

The default TOS value is 0.

Command Mode

Interface mode

Examples

```
#configure terminal
(config)#interface tunnel 0
(config-if)#tunnel mode gre
(config-if)#tunnel destination 192.168.10.2
(config-if)#tunnel source 192.168.11.1
(config-if)#tunnel tos 10
```

tunnel ttl

Use this command to specify a value of Time to Live (TTL) in the tunnel IPv4 encapsulation header. Enable the `pathmtu-discovery` before setting the TTL value. However, the first time you set the TTL value, and the `path-mtudiscovery` is not set, the system automatically enables the `path-mtu-discovery`.

Use the `no` parameter to inheriting the underlying physical interface value by default.

Command Syntax `tunnel`

`ttl <1-255> no tunnel`

`ttl <1-255>`

Parameter

`<1-255>`	Specify a Time to Live integer.

Default

By default, physical interface value is inherited.

Command Mode

Interface mode

Example

```
#configure terminal
(config)#interface tunnel 0
(config-if)#tunnel mode gre
(config-if)#tunnel destination 192.168.128.1
(config-if)#tunnel source 192.168.0.1
```

```
(config-if)#tunnel ttl 255
```

© Symanitron Proprietary

CHAPTER 10 Remote Monitoring Commands

This chapter provides an alphabetized reference for each Remote Monitoring (RMON) CLI command. It includes the following commands:

- rmon alarm
- rmon clear
- rmon collection history
- rmon collection stats
- rmon debug
- rmon event
- show rmon alarm
- show rmon event
- show rmon history
- show rmon statistics
- snmp restart rmon

rmon alarm

Use this command to configure alarm parameters, such as, alarm type, thresholds, and corresponding events on crossing the threshold for a particular variable.

Use the `no` form of this command to remove the alarm configuration.

Command Syntax

```
rmon alarm <1-65535> (WORD) interval <1-4294967295> (delta | absolute) rising-threshold
            event <1-65535> falling-threshold event <1-65535> (owner WORD|)
  no rmon alarm <1-65535>
```

Parameters

`<1-65535>`	Alarm entry index value.
`WORD`	Variable Object Identifier (OID) name to be monitored.
`interval`	Polling interval in seconds <1-4294967295>.
`delta`	Alarm sample type of delta.
`absolute`	Alarm sample type of absolute.
`rising-threshold`	Rising threshold value of the alarm entry.
`event`	Event corresponding to the alarm crossing the rising threshold value of the alarm entry <165535>.
`falling-threshold`	Falling threshold value of the alarm entry.
`event`	Event corresponding to the alarm crossing the falling threshold value of the alarm entry <1-65535>.
`owner`	Owner name to identify entry.

Default

No default alarm is created.

Command Mode

Configure mode

Examples

```
#configure terminal
(config)#rmon alarm 229 etherStatsEntry.1.5 interval 50 delta rising-threshold
400 event 70 falling-threshold 600 event 1 owner new
```

rmon clear

Use this command to clear RMON counters.

Command Syntax `rmon clear counters`

Parameters `counters` Clears RMON counters.

Command Mode

Interface mode

Example

```
(config-if)#rmon clear counters
```

rmon collection history

Use this command to configure a history statistics control group. History statistics parameters can be requested buckets, interval and owner name on a particular interface. The number of history statistics buckets, and the interval to collect them, can be specified. The system based on the available memory configures the granted buckets. The granted buckets are same as the requested buckets.

Use the `no` form of this command to remove the history control configuration.

Command Syntax

```
rmon collection history <1-65535> (buckets <1-65535>|)(interval <1-3600>|)
(owner

  WORD|)   no   rmon   collection

history <1-65535>
```

Parameters

`<1-65535>`	Alarm entry index value.
`interval`	Polling interval in seconds <1-4294967295>.
`buckets`	Number of requested buckets <1-65535>.
`owner`	Owner name to identify entry.

Default

No default alarm is created.

Command Mode

Interface mode

Example

```
#configure terminal
(config)#interface eth1
```

```
(config-if)#rmon collection history 200 buckets 500 interval 600 owner
herbert
```

rmon collection stats

Use this command to configure an Ethernet statistics parameter, such as, index and owner name, on a particular interface.

Use the `no` form of this command to remove the collection statistics configuration.

Command Syntax `rmon collection stats <1-65535> (owner WORD|) no rmon collection stats <1-65535>`

Parameters

`<1-65535>` Specify buckets history index <1-65535>. Default is 50. `owner`

Owner name to identify entry.

Default

Ethernet statistics probe is not running.

Command Mode

Interface mode

Example

```
#configure terminal
(config)#interface eth1
(config-if)#rmon collection stats 200 owner herbert
```

rmon debug

Use this command to specify the set of debug options for RMON.

Use the `no` parameter with this command to disable the debugging option.

Command Syntax `rmon debug no rmon debug`

Parameters

None

Command Mode

Exec mode and Privileged Exec mode Example

```
#rmon debug
```

rmon event

Use this command to configure event parameters, such as, event type, description, and the community string corresponding to the trap if the event type is trap. The configured trap community does not take effect as the trap sending is handled by the SNMP daemon.

Use the `no` form of this command to remove the event configuration.

Command Syntax `rmon event <1-65535> (log |)(trap WORD |) (description WORD|) (owner WORD|) no rmon event <1-65535>`

Parameters

`<1-65535>`	Event entry index value.
`log`	Log event type
`trap`	Trap event type
`description`	Event entry description
`owner`	Owner name to identify entry.
`WORD`	Community string corresponding to the trap

Default

No default event is created.

Command Mode

Configure mode

Example

```
#configure terminal
(config)#rmon event 299 log description cond3 owner alfred
```

show rmon alarm

Use this command to display the alarms and threshold configured for the RMON probe.

Command Syntax `show rmon alarm`

Parameters

None

Command Mode

Exec and Privileged Exec modes

Example

```
#show rmon alarm
```

show rmon event

Use this command to display the events configured for the RMON probe.

Command Syntax `show rmon event`

Parameters

None

Command Mode

Exec and Privileged Exec modes

Example

```
#show rmon event
```

show rmon history

Use this command to display the history Ethernet statistics collected on a particular interface.

Command Syntax `show rmon history`

Parameters

None

Command Mode

Exec and Privileged Exec modes

Example

```
#show rmon history
```

show rmon statistics

Use this command to display the Ethernet statistics collected on a particular interface.

Command Syntax `show rmon statistics`

Parameters

None

Command Mode

Exec and Privileged Exec modes

Example

```
#show rmon statistics
```

snmp restart rmon

Use this command to restart SNMP in Remote Monitoring (RMON).

Command Syntax `snmp restart rmon`

Parameters

None

Command Mode

Configure mode

Examples

```
(config)#snmp restart rmon
```

CHAPTER 11 Unicast Reverse Path Forwarding Check

This chapter provides an alphabetized reference for each of the Unicast Reverse Path Forwarding (uRPF) commands. It includes the following commands:

- ip verify unicast source reachable-via
- ipv6 verify unicast source reachable-via

ip verify unicast source reachable-via

Use this command to enable Unicast Reverse Path Forwarding (uRPF) checking on the interface for IPv4. The interface should be a Layer 3 type.

Use the no form of this command to disable uRPF checking.

Command Syntax `ip verify unicast source reachable-via {any [allow-default] | rx} no ip verify unicast source reachable-via`

Parameters `any` Loose mode: source is reachable via any interface; the source IP address for a packet must appear in the routing table

`allow-default`
Allow default route to match when checking source address; otherwise, a default route is not considered in loose mode

`rx` Strict mode: source is reachable via the interface on which the packet was received

Command Mode

Interface mode

Examples

```
(config-if)#ip verify unicast source reachable-via rx
```

```
(config-if)#ip verify unicast source reachable-via any (config-if)#no ip
verify unicast source reachable-via
```


ipv6 verify unicast source reachable-via

Use this command to enable Unicast Reverse Path Forwarding (uRPF) checking on the interface for IPv6. The interface should be a Layer 3 type.

Use the no form of this command to disable uRPF checking.

Command Syntax `ipv6 verify unicast source reachable-via {any [allow-default] | rx} no ipv6 verify unicast source reachable-via`

Parameters `any` Loose mode: source is reachable via any interface; the source IP address for a packet must appear in the routing table

`allow-default` Allow default route to match when checking source address; otherwise, a default route is not considered in loose mode

`rx` Strict mode: source is reachable via the interface on which the packet was received

Command Mode

Interface mode

Examples

```
(config-if)#ipv6 verify unicast source reachable-via rx (config-
if)#ipv6 verify unicast source reachable-via any (config-if)#no

ipv6 verify unicast source reachable-via
```

© Symanitron Proprietary

CHAPTER 12 Internet Protocol Security Commands

This chapter is a reference for the Internet Protocol Security (IPsec) commands.

- address
- authentication
- clear crypto isakmp
- clear crypto sa
- clear crypto sa entry
- clear crypto sa map
- clear crypto sa peer
- crypto ipsec security-association lifetime
- crypto ipsec transform-set
- crypto isakmp enable
- crypto isakmp policy
- crypto key generate rsa
- crypto map (Configure Mode)
- crypto map (Interface Mode)
- crypto map local-address
- encryption
- group
- hash
- ike-version
- ipv6-address
- lifetime
- match address
- mode
- peer
- peer public-key
- psk key
- rsa key
- set ipv6 peer
- set peer
- set security-association lifetime

- set session-key
- set transform-set
- show crypto ipsec transform-set
- show crypto isakmp policy
- show crypto-map interface
- show ipsec status

address

Use this command to set the IPv4 address of an peer in an IKE (Internet Key Exchange) policy created with the crypto isakmp policy command.

Use the `no` form of this command to remove a peer address.

Command Syntax

```
address A.B.C.D no
address A.B.C.D
```

Parameters

`A.B.C.D`	IPv4 address.

Command Mode

ISAKMP policy configuration mode

Example

```
(config)#crypto isakmp policy 1
(config-isakmp)#address 10.1.1.2
```

authentication

Use this command to set the authentication method in an IKE (Internet Key Exchange) policy created with the crypto isakmp policy command.

Use the `no` form of this command to reset the authentication method to its default (pre-share).

Command Syntax

```
authentication  pre-share
no authentication
```

Parameters `pre-share` Preshared keys specified manually

Defaults

Pre-share

Command Mode

ISAKMP policy configuration mode

Example

```
(config)#crypto isakmp policy 1
(config-isakmp)#authentication pre-share
```

clear crypto isakmp

Use this command to clear active IKE (Internet Key Exchange) connections.

Command Syntax `clear crypto isakmp`

Parameters

None

Command Mode

Exec mode

Example

```
#clear crypto isakmp
```

clear crypto sa

Use this command to clear and reinitialize (if appropriate) IPSec security associations at the router. If the security associations are manually established, the security associations are deleted and reinitialized.

If you make configuration changes to security associations, the changes do not apply to existing security associations but to negotiations for future security associations. Use this command to restart all security associations so they use the most recent configuration settings. For manually established security associations, if you make changes that affect security associations you must give this command before the changes take effect.

Command Syntax

```
clear crypto sa
```

Parameters

None

Command Mode

Exec mode

Example

```
#clear crypto sa
```

clear crypto sa entry

Use this command to delete IPSec security associations for a given IP address, protocol, and security parameter index.

If you make configuration changes to security associations, these changes do not apply to existing security associations but to negotiations for future security associations. Use this command to restart all security associations so they use the most recent configuration settings. For manually established security associations, if you make changes that affect security associations you must give this command before the changes take effect.

Command Syntax `clear crypto sa entry destination-address A.B.C.D protocol (ah|esp) spi SPI`

Parameters

`A.B.C.D`	Destination address
`ah`	Authentication Header protocol
`esp`	Encapsulating Security Payload protocol
`SPI`	Security parameter index (0-4096)

Command Mode

Exec mode

Example

```
(config)#clear crypto sa entry destination-address 10.1.1.2 protocol esp
spi 100
```

clear crypto sa map

Use this command to delete IPSec security associations for a given name.

If you make configuration changes to security associations, these changes do not apply to existing security associations but to negotiations for future security associations. Use this command to restart all security associations so they use the most recent configuration settings. For manually established security associations, if you make changes that affect security associations you must give this command before the changes take effect.

Command Syntax `clear crypto sa map MAP_NAME`

Parameter

`MAP_NAME`	Name of IP security associations (maximum length 127).

Command Mode

Exec mode

Example

```
(config)#clear crypto sa map New-map
```

clear crypto sa peer

Use this command to delete IPSec security associations for a given peer.

If you make configuration changes to security associations, these changes do not apply to existing security associations but to negotiations for future security associations. Use this command to restart all security associations so they use the most current configuration settings. In the case of manually established security associations, if you make changes that affect security associations you must give this command before the changes take effect.

Command Syntax `clear crypto sa ipv4 peer A.B.C.D clear crypto sa ipv6 peer X:X::X:X`

Parameter

`A.B.C.D`	IPv4 address of the peer.
`X:X::X:X`	IPv4 address of the peer.

Command Mode

Exec mode

Example

```
(config)#clear crypto sa ipv4 peer 123.12.12.123
```

crypto ipsec security-association lifetime

Use this command to change global lifetime values used when negotiating IPSec security associations. IPSec security associations use shared secret keys. These keys and their security associations time out together.

Assuming that a crypto map entry does not have lifetime values configured, when the router requests new security associations during negotiation, it specifies its global lifetime value in the request to the peer. When the router receives a negotiation request from the peer, it uses the smaller of the lifetime value proposed by the peer or the locally configured lifetime as the lifetime of the new security associations.

If you change a global lifetime, the change is only applied when the crypto map entry does not have a lifetime value specified. The change is not applied to existing security associations, but is used in future negotiations to establish new security associations. If you want the new settings to take effect sooner, you can clear all or part of the security association database by using the clear crypto sa command. The lifetime values are ignored for manually established security associations.

Use the `no` form of the command to reset the lifetime to its default value (3600 seconds).

Command Syntax `crypto ipsec security-association lifetime seconds LIFETIME no crypto ipsec security-association lifetime seconds`

Parameters

`LIFETIME`	Duration of the security association before expiring (120-2592000 seconds).

Default

3600 seconds (one hour)

Command Mode

Configure mode

Example

```
(config)#crypto ipsec security-association lifetime seconds 2000
```

crypto ipsec transform-set

Use this command to configure a transform set that defines protocols and algorithm settings to apply to IPSec protected traffic.

During security association negotiation, peers use a transform set when protecting data flows. Multiple sets can be configured, with one or more specified in a crypto map entry. When IKE is not used to establish security associations, one transform set must be used. The transform set is not negotiated.

A transform set specifies one or two IPSec security protocols (either ESP or AH or both) and algorithms. If one or more transforms are specified in this command for an existing transform set, the specified transforms replace the existing transforms.

If you change a transform set definition, the change is only applied to crypto map entries that reference the transform set. The change is not applied to existing security associations, but is used in future negotiations to establish new security associations. If you want the new settings to take effect sooner, you can clear all or part of the security association database using the clear crypto sa command. Use the `no` form of the command to delete a transform set.

Command Syntax `crypto ipsec transform-set NAME ah (none|ah-md5|ah-sha1) crypto ipsec transform-set NAME esp-auth (none|esp-md5|esp-sha1) esp-enc (esp-null|esp-3des|esp-aes|esp-aes192|esp-aes256|esp-blf|esp-blf192|esp-blf256|espcast)`

`no crypto ipsec transform-set NAME`

Parameters

`NAME`	Name of the transform set.
`ah`	Authentication Header protocol
`none`	No authentication.
`ah-md5`	Authentication Header with Message Digest 5 (MD5) Hashed Message Authentication Code (HMAC) variant.
`ah-sha1`	Authentication Header with Secure Hash Algorithm 1 (SHA-1) Hashed Message Authentication Code (HMAC) variant.
`esp-auth`	Encapsulating Security Payload authentication protocol
`none`	No authentication.
`esp-md5`	Encapsulating Security Payload with Message Digest 5 (MD5) Hashed Message Authentication Code (HMAC) variant.
`esp-sha1`	Encapsulating Security Payload with Secure Hash Algorithm 1 (SHA-1) Hashed Message Authentication Code (HMAC) variant.
`esp-enc`	Encapsulating Security Payload encryption protocol
`esp-null`	Encapsulating Security Payload null encryption.
`esp-3des`	Encapsulating Security Payload with 168-bit DES encryption (3DES or Triple DES).
`esp-aes`	Alternative AES.
`esp-aes192`	Alternative AES192.
`esp-aes256`	Alternative AES256.

`esp-blf` Alternative Blowfish. `esp-blf192` Alternative Blowfish192. `esp-blf256` Alternative Blowfish256. `esp-cast` Alternative Cast (IKEv1 not supported).

Command Mode

Configure mode

Example

```
(config)#crypto ipsec transform-set TS1 esp-auth esp-md5 esp-enc esp-
3des (config-transform)#
```

crypto isakmp enable

Use this command to globally enable IKE (Internet Key Exchange) for a peer router.

If you do not want IKE to be used in your IPSec implementation, disable IKE at all IPSec peers. If you disable IKE at one peer, you must disable it at all IPSec peers.

Use the `no` form of this command to disable IKE at the peer.

Command Syntax `crypto isakmp enable`

`no crypto isakmp enable`

Parameters

None

Default

IKE is disabled by default. IKE does not have to be enabled for individual interfaces, but is enabled globally for all interfaces at the router.

Command Mode

ISAKMP policy configuration mode

Example

```
(config)#crypto isakmp policy 1
(config-isakmp)#crypto isakmp enable
```

crypto isakmp policy

Use this command to define an IKE (Internet Key Exchange) policy and enter ISAKMP (Internet Security Association and Key Management Protocol) policy configuration mode.

IKE policies define a set of parameters to use during the IKE negotiation. These parameters are used to create IKE security associations.

You can configure multiple IKE policies for each peer participating in IPSec. When the IKE negotiation begins, it tries to find a common policy configured on both peers, starting with the highest priority policies as specified on the remote peer.

Use the `no` form of this command to delete an IKE policy.

Command Syntax `crypto isakmp policy`

`PRIORITY no crypto isakmp policy`

`PRIORITY`

Parameter

`PRIORITY`	Identifier/priority of the policy (<1-10000>).

Command Mode

Configure mode

Example

```
(config)#crypto isakmp policy 10
(config-isakmp)#
```

crypto key generate rsa

Use this command to generate a local RSA (Rivest-Shamir-Adleman) key.

Note: All keys are suffixed by `*.der`.

Use the `no` form of this command to delete a local RSA key.

Command Syntax `crypto key generate rsa KEYLABEL dn DNNAME (length <360-2048>|) no crypto key generate rsa KEYLABEL`

Parameters

`KEYLABEL`	Local key identifier for RSA key
`DNNAME`	Distinguished name of the RSA key-pair. Use the same name on the remote peer.
`<360-2048>`	Key length in bits (default 2048).

Command Mode

Configure mode

Example

```
(config)#crypto key generate rsa k1 dn moon
```

crypto map (Configure Mode)

Use this command to create or change a crypto map entry and enter crypto map configuration mode.

Once a crypto map entry has been created, you cannot change its setting at the global configuration level because these parameters determine which of the configuration commands are valid at the crypto map level. For example, once a map entry has been created as `ipsec-isakmp`, you cannot change it to `ipsec-manual`; you must delete and reenter the map entry.

A single crypto map set can contain a combination of `ipsec-isakmp` and `ipsec-manual` crypto map entries.

After you define crypto map entries, you can assign the crypto map set to interfaces using the crypto map (Interface Mode) command.

Use the `no` form of this command to delete a crypto map entry or set.

Command Syntax `crypto map MAP-NAME SEQ-NUM`

`ipsec-manual crypto map MAP-NAME SEQ-NUM`

`ipsec-isakmp no crypto map MAP-NAME`

`(SEQ-NUM|)`

Parameters

`MAP-NAME`	Name of the crypto map set (maximum length 127).
`SEQ-NUM`	Number of the crypto map entry <1-65535>.
`ipsec-manual`	Do not use IKE to establish IPSec security associations. `ipsec-isakmp` Use IKE to establish the IPSec security associations.

Command Mode

Configure mode

Example

```
(config)#crypto map MAP1 5 ipsec-isakmp
(config-crypto)#
```

crypto map (Interface Mode)

Use this command to apply a crypto map set to an interface.

Only one crypto map set can be assigned to an interface. If multiple crypto map entries have the same map name but a different `SEQ-NUM`, they are considered to be part of the same set and all are applied to the interface. The crypto map entry with the lowest `SEQ-NUM` is considered the highest priority and is evaluated first.

Use the `no` form of this command to remove a crypto map set from an interface.

Command Syntax `crypto map`

`MAP-NAME no crypto map`

`MAP-NAME`

Parameter

`MAP-NAME`Name of the crypto map set (maximum length 127).

Command Mode

Interface mode

Example

```
(config)#interface eth1
(config-if)#crypto map MAP1
```

crypto map local-address

Use this command to specify an interface to use for this crypto map to identify itself to peers.

If you apply the same crypto map to two interfaces and do not use this command, two separate security associations (with different local IP addresses) could be established to the same peer for similar traffic. If you use the second interface as redundant to the first interface, it might be preferable to have a single security association (with a single local IP address) created for traffic sharing the two interfaces. Having a single security association decreases overhead and makes administration simpler.

Use the `no` form of this command to remove the configuration.

Command Syntax `crypto map MAP-NAME local-address IFNAME no crypto map MAP-NAME local-address`

Parameters

`MAP-NAME`	Name of the crypto map set (maximum length 127).
`IFNAME`	Interface name.

Command Mode

Configure mode

Example

```
(config)#crypto map MAP1 local-address eth1
```

encryption

Use this command to set the encryption algorithm in an IKE (Internet Key Exchange) policy created with the crypto isakmp policy command.

Use the `no` form of this command to set the encryption algorithm to its default value (3DES).

Command Syntax `encryption (aes|3des) no encryption`

Parameters

`aes`	Use 56-bit AES-CBC as the encryption algorithm.
`3des`	Use 168-bit DES (3DES or triple DES) as the encryption algorithm.

Default

3DES

Command Mode

ISAKMP policy configuration mode

Example

```
(config)#crypto isakmp policy 1
(config-isakmp)#encryption 3des
```

group

Use this command to set a Diffie-Hellman group identifier (length of the modulus) in an IKE (Internet Key Exchange) policy created with the crypto isakmp policy command.

Use the `no` form of this command to set the group identifier to its default value (group 14: 2048 bits).

Command Syntax

```
group (1|2|14)
no group
```

Parameters

`1`	Group 1: 768 bits (modp768)
`2`	Group 2: 1024 bits (modp1024)
`14`	Group 14: 2048 bits (modp2048) (default)

Defaults

Group 14: 2048 bits (modp2048)

Command Mode

ISAKMP policy configuration mode

Example

```
(config)#crypto isakmp policy 1
(config-isakmp)#group 1
```

hash

Use this command to specify the hash algorithm in an IKE (Internet Key Exchange) policy created with the crypto isakmp policy command.

Use the `no` form of this command to set the hash algorithm to its default (SHA-1).

Command Syntax

```
hash (md5|sha)
no hash
```

Parameters `md5` Message Digest 5 (MD5) Hashed Message Authentication Code (HMAC) variant `sha`

Secure Hash Algorithm 1 (SHA-1) Hashed Message Authentication Code (HMAC) variant

Default

SHA-1 hash algorithm.

Command Mode

ISAKMP policy configuration mode

Example

```
(config)#crypto isakmp policy 1
(config-isakmp)#hash md5
```

ike-version

Use this command to set the version of IKE (Internet Key Exchange). Use the `no` form of this command to set the default (version 1 and 2).

Command Syntax `ike-version (1|2|both) no ike-version`

Parameters

`1`	IKE version 1
`2`	IKE version 2
`both`	IKE version 1 and 2 (default)

Default

SHA-1 hash algorithm.

Command Mode

ISAKMP policy configuration mode

Example

```
(config)#crypto isakmp policy 1
(config-isakmp)#ike-version 2
```

ipv6-address

Use this command to set the IP address of an peer in an IKE (Internet Key Exchange) policy created with the crypto isakmp policy command.

Use the `no` form of this command to remove a peer address.

Command Syntax `ipv6-address`

`X:X::X:X no ipv6-address`

`X:X::X:X`

Parameters

`X:X::X:X`	IPv6 address.

Command Mode

ISAKMP policy configuration mode

Example

```
(config)#crypto isakmp policy 1
(config-isakmp)#ipv6-address 2001:db8:0:1
```

lifetime

Use this command to set the lifetime of an IKE (Internet Key Exchange) security association.

When IKE begins negotiations, it first agrees upon the security parameters for its own session. The agreed-upon parameters are then referenced by an security association at each peer. The security association is retained by each peer until the security association's lifetime expires. Before a security association expires, it can be reused by subsequent IKE negotiations, which can save time when setting up new IPSec security associations. New IPSec security associations are negotiated before current IPSec security associations expire.

To save setup time for IPSec, configure a longer IKE security association lifetime. However, shorter lifetimes limit the exposure to attackers of this security association. The longer an security association is used, the more encrypted traffic can be gathered by an attacker and possibly used in an attack.

Note: When your local peer starts an IKE negotiation with a remote peer, an IKE policy can be selected only if the lifetime of the remote peer's policy is longer than or equal to the lifetime of the local peer's policy. Then, if the lifetimes are not equal, the shorter lifetime is selected. To restate this behavior: If the two peer's policies' lifetimes are not the same, the initiating peer's lifetime must be shorter and the responding peer's lifetime must be longer, and the shorter lifetime is used.

Use the `no` form of this command to reset the SA lifetime to its default value (10,800 seconds).

Command Syntax

```
lifetime
LIFETIME        no
lifetime
```

Parameters

`LIFETIME`	Duration of a security association before expiring (<60-86400> seconds).

Defaults

10,800 seconds

Command Mode

ISAKMP policy configuration mode

Example

```
(config)#crypto isakmp policy 1
(config-isakmp)#lifetime 20000
```

match address

Use this command to match an access list name for traffic which is protected by IPSec.

Use the `no` form of this command to remove an ACL from IPsec protection.

Command Syntax `match address ACCESSLIST-ID match ipv6-address ACCESSLIST-NAME no match address ACCESSLIST-ID no match ipv6-address ACCESSLIST-NAM`

Parameter

ACCESSLIST-ID

ACCESSLIST-NAME

Access-list name.

Command Mode

Crypto map configuration mode

Example

```
(config)#crypto map MAP1 5 ipsec-isakmp
(config-crypto)#match address ACL-25
```

mode

Use this command to set the mode of negotiation for a transform set.

Use the `no` form of this command to reset the mode to its default (tunnel).

Command Syntax `mode`

```
(tunnel|transport) no mode
```

Parameter

`tunnel`	The entire original IP packet is protected (default).
`transport`	The payload (data) of the original IP packet is protected.

Defaults

Tunnel mode

Command Mode

Transform set mode

Example

```
(config)#crypto ipsec transform set t1 esp-auth esp-sha1 esp-enc espaes192
(config-transform)#mode transport
```

peer

Use this command to set the IPSec peer name.

Use the `no` form of this command to remove the peer name.

Command Syntax `peer`

```
NAME   no   peer
NAME
```

Parameters

`NAME`	Peer name. This name should be same as the `DNNAME` parameter in the crypto key generate rsa command on the remote peer during RSA key generation.

Command Mode

ISAKMP policy configuration mode

Example

```
(config)#crypto isakmp policy 1
(config-isakmp)#peer SUN
```

peer public-key

Use this command to set an RSA (Rivest-Shamir-Adleman) public key for the peer. You must configure this key when you specify authentication as `rsa-sig` in an IKE policy.

This command enters ISAKMP public key mode, where you enter the public key from the RSA peer. You can enter up to four “chunks” of key data separated by spaces per line, on multiple lines. Use the `exit-key` command to terminate public key mode. The strings you enter are concatenated into a single key string.

Use the `no` form of this command to remove a public key.

Command Syntax `peer`

```
public-key no peer
public-key
```

Parameters

None

Command Mode

ISAKMP policy configuration mode

Example

```
(config)#crypto isakmp policy 1 (config-
isakmp)#peer public-key (config-isakmp-
pubkey)#abcd 1w22w ssss2 sskk3 (config-
isakmp-pubkey)#ddjjj 33 ddddd22 kkff (config-
isakmp-pubkey)#ffff eeqq (config-isakmp-
pubkey)#exit-key (config-isakmp)#
```

psk key

Use this command to configure a preshared authentication key. You must configure this key when you specify preshared keys in an IKE policy and at both peers.

If an IKE policy includes preshared keys as the authentication method, these preshared keys must be configured at both peers. Otherwise, the policy cannot be used and the policy is not submitted for matching by the IKE process.

Use the `no` form of this command to remove a preshared authentication key.

Command Syntax `psk`

```
key  KEY  no  psk
key KEY
```

Parameters

`KEY`	Preshared key; any combination of alphanumeric characters up to 128 bytes.

Command Mode

ISAKMP policy configuration mode

Example

```
(config)#crypto isakmp policy 1
(config-isakmp)#psk key myKey123
```

rsa key

Use this command to configure a local RSA (Rivest-Shamir-Adleman) key. You must configure this key when you specify authentication as `rsa-sig` in an IKE policy.

Use the `no` form of this command to remove a local RSA key.

Command Syntax `rsa`

```
key LABEL no rsa
key LABEL
```

Parameters

`LABEL`	Local RSA key identifier. This should be same as specified when generating a local RSA key.

Command Mode

ISAKMP policy configuration mode

Example

```
(config)#crypto key generate rsa k1 dn moon
(config)#crypto isakmp policy 1 (config-
isakmp)#authentication rsa-sig (config-
isakmp)#rsa key k1
```

set ipv6 peer

Use this command to specify an IPSec IPv6 peer in a crypto map entry created by the crypto map (Configure Mode) command.

For `ipsec-isakmp` crypto map entries, you can specify multiple peers by repeating this command. The peer to which packets are actually sent is determined by the last peer from which the router received either traffic or a negotiation request for a given data flow. If the attempt fails with the first peer, IKE tries the next peer on the crypto map list.

For `ipsec-manual` crypto map entries, you can only specify one IPSec peer per crypto map. If you want to change the peer, you must first delete the old peer and then specify the new peer.

Use the `no` form of this command to remove an IPSec peer from a crypto map entry.

Command Syntax `set ipv6 peer`

`X:X::X:X no set ipv6 peer`

`X:X::X:X`

Parameters

`X:X::X:X` IPv6 address.

Command Mode

Crypto map configuration mode

Example

```
(config)#crypto map MAP1 5 ipsec-isakmp (config-
crypto)#set ipv6 peer fe80::200:f8ff:fe21:67cf
```

set peer

Use this command to specify an IPSec IPv4 peer in a crypto map entry created by the crypto map (Configure Mode) command.

For `ipsec-isakmp` crypto map entries, you can specify multiple peers by repeating this command. The peer to which packets are actually sent is determined by the last peer from which the router received either traffic or a negotiation request for a given data flow. If the attempt fails with the first peer, IKE tries the next peer on the crypto map list.

For `ipsec-manual` crypto map entries, you can only specify one IPSec peer per crypto map. If you want to change the peer, you must first delete the old peer and then specify the new peer.

Use the `no` form of this command to remove an IPSec peer from a crypto map entry.

Command Syntax `set`

`peer A.B.C.D no set`

`peer A.B.C.D`

Parameters

`A.B.C.D` IPv4 address.

Command Mode

Crypto map configuration mode

Example

```
(config)#crypto map MAP1 5 ipsec-isakmp
(config-crypto)#set peer 1.1.1.1
```

set security-association lifetime

Use this command to override the global lifetime value for a crypto map entry created by the crypto map (Configure Mode) command. The global lifetime value is used when negotiating IPSec security associations.

This command is only available for `ipsec-isakmp` crypto map entries and dynamic crypto map entries.

IPSec security associations use shared secret keys. These keys and their security associations time out together.

Assuming that a crypto map entry has lifetime values configured, when the router requests new security associations during negotiation, it specifies its crypto map lifetime value in the request to the peer. When the router receives a negotiation request from the peer, it uses the smaller of the lifetime value proposed by the peer or the locally configured lifetime value as the lifetime of the new security associations.

Use the `no` form of this command to reset a crypto map entry's lifetime value to the global value.

Command Syntax `set security-association lifetime seconds LIFETIME` `no set security-association lifetime seconds`

Parameters

`LIFETIME`	Duration of a security association before expiring (<120-2592000> seconds)

Defaults

The crypto map's security associations are negotiated according to the global lifetimes.

Command Mode

Crypto map configuration mode

Example

```
(config)#crypto map MAP1 5 ipsec-isakmp (config-
crypto)#set security-association lifetime 20000
```

set session-key

Use this command to define IPSec keys for security associations with `ipsec-manual` crypto map entries created by the crypto map (Configure Mode) command.

If the crypto ipsec transform-set command specifies an AH protocol, an ESP encryption protocol, or an ESP authentication protocol, you must define IPSec keys for both inbound and outbound traffic with this command.

When you define multiple IPSec session keys within a single crypto map, you can assign the same security parameter index (SPI) number to all the keys. The SPI identifies the security association used with the crypto map. You must coordinate SPI assignment with your peer's operator, making certain that the same SPI is not used more than once for the same destination address/protocol combination.

Security associations created with this command do not expire (unlike security associations established via IKE). Session keys at one peer must match the session keys at the remote peer. If you change a session key, the security association using the key is deleted and reinitialized.

For `ipsec-isakmp` crypto map entries, the security associations with their corresponding keys are automatically established via the IKE negotiation.

Use the `no` form of this command to remove a session key from a crypto map entry.

Command Syntax `set session-key (inbound|outbound) ah SPI`

`HEX-KEY-DATA`

`set session-key (inbound|outbound) esp SPI cipher HEX-KEY-DATA authenticator HEX_KEY_DATA no set session-key`

`(inbound|outbound) ah no set session-key`

`(inbound|outbound) esp`

Parameters

`inbound` Inbound IPSec session key.

`outbound` Outbound IPSec session key.

`ah` Session key for the Authentication Header protocol.

`SPI` Security parameter index that uniquely identifies a security association (0-4096).

`HEX-KEY-DATA`

Session key in hexadecimal format. Use an appropriate session key length for the encryption/authentication algorithm:

AES: 128 bits

AES-192: 192 bits

AES-256: 256 bits

3des: 192 bits blf:

32-256 bits cast:

96 or 128 bits

SHA1/MD5: 32-128 bits

`esp` Session key for the Encapsulating Security Payload protocol.

`SPI` Security parameter index that uniquely identifies a security association (0-4096).

`cipher` Encryption key.

`HEX-KEY-DATA`

Encryption key in hexadecimal format (maximum length 128).

`authenticator` Authentication key. `HEX-KEY-DATA`

Authentication key in hexadecimal format (maximum length 32).

Command Mode

Crypto map configuration mode

Example

```
(config)#crypto map MAP2 10 ipsec-manual (config-
crypto)#set session-key inbound ah SPI cipher
```

set transform-set

Use this command to specify the transform sets to use with a crypto map entry created by the crypto map (Configure Mode) command.

For an `ipsec-isakmp` crypto map entry, you can list multiple transform sets with this command. List the higher priority transform sets first. If the local router starts the negotiation, the transform sets are presented to the peer in the order specified in the crypto map entry. If the peer starts the negotiation, the local router accepts the first transform set that matches one of the transform sets specified in the crypto map entry.

The first matching transform set that is found at both peers is used for the security association. If no match is found, IPSec does not establish a security association. The traffic is dropped because there is no security association to protect the traffic.

For an `ipsec-manual` crypto map entry, you can specify only one transform set. If the transform set does not match the transform in the remote peer's crypto map, the two peers fail to communicate because they are using different rules to process the traffic.

To change the list of transform sets, specify a new list of transform sets to replace the old list. This change is only applied to crypto map entries that reference this transform set. The change is not applied to existing security associations, but is used in future negotiations to establish new security associations. If you want the new settings to take effect sooner, clear all or part of the security association database by using the clear crypto sa command.

Any transform sets included in a crypto map must have been defined using the crypto ipsec transform-set command.

Use the `no` form of this command to remove all transform sets from a crypto map entry.

Command

Synta

x `set trans form-set NAME`

`no set trans`

```
form-
set
NAME
```

Parameter

NAME	Name of the crypto map set (maximum length 127).

Command Mode

Crypto map configuration mode

Example

```
(config)#crypto map MAP1 5 ipsec-isakmp
(config-crypto)#set transform-set new
```

show crypto ipsec transform-set

Use this command to display one or all transform sets.

Command Syntax `show crypto ipsec transform-set (NAME|)`

Parameter

NAME	Name of the transform set (maximum length 127)

Command Mode

Exec mode

Example

```
#show crypto ipsec transform-set t1
Transform set t1
  Mode is Tunnel
  Algorithm esp-aes esp-md5
```

show crypto isakmp policy

Use this command to display the parameters for all IKE (Internet Key Exchange) policies.

Command Syntax `show crypto isakmp policy`

Parameters

None

Command Mode

Exec mode

Example

```
#show  crypto  isakmp  policy  Protection
suite priority 1
  encryption algorithm: 3DES - Data Encryption Standard
hash algorithm: Message Digest 5    authentication method:
preshared Key   Diffie-Hellman Group: #14 (modp2048)
lifetime: 15000
psk key: v+NkxY9LLZvwj4qCC2o/gGrWDF2d21jL
peer address: 11.11.11.2
```

show crypto-map interface

Use this command to display the crypto map configuration for an interface.

Command Syntax `show crypto-map interface IFNAME`

Parameter

`IFNAME`	Interface name.

Command Mode

Exec mode

Example

```
#show crypto-map interface p7p1
Interface p7p1
Crypto-map MAP1
Crypto-spi 0
Crypto-access-list-name
Crypto-Transform set t1
Crypto-map peer: 11.11.11.2
```

show ipsec status

Use this command to display the status of IPsec.

Command

Syntax

```
show
ipsec
status
```

Parameter

None

Command Mode

Exec mode

Example

```
#show ipsec status
Security Associations (1 up, 0 connecting):
map1-1[1]: ESTABLISHED 5 minutes ago,
11.11.11.1[11.11.11.1]...11.11.11.2[11.11.11.
2]
       map1-1{6}: INSTALLED, TUNNEL, ESP SPIs: c492556c_i
ccf5790f_o       map1-1{6}: 11.11.11.1/32 === 11.11.11.2/32
       map1-1{6}: INSTALLED, TUNNEL, ESP SPIs: cb43a379_i
cedc90fc_o       map1-1{6}: 11.11.11.1/32 === 11.11.11.2/32
```

Chassis Monitoring Module Command Reference

Contents

This document contains these chapters:

- Chapter 1, *Chassis Management Module Commands*
- Chapter 2, *Digital Diagnostic Monitoring Commands*

© Symanitron

Chassis Monitoring Module Command Reference

CHAPTER 1 Chassis Management Module Commands

This chapter provides a description, syntax, and examples of CMM feature commands:

- debug cmm
- locator led
- show hardware-information
- show system-information

You can retrieve the same set of information through SNMP that these commands display. This MIB is defined in `CMMCHASSIS-MIB.txt`:

Symanitron. enterprise identifier	36673
Chassis MIB identifier	100

The MIB definition is available at:

debug cmm

Use this command to enable or disable debugging for CMM.

Command Syntax `debug cmm (enable|disable)`

Parameters

`enable` Enable debugging. `disable` Disable debugging.

Default

By default, debug command is disabled.

Command Mode

Configuration mode and exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#debug cmm enable
(config)#debug cmm disable
```

locator led

Use this command to turn on the locator LED.

Use the no form of this command to turn off the locator LED.

Command Syntax `locator-led on no locator-led`

Parameters

None

Default

By default, locator LED is turned off.

Command Mode

Configuration mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#locator-led on
(config)#no locator-led
```

show hardware-information

Use this command to display hardware information.

Command Syntax `show hardware-information (memory|fan|temperature|led|power|transceiver|all)` **Parameter**

`all`	Hardware details of all modules.
`fan`	Fan status of the boards.
`led`	LED status of the boards.
`memory`	Memory information of the boards.
`power`	PSU information.
`temperature`	Temperature sensor information of the boards.
`transceiver`	Transceiver presence status and supported list of transceivers.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show hardware-information all
-------------------------------------------------------
                RAM INFORMATION
-------------------------------------------------------

Total                                    : 7989 MBytes
Used                                     : 870 MBytes
Free                                     : 7119 MBytes
Shared                                   : 0 MBytes
Buffers                                  : 152 MBytes
Total Swap                               : 0 MBytes
Free Swap                                : 0 MBytes
Current Processes                        : 165
Total High Memory                        : 0 MBytes
Available High Memory                    : 0 MBytes
Unit Size                                : 1 Bytes

-------------------------------------------------------
                HARD DISK INFORMATION
-------------------------------------------------------

    Serial Number                          : B06150190009000000FC
Model Number                             : 16GB SATA Flash Drive
Firmware Revision                        : SFDDA01C16GB SATA Flash Drive
Cylinders                                : 16383
Heads                                    : 16
Sectors                                  : 31277232
```

```
Unformatted Bytes/Track                  : 0
Unformatted Bytes/Sector                 : 0
Revision No                              : 496.0
Total Size                               : 14.9 GB

-----------------------------------------------
FAN TRAY             FAN                  RPM
-----------------------------------------------
1                    1                    7021
1                    2                    7021
2                    1                    7021
2                    2                    7021
3                    1                    7072
3                    2                    7021

Board Temp Sensors Temperature
-------------------------------------------------------------------------------
SENSOR TYPE                                CURRENT TEMP         OPERATING
RANGE
                                           (Degree C)           (Degree C)
-------------------------------------------------------------------------------
Trident2                                    29.0                <0 - 75>
Nic                                         22.0                <0 - 70>
Ambient                                     23.0                <0 - 75>

BCM Chip Internal Temperature
-----------------------------------------------------
TEMP MONITOR         CURRENT TEMP          PEAK TEMP
                     (Degree C)            (Degree C)
-----------------------------------------------------
0                     41.1                 42.2
1                     42.2                 43.3
2                     40.6                 41.7
3                     40.6                 41.7
4                     40.0                 41.1
5                     40.6                 41.1
6                     39.5                 40.6
7                     39.5                 40.6
Average Current Temperature: 40.5C

-----------------------------------------------------
                System Power Information
-----------------------------------------------------
VCC 5V POWER RAIL                        : GOOD
VCC 3.3V POWER RAIL                      : GOOD
VCC 1.05V POWER RAIL                     : GOOD
VCC 1.5V POWER RAIL                      : FAIL
VCC 1.8V POWER RAIL                      : FAIL
MAC 1V POWER RAIL                        : GOOD
MAC AVS 1V POWER RAIL                    : GOOD
POWER VDDR                               : GOOD
3.3V POWER RAIL                          : FAIL
```

```
1.8V POWER RAIL                          : FAIL
1.05V POWER RAIL                         : GOOD
1.5V POWER RAIL                          : GOOD
VCC POWER RAIL                           : GOOD
1.5V SB POWER RAIL                       : FAIL
MAIN BOARD POWER RAIL                    : GOOD
HOT SWAP1 POWER RAIL                     : GOOD
HOT SWAP2 POWER RAIL                     : GOOD
CMM_PS1_12V_PG                           : FAIL
CMM_PS2_12V_PG                           : GOOD
```

PSU	VOLT-IN (Volt)	VOLT-OUT (Volt)	CURR-IN (Ampere)	CURR-OUT (Ampere)	PWR-IN (Watt)	PWR-OUT (Watt)	TEMP-1 (Celsius)	TEMP-2 (Celsius)	FAN-1 (Rpm)	FAN-2 (Rpm)
Max						460.00				
2	118.25	11.92	0.83	7.25	97.75	86.38	30.50	29.00	2040.00	NA

```
-------------------------------------------------
LED              STATE               DESCRIPTION
-------------------------------------------------
POWER            BLINKING YELLOW     Power Supply Failed
FAN TRAY 1       GREEN               Normal
FAN TRAY 2       GREEN               Normal
FAN TRAY 3       GREEN               Normal
SYSTEM           GREEN               Normal
MASTER           GREEN               Unit in Master mode
LOCATOR          OFF
FRONT FAN        GREEN               Fan is Normal

-----------------------------------------------------
           Transceiver DDM support list
-----------------------------------------------------
Type                        :QSFP
Vendor Name                 :AVAGO
Vendor Part Number          :AFBR-79E4Z
DDM Supported               :Yes


----------------------------------------
PORT NO    TYPE       STATUS
----------------------------------------
1          QSFP       Not Present
2          QSFP       Present
3          QSFP       Not Present
4          QSFP       Present
5          QSFP       Not Present
6          QSFP       Present
7          QSFP       Not Present
8          QSFP       Present
9          QSFP       Present
10         QSFP       Not Present
11         QSFP       Present
12         QSFP       Not Present
13         QSFP       Not Present
```

```
14          QSFP        Not Present
15          QSFP        Not Present
16          QSFP        Not Present
17          QSFP        Not Present
18          QSFP        Not Present
19          QSFP        Not Present
20          QSFP        Not Present
21          QSFP        Present
22          QSFP        Present
23          QSFP        Not Present
24          QSFP        Not Present
25          QSFP        Not Present
26          QSFP        Not Present
27          QSFP        Not Present
28          QSFP        Present
29          QSFP        Not Present
30          QSFP        Present
31          QSFP        Not Present
32          QSFP        Present
```

Table 1-60 explains the show command output fields.

Table 1-60: show hardware-information all output

Entry	Description
Ram Information	Displays the used memory, free memory, shared, buffers, total swap, and free swap memory.
Hard Disk Information	Displays hard drive serial number, model, firmware revision, cylinders, heads, and sectors, as well as revision number and total size.
Fans	Displays the fan tray numbers, numbers of fans per tray, and their speed in RPM.
Board Temp Sensors Temperature	Displays sensor type, current temperature, and operating range.
BCM Chip Internal Temperature	Displays broadcom chips current internal temperature, Operating range and average temperature.
System Power Information	Displays system power Information. Shows Voltage on all rails, and whether the power is up or has failed.
PSU	Show main power supply statistics – Volts in, Volts out, current in and out Amperes, power in and out in Watts, temperature of each power supply, and fan speed in RPM.
LED	Shows a list of what the LEDs represent, what state the LEDs mean, and a description of what the LEDs current color means.

Transceiver DDM support list	Show a list of transceivers that support Digital Diagnostic Monitoring (DDM) – type, vendor name, part number, and whether DDM is supported.
Port Number	Displays a list of the port numbers, port type (SFP,QSFP, etc) and whether a transceiver is or is not in the port.

show system-information

Use this command to display system information.

Command Syntax `show system-information (all|fan|psu|os|cpu|bios|cpu-load|board-info)`

Parameter

`all`	System information of all modules.
`bios`	BIOS information.
`board-info`	Board EEPROM details.
`cpu`	Processor information.
`cpu-load`	CPU load information.
`fan`	Fan Field Replaceable Units (FRU) EEPROM information.
`os`	OS and Kernel version information.
`psu`	Power Supply Field Replaceable Units (FRU) EEPROM information.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show system-information psu
System PSU FRU Information
==========================
PSU 2 Country of Origin          : CN
PSU 2 PPID Part Number           : 0T9FNW
PSU 2 PPID Part Number Rev       : A00
PSU 2 Manufacturer ID            : 28298
PSU 2 Date Code                  : 52R
PSU 2 Serial Number              : 0298
PSU 2 Part Number                : 0T9FNW
PSU 2 Part Number Revision       : A00
PSU 2 Number of Fans in the tray : 1
PSU 2 Type                       : AC Normal
PSU 2 Service Tag                : AEIOU
```

The following tables explain the show command output fields.

Table 1-61: show system-information topics

Topic	Description
all	Show all topics of system information..
bios	Display BIOS information.
board-info	Display information related to the board.
cpu	Displays Central Processing Unit information
cpu-load	Displays the load on the system's CPU.
fan	Displays fan information contain in the EEPROM.
os	Displays information regarding the host operating system
psu	Displays information regarding Field Replaceable Units (FRU).

Table 1-62: Show fan topic displays

System Fan FRU Information	Description
Fan Tray "#" PPID Part Number	The vendor's part number for the fan.
Fan Tray Serial Number	As stated
Service Tag	The Service Tag can help identify your device for on-line support and upgrading drivers
Vendor Name	As stated

Table 1-63: Show system BIOS information

BIOS Information	Description
# dmidecode	The dmidecode is a tool for dumping a computer's DMI table contents in a humanreadable format. This table contains a description of the system's hardware components, as well as other useful pieces of information such as serial numbers and BIOS revisions.

SMBIOS	The System Management BIOS (SMBIOS) defines data structures (and access methods) that can be used to read management information produced by the BIOS of a computer. Also, it is involved with the DMI Address –
Handle 0x0000, DMI type 0, 24 bytes	Handle of the Desktop Management Interface (DMI) and the DMI type, where type value identifies what the DMI contains. DMI = 0 indicates the following information is specific to BIOS properties, and is 24 bytes long.
BIOS Physical Information	• Vendor – The manufacture of the BIOS. • Version – The Version number. • Release Date – as stated. • Address – starting address (in memory) of the BIOS.

Table 1-63: Show system BIOS information (Continued)

BIOS Information	Description
Characteristics	• Is PCI supported. • Is BIOS upgradeable. • Is boot from a CD supported. • Is selectable boot devices supported. • Is BIOS ROM socketed. • Is Enhanced Disk Drive (EDD) vectoring supported. • Is 5.25"/1.2 MB floppy services supported (int 13h)• Is 3.5"/720 kB floppy services supported (int 13h) • Is 3.5"/2.88 MB floppy services supported (int 13h) • Is Print screen service supported (int 5h) • Is 8042 keyboard services supported (int 9h) • Is Serial services supported (int 14h) • Is Printer services supported (int 17h) • Is Advanced Configuration and Power Interface (ACPI) supported • Is USB legacy supported • Is BIOS boot specification supported • Is Targeted content distribution supported • Is Unified Extensible Firmware Interface (UEFI) supported
BIOS Revision	The BIOS revision number.
Handle 0x0043, DMI type 13, 22 bytes	Handle of the Desktop Management Interface (DMI) and the DMI type, where type value identifies what the DMI contains. DMI = 13 indicates the following information is specific to BIOS language information, and is 22 bytes long.
BIOS Language Informantion	• Language Description Format – A term that describes the number of bits used to represent the BIOS Language information parameters. • Installable Languages – The number of languages that can be used by the BIOS at any time. • Currently Installed Language – United States English (or Latin-1) as described by the ISO standard, en|US|iso8859-1.

Load Information	Description
Load Average for past 15 min	As stated in percent.
CPU Usage at this instant	As stated in percent.
Max threshold for CPU-usage	As stated in percent.

Table 1-64: Show CPU information

System CPU Information	Description
processor	The processor number of each CPU
model name	Details about each CPU. For example, Intel(R) Atom(TM) CPU C2538 @ 2.40GHz.

Table 1-65: Show system CPU load information

Load Information	Description
Uptime	As stated in days, hours, minutes, and seconds.
Load Average for past 1min	As stated in percent.
Load Average for past 5 min	As stated in percent.

Table 1-65: (Continued)Show system CPU load information

Table 1-66: Show system board information

System Information	Description
Product Name	Model number of the device.
Serial Number	As stated
Base MAC Address	As stated
Manufacture Date	As state
Platform Name	The platform on which the product is based.
ONIE Version	The version of the Open Network Install Environment (ONIE).

MAC addresses	Number of MAC addresses related to the device.
Manufacture	As stated
Country Code	The code that represents the country of manufacture. For example, US = United States, TW = Taiwan, and so on.
Diag Version	As stated
CRC-32	Cyclic Redundancy Check value.
Switch Chip Revision	As stated
MAIN BOARD REVISION	As stated
CPU CPLD VERSION	The version of the Complex Programmable Logic Device (CPLD) use by the CPU.
SW CPLD VERSION	The version of the Complex Programmable Logic Device (CPLD) use by the switch.
MAIN BOARD TYPE	An identifying string for the main board.
CPU BOARD ID	An identifying string for the CPU board.
CPU BOARD VERSION	As stated
SW BOARD ID	NA
SW BOARD VERSION	As stated
VCC 5V	The state of the VCC 5V power rail (Enabled \ Disabled)
MAC 1V	The state of the MAC 1V power rail Enabled \ Disabled

Table 1-66: (Continued)Show system board information

System Information	**Description**
VCC 1.8V	The state of the VCC 1.8V power rail (Enabled \ Disabled)
MAC AVS 1V	The state of the MAC AVS 1V power rail (Enabled \ Disabled)
HOT SWAP1	Enabled \ Disabled

HOT SWAP2	Enabled \ Disabled

Table 1-67: Show host system details

Host Information	Description
OS Distribution	The operating system on which the device is to run.
Kernel Version	A string that identifies the operating kernel.

CHAPTER 2 Digital Diagnostic Monitoring Commands

This chapter provides a description, syntax, and examples of DDM feature commands:

- clear ddm transceiver alarm
- ddm monitor
- ddm monitor all
- ddm monitor interval
- ddm monitor interval
- service unsupported-transceiver
- show controller details
- show supported-transceiver
- show interface transceiver details

clear ddm transceiver alarm

Use this command to clear the transceiver alarm in the DDM monitor interface.

Command Syntax `clear ddm transceiver alarm (PORTNUM|)`

Parameters

`PORTNUM` Port number. If this parameter is not specified, this command clears the transceiver alarms for all interfaces.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear ddm transceiver alarm
```

ddm monitor

Use this command to enable DDM monitoring for interfaces which have a supported transceiver.

Use the `no` form of this command to disable DDM monitoring for all transceivers.

Command Syntax `ddm monitor`

`no ddm monitor`

Parameters

None

Default

By default, DDM monitoring is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface xe1
(config-if)#ddm monitor (config-if)#exit

(config)#interface xe1
(config-if)#no ddm monitor
(config-if)#exit
```

ddm monitor all

Use this command to enable DDM monitoring for all transceiver.s

Use the `no` form of this command to disable DDM monitoring for all transceivers.

Command Syntax `ddm monitor all no ddm monitor all`

Parameters

None

Default

By default, DDM monitoring is disabled.

Command Mode

Configuration mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ddm monitor all

(config)#no ddm monitor all
```

ddm monitor interval

Use this command to set the monitoring interval for the transceiver.

Use no form with this command to set the monitoring interval to its default.

Command Syntax `ddm monitor interval <60-3600> no ddm monitor interval`

Parameters

`<60-3600>`	Interval period in seconds.

Default

The default monitoring interval is 60 seconds.

Command Mode

Configuration mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ddm monitor interval 60
```

debug ddm

Use this command to enable/disable debugging for DDM.

Command Syntax `debug ddm (enable|disable)`

Parameters

`enable`	Enable debugging.
`disable`	Disable debugging.

Default

By default, debug command is disabled.

Command Mode

Configuration mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#debug ddm enable
(config)#debug ddm disable
```

service unsupported-transceiver

Use this command to allow an unsupported transceiver to be enabled for DDM monitoring.

Use the `no` form of this command to disable DDM on an unsupported transceiver.

Command Syntax `service unsupported-transceiver`

`no service unsupported-transceiver`

Parameters

None

Default

By default, DDM on an unsupported transceiver is disabled.

Command Mode

Configuration mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#service unsupported-transceiver

(config)#no service unsupported-transceiver
```

show controller details

Use this command to display the EEPROM details of transceiver.s

Command Syntax `show interface`

`(IFNAME|) controllers`

Parameters

`IFNAME`	Interface name. If not specified, this command displays details of all connected transceivers.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show interface xe52/1 controllers

Port Number             : 52
Vendor oui              : 0x0 0x17 0x6a
Vendor name             : AVAGO
Vendor part_no          : AFBR-
79E4Z serial_number           :
QB380161 transceiver_type         :
QSFP OR LATER connector_type
: MPO 1x12 qsfp_transceiver_code
: 1X-LX vendor_rev               :
01
date_code              : 110920  (yymmddvv, v=vendor specific)
encoding                 : SONET br_nominal             : 103
(100 MHz) length_km               : 0 length_mtr             :
50 length_50mt               : 0 length_62_5mt            : 0
length_cu                  : 0 cc_base                  : 0x7d
cc_ext                   : 0x28 DDM Support             : yes
```

show supported-transceiver

Use this command to display supported transceivers.

Command Syntax `show supported-transceiver`

Parameters

None

Default

None

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#show supported-transceiver
-----------------------------------------------------
```

```
            Transceiver DDM support list
-----------------------------------------------------
Type                        :SFP
Vendor Name                 :FINISAR CORP
Vendor Part Number          :FTLF8519P2BNL
DDM Supported               :Yes

Type                        :SFP
Vendor Name                 :EVERTZ
Vendor Part Number          :SFP10G-TR13S
DDM Supported               :Yes

Type                        :QSFP
Vendor Name                 :AVAGO
Vendor Part Number          :AFBR-79E4Z
DDM Supported               :Yes
```

show interface transceiver details

Use this command to display details of transceivers and threshold violations.

Command Syntax `show interface (IFNAME|) transceiver (detail|threshold violation|)`

Parameters

`IFNAME`	Interface name. If not specified, this command displays details of all connected transceivers.
`detail`	Transceiver information such as voltage, temperature, power, and current.
`threshold violation`	Transceiver threshold violations.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show interface transceiver detail
PORT   Temp High Alarm High Warn Low Warn Low Alarm
       (Celsius) (Celsius) (Celsius) (Celsius) (Celsius)

-----------------------------------------------------
5         30.060      95          90        -20      -25
6         30.463      95          90        -20      -25
52        34.486      75          70          0       -5
```

```
53        30.764      75          70          0      -5
```

	Voltage (Volts)	High Alarm (Volts)	High Warn (Volts)	Low Warn (Volts)	Low Alarm (Volts)
5	3.339	3.900	3.700	2.900	2.700
6	3.365	3.900	3.700	2.900	2.700
52	3.360	3.630	3.465	3.135	2.970
53	3.353	3.630	3.465	3.135	2.970

	Current (mA)	High Alarm (mA)	High Warn (mA)	Low Warn (mA)	Low Alarm (mA)
5	6.468	17.000	14.000	2.000	0.034
6	7.014	17.000	14.000	2.000	0.034
52	7.250	10.000	9.500	1.000	0.500
53	7.284	10.000	9.500	1.000	0.500

```
          RxPower  High Alarm High Warn Low Warn Low Alarm
          (dBm)       (dBm)       (dBm)      (dBm)     (dBm)
-------------------------------------------------------------
5          0.332       1.259       0.794     0.016      0.010
6          0.321       1.259       0.794     0.016      0.010
52         0.727       2.188       1.738     0.112      0.000
53         0.352       2.188       1.738     0.112      0.000

          TxPower  High Alarm High Warn Low Warn Low Alarm
            (mW)       (mW)         (mW)       (mW)      (mW)
-------------------------------------------------------------
 5         0.342        0.631      0.631     0.079     0.067
 6         0.342        0.631      0.631     0.079     0.067
```

Table 2-68 explains the output fields.

Table 2-68: show interface transceiver details output

Field	Description
Port	The number of the transceiver port.
Temp	Temperature in degrees Celsius of the transceiver.
Voltage	Voltage in Volts on the transceiver.
Current	Current in Milliamperes used by the transceiver.
Rx Power	Power received in Decibel-milliwatts (dBm) by the transceiver.
Tx Power	Power being transmitted in milliWatts by the transceiver.
High Alarm	The level that is needed to be reached to trigger a high alarm.
High Warn	The level that is needed to be reached to trigger a high warning.
Low Warn	The level that is needed to be reached to trigger a low warning.
Low Alarm	The level that is needed to be reached to trigger a low alarm.

SECTION 5

Layer 2

Layer 2 Configuration Guide

Contents

This guide contains these chapters:

- Chapter 1, *Spanning Tree Protocol Configuration*
- Chapter 2, *RSTP Configuration*
- Chapter 3, *MSTP Configuration*
- Chapter 4, *Disable Spanning Tree Configuration*
- Chapter 5, *RPVST+ Configuration*
- Chapter 6, *VLAN Configuration*
- Chapter 7, *802.1X Configuration*
- Chapter 8, *LACP Configuration*
- Chapter 9, *MC-LAG Configuration*
- Chapter 10, *Traffic Mirroring Configuration*
- Chapter 11, *Maximum MST Instances Configuration*
- Chapter 12, *MC-LAG Configuration*

CHAPTER 1 Spanning Tree Protocol Configuration

This chapter contains a complete sample STP configuration. STP prevents duplication of packets by eliminating loops in the network.

Topology

The following example is a simple multi-bridge topology.

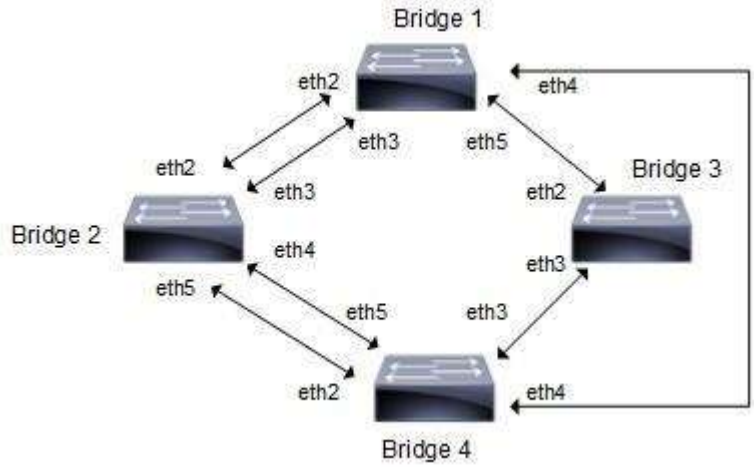


Figure 1-50: STP Topology

Note: Run the `switchport` command on each port to change to Layer-2 mode.

Configurations

Bridge 1

`Bridge1#configure terminal`	Enter configure mode.
`Bridge1(config)#bridge 1 protocol ieee`	Add a bridge `(1)` to the spanning tree table
`Bridge1(config)#interface eth2`	Enter interface mode.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth3`	Enter interface mode.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth4`	Enter interface mode.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth5`	Enter interface mode
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.

Bridge 2

`Bridge2#configure terminal`	Enter configure mode.
`Bridge2(config)#bridge 2 protocol ieee`	Add a bridge (`2`) to the spanning tree table
`Bridge2(config)#interface eth2`	Enter interface mode.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth3`	Enter interface mode.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth4`	Enter interface mode.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth5`	Enter interface mode
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.

Bridge 4

`Bridge4#configure terminal`	Enter configure mode.
`Bridge4(config)#bridge 4 protocol ieee`	Add a bridge (`4`) to the spanning tree table
`Bridge4(config)#interface eth2`	Enter interface mode.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth3`	Enter interface mode.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth4`	Enter interface mode.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth5`	Enter interface mode
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.

Bridge 3

`Bridge3#configure terminal`	Enter configure mode.
`Bridge3(config)#bridge 3 protocol ieee`	Add a bridge `(3)` to the spanning tree table
`Bridge3(config)#interface eth2`	Enter interface mode.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group `3`.
`Bridge3(config-if)#exit`	Exit interface mode.
`Bridge3(config)#interface eth3`	Enter interface mode.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group `3`.

Validation

show spanning-tree, show spanning-tree interface <if-name>

Bridge 1

```
#sh spanning-tree
% 1: Bridge up - Spanning Tree Enabled - topology change - topology change
detected
% 1: Root Path Cost 0 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root
port 0
% 1: Root Id 8000525400045cf1
% 1: Bridge Id 8000525400045cf1
% 1: 9 topology changes - last topology change Fri Mar  4 10:44:30 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - path cost 19 - designated
cost 0
%   eth2: Designated Port Id 0x8004 - state Forwarding -Priority 128
%   eth2: Designated root 8000525400045cf1
%   eth2: Designated Bridge 8000525400045cf1
%   eth2: Message Age 0 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%   eth2: forward-transitions 1
%   eth2: portfast disabled
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - path cost 19 - designated
cost 0
%   eth3: Designated Port Id 0x8005 - state Forwarding -Priority 128
%   eth3: Designated root 8000525400045cf1
%   eth3: Designated Bridge 8000525400045cf1
%   eth3: Message Age 0 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%   eth3: forward-transitions 1
%   eth3: portfast disabled
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - path cost 19 - designated
cost 0
%   eth4: Designated Port Id 0x8006 - state Forwarding -Priority 128
```

```
    %   eth4: Designated root 8000525400045cf1
    %   eth4: Designated Bridge 8000525400045cf1
    %   eth4: Message Age 0 - Max Age 20
    %   eth4: Hello Time 2 - Forward Delay 15
    %   eth4: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%   eth4: forward-transitions 1
%   eth4: portfast disabled
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - path cost 19 - designated cost
0
%   eth5: Designated Port Id 0x8007 - state Forwarding -Priority 128
%   eth5: Designated root 8000525400045cf1
%   eth5: Designated Bridge 8000525400045cf1
%   eth5: Message Age 0 - Max Age 20
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth5: forward-transitions 1
%   eth5: portfast disabled
%   eth5: bpdu-guard  default  - Current bpdu-guard off
%   eth5: bpdu-filter default  - Current bpdu-filter off
%   eth5: no root guard configured     - Current root guard off
%
%
% Default: Bridge up - Spanning Tree Enabled
% Default: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% Default: Root Id 8000000000000000
% Default: Bridge Id 8000000000000000
% Default: last topology change Wed Dec 31 19:00:00 1969
% Default: 0 topology change(s)  - last topology change Wed Dec 31 19:00:00 1969

% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled
% Default: portfast errdisable timeout disabled
% Default: portfast errdisable timeout interval 300 sec %

#sh spanning-tree interface eth2
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root port
0
% 1: Root Id 8000525400045cf1
% 1: Bridge Id 8000525400045cf1
% 1: 9 topology changes - last topology change Fri Mar  4 10:44:30 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
```

```
% 1: portfast errdisable timeout interval 300 sec
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - path cost 19 - designated cost
0
%   eth2: Designated Port Id 0x8004 - state Forwarding -Priority 128
%   eth2: Designated root 8000525400045cf1
%   eth2: Designated Bridge 8000525400045cf1
%   eth2: Message Age 0 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth2: forward-transitions 1
%   eth2: portfast disabled
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%
%
#sh spanning-tree interface eth3
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root port
0
% 1: Root Id 8000525400045cf1
% 1: Bridge Id 8000525400045cf1
% 1: 9 topology changes - last topology change Fri Mar  4 10:44:30 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - path cost 19 - designated cost
0
%   eth3: Designated Port Id 0x8005 - state Forwarding -Priority 128
%   eth3: Designated root 8000525400045cf1
%   eth3: Designated Bridge 8000525400045cf1
%   eth3: Message Age 0 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%   eth3: forward-transitions 1
%   eth3: portfast disabled
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%
%

#sh spanning-tree interface eth4
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root port
0
% 1: Root Id 8000525400045cf1
```

```
% 1: Bridge Id 8000525400045cf1
% 1: 9 topology changes - last topology change Fri Mar  4 10:44:30 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - path cost 19 - designated cost
0
%   eth4: Designated Port Id 0x8006 - state Forwarding -Priority 128
%   eth4: Designated root 8000525400045cf1
%   eth4: Designated Bridge 8000525400045cf1
%   eth4: Message Age 0 - Max Age 20
%   eth4: Hello Time 2 - Forward Delay 15
    %   eth4: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
    %   eth4: forward-transitions 1
    %   eth4: portfast disabled
    %   eth4: bpdu-guard  default  - Current bpdu-guard off
    %   eth4: bpdu-filter default  - Current bpdu-filter off
    %   eth4: no root guard configured     - Current root guard off
    %
    %
```

Bridge 2

```
    #sh spanning-tree
    % 2: Bridge up - Spanning Tree Enabled
    % 2: Root Path Cost 19 - Priority 32768
    % 2: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root
    port 4
    % 2: Root Id 8000525400045cf1
    % 2: Bridge Id 8000525400f8eafe
    % 2: 9 topology changes - last topology change Fri Mar  4 10:44:31 2016
    % 2: portfast bpdu-filter disabled
    % 2: portfast bpdu-guard disabled
    % 2: portfast errdisable timeout disabled
    % 2: portfast errdisable timeout interval 300 sec
    %   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - path cost 19 - designated
    cost 0
    %   eth2: Designated Port Id 0x8004 - state Forwarding -Priority 128
    %   eth2: Designated root 8000525400045cf1
    %   eth2: Designated Bridge 8000525400045cf1
    %   eth2: Message Age 0 - Max Age 20
    %   eth2: Hello Time 2 - Forward Delay 15
    %   eth2: Forward Timer 0 - Msg Age Timer 19 - Hello Timer 0 - topo change timer
    0
    %   eth2: forward-transitions 1
    %   eth2: portfast disabled
    %   eth2: bpdu-guard  default  - Current bpdu-guard off
    %   eth2: bpdu-filter default  - Current bpdu-filter off
    %   eth2: no root guard configured     - Current root guard off
```

```
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - path cost 19 - designated
cost 0
%   eth3: Designated Port Id 0x8005 - state Blocked -Priority 128
%   eth3: Designated root 8000525400045cf1
%   eth3: Designated Bridge 8000525400045cf1
%   eth3: Message Age 0 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 19 - Hello Timer 0 - topo change timer
0
%   eth3: forward-transitions 1
%   eth3: portfast disabled
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - path cost 19 - designated
cost 19
%   eth4: Designated Port Id 0x8007 - state Blocked -Priority 128
%   eth4: Designated root 8000525400045cf1
%   eth4: Designated Bridge 800052540066d3de
%   eth4: Message Age 2 - Max Age 20
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 17 - Hello Timer 1 - topo change timer
0
%   eth4: forward-transitions 1
%   eth4: portfast disabled
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - path cost 19 - designated
cost 19
%   eth5: Designated Port Id 0x8004 - state Blocked -Priority 128
%   eth5: Designated root 8000525400045cf1
%   eth5: Designated Bridge 800052540066d3de
%   eth5: Message Age 1 - Max Age 20
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 18 - Hello Timer 0 - topo change timer
0
%   eth5: forward-transitions 1
%   eth5: portfast disabled
%   eth5: bpdu-guard  default  - Current bpdu-guard off
%   eth5: bpdu-filter default  - Current bpdu-filter off
%   eth5: no root guard configured     - Current root guard off
%
%
% Default: Bridge up - Spanning Tree Enabled
% Default: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
```

```
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% Default: Root Id 8000000000000000
% Default: Bridge Id 8000000000000000
% Default: last topology change Wed Dec 31 19:00:00 1969
% Default: 0 topology change(s)  - last topology change Wed Dec 31 19:00:00 1969

% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled
% Default: portfast errdisable timeout disabled
% Default: portfast errdisable timeout interval 300 sec %
```

Bridge 3

```
#sh spanning-tree
% 3: Bridge up - Spanning Tree Enabled
% 3: Root Path Cost 19 - Priority 32768
% 3: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root
port 4
% 3: Root Id 8000525400045cf1
% 3: Bridge Id 8000525400401fcb
% 3: 10 topology changes - last topology change Fri Mar  4 10:40:03 2016
% 3: portfast bpdu-filter disabled
% 3: portfast bpdu-guard disabled
% 3: portfast errdisable timeout disabled
% 3: portfast errdisable timeout interval 300 sec
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - path cost 19 - designated
cost 0
%   eth2: Designated Port Id 0x8007 - state Forwarding -Priority 128
%   eth2: Designated root 8000525400045cf1
%   eth2: Designated Bridge 8000525400045cf1
%   eth2: Message Age 0 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 18 - Hello Timer 1 - topo change timer
0
%   eth2: forward-transitions 1
%   eth2: portfast disabled
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - path cost 19 - designated
cost 19
%   eth3: Designated Port Id 0x8005 - state Forwarding -Priority 128
%   eth3: Designated root 8000525400045cf1
%   eth3: Designated Bridge 8000525400401fcb
%   eth3: Message Age 1 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%   eth3: forward-transitions 1
%   eth3: portfast disabled
%   eth3: bpdu-guard  default  - Current bpdu-guard off
```

```
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%
%
% Default: Bridge up - Spanning Tree Enabled
% Default: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% Default: Root Id 8000000000000000
% Default: Bridge Id 8000000000000000
% Default: last topology change Wed Dec 31 19:00:00 1969
% Default: 0 topology change(s)  - last topology change Wed Dec 31 19:00:00 1969

% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled
% Default: portfast errdisable timeout disabled
% Default: portfast errdisable timeout interval 300 sec %
```

Bridge 4

```
#sh spanning-tree
% 4: Bridge up - Spanning Tree Enabled
% 4: Root Path Cost 19 - Priority 32768
% 4: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root
port 6
% 4: Root Id 8000525400045cf1
% 4: Bridge Id 800052540066d3de
% 4: 5 topology changes - last topology change Fri Mar  4 10:43:24 2016
% 4: portfast bpdu-filter disabled
% 4: portfast bpdu-guard disabled
% 4: portfast errdisable timeout disabled
% 4: portfast errdisable timeout interval 300 sec
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - path cost 19 - designated cost
19
%   eth2: Designated Port Id 0x8004 - state Forwarding -Priority 128
%   eth2: Designated root 8000525400045cf1
%   eth2: Designated Bridge 800052540066d3de
%   eth2: Message Age 1 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth2: forward-transitions 1
%   eth2: portfast disabled
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - path cost 19 - designated cost
19
%   eth3: Designated Port Id 0x8005 - state Blocked -Priority 128
%   eth3: Designated root 8000525400045cf1
%   eth3: Designated Bridge 8000525400401fcb
%   eth3: Message Age 1 - Max Age 20
```

```
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 17 - Hello Timer 0 - topo change timer 0
%   eth3: forward-transitions 1
%   eth3: portfast disabled
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - path cost 19 - designated cost
0
%   eth4: Designated Port Id 0x8006 - state Forwarding -Priority 128
%   eth4: Designated root 8000525400045cf1
%   eth4: Designated Bridge 8000525400045cf1
%   eth4: Message Age 0 - Max Age 20
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 19 - Hello Timer 0 - topo change timer 0
%   eth4: forward-transitions 1
%   eth4: portfast disabled
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - path cost 19 - designated cost
19
%   eth5: Designated Port Id 0x8007 - state Forwarding -Priority 128
%   eth5: Designated root 8000525400045cf1
%   eth5: Designated Bridge 800052540066d3de
%   eth5: Message Age 1 - Max Age 20
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%   eth5: forward-transitions 1
%   eth5: portfast disabled
%   eth5: bpdu-guard  default  - Current bpdu-guard off
%   eth5: bpdu-filter default  - Current bpdu-filter off
%   eth5: no root guard configured     - Current root guard off
%
%
% Default: Bridge up - Spanning Tree Enabled
% Default: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% Default: Root Id 8000000000000000
% Default: Bridge Id 8000000000000000
% Default: last topology change Wed Dec 31 19:00:00 1969
% Default: 0 topology change(s)  - last topology change Wed Dec 31 19:00:00 1969

% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled
% Default: portfast errdisable timeout disabled
% Default: portfast errdisable timeout interval 300 sec %
```

CHAPTER 2 RSTP Configuration

This chapter contains a complete sample Rapid Spanning Tree Protocol (RSTP) configuration. RSTP provides rapid convergence of a spanning tree. It speeds up the reconfiguration of the tree after a change by using alternate ports.

Topology

The following example is a simple multi-bridge topology.

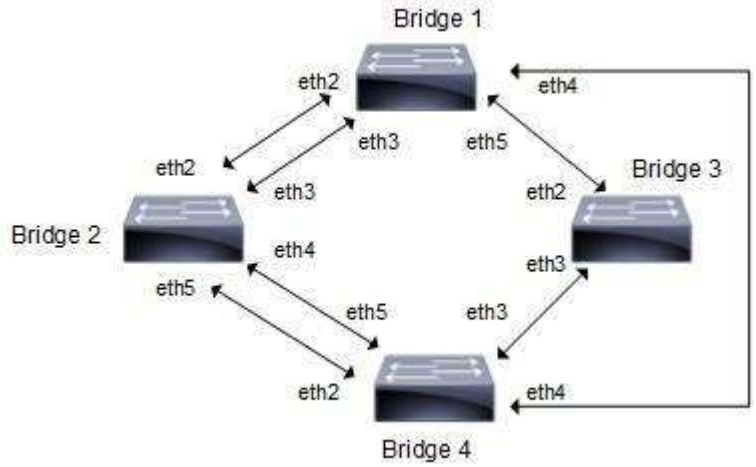


Figure 2-51: RSTP Topology

Note: Run the `switchport` command on each port to change to Layer-2 mode.

Configuration

Bridge 1

`Bridge1#configure terminal`	Enter configure mode.
`Bridge1(config)#bridge 1 protocol rstp`	Add a bridge (`1`) to the rapid spanning tree table
`Bridge1(config)#interface eth2`	Enter interface mode.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth3`	Enter interface mode.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth4`	Enter interface mode.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth5`	Enter interface mode
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.

Bridge 2

`Bridge2#configure terminal`	Enter configure mode.
`Bridge2(config)#bridge 2 protocol rstp`	Add a bridge (`2`) to the rapid spanning tree table
`Bridge2(config)#interface eth2`	Enter interface mode.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth3`	Enter interface mode.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth4`	Enter interface mode.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth5`	Enter interface mode
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.

Bridge 3

`Bridge3#configure terminal`	Enter configure mode.
`Bridge3(config)#bridge 3 protocol rstp`	Add a bridge `(3)` to the rapid spanning tree table
`Bridge3(config)#interface eth2`	Enter interface mode.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group `3`.
`Bridge3(config-if)#exit`	Exit interface mode.
`Bridge3(config)#interface eth3`	Enter interface mode.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group `3`.

Bridge 4

`Bridge4#configure terminal`	Enter configure mode.
`Bridge4(config)#bridge 4 protocol rstp`	Add a bridge `(4)` to the rapid spanning tree table
`Bridge4(config)#interface eth2`	Enter interface mode.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth3`	Enter interface mode.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth4`	Enter interface mode.
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth5`	Enter interface mode
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.

Validation

show spanning-tree, show spanning-tree interface <if-name>

Bridge 1

```
#sh spanning-tree
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 8000525400045cf1
% 1: Bridge Id 8000525400045cf1
% 1: last topology change Fri Mar  4 10:53:59 2016
% 1: 19 topology change(s)  - last topology change Fri Mar  4 10:53:59 2016

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated -
State Forwarding
%   eth2: Designated Path Cost 0
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth2: Designated Port Id 0x8004 - Priority 128  -
%   eth2: Root 8000525400045cf1
%   eth2: Designated Bridge 8000525400045cf1
%   eth2: Message Age 0 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer
0
%   eth2: forward-transitions 1
%   eth2: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated -
State Forwarding
%   eth3: Designated Path Cost 0
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth3: Designated Port Id 0x8005 - Priority 128  -
%   eth3: Root 8000525400045cf1
%   eth3: Designated Bridge 8000525400045cf1
%   eth3: Message Age 0 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer
0
```

```
    %   eth3: forward-transitions 1
    %   eth3: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
    %   eth3: No portfast configured - Current  portfast off
    %   eth3: bpdu-guard  default  - Current bpdu-guard off
    %   eth3: bpdu-filter default  - Current bpdu-filter off
    %   eth3: no root guard configured     - Current root guard off
    %   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Designated - State
Forwarding
%   eth4: Designated Path Cost 0
%   eth4: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth4: Designated Port Id 0x8006 - Priority 128  -
%   eth4: Root 8000525400045cf1
%   eth4: Designated Bridge 8000525400045cf1
%   eth4: Message Age 0 - Max Age 20
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%   eth4: forward-transitions 1
%   eth4: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%   eth4: Configured Link Type point-to-point - Current point-to-point
%   eth4: No auto-edge configured - Current port Auto Edge off
%
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Designated - State
Forwarding
%   eth5: Designated Path Cost 0
%   eth5: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth5: Designated Port Id 0x8007 - Priority 128  -
%   eth5: Root 8000525400045cf1
%   eth5: Designated Bridge 8000525400045cf1
%   eth5: Message Age 0 - Max Age 20
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%   eth5: forward-transitions 1
%   eth5: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
%   eth5: No portfast configured - Current  portfast off
%   eth5: bpdu-guard  default  - Current bpdu-guard off
%   eth5: bpdu-filter default  - Current bpdu-filter off
%   eth5: no root guard configured     - Current root guard off
%   eth5: Configured Link Type point-to-point - Current point-to-point
%   eth5: No auto-edge configured - Current port Auto Edge off
%
%
% Default: Bridge up - Spanning Tree Enabled
```

```
% Default: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% Default: Root Id 8000000000000000
% Default: Bridge Id 8000000000000000
% Default: last topology change Wed Dec 31 19:00:00 1969
% Default: 0 topology change(s)  - last topology change Wed Dec 31 19:00:00 1969

% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled
% Default: portfast errdisable timeout disabled
% Default: portfast errdisable timeout interval 300 sec
%#sh spanning-tree interface eth2
    % 1: Bridge up - Spanning Tree Enabled  - topology change detected
    % 1: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
    % 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
    % 1: Root Id 8000525400045cf1
    % 1: Bridge Id 8000525400045cf1
    % 1: last topology change Fri Mar  4 10:53:59 2016
    % 1: 19 topology change(s)  - last topology change Fri Mar  4 10:53:59 2016

    % 1: portfast bpdu-filter disabled
    % 1: portfast bpdu-guard disabled
    % 1: portfast errdisable timeout disabled
    % 1: portfast errdisable timeout interval 300 sec
    %   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated -
    State Forwarding
    %   eth2: Designated Path Cost 0
    %   eth2: Configured Path Cost 200000  - Add type Explicit ref count 1
    %   eth2: Designated Port Id 0x8004 - Priority 128  -
    %   eth2: Root 8000525400045cf1
    %   eth2: Designated Bridge 8000525400045cf1
    %   eth2: Message Age 0 - Max Age 20
    %   eth2: Hello Time 2 - Forward Delay 15
    %   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer
    0
    %   eth2: forward-transitions 1
    %   eth2: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
    %   eth2: No portfast configured - Current  portfast off
    %   eth2: bpdu-guard  default  - Current bpdu-guard off
    %   eth2: bpdu-filter default  - Current bpdu-filter off
    %   eth2: no root guard configured     - Current root guard off
    %   eth2: Configured Link Type point-to-point - Current point-to-point
    %   eth2: No auto-edge configured - Current port Auto Edge off
    %
    %
```

Bridge 2

```
    #sh spanning-tree
    % 2: Bridge up - Spanning Tree Enabled  - topology change detected
    % 2: Root Path Cost 200000 - Root Port 4 -  Bridge Priority 32768
```

```
    % 2: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
    % 2: Root Id 8000525400045cf1
    % 2: Bridge Id 8000525400f8eafe
    % 2: last topology change Fri Mar  4 10:54:00 2016
    % 2: 5 topology change(s)  - last topology change Fri Mar  4 10:54:00 2016

    % 2: portfast bpdu-filter disabled
    % 2: portfast bpdu-guard disabled
    % 2: portfast errdisable timeout disabled
    % 2: portfast errdisable timeout interval 300 sec
    %   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Rootport -
    State Forwarding
    %   eth2: Designated Path Cost 0
    %   eth2: Configured Path Cost 200000  - Add type Explicit ref count 1
    %   eth2: Designated Port Id 0x8004 - Priority 128  -
    %   eth2: Root 8000525400045cf1
    %   eth2: Designated Bridge 8000525400045cf1
    %   eth2: Message Age 0 - Max Age 20
    %   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 1 - topo change timer 0
%   eth2: forward-transitions 1
%   eth2: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Alternate - State
Discarding
%   eth3: Designated Path Cost 0
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth3: Designated Port Id 0x8005 - Priority 128  -
%   eth3: Root 8000525400045cf1
%   eth3: Designated Bridge 8000525400045cf1
%   eth3: Message Age 0 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 1 - topo change timer 0
%   eth3: forward-transitions 0
%   eth3: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
%
```

```
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Alternate - State
Discarding
%   eth4: Designated Path Cost 200000
%   eth4: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth4: Designated Port Id 0x8007 - Priority 128  -
%   eth4: Root 8000525400045cf1
%   eth4: Designated Bridge 800052540066d3de
%   eth4: Message Age 1 - Max Age 20
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1 - topo change timer 0
%   eth4: forward-transitions 0
%   eth4: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%   eth4: Configured Link Type point-to-point - Current point-to-point
%   eth4: No auto-edge configured - Current port Auto Edge off
%
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Alternate - State
Discarding
%   eth5: Designated Path Cost 200000
%   eth5: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth5: Designated Port Id 0x8004 - Priority 128  -
%   eth5: Root 8000525400045cf1
%   eth5: Designated Bridge 800052540066d3de
    %   eth5: Message Age 1 - Max Age 20
    %   eth5: Hello Time 2 - Forward Delay 15
    %   eth5: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1 - topo change timer
    0
    %   eth5: forward-transitions 0
    %   eth5: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
    %   eth5: No portfast configured - Current  portfast off
    %   eth5: bpdu-guard  default  - Current bpdu-guard off
    %   eth5: bpdu-filter default  - Current bpdu-filter off
    %   eth5: no root guard configured     - Current root guard off
    %   eth5: Configured Link Type point-to-point - Current point-to-point
    %   eth5: No auto-edge configured - Current port Auto Edge off
    %
    %
    % Default: Bridge up - Spanning Tree Enabled
    % Default: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
    % Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
    % Default: Root Id 8000000000000000
    % Default: Bridge Id 8000000000000000
    % Default: last topology change Wed Dec 31 19:00:00 1969
    % Default: 0 topology change(s)  - last topology change Wed Dec 31 19:00:00 1969

    % Default: portfast bpdu-filter disabled
```

```
% Default: portfast bpdu-guard disabled
% Default: portfast errdisable timeout disabled
% Default: portfast errdisable timeout interval 300 sec %
```

Bridge 3

```
#sh spanning-tree
% 3: Bridge up - Spanning Tree Enabled  - topology change detected
% 3: Root Path Cost 200000 - Root Port 4 -  Bridge Priority 32768
% 3: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 3: Root Id 8000525400045cf1
% 3: Bridge Id 8000525400401fcb
% 3: last topology change Fri Mar  4 10:54:00 2016
% 3: 4 topology change(s)  - last topology change Fri Mar  4 10:54:00 2016

% 3: portfast bpdu-filter disabled
% 3: portfast bpdu-guard disabled
% 3: portfast errdisable timeout disabled
% 3: portfast errdisable timeout interval 300 sec
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Rootport -
State Forwarding
%   eth2: Designated Path Cost 0
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth2: Designated Port Id 0x8007 - Priority 128  -
%   eth2: Root 8000525400045cf1
%   eth2: Designated Bridge 8000525400045cf1
%   eth2: Message Age 0 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 1 - topo change timer
0
%   eth2: forward-transitions 1
%   eth2: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated -
State Forwarding
%   eth3: Designated Path Cost 200000
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth3: Designated Port Id 0x8005 - Priority 128  -
%   eth3: Root 8000525400045cf1
%   eth3: Designated Bridge 8000525400401fcb
%   eth3: Message Age 1 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer
0
%   eth3: forward-transitions 1
```

```
    %   eth3: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
    %   eth3: No portfast configured - Current  portfast off
    %   eth3: bpdu-guard  default  - Current bpdu-guard off
    %   eth3: bpdu-filter default  - Current bpdu-filter off
    %   eth3: no root guard configured     - Current root guard off
    %   eth3: Configured Link Type point-to-point - Current point-to-point
    %   eth3: No auto-edge configured - Current port Auto Edge off
    %
    %
    % Default: Bridge up - Spanning Tree Enabled
    % Default: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
    % Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
    % Default: Root Id 8000000000000000
    % Default: Bridge Id 8000000000000000
    % Default: last topology change Wed Dec 31 19:00:00 1969
    % Default: 0 topology change(s)  - last topology change Wed Dec 31 19:00:00 1969

    % Default: portfast bpdu-filter disabled
    % Default: portfast bpdu-guard disabled
    % Default: portfast errdisable timeout disabled
    % Default: portfast errdisable timeout interval 300 sec %
```

Bridge 4

```
    #show  spanning-tree
    % 4: Bridge up - Spanning Tree Enabled  - topology change detected
    % 4: Root Path Cost 200000 - Root Port 6 -  Bridge Priority 32768
    % 4: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
    % 4: Root Id 8000525400045cf1
    % 4: Bridge Id 800052540066d3de
    % 4: last topology change Fri Mar  4 10:53:58 2016
    % 4: 3 topology change(s)  - last topology change Fri Mar  4 10:53:58 2016

    % 4: portfast bpdu-filter disabled
    % 4: portfast bpdu-guard disabled
    % 4: portfast errdisable timeout disabled
% 4: portfast errdisable timeout interval 300 sec
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated Path Cost 200000
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth2: Designated Port Id 0x8004 - Priority 128  -
%   eth2: Root 8000525400045cf1
%   eth2: Designated Bridge 800052540066d3de
%   eth2: Message Age 1 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth2: forward-transitions 1
%   eth2: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
```

```
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Alternate - State
Discarding
%   eth3: Designated Path Cost 200000
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth3: Designated Port Id 0x8005 - Priority 128  -
%   eth3: Root 8000525400045cf1
%   eth3: Designated Bridge 8000525400401fcb
%   eth3: Message Age 1 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0 - topo change timer 0
%   eth3: forward-transitions 0
%   eth3: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Rootport - State
Forwarding
%   eth4: Designated Path Cost 0
%   eth4: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth4: Designated Port Id 0x8006 - Priority 128  -
%   eth4: Root 8000525400045cf1
%   eth4: Designated Bridge 8000525400045cf1
%   eth4: Message Age 0 - Max Age 20
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0 - topo change timer 0
%   eth4: forward-transitions 1
%   eth4: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%   eth4: Configured Link Type point-to-point - Current point-to-point
%   eth4: No auto-edge configured - Current port Auto Edge off
%
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Designated - State
Forwarding
%   eth5: Designated Path Cost 200000
%   eth5: Configured Path Cost 200000  - Add type Explicit ref count 1
%   eth5: Designated Port Id 0x8007 - Priority 128  -
%   eth5: Root 8000525400045cf1
```

```
%   eth5: Designated Bridge 800052540066d3de
%   eth5: Message Age 1 - Max Age 20
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth5: forward-transitions 1
%   eth5: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
%   eth5: No portfast configured - Current  portfast off
%   eth5: bpdu-guard  default  - Current bpdu-guard off
%   eth5: bpdu-filter default  - Current bpdu-filter off
%   eth5: no root guard configured     - Current root guard off
%   eth5: Configured Link Type point-to-point - Current point-to-point
%   eth5: No auto-edge configured - Current port Auto Edge off
%
%
% Default: Bridge up - Spanning Tree Enabled
% Default: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% Default: Root Id 8000000000000000
% Default: Bridge Id 8000000000000000
% Default: last topology change Wed Dec 31 19:00:00 1969
% Default: 0 topology change(s)  - last topology change Wed Dec 31 19:00:00 1969

% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled
% Default: portfast errdisable timeout disabled
% Default: portfast errdisable timeout interval 300 sec %
```

CHAPTER 3 MSTP Configuration

This chapter contains a complete sample Multiple Spanning Tree Protocol (MSTP) configuration. MSTP allows multiple VLANs to be grouped into one spanning-tree instance. Every MST instance has a spanning-tree that is independent of other spanning-tree instances providing multiple forwarding paths for data traffic.

Topology

This example gives a simple multi-bridge topology and its configuration.

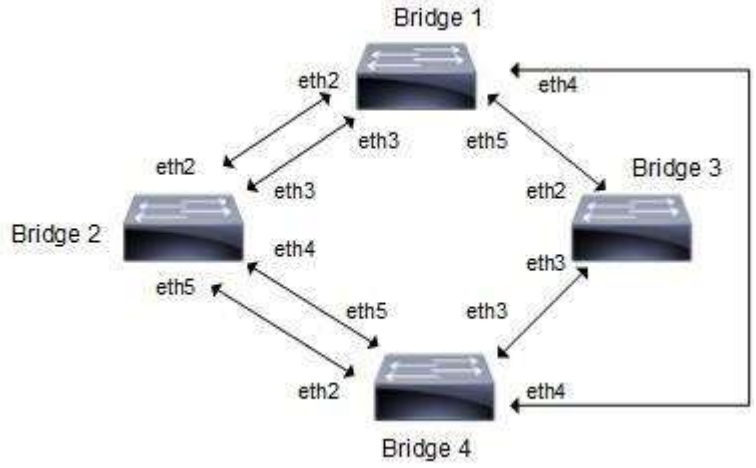


Figure 3-52: MSTP Topology

Note: Run the `switchport` command on each port to change to Layer-2 mode.

Configuration

Bridge 1

`Bridge1#configure terminal`	Enter configure mode.
`Bridge1(config)#bridge 1 protocol mstp`	Add a bridge (1) to the multiple spanning tree table.
`Bridge1(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge1(config-vlan)#vlan 2 bridge 1 state enable`	Enable the state of VLAN 2 on bridge 1. Specifying an enable state allows forwarding of frames over VLAN 2 on bridge 1.
`Bridge1(config-vlan)#vlan 3 bridge 1 state enable`	Enable the state of VLAN 3 on bridge 1. Specifying an enable state allows forwarding of frames over VLAN 3 on bridge 1.
`Bridge1(config-vlan)#vlan 4 bridge 1 state enable`	Enable the state of VLAN 4 on bridge 1. Specifying an enable state allows forwarding of frames over VLAN 4 on bridge 1.
`Bridge1(config-vlan)#vlan 5 bridge 1 state enable`	Enable the state of VLAN 5 on bridge 1. Specifying an enable state allows forwarding of frames over VLAN 5 on bridge 1.
`Bridge1(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge1(config)#spanning-tree mst configuration`	Enter the Multiple Spanning Tree

`Bridge1(config-mst)#bridge 1 instance 2 vlan 2`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge1(config-mst)#bridge 1 instance 3 vlan 3`	Create another instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge1(config-mst)#bridge 1 instance 4 vlan 4`	same as mention above.
`Bridge1(config-mst)#bridge 1 instance 5 vlan 5`	same as mention above.
`Bridge1(config-mst)#exit`	Exit MST Configuration mode.
`Bridge1(config)#interface eth2`	Enter the Interface mode for eth2
`Bridge1(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`Bridge1(config-if)#bridge-group 1 instance 2`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 3`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 4`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 5`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth3`	Enter the Interface mode for eth3.
`Bridge1(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`Bridge1(config-if)#bridge-group 1 instance 2`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 3`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 4`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 5`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth4`	Enter the Interface mode for eth4.
`Bridge1(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`Bridge1(config-if)#bridge-group 1 instance 2`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 3`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 4`	Assigning bridge-group 1 to this instance

`Bridge1(config-if)#bridge-group 1 instance 5`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth5`	Enter the Interface mode for eth5.
`Bridge1(config-if)#bridge-group 1`	Associating the interface to bridge-group 1
`Bridge1(config-if)#bridge-group 1 instance 2`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 3`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 4`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#bridge-group 1 instance 5`	Assigning bridge-group 1 to this instance
`Bridge1(config-if)#exit`	Exit interface mode.

Bridge 2

`Bridge2#configure terminal`	Enter configure mode.
`Bridge2(config)#bridge 2 protocol mstp`	Add a bridge (2) to the multiple spanning
`Bridge2(config)#bridge 2 priority 4096`	Assign priority to this bridge.
`Bridge2(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge2(config-vlan)#vlan 2 bridge 2 state enable`	Enable the state of VLAN 2 on bridge 2. Specifying an enable state allows forwarding of frames over VLAN 2 on bridge 2.
`Bridge2(config-vlan)#vlan 3 bridge 2 state enable`	Enable the state of VLAN 3 on bridge 2. Specifying an enable state allows forwarding of frames over VLAN 3 on bridge 2
`Bridge2(config-vlan)#vlan 4 bridge 2 state enable`	Enable the state of VLAN 4 on bridge 2. Specifying an enable state allows forwarding of frames over VLAN 4 on bridge 2
`Bridge2(config-vlan)#vlan 5 bridge 2 state enable`	Enable the state of VLAN 5 on bridge 2. Specifying an enable state allows forwarding of frames over VLAN 5 on bridge 2
`Bridge2(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge2(config)#spanning-tree mst configuration`	Enter the Multiple Spanning Tree configuration mode
`Bridge2(config-mst)#bridge 2 instance 2 vlan 2`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge2(config-mst)#bridge 2 instance 3 vlan 3`	same as mention above.
`Bridge2(config-mst)#bridge 2 instance 4 vlan 4`	same as mention above.
`Bridge2(config-mst)#bridge 2 instance 5 vlan 5`	same as mention above.
`Bridge2(config-mst)#exit`	Exit MST Configuration mode.
`Bridge2(config)#interface eth2`	Enter the Interface mode for eth2
`Bridge2(config-if)#bridge-group 2`	Associating the interface to bridge-group 2

`Bridge2(config-if)#bridge-group 2 instance 2`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 3`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 4`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 5`	Assigning bridge-group 2 to this instance

`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth3`	Enter the Interface mode for eth3
`Bridge2(config-if)#bridge-group 2`	Associating the interface to bridge-group 2
`Bridge2(config-if)#bridge-group 2 instance 2`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 3`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 3 priority 16`	Assign bridge-group 2 to this instance and set a port priority in order of 16 for it. MSTP uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies better priority.
`Bridge2(config-if)#bridge-group 2 instance 4`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 4 priority 16`	Assign bridge-group 2 to this instance and set a port priority in order of 16 for it. MSTP uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies better priority
`Bridge2(config-if)#bridge-group 2 instance 5`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#exit`	Exit interface mode
`Bridge2(config)#interface eth4`	Enter the Interface mode for eth4
`Bridge2(config-if)#bridge-group 2`	Associating the interface to bridge-group 2
`Bridge2(config-if)#bridge-group 2 instance 2`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 3`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 4`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 5`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth5`	Enter the Interface mode for eth5
`Bridge2(config-if)#bridge-group 2`	Associating the interface to bridge-group 2

`Bridge2(config-if)#bridge-group 2 instance 2`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 3`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 4`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#bridge-group 2 instance 5`	Assigning bridge-group 2 to this instance
`Bridge2(config-if)#exit`	Exit interface mode.

Bridge 3

`Bridge3#configure terminal`	Enter configure mode.
`Bridge3(config)#bridge 3 protocol mstp`	Add a bridge (3) to the multiple spanning tree table
`Bridge3(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge3(config-vlan)#vlan 2 bridge 3 state enable`	Enable the state of VLAN 2 on bridge 3. Specifying an enable state allows forwarding of frames over VLAN 2 on bridge 3.
`Bridge3(config-vlan)#vlan 3 bridge 3 state enable`	Enable the state of VLAN 3 on bridge 3. Specifying an enable state allows forwarding of frames over VLAN 3 on bridge 3.
`Bridge3(config-vlan)#vlan 4 bridge 3 state enable`	Enable the state of VLAN 4 on bridge 3. Specifying an enable state allows forwarding of frames over VLAN 4 on bridge 3.
`Bridge3(config-vlan)#vlan 5 bridge 3 state enable`	Enable the state of VLAN 5 on bridge 3. Specifying an enable state allows forwarding of frames over VLAN 5 on bridge 3.
`Bridge3(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge3(config)#spanning-tree mst configuration`	Enter the Multiple Spanning Tree Configuration mode.
`Bridge3(config-mst)#bridge 3 instance 2 vlan 2`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge3(config-mst)#bridge 3 instance 3 vlan 3`	same as mention above.
`Bridge3(config-mst)#bridge 3 instance 4 vlan 4`	same as mention above.
`Bridge3(config-mst)#bridge 3 instance 5 vlan 5`	same as mention above.
`Bridge3(config-mst)#exit`	Exit MST Configuration mode.
`Bridge3(config)#interface eth2`	Enter the Interface mode for eth2
`Bridge3(config-if)#bridge-group 3`	Associating the interface to bridge-group 3

`Bridge3(config-if)#bridge-group 3 instance 2`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 3`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 4`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 5`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#exit`	Exit interface mode.
`Bridge3(config)#interface eth3`	Enter the Interface mode for eth3
`Bridge3(config-if)#bridge-group 3`	Associating the interface to bridge-group 3
`Bridge3(config-if)#bridge-group 3 instance 2`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 3`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 4`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#bridge-group 3 instance 5`	Assigning bridge-group 3 to this instance
`Bridge3(config-if)#exit`	Exit interface mode.

Bridge 4

`Bridge4#configure terminal`	Enter configure mode.
`Bridge4(config)#bridge 4 protocol mstp`	Add a bridge (4) to the multiple spanning tree table
`Bridge4(config)#vlan database`	Enter the VLAN configuration mode.
`Bridge4(config-vlan)#vlan 2 bridge 4 state enable`	Enable the state of VLAN 2 on bridge 4. Specifying an enable state allows forwarding of frames over VLAN 2 on bridge 4.
`Bridge4(config-vlan)#vlan 3 bridge 4 state enable`	Enable the state of VLAN 3 on bridge 4. Specifying an enable state allows forwarding of frames over VLAN 3 on bridge 4.
`Bridge4(config-vlan)#vlan 4 bridge 4 state enable`	Enable the state of VLAN 4 on bridge 4. Specifying an enable state allows forwarding of frames over VLAN 4 on bridge 4.
`Bridge4(config-vlan)#vlan 5 bridge 4 state enable`	Enable the state of VLAN 5 on bridge 4. Specifying an enable state allows forwarding of frames over VLAN 5 on bridge 4.
`Bridge4(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge4(config)#spanning-tree mst configuration`	Enter the Multiple Spanning Tree Configuration mode.
`Bridge4(config-mst)#bridge 4 instance 2 vlan 2`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified the MSTI will not be created.
`Bridge4(config-mst)#bridge 4 instance 3 vlan 3`	same as mention above.
`Bridge4(config-mst)#bridge 4 instance 4 vlan 4`	same as mention above.
`Bridge4(config-mst)#bridge 4 instance 5 vlan 5`	same as mention above.

Bridge4(config-mst)#exit	Exit MST Configuration mode.
Bridge4(config)#interface eth2	Enter the Interface mode for eth2
Bridge4(config-if)#bridge-group 4	Associating the interface to bridge-group 4
Bridge4(config-if)#bridge-group 4 instance 2	Assigning bridge-group 4 to this instance
Bridge4(config-if)#bridge-group 4 instance 3	Assigning bridge-group 4 to this instance
Bridge4(config-if)#bridge-group 4 instance 4	Assigning bridge-group 4 to this instance
Bridge4(config-if)#bridge-group 4 instance 5	Assigning bridge-group 4 to this instance
Bridge4(config-if)#exit	Exit interface mode.
Bridge4(config)#interface eth3	Enter the Interface mode for eth3
Bridge4(config-if)#bridge-group 4	Associating the interface to bridge-group 4
Bridge4(config-if)#bridge-group 4 instance 2	Assigning bridge-group 4 to this instance
Bridge4(config-if)#bridge-group 4 instance 3	Assigning bridge-group 4 to this instance
Bridge4(config-if)#bridge-group 4 instance 4	Assigning bridge-group 4 to this instance
Bridge4(config-if)#bridge-group 4 instance 5	Assigning bridge-group 4 to this instance
Bridge4(config-if)#exit	Exit interface mode.
Bridge4(config)#interface eth4	Enter the Interface mode for eth4
Bridge4(config-if)#bridge-group 4	Associating the interface to bridge-group 4
Bridge4(config-if)#bridge-group 4 instance 2	Assigning bridge-group 4 to this instance
Bridge4(config-if)#bridge-group 4 instance 3	Assigning bridge-group 4 to this instance
Bridge4(config-if)#bridge-group 4 instance 4	Assigning bridge-group 4 to this instance
Bridge4(config-if)#bridge-group 4 instance 5	Assigning bridge-group 4 to this instance
Bridge4(config-if)#exit	Exit interface mode.
Bridge4(config)#interface eth5	Enter the Interface mode for eth5
Bridge4(config-if)#bridge-group 4	Associating the interface to bridge-group 4
Bridge4(config-if)#bridge-group 4 instance 2	Assigning bridge-group 4 to this instance
Bridge4(config-if)#bridge-group 4 instance 3	Assigning bridge-group 4 to this instance
Bridge4(config-if)#bridge-group 4 instance 4	Assigning bridge-group 4 to this instance

Bridge4(config-if)#bridge-group 4 instance 5	Assigning bridge-group 4 to this instance
Bridge4(config-if)#exit	Exit interface mode.

Validation

show spanning-tree, show spanning-tree mst detail

```
    #sh spanning-tree mst detail
    % 1: Bridge up - Spanning Tree Enabled  - topology change detected
    % 1: CIST Root Path Cost 0 - CIST Root Port 4 - CIST Bridge Priority 32768 % 1:
    Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Max-hops
    20
    % 1: CIST Root Id 1000525400f8eafe
    % 1: CIST Reg Root Id 1000525400f8eafe
    % 1: CIST Bridge Id 8000525400045cf1
    % 1: 38 topology change(s)  - last topology change Fri Mar  4 11:09:23 2016

    % 1: portfast bpdu-filter disabled
    % 1: portfast bpdu-guard disabled
    % 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Rootport - State
Forwarding
%   eth2: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth2: Designated Port Id 0x8004 - CIST Priority 128  -
%   eth2: CIST Root 1000525400f8eafe
%   eth2: Regional Root 1000525400f8eafe
%   eth2: Designated Bridge 1000525400f8eafe
%   eth2: Message Age 0 - Max Age 20
%   eth2: CIST Hello Time 2 - Forward Delay 15
%   eth2: CIST Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0 - topo change timer
0
%   eth2: forward-transitions 2
%   eth2: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Alternate - State
Discarding
%   eth3: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth3: Designated Port Id 0x8005 - CIST Priority 128  -
%   eth3: CIST Root 1000525400f8eafe
%   eth3: Regional Root 1000525400f8eafe
```

```
%   eth3: Designated Bridge 1000525400f8eafe
%   eth3: Message Age 0 - Max Age 20
%   eth3: CIST Hello Time 2 - Forward Delay 15
%   eth3: CIST Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0 - topo change timer
0
%   eth3: forward-transitions 2
%   eth3: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Designated - State
Forwarding
%   eth4: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth4: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth4: Designated Port Id 0x8006 - CIST Priority 128  -
%   eth4: CIST Root 1000525400f8eafe
%   eth4: Regional Root 1000525400f8eafe
%   eth4: Designated Bridge 8000525400045cf1
%   eth4: Message Age 0 - Max Age 20
%   eth4: CIST Hello Time 2 - Forward Delay 15
%   eth4: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer
0
%   eth4: forward-transitions 3
%   eth4: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%   eth4: Configured Link Type point-to-point - Current point-to-point
%   eth4: No auto-edge configured - Current port Auto Edge off
%
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Designated - State
Forwarding
%   eth5: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth5: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth5: Designated Port Id 0x8007 - CIST Priority 128  -
%   eth5: CIST Root 1000525400f8eafe
%   eth5: Regional Root 1000525400f8eafe
%   eth5: Designated Bridge 8000525400045cf1
%   eth5: Message Age 0 - Max Age 20
%   eth5: CIST Hello Time 2 - Forward Delay 15
%   eth5: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer
0
%   eth5: forward-transitions 3
%   eth5: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
```

```
%   eth5: No portfast configured - Current  portfast off
%   eth5: bpdu-guard  default  - Current bpdu-guard off
%   eth5: bpdu-filter default  - Current bpdu-filter off
%   eth5: no root guard configured     - Current root guard off
%   eth5: Configured Link Type point-to-point - Current point-to-point
%   eth5: No auto-edge configured - Current port Auto Edge off
%
% Instance  2:  Vlans: 2

% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 8002525400045cf1
% 1: MSTI Bridge Id 8002525400045cf1
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Designated - State
Forwarding
%   eth5: Designated Internal Path Cost 0  - Designated Port Id 0x8007
%   eth5: Configured Internal Path Cost 200000
%   eth5: Configured CST External Path cost 200000
%   eth5: CST Priority 128  - MSTI Priority 128
%   eth5: Designated Root 8002525400045cf1
%   eth5: Designated Bridge 8002525400045cf1
%   eth5: Message Age 0
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Designated - State
Forwarding
%   eth4: Designated Internal Path Cost 0  - Designated Port Id 0x8006
%   eth4: Configured Internal Path Cost 200000
%   eth4: Configured CST External Path cost 200000
%   eth4: CST Priority 128  - MSTI Priority 128
%   eth4: Designated Root 8002525400045cf1
%   eth4: Designated Bridge 8002525400045cf1
%   eth4: Message Age 0
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated - State
Forwarding
%   eth3: Designated Internal Path Cost 0  - Designated Port Id 0x8005
%   eth3: Configured Internal Path Cost 200000
%   eth3: Configured CST External Path cost 200000
%   eth3: CST Priority 128  - MSTI Priority 128
%   eth3: Designated Root 8002525400045cf1
%   eth3: Designated Bridge 8002525400045cf1
%   eth3: Message Age 0
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
```

```
%   eth2: Designated Internal Path Cost 0  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 200000
%   eth2: Configured CST External Path cost 200000
%   eth2: CST Priority 128  - MSTI Priority 128
%   eth2: Designated Root 8002525400045cf1
%   eth2: Designated Bridge 8002525400045cf1
%   eth2: Message Age 0
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

% Instance  3:  Vlans: 3

% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 8003525400045cf1
% 1: MSTI Bridge Id 8003525400045cf1
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Designated - State
Forwarding
%   eth5: Designated Internal Path Cost 0  - Designated Port Id 0x8007
%   eth5: Configured Internal Path Cost 200000
%   eth5: Configured CST External Path cost 200000
%   eth5: CST Priority 128  - MSTI Priority 128
%   eth5: Designated Root 8003525400045cf1
%   eth5: Designated Bridge 8003525400045cf1
%   eth5: Message Age 0
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Designated - State
Forwarding
%   eth4: Designated Internal Path Cost 0  - Designated Port Id 0x8006
%   eth4: Configured Internal Path Cost 200000
%   eth4: Configured CST External Path cost 200000
%   eth4: CST Priority 128  - MSTI Priority 128
%   eth4: Designated Root 8003525400045cf1
%   eth4: Designated Bridge 8003525400045cf1
%   eth4: Message Age 0
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Designated - State
Forwarding
%   eth3: Designated Internal Path Cost 0  - Designated Port Id 0x8005
%   eth3: Configured Internal Path Cost 200000
%   eth3: Configured CST External Path cost 200000
%   eth3: CST Priority 128  - MSTI Priority 128
%   eth3: Designated Root 8003525400045cf1
%   eth3: Designated Bridge 8003525400045cf1
%   eth3: Message Age 0
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
```

```
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated Internal Path Cost 0  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 200000
%   eth2: Configured CST External Path cost 200000
%   eth2: CST Priority 128  - MSTI Priority 128
%   eth2: Designated Root 8003525400045cf1

#sh spanning-tree
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
 % 1: CIST Root Path Cost 0 - CIST Root Port 4 -  CIST Bridge Priority 32768 % 1:
Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Max-hops 20
% 1: CIST Root Id 1000525400f8eafe
% 1: CIST Reg Root Id 1000525400f8eafe
% 1: CIST Bridge Id 8000525400045cf1
% 1: 38 topology change(s)  - last topology change Fri Mar  4 11:09:23 2016

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Rootport - State
Forwarding
%   eth2: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth2: Designated Port Id 0x8004 - CIST Priority 128  -
%   eth2: CIST Root 1000525400f8eafe
%   eth2: Regional Root 1000525400f8eafe
%   eth2: Designated Bridge 1000525400f8eafe
%   eth2: Message Age 0 - Max Age 20
%   eth2: CIST Hello Time 2 - Forward Delay 15
%   eth2: CIST Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1 - topo change timer
0
%   eth2: forward-transitions 2
%   eth2: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point
%   eth2: No auto-edge configured - Current port Auto Edge off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - Role Alternate - State
Discarding
%   eth3: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth3: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth3: Designated Port Id 0x8005 - CIST Priority 128  -
%   eth3: CIST Root 1000525400f8eafe
%   eth3: Regional Root 1000525400f8eafe
%   eth3: Designated Bridge 1000525400f8eafe
```

```
%   eth3: Message Age 0 - Max Age 20
%   eth3: CIST Hello Time 2 - Forward Delay 15
%   eth3: CIST Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1 - topo change timer
0
%   eth3: forward-transitions 2
%   eth3: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   eth3: No portfast configured - Current  portfast off
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%   eth3: Configured Link Type point-to-point - Current point-to-point
%   eth3: No auto-edge configured - Current port Auto Edge off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - Role Designated - State
Forwarding
%   eth4: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth4: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth4: Designated Port Id 0x8006 - CIST Priority 128  -
%   eth4: CIST Root 1000525400f8eafe
%   eth4: Regional Root 1000525400f8eafe
%   eth4: Designated Bridge 8000525400045cf1
%   eth4: Message Age 0 - Max Age 20
%   eth4: CIST Hello Time 2 - Forward Delay 15
%   eth4: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer
0
%   eth4: forward-transitions 3
%   eth4: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   eth4: No portfast configured - Current  portfast off
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%   eth4: Configured Link Type point-to-point - Current point-to-point
%   eth4: No auto-edge configured - Current port Auto Edge off
%
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - Role Designated - State
Forwarding
%   eth5: Designated External Path Cost 0 -Internal Path Cost 200000
%   eth5: Configured Path Cost 200000  - Add type Explicit ref count 5
%   eth5: Designated Port Id 0x8007 - CIST Priority 128  -
%   eth5: CIST Root 1000525400f8eafe
%   eth5: Regional Root 1000525400f8eafe
%   eth5: Designated Bridge 8000525400045cf1
%   eth5: Message Age 0 - Max Age 20
%   eth5: CIST Hello Time 2 - Forward Delay 15
%   eth5: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer
0
%   eth5: forward-transitions 3
%   eth5: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   eth5: No portfast configured - Current  portfast off
```

```
%   eth5: bpdu-guard  default  - Current bpdu-guard off
%   eth5: bpdu-filter default  - Current bpdu-filter off
%   eth5: no root guard configured     - Current root guard off
%   eth5: Configured Link Type point-to-point - Current point-to-point
%   eth5: No auto-edge configured - Current port Auto Edge off
%
%
% Default: Bridge up - Spanning Tree Enabled
% Default: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% Default: Root Id 8000000000000000
% Default: Bridge Id 8000000000000000
% Default: last topology change Wed Dec 31 19:00:00 1969
% Default: 0 topology change(s)  - last topology change Wed Dec 31 19:00:00 1969

% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled
% Default: portfast errdisable timeout disabled
% Default: portfast errdisable timeout interval 300 sec %
```

CHAPTER 4 Disable Spanning Tree Configuration

This chapter describes disabling spanning tree operation on a per Multiple Spanning Tree Instance (MSTI) basis.

Topology

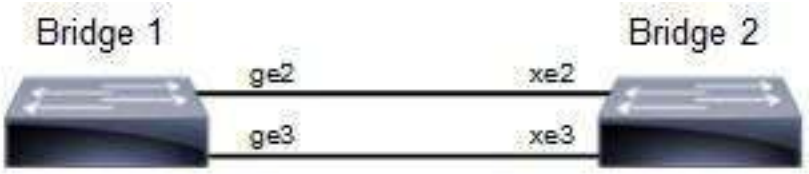


Figure 4-53: Disable Spanning Tree Topology Note:

Run the `switchport` command on each port to change to Layer-2 mode.

Disabling MSTP Configuration

Bridge 1

Disabling MSTP per instance

`Bridge1(config-mst)#no bridge 1 instance 2`	Disable spanning tree for MSTP on instance 2
`Bridge1(config-mst)#no bridge 1 instance 2`	Disable spanning tree for MSTP on instance 3

Disabling MSTP globally

`Bridge1(config)#no bridge 1 multiplespanning-tree enable bridge-forward`	Disable spanning tree globally for MSTP and keeping the ports in forwarding state.

Disabling MSTP per port

`Bridge1(config)#interface ge2`	Enter the Interface mode for ge2.
`Bridge1(config-if)#bridge-group 1 spanningtree disable`	Disable spanning tree per port for MSTP and put port on forwarding state [This command disable any type of STP on the port].

Bridge 2

Disabling MSTP per instance

`Bridge1(config-mst)#no bridge 1 instance 2`	Disable spanning tree for MSTP on instance 2
`Bridge1(config-mst)#no bridge 1 instance 2`	Disable spanning tree for MSTP on instance 3

Disabling MSTP globally

`Bridge1(config)#no bridge 1 multiplespanning-tree`	Disable spanning tree globally for MSTP.

Disabling MSTP per port

`Bridge1(config)#interface xe2`	Enter the Interface mode for xe2.
`Bridge1(config-if)#bridge-group 1 spanningtree disable`	Disable spanning tree per port for MSTP and put port on forwarding state [This command disable any type of STP on the port].

Validation

show spanning-tree mst detail, show spanning-tree mst instance<instance_id>, show spanning-tree **Bridge 1**

Verify MSTP details when applying "`show spanning-tree mst detail`" command

```
#show spanning-tree mst detail
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: CIST Root Path Cost 0 - CIST Root Port 905 -  CIST Bridge Priority 32768 %
1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 -
Max-hops 20
% 1: CIST Root Id 80003417ebfbe9c4
% 1: CIST Reg Root Id 80003417ebfbe9c4
% 1: CIST Bridge Id 800064006ac779a0
% 1: 9 topology change(s)  - last topology change Thu Nov 17 15:06:17 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Rootport -
State Forwarding
%   ge2: Designated External Path Cost 0 -Internal Path Cost 20000
%   ge2: Configured Path Cost 20000  - Add type Explicit ref count 2
%   ge2: Designated Port Id 0x838a - CIST Priority 128  -
%   ge2: CIST Root 80003417ebfbe9c4
%   ge2: Regional Root 80003417ebfbe9c4
%   ge2: Designated Bridge 80003417ebfbe9c4
%   ge2: Message Age 0 - Max Age 20
%   ge2: CIST Hello Time 2 - Forward Delay 15
%   ge2: CIST Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change
timer 0
%   ge2: forward-transitions 1
%   ge2: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   ge2: No portfast configured - Current  portfast off
%   ge2: bpdu-guard  default  - Current bpdu-guard off
%   ge2: bpdu-filter default  - Current bpdu-filter off
%   ge2: no root guard configured     - Current root guard off
```

```
%   ge2: Configured Link Type point-to-point - Current point-to-point
%   ge2: No auto-edge configured - Current port Auto Edge off %
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Alternate
- State Discarding
%   ge3: Designated External Path Cost 0 -Internal Path Cost 20000
%   ge3: Configured Path Cost 20000  - Add type Explicit ref count 2
%   ge3: Designated Port Id 0x838b - CIST Priority 128  -
%   ge3: CIST Root 80003417ebfbe9c4
%   ge3: Regional Root 80003417ebfbe9c4
%   ge3: Designated Bridge 80003417ebfbe9c4
%   ge3: Message Age 0 - Max Age 20
%   ge3: CIST Hello Time 2 - Forward Delay 15
%   ge3: CIST Forward Timer 0 - Msg Age Timer 5 - Hello Timer 1 - topo change
timer 0
%   ge3: forward-transitions 2
%   ge3: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   ge3: No portfast configured - Current  portfast off
%   ge3: bpdu-guard  default  - Current bpdu-guard off
%   ge3: bpdu-filter default  - Current bpdu-filter off
%   ge3: no root guard configured     - Current root guard off
%   ge3: Configured Link Type point-to-point - Current point-to-point
%   ge3: No auto-edge configured - Current port Auto Edge off

% Instance  2:  Vlans: 2

% 1: MSTI Root Path Cost 20000 -MSTI Root Port 5001 - MSTI Bridge Priority
32768
% 1: MSTI Root Id 80023417ebfbe9c4
% 1: MSTI Bridge Id 800264006ac779a0
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Rootport -
State Forwarding
%   ge2: Designated Internal Path Cost 0  - Designated Port Id 0x838a
%   ge2: Configured Internal Path Cost 20000
%   ge2: Configured CST External Path cost 20000
%   ge2: CST Priority 128  - MSTI Priority 128
%   ge2: Designated Root 80023417ebfbe9c4
%   ge2: Designated Bridge 800264006ac779a0
%   ge2: Message Age 0
%   ge2: Hello Time 2 - Forward Delay 15
%   ge2: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0

% Instance  3:  Vlans: 3

% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 800364006ac779a0
% 1: MSTI Bridge Id 800364006ac779a0
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Designated
- State Forwarding
%   ge3: Designated Internal Path Cost 0  - Designated Port Id 0x838c
%   ge3: Configured Internal Path Cost 20000
%   ge3: Configured CST External Path cost 20000
```

```
%   ge3: CST Priority 128  - MSTI Priority 128
%   ge3: Designated Root 800364006ac779a0
%   ge3: Designated Bridge 800364006ac779a0
%   ge3: Message Age 0
%   ge3: Hello Time 2 - Forward Delay 15
%   ge3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
```

- MSTP global configurations
- Verify MSTP configurations when MSTP is enabled globally

```
#show running-config
!
bridge 1 protocol mstp !
```

- Verify MSTP configurations when MSTP is disabled globally

```
#show running-config
! bridge 1 protocol mstp
no bridge 1 multiple-spanning-tree enable bridge-forward !
```

- MSTP per instance configurations
- Verify MSTP configurations when MSTP instance 2 and 3 is enabled.

```
#show running-config spanning-tree
! spanning-tree mst configuration bridge 1 instance 2
bridge 1 instance 2 vlan 2 bridge 1 instance 3 bridge
1 instance 3 vlan 3
! interface xe2 bridge-group 1 instance 2
! interface xe3 bridge-group 1 instance 3 !
```

- Verify MSTP configurations when MSTP instance 2 is disabled

```
#show running-config spanning-tree
! spanning-tree mst configuration bridge 1 instance
3 bridge 1 instance 3 vlan 3
! interface ge3 bridge-group 1 instance 3 !
```

- MSTP interface configurations
- Verify MSTP configurations when spanning-tree is enabled on interface.

```
#show running-config interface ge2
! interface ge2 switchport bridge-group 1
switchport mode access switchport access vlan
2 bridge-group 1 instance 2 !
```

- Verify MSTP configurations when spanning-tree is disabled on interface.

```
#show running-config interface ge2
! interface ge2 switchport
bridge-group 1 spanning-tree disable
switchport mode access switchport
access vlan 2 bridge-group 1
instance 2
```

- Verify MSTP details after disabling spanning-tree on interface ge2 by applying “show spanning-tree mst details” command.

```
#show spanning-tree mst detail
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: CIST Root Path Cost 0 - CIST Root Port 908 -  CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Max-
hops 20
% 1: CIST Root Id 80003417ebfbe9c4
% 1: CIST Reg Root Id 80003417ebfbe9c4
% 1: CIST Bridge Id 800064006ac779a0
% 1: 10 topology change(s)  - last topology change Fri Nov 25 21:21:05 2016

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
```

```
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Disabled - State
Forwarding
%   ge2: Designated External Path Cost 0 -Internal Path Cost 20000
%   ge2: Configured Path Cost 20000  - Add type Explicit ref count 2
%   ge2: Designated Port Id 0x838a - CIST Priority 128  -
%   ge2: Message Age 0 - Max Age 20
%   ge2: CIST Hello Time 2 - Forward Delay 15
%   ge2: CIST Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change
timer 0
%   ge2: forward-transitions 2
%   ge2: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   ge2: No portfast configured - Current  portfast off
%   ge2: bpdu-guard  default  - Current bpdu-guard off
%   ge2: bpdu-filter default  - Current bpdu-filter off
%   ge2: no root guard configured     - Current root guard off
%   ge2: Configured Link Type point-to-point - Current point-to-point
%   ge2: No auto-edge configured - Current port Auto Edge off
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Rootport - State
Forwarding
%   ge3: Designated External Path Cost 0 -Internal Path Cost 20000
%   ge3: Configured Path Cost 20000  - Add type Explicit ref count 2
%   ge3: Designated Port Id 0x838b - CIST Priority 128  -
%   ge3: CIST Root 80003417ebfbe9c4
%   ge3: Regional Root 80003417ebfbe9c4
%   ge3: Designated Bridge 80003417ebfbe9c4
%   ge3: Message Age 0 - Max Age 20
%   ge3: CIST Hello Time 2 - Forward Delay 15
%   ge3: CIST Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1 - topo change
timer 0
%   ge3: forward-transitions 3
%   ge3: Version Multiple Spanning Tree Protocol - Received MSTP - Send MSTP
%   ge3: No portfast configured - Current  portfast off
%   ge3: bpdu-guard  default  - Current bpdu-guard off
%   ge3: bpdu-filter default  - Current bpdu-filter off
%   ge3: no root guard configured     - Current root guard off
%   ge3: Configured Link Type point-to-point - Current point-to-point
%   ge3: No auto-edge configured - Current port Auto Edge off
  % Instance  2:  Vlans: 2

  % 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
  % 1: MSTI Root Id 800264006ac779a0
  % 1: MSTI Bridge Id 800264006ac779a0
  %   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Disabled -
  State Discarding
  %   ge2: Designated Internal Path Cost 0  - Designated Port Id 0x8389
  %   ge2: Configured Internal Path Cost 20000
  %   ge2: Configured CST External Path cost 20000
```

```
%   ge2: CST Priority 128  - MSTI Priority 128
%   ge2: Designated Root 800264006ac779a0
%   ge2: Designated Bridge 800264006ac779a0
%   ge2: Message Age 0
%   ge2: Hello Time 2 - Forward Delay 15
%   ge2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0

% Instance  3:  Vlans: 3

% 1: MSTI Root Path Cost 20000 -MSTI Root Port 5004 - MSTI Bridge Priority
32768
% 1: MSTI Root Id 80033417ebfbe9c4
% 1: MSTI Bridge Id 800364006ac779a0
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Rootport -
State Forwarding
%   ge3: Designated Internal Path Cost 0  - Designated Port Id 0x838b
%   ge3: Configured Internal Path Cost 20000
%   ge3: Configured CST External Path cost 20000
%   ge3: CST Priority 128  - MSTI Priority 128
%   ge3: Designated Root 80033417ebfbe9c4
%   ge3: Designated Bridge 800364006ac779a0
%   ge3: Message Age 0
%   ge3: Hello Time 2 - Forward Delay 15
%   ge3: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1
```

STP Configuration

Bridge 1

Disabling STP globally

`Bridge1(config)#no bridge 1 spanning-tree enable bridge-forward`	Disable spanning tree globally for STP.

Disabling STP per port

`Bridge1(config)#interface ge2`	Enter the Interface mode for ge2.
`Bridge1(config-if)#bridge-group 1 spanningtree disable`	Disable spanning tree per port for STP and put port on forwarding state [This command disable any type of STP on the port]

Bridge 2

Disabling STP globally

`Bridge1(config)#no bridge 1 spanning-tree enable bridge-forward`	Disable spanning tree globally for STP.

Disabling STP per port

`Bridge1(config)#interface xe2`	Enter the Interface mode for xe2.
`Bridge1(config-if)#bridge-group 1 spanningtree disable`	Disable spanning tree per port for STP and put port on forwarding state [This command disable any type of STP on the port]

Validation

show spanning-tree, show spanning-tree <interface name> **Bridge 1**

- Verify STP details when stp is enabled globally and ge2 and ge3 are part of the bridge using “show spanningtree” command.

```
#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled - topology change
% 1: Root Path Cost 4 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root port 905
% 1: Root Id 80003417ebfbe9c4
% 1: Bridge Id 800064006ac779a0
% 1: 3 topology changes - last topology change Tue Nov 15 21:33:53 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec

%ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - path cost 4
- designated cost 0
%ge2: Designated Port Id 0x838a - state Forwarding -Priority 128
%ge2: Designated root 80003417ebfbe9c4
%ge2: Designated Bridge 80003417ebfbe9c4
%ge2: Message Age 0 - Max Age 20
%ge2: Hello Time 2 - Forward Delay 15
%ge2: Forward Timer 0 - Msg Age Timer 18 - Hello Timer 1 - topo change  timer0
%ge2: forward-transitions 1
%ge2: No portfast configured – Current  portfast
%ge2: bpdu-guard default- Current bpdu-guard off
%ge2: bpdu-filter default- Current bpdu-filter off
%ge2: no root guard configured- Current root guard off
%ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - path cost 4 - designated cost 0
%ge3: Designated Port Id 0x838b - state Blocked -Priority 128
```

```
%ge3: Designated root 80003417ebfbe9c4
%ge3: Designated Bridge 80003417ebfbe9c4
%ge3: Message Age 0 - Max Age 20
%ge3: Hello Time 2 - Forward Delay 15
%ge3: Forward Timer 0 - Msg Age Timer 19 - Hello Timer 1 - topo change timer0
%ge3: forward-transitions 0
%ge3: No portfast configured - Currentportfast off
%ge3: bpdu-guarddefault- Current bpdu-guard off
%ge3: bpdu-filter default- Current bpdu-filter off
%ge3: no root guard configured- Current root guard off %
```

- STP global configurations
- Verify STP configurations when STP is enabled globally

```
#show running-config
!
bridge 1 protocol ieee vlan-bridge !
```

- Verify STP configurations when STP is disabled globally

```
#show running-config
!
bridge 1 protocol ieee vlan-bridge
no bridge 1 spanning-tree enable bridge-forward !
```

- STP interface configurations
- Verify STP configurations when spanning-tree is enabled on interface.

```
#show running-config interface ge2
! interface ge2 switchport bridge-
group 1 switchport mode trunk
switchport trunk allowed vlan all !
```

- Verify STP configurations when spanning-tree is disabled on interface.

```
#show running-config interface ge2
! interface ge2
switchport
bridge-group 1 spanning-tree disable
switchport mode trunk switchport trunk
allowed vlan all !
```

- Verify STP details after disabling spanning-tree on interface ge2 by applying “show spanning-tree” command

```
#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 4 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6 - Root
port 908
% 1: Root Id 80003417ebfbe9c4
% 1: Bridge Id 800064006ac779a0
% 1: 5 topology changes - last topology change Fri Nov 25 21:15:35 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - path cost 4
- designated cost 0
%   ge2: Designated Port Id 0x838a - state Disabled -Priority 128
```

```
%   ge2: Message Age 0 - Max Age 20
%   ge2: Hello Time 2 - Forward Delay 15
%   ge2: Forward Timer 0 - Msg Age Timer 18 - Hello Timer 0 - topo change timer
23
%   ge2: forward-transitions 2
%   ge2: No portfast configured - Current  portfast off
%   ge2: bpdu-guard  default  - Current bpdu-guard off
%   ge2: bpdu-filter default  - Current bpdu-filter off
%   ge2: no root guard configured     - Current root guard off
%
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - path cost 4
- designated cost 0
%   ge3: Designated Port Id 0x838b - state Forwarding -Priority 128
%   ge3: Designated root 80003417ebfbe9c4
%   ge3: Designated Bridge 80003417ebfbe9c4
%   ge3: Message Age 0 - Max Age 20
%   ge3: Hello Time 2 - Forward Delay 15
%   ge3: Forward Timer 0 - Msg Age Timer 19 - Hello Timer 1 - topo change timer
23
%   ge3: forward-transitions 2
%   ge3: No portfast configured - Current  portfast off
%   ge3: bpdu-guard  default  - Current bpdu-guard off
%   ge3: bpdu-filter default  - Current bpdu-filter off
%   ge3: no root guard configured     - Current root guard off
```

RSTP Configuration

Bridge 1

Disabling RSTP globally

`Bridge1(config)#no bridge 1 rapid-spanningtree enable bridge-forward`	Disable spanning tree globally for RSTP.

Disabling RSTP per port

`Bridge1(config)#interface ge2`	Enter the Interface mode for ge2.
`Bridge1(config-if)#bridge-group 1 spanningtree disable`	Disable spanning tree per port for RSTP and put port on forwarding state [This command disable any type of STP on the port]

Bridge 2

Disabling RSTP globally

`Bridge1(config)#no bridge 1 rapid-spanningtree enable bridge-forward`	Disable spanning tree globally for RSTP.

Disabling RSTP per port

`Bridge1(config)#interface xe2`	Enter the Interface mode for xe2.
`Bridge1(config-if)#bridge-group 1 spanningtree disable`	Disable spanning tree per port for RSTP and put port on forwarding state [This command disable any type of STP on the port]

Validation

show spanning-tree, show spanning-tree <interface name>

Bridge 1

• Verify RSTP details when rstp is enabled globally and ge2 and ge3 are part of the bridge using “show spanningtree” command.

```
#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled- topology change detected
% 1: Root Path Cost 20000 - Root Port 905 -Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 80003417ebfbe9c4
% 1: Bridge Id 800064006ac779a0
% 1: last topology change Tue Nov 15 21:44:31 2016
% 1: 7 topology change(s)- last topology change Tue Nov 15 21:44:31 2016
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Rootport -
State Forwarding
% ge2: Designated Path Cost 0
% ge2: Configured Path Cost 20000- Add type Explicit ref count 1
% ge2: Designated Port Id 0x838a - Priority 128-
% ge2: Root 80003417ebfbe9c4
% ge2: Designated Bridge 80003417ebfbe9c4
% ge2: Message Age 0 - Max Age 20
% ge2: Hello Time 2 - Forward Delay 15
% ge2: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 1 - topo change timer
0
% ge2: forward-transitions 1
% ge2: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
% ge2: No portfast configured - Currentportfast off
% ge2: bpdu-guarddefault- Current bpdu-guard off
% ge2: bpdu-filter default- Current bpdu-filter off
% ge2: no root guard configured- Current root guard off
% ge2: Configured Link Type point-to-point - Current point-to-point
% ge2: No auto-edge configured - Current port Auto Edge off
% ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Alternate -
State Discarding
% ge3: Designated Path Cost 0
```


© Symanitron Proprietary

```
% ge3: Configured Path Cost 20000- Add type Explicit ref count 1
% ge3: Designated Port Id 0x838b - Priority 128-
% ge3: Root 80003417ebfbe9c4
% ge3: Designated Bridge 80003417ebfbe9c4
% ge3: Message Age 0 - Max Age 20
% ge3: Hello Time 2 - Forward Delay 15
% ge3: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0 - topo change timer
0
% ge3: forward-transitions 2
% ge3: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
% ge3: No portfast configured - Currentportfast off
% ge3: bpdu-guarddefault- Current bpdu-guard off
% ge3: bpdu-filter default- Current bpdu-filter off
% ge3: no root guard configured- Current root guard off
% ge3: Configured Link Type point-to-point - Current point-to-point
% ge3: No auto-edge configured - Current port Auto Edge off %
```

- RSTP global configurations
- Verify RSTP configurations when RSTP is enabled globally

```
#show running-config
!
bridge 1 protocol rstp vlan-bridge !
```

- Verify RSTP configurations when RSTP is disabled globally

```
#show running-config
! bridge 1 protocol rstp vlan-bridge
no bridge 1 rapid-spanning-tree enable bridge-forward !
```

- RSTP interface configurations
- Verify RSTP configurations when spanning-tree is enabled on interface.

```
#show running-config interface ge2
! interface ge2 switchport bridge-
group 1 switchport mode trunk
switchport trunk allowed vlan all !
```

- Verify RSTP configurations when spanning-tree is enabled on interface.

```
#show running-config interface ge2
! interface ge2
switchport
bridge-group 1 spanning-tree disable
switchport mode trunk switchport trunk
allowed vlan all
```

- Verify RSTP details after disabling spanning-tree on interface ge2 by applying “show spanning-tree” command

```
#sh spanning-tree
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: Root Path Cost 20000 - Root Port 908 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 80003417ebfbe9c4
% 1: Bridge Id 800064006ac779a0
% 1: last topology change Fri Nov 25 21:08:56 2016
% 1: 11 topology change(s)  - last topology change Fri Nov 25 21:08:56 2016
```

```
    % 1: portfast bpdu-filter disabled
    % 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   ge2: Port Number 905 - Ifindex 5001 - Port Id 0x8389 - Role Disabled - State
Forwarding
%   ge2: Designated Path Cost 0
%   ge2: Configured Path Cost 20000  - Add type Explicit ref count 1
%   ge2: Designated Port Id 0x838a - Priority 128  -
%   ge2: Message Age 0 - Max Age 20
%   ge2: Hello Time 2 - Forward Delay 15
%   ge2: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0 - topo change timer 0
%   ge2: forward-transitions 2
%   ge2: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
%   ge2: No portfast configured - Current  portfast off
%   ge2: bpdu-guard  default  - Current bpdu-guard off
%   ge2: bpdu-filter default  - Current bpdu-filter off
%   ge2: no root guard configured     - Current root guard off
%   ge2: Configured Link Type point-to-point - Current point-to-point
%   ge2: No auto-edge configured - Current port Auto Edge off
%
%   ge3: Port Number 908 - Ifindex 5004 - Port Id 0x838c - Role Rootport - State
Forwarding
%   ge3: Designated Path Cost 0
%   ge3: Configured Path Cost 20000  - Add type Explicit ref count 1
%   ge3: Designated Port Id 0x838b - Priority 128  -
%   ge3: Root 80003417ebfbe9c4
%   ge3: Designated Bridge 80003417ebfbe9c4
%   ge3: Message Age 0 - Max Age 20
%   ge3: Hello Time 2 - Forward Delay 15
%   ge3: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 1 - topo change timer 0
%   ge3: forward-transitions 3
%   ge3: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
%   ge3: No portfast configured - Current  portfast off
%   ge3: bpdu-guard  default  - Current bpdu-guard off
%   ge3: bpdu-filter default  - Current bpdu-filter off
%   ge3: no root guard configured     - Current root guard off
%   ge3: Configured Link Type point-to-point - Current point-to-point
%   ge3: No auto-edge configured - Current port Auto Edge off
```

CHAPTER 5 RPVST+ Configuration

This chapter contains a complete example of an RPVST+ configuration.

Topology

Figure 5-54: RPVST+ configuration

Configuration

Switch 2

`#configure terminal`	Enter configure mode for the switch.
`(config)#bridge 1 protocol rpvst+`	Configure bridge 1 as an RPVST+ bridge.
`(config)#vlan 2-3 bridge 1`	Configure VLAN 2 and 3 and associate it to bridge 1.
`(config)#spanning-tree rpvst+ configuration`	Enter Rapid Per-VLAN Spanning Tree configuration mode.
`(config-rpvst+)#bridge 1 vlan 2`	Associate a configured VLAN with bridge 1.
`(config-rpvst+)#bridge 1 vlan 3`	Associate a configured VLAN with bridge 1,.
`(config-rvpst+)#exit`	Exit RPVST+ configuration mode.
`(config)#interface eth1`	Enter the interface mode for `eth1`.
`(config-if)#switchport`	Configure `eth1` as a Layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to interface.
`(config-if)#switchport mode trunk`	Configure port as trunk.
`(config-if)#switchport trunk allowed vlan add 2,3`	Configure VLAN 2 and VLAN 3 on interface.
`(config-if)#bridge-group 1 vlan 2`	Configure bridge group to interface with VLAN 2.
`(config-if)#bridge-group 1 vlan 3`	Configure bridge group to interface with VLAN 3.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode for `eth2`.
`(config-if)#switchport`	Configure `eth2` as a Layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to interface/
`(config-if)#switchport mode trunk`	Configure port as trunk
`(config-if)#switchport trunk allowed vlan add 2,3`	Configure VLAN 2 and VLAN 3 on interface.
`(config-if)#bridge-group 1 vlan 2`	Configure bridge group to interface with VLAN 2.

(config-if)#bridge-group 1 vlan 3	Configure bridge group to interface with VLAN3.
(config-if)#exit	Exit interface mode.

Switch 1

#configure terminal	Enter configure mode for the switch.
(config)#bridge 1 protocol rpvst+	Configure bridge 1 as an rpvst+ bridge.
(config)#vlan 2-3 bridge 1	Configure VLAN 2 and 3 and associate it to bridge 1.
(config)#interface eth1	Enter the Interface mode for `eth1`.
(config-if)#switchport	Configure `eth1` as a Layer 2 port.
(config-if)#bridge-group 1	Associate bridge to interface.
(config-if)#switchport mode trunk	Configure port as trunk.
(config-if)#switchport trunk allowed vlan add 2,3	Configure VLAN 2 and VLAN 3 on interface.
(config-if)#bridge-group 1 vlan 2	Configure bridge group to interface with VLAN 2.
(config-if)#bridge-group 1 vlan 3	Configure bridge group to interface with VLAN3.
(config-if)#exit	Exit interface mode.

Switch 3

#configure terminal	Enter configure mode for the switch.
(config)#bridge 1 protocol rpvst+	Configure bridge 1 as an rpvst+ bridge
(config)#vlan 2-3 bridge 1	Configure VLAN 2 and 3 and associate it to bridge 1.
(config)#interface eth1	Enter the Interface mode for `eth1`.
(config-if)#switchport	Configure `eth1` as a Layer 2 port.
(config-if)#bridge-group 1	Associate bridge to interface.
(config-if)#switchport mode trunk	Configure port as trunk.
(config-if)#switchport trunk allowed vlan add 2,3	Configure VLAN 2 and VLAN 3 on interface.
(config-if)#exit	Exit interface mode.

Validation

Switch2

```
#show spanning-tree rpvst+ vlan 2
% vlan 2 Instance 1 configured
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Root Id 8002525400b7bfa7
% 1: Bridge Id 8002525400b7bfa7
%    eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State
Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 200000
%   eth1: Configured External Path cost 200000
```

```
%   eth1: Configured Internal Priority 128 %
eth1: Configured External Priority 128 %
eth1: Designated Root 8002525400b7bfa7
%   eth1: Designated Bridge 8002525400b7bfa7
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated -
State Forwarding
%   eth2: Designated Internal Path Cost 0  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 200000
%   eth2: Configured External Path cost 200000
%   eth2: Configured Internal Priority 128
%   eth2: Configured External Priority 128
%   eth2: Designated Root 8002525400b7bfa7
%   eth2: Designated Bridge 8002525400b7bfa7
%   eth2: Message Age 0 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
%

#show spanning-tree rpvst+ interface eth1
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 8001525400b7bfa7
% 1: Bridge Id 8001525400b7bfa7
% 1: last topology change Wed Mar 28 15:33:06 2018
% 1: 2 topology change(s)  - last topology change Wed Mar 28 15:33:06 2018

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated -
State Forwarding
%   eth1: Designated External Path Cost 0 -Internal Path Cost 0
%   eth1: Configured Path Cost 200000  - Add type Explicit ref count 3
%   eth1: Designated Port Id 0x8003 - Priority 128  -
%   eth1: Root 8001525400b7bfa7
%   eth1: Designated Bridge 8001525400b7bfa7
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 2 - topo change timer 0
%   eth1: forward-transitions 1
%   eth1: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
```

```
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
%    eth1: Configured Link Type point-to-point - Current point-to-point
%   eth1: No auto-edge configured - Current port Auto Edge off
%
%
%
In
st
an
ce
VL
AN
%    0:             1
%    1:             2
%    2:             3



#show spanning-tree rpvst+ detail
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 8001525400b7bfa7
% 1: Bridge Id 8001525400b7bfa7
% 1: last topology change Wed Mar 28 15:33:06 2018
% 1: 2 topology change(s)  - last topology change Wed Mar 28 15:33:06 2018

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated -
State Forwarding
%   eth1: Designated External Path Cost 0 -Internal Path Cost 0
%   eth1: Configured Path Cost 200000  - Add type Explicit ref count 3
%   eth1: Designated Port Id 0x8003 - Priority 128  -
%   eth1: Root 8001525400b7bfa7
%   eth1: Designated Bridge 8001525400b7bfa7
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth1: forward-transitions 1
%   eth1: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
```

```
%    eth1: Configured Link Type point-to-point - Current point-to-point
%    eth1: No auto-edge configured - Current port Auto Edge off
%
%   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated -
State Forwarding
%   eth2: Designated External Path Cost 0 -Internal Path Cost 0
%   eth2: Configured Path Cost 200000  - Add type Explicit ref count 3
%   eth2: Designated Port Id 0x8004 - Priority 128  -
%   eth2: Root 8001525400b7bfa7
%   eth2: Designated Bridge 8001525400b7bfa7
%   eth2: Message Age 0 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%   eth2: forward-transitions 1
%   eth2: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
%   eth2: No portfast configured - Current  portfast off
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%   eth2: Configured Link Type point-to-point - Current point-to-point %
eth2: No auto-edge configured - Current port Auto Edge off %

% Instance  1:  Vlans: 2
%    eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State
Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 200000
%   eth1: Configured External Path cost 200000
%   eth1: Configured Internal Priority 128 %
eth1: Configured External Priority 128 %
eth1: Designated Root 8002525400b7bfa7
%   eth1: Designated Bridge 8002525400b7bfa7
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0


% Instance  1:  Vlans: 2
%    eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated Internal Path Cost 0  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 200000
%   eth2: Configured External Path cost 200000
%   eth2: Configured Internal Priority 128 %
eth2: Configured External Priority 128 %
eth2: Designated Root 8002525400b7bfa7
%   eth2: Designated Bridge 8002525400b7bfa7
%   eth2: Message Age 0 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
```

```
% Instance  2:  Vlans: 3
%    eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State
Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 200000
%   eth1: Configured External Path cost 200000
%   eth1: Configured Internal Priority 128 %
eth1: Configured External Priority 128 %
eth1: Designated Root 8003525400b7bfa7
%   eth1: Designated Bridge 8003525400b7bfa7
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
% Instance  2:  Vlans: 3
%    eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - Role Designated - State
Forwarding
%   eth2: Designated Internal Path Cost 0  - Designated Port Id 0x8004
%   eth2: Configured Internal Path Cost 200000
%   eth2: Configured External Path cost 200000
%   eth2: Configured Internal Priority 128 %
eth2: Configured External Priority 128 %
eth2: Designated Root 8003525400b7bfa7
%   eth2: Designated Bridge 8003525400b7bfa7
%   eth2: Message Age 0 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
```

CHAPTER 6 VLAN Configuration

This chapter contains a complete VLAN configuration.

Configuring VLAN Tags

Topology

This shows configuring a spanning tree bridge with VLAN tags on forwarding frames. VLAN port access is configured on port `eth2` on bridge 2, port `eth2` and `eth4` on bridge 1 and port `eth4` on bridge 4. Incoming tagged packets to bridge 2 will be forwarded only on these ports configured with VLAN port access.

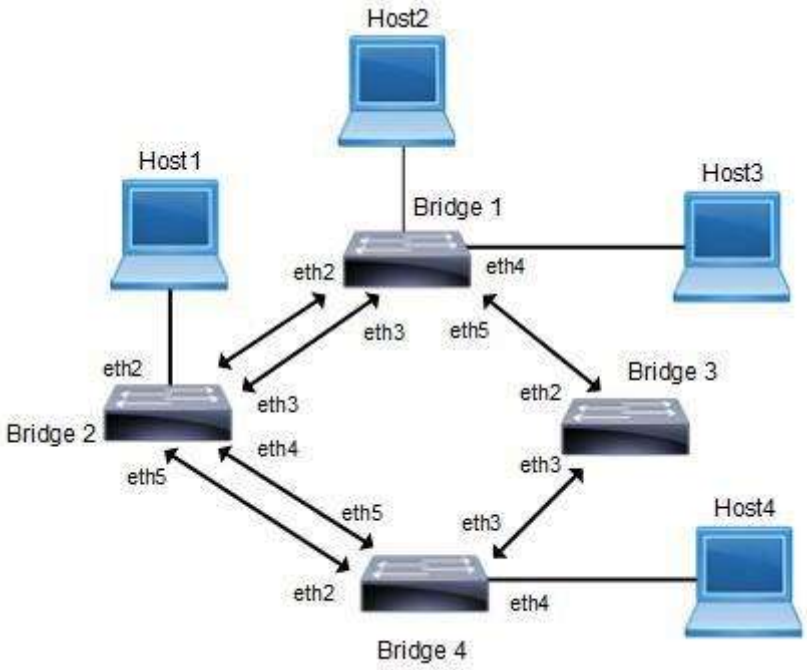


Figure 6-55: VLAN Topology

Note: Run the `switchport` command on each port to change to Layer-2 mode.

Bridge 1

`Bridge1#configure terminal`	Enter configure mode.
`Bridge1(config)#bridge 1 protocol ieee vlanbridge`	Specify VLAN for bridge `1`.
`Bridge1(config)#vlan database`	Enter the `VLAN` configuration mode.
`Bridge1(config-vlan)#vlan 5 bridge 1 state enable`	Enable VLAN `(5)` on bridge `1`. Specifying the `enable` state allows forwarding of frames on this VLAN-aware bridge.
`Bridge1(config-vlan)#exit`	Exit the `VLAN` configuration mode.
`Bridge1(config)#interface eth2`	Enter interface mode.

`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#switchport mode access`	Set the switching characteristics of this interface to access mode.
`Bridge1(config-if)#switchport access vlan 5`	Enable VLAN port access by specifying the VLAN ID `5` on this interface.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth3`	Enter interface mode.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#switchport mode access`	Set the switching characteristics of this interface to access mode.
`Bridge1(config-if)#switchport access vlan 5`	Enable all VLAN IDs on this port.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth4`	Enter interface mode.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#switchport mode access`	Set the switching characteristics of this interface to access mode.
`Bridge1(config-if)#switchport access vlan 5`	Enable VLAN port access by specifying the VLAN ID `5` on this interface.
`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth5`	Enter interface mode
`Bridge1(config-if)#bridge-group 1`	Associate the interface with bridge group `1`.
`Bridge1(config-if)#switchport mode access`	Set the switching characteristics of this interface to access mode.
`Bridge1(config-if)#switchport access vlan 5`	Enable all VLAN IDs on this port.

Bridge 2

`Bridge2#configure terminal`	Enter configure mode.
`Bridge2(config)#bridge 2 protocol ieee vlanbridge`	Specify VLAN for bridge `2`.
`Bridge2(config)#vlan database`	Enter the `VLAN` configuration mode.
`Bridge2(config-vlan)#vlan 5 bridge 2 state enable`	Enable VLAN `(5)` on bridge `2`. Specifying the `enable` state allows forwarding of frames on this VLAN-aware bridge.
`Bridge2(config-vlan)#exit`	Exit the `VLAN` configuration mode.
`Bridge2(config)#interface eth2`	Enter interface mode.
`Bridge2(config-if)#bridge-group 2`	Associate the interface with bridge group `2`.
`Bridge2(config-if)#switchport mode access`	Set the switching characteristics of this interface to access mode.
`Bridge2(config-if)#switchport access vlan 5`	Enable VLAN port access by specifying the VLAN ID `5` on this interface.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth3`	Enter interface mode.

Bridge2(config-if)#bridge-group 2	Associate the interface with bridge group 2.
Bridge2(config-if)#switchport mode access	Set the switching characteristics of this interface to access mode.
Bridge2(config-if)#switchport access vlan 5	Enable all VLAN IDs on this port.
Bridge2(config-if)#exit	Exit interface mode.
Bridge2(config)#interface eth4	Enter interface mode.
Bridge2(config-if)#bridge-group 2	Associate the interface with bridge group 2.
Bridge2(config-if)#switchport mode access	Set the switching characteristics of this interface to access mode.
Bridge2(config-if)#switchport access vlan 5	Enable all VLAN IDs on this port.
Bridge2(config-if)#exit	Exit interface mode.
Bridge2(config)#interface eth5	Enter interface mode
Bridge2(config-if)#bridge-group 2	Associate the interface with bridge group 2.
Bridge2(config-if)#switchport mode access	Set the switching characteristics of this interface to access mode.
Bridge2(config-if)#switchport access vlan 5	Enable all VLAN IDs on this port.

Bridge 4

Bridge4#configure terminal	Enter configure mode.
Bridge4(config)#bridge 4 protocol ieee vlanbridge	Specify VLAN for bridge 4.
Bridge4(config)#vlan database	Enter the VLAN configuration mode.
Bridge4(config-vlan)#vlan 5 bridge 4 state enable	Enable VLAN (5) on bridge 4. Specifying the enable state allows forwarding of frames on this VLAN-aware bridge.
Bridge4(config-vlan)#exit	Exit the VLAN configuration mode.
Bridge4(config)#interface eth2	Enter interface mode.
Bridge4(config-if)#bridge-group 4	Associate the interface with bridge group 4.
Bridge4(config-if)#switchport mode access	Set the switching characteristics of this interface to access mode.
Bridge4(config-if)#switchport access vlan 5	Enable all VLAN IDs on this port.
Bridge4(config-if)#exit	Exit interface mode.
Bridge4(config)#interface eth3	Enter interface mode.
Bridge4(config-if)#bridge-group 4	Associate the interface with bridge group 4.
Bridge4(config-if)#switchport mode access	Set the switching characteristics of this interface to access mode.
Bridge4(config-if)#switchport access vlan 5	Enable all VLAN IDs on this port.
Bridge4(config-if)#exit	Exit interface mode.
Bridge4(config)#interface eth4	Enter interface mode.
Bridge4(config-if)#bridge-group 4	Associate the interface with bridge group 4.

`Bridge4(config-if)#switchport mode access`	Set the switching characteristics of this interface to access mode.
`Bridge4(config-if)#switchport access vlan 5`	Enable VLAN port access by specifying the VLAN ID `5` on this interface.
`Bridge4(config-if)#exit`	Exit interface mode.
`Bridge4(config)#interface eth5`	Enter interface mode
`Bridge4(config-if)#bridge-group 4`	Associate the interface with bridge group `4`.
`Bridge4(config-if)#switchport mode access`	Set the switching characteristics of this interface to access mode.
`Bridge4(config-if)#switchport access vlan 5`	Enable all VLAN IDs on this port.

Bridge 3

`Bridge3#configure terminal`	Enter configure mode.
`Bridge3(config)#bridge 3 protocol ieee vlanbridge`	Specify VLAN for bridge `3`.
`Bridge3(config)#vlan database`	Enter the `VLAN` configuration mode.
`Bridge3(config-vlan)#vlan 5 bridge 3 state enable`	Enable VLAN `(5)` on bridge `3`. Specifying the `enable` state allows forwarding of frames on this VLAN-aware bridge.
`Bridge3(config-vlan)#exit`	Exit the `VLAN` configuration mode.
`Bridge3(config)#interface eth2`	Enter interface mode.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group `3`.
`Bridge3(config-if)#switchport mode access`	Set the switching characteristics of this interface to access mode.
`Bridge3(config-if)#switchport access vlan 5`	Enable all VLAN IDs on this port.
`Bridge3(config-if)#exit`	Exit interface mode.
`Bridge3(config)#interface eth3`	Enter interface mode.
`Bridge3(config-if)#bridge-group 3`	Associate the interface with bridge group `3`.
`Bridge3(config-if)#switchport mode access`	Set the switching characteristics of this interface to access mode.
`Bridge3(config-if)#switchport access vlan 5`	Enable all VLAN IDs on this port.

Validation

show spanning-tree, show bridge, show vlan all bridge <1-32>

Bridge 1

```
#sh spanning-tree
% 1: Bridge up - Spanning Tree Enabled - topology change - topology change
detected
% 1: Root Path Cost 0 - Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
- Root port 0
% 1: Root Id 8000525400045cf1
```

```
    % 1: Bridge Id 8000525400045cf1
    % 1: 25 topology changes - last topology change Fri Mar  4 11:21:33 2016
    % 1: portfast bpdu-filter disabled
    % 1: portfast bpdu-guard disabled
    % 1: portfast errdisable timeout disabled
    % 1: portfast errdisable timeout interval 300 sec
    %   eth2: Port Number 4 - Ifindex 4 - Port Id 0x8004 - path cost 19
    - designated cost 0
    %   eth2: Designated Port Id 0x8004 - state Forwarding -Priority 128
%   eth2: Designated root 8000525400045cf1
%   eth2: Designated Bridge 8000525400045cf1
%   eth2: Message Age 0 - Max Age 20
%   eth2: Hello Time 2 - Forward Delay 15
%   eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth2: forward-transitions 1
%   eth2: portfast disabled
%   eth2: bpdu-guard  default  - Current bpdu-guard off
%   eth2: bpdu-filter default  - Current bpdu-filter off
%   eth2: no root guard configured     - Current root guard off
%
%   eth3: Port Number 5 - Ifindex 5 - Port Id 0x8005 - path cost 19 - designated
cost 0
%   eth3: Designated Port Id 0x8005 - state Forwarding -Priority 128
%   eth3: Designated root 8000525400045cf1
%   eth3: Designated Bridge 8000525400045cf1
%   eth3: Message Age 0 - Max Age 20
%   eth3: Hello Time 2 - Forward Delay 15
%   eth3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth3: forward-transitions 1
%   eth3: portfast disabled
%   eth3: bpdu-guard  default  - Current bpdu-guard off
%   eth3: bpdu-filter default  - Current bpdu-filter off
%   eth3: no root guard configured     - Current root guard off
%
%   eth4: Port Number 6 - Ifindex 6 - Port Id 0x8006 - path cost 19 - designated
cost 0
%   eth4: Designated Port Id 0x8006 - state Forwarding -Priority 128
%   eth4: Designated root 8000525400045cf1
%   eth4: Designated Bridge 8000525400045cf1
%   eth4: Message Age 0 - Max Age 20
%   eth4: Hello Time 2 - Forward Delay 15
%   eth4: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%   eth4: forward-transitions 1
%   eth4: portfast disabled
%   eth4: bpdu-guard  default  - Current bpdu-guard off
%   eth4: bpdu-filter default  - Current bpdu-filter off
%   eth4: no root guard configured     - Current root guard off
%
```

```
%   eth5: Port Number 7 - Ifindex 7 - Port Id 0x8007 - path cost 19 - designated
cost 0
%   eth5: Designated Port Id 0x8007 - state Forwarding -Priority 128
%   eth5: Designated root 8000525400045cf1
%   eth5: Designated Bridge 8000525400045cf1
%   eth5: Message Age 0 - Max Age 20
%   eth5: Hello Time 2 - Forward Delay 15
%   eth5: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
%   eth5: forward-transitions 1
%   eth5: portfast disabled
%   eth5: bpdu-guard  default  - Current bpdu-guard off
%   eth5: bpdu-filter default  - Current bpdu-filter off
%   eth5: no root guard configured     - Current root guard off
%
%
    % Default: Bridge up - Spanning Tree Enabled
    % Default: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
    % Default: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count
    6
    % Default: Root Id 8000000000000000
    % Default: Bridge Id 8000000000000000
    % Default: last topology change Wed Dec 31 19:00:00 1969
    % Default: 0 topology change(s) - last topology change Wed Dec 31 19:00:00
    1969

    % Default: portfast bpdu-filter disabled
    % Default: portfast bpdu-guard disabled
    % Default: portfast errdisable timeout disabled
    % Default: portfast errdisable timeout interval 300 sec
    %

    #sh bridge
     Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
     --------+------+------+------+-----------+-----------------+-----+---------+
     1         1                   eth3         5254.0080.580f    1     0
     1         1                   eth2         5254.0004.5cf1    1     0
     1         1                   eth4         5254.0076.d6ca    1     0
     1         1                   eth5         5254.009c.2980    1     0
     1         5                   eth4         5254.00df.9a70    1     0

    #sh vlan all bridge 1
    Bridge  VLAN ID     Name          State   H/W Status      Member ports
                                                            (u)-Untagged, (t)-Tagged
    ======= ======= ================ ======= ========== =========================
    1       1       default          ACTIVE  Up
    1          5      VLAN0005         ACTIVE  Up         eth5(u) eth4(u) eth3(u)
              eth2(u)
```

Bridge 2

```
    #sh bridge
```

```
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 --------+------+------+------+-----------+-----------------+-----+---------+
2         1                   eth3         5254.00af.5bc8    1     0
 2         1                   eth2         5254.00f8.eafe    1     0
 2         1                   eth5         5254.0087.be52    1     0
 2         1                   eth4         5254.00ec.944d    1     0
 2         5                   eth2         5254.0004.5cf1    1     298

#sh vlan all bridge 2
Bridge  VLAN ID     Name          State   H/W Status      Member ports
                                                        (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ============================
2       1        default          ACTIVE  Up
2         5        VLAN0005         ACTIVE  Up         eth5(u) eth4(u) eth3(u)
          eth2(u)
```

Bridge 3

```
#sh bridge
 Bridge    CVLAN   SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 --------  +------ +------+------+----------  +----------------  +-----+---------+
3         1                   eth3         5254.0070.ee80    1     0
 3         1                   eth2         5254.0040.1fcb    1     0
 3         5                   eth2         eead.6f29.c890    1     232
 3         5                   eth2         5254.009c.2980    1     298

#sh vlan all bridge 3
Bridge  VLAN ID     Name          State   H/W Status      Member ports
                                                        (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ============================
3       1        default          ACTIVE  Up
3         5        VLAN0005         ACTIVE  Up         eth2(u) eth3(u)
```

Bridge 4

```
#sh bridge
 Bridge    CVLAN   SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 --------  +------ +------+------+----------  +----------------  +-----+---------+
4         1                   eth5         5254.00ce.b49e    1     0
 4         1                   eth3         5254.00a9.f69f    1     0
 4         5                   eth4         5254.0076.d6ca    1     298
 4         1                   eth2         5254.0066.d3de    1     0
 4         1                   eth4         5254.00df.9a70    1     0

#sh vlan all bridge 4
Bridge  VLAN ID     Name          State   H/W Status      Member ports
                                                        (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ============================
4       1        default          ACTIVE  Up
4       5       VLAN0005         ACTIVE  Up         eth5(u) eth4(u) eth3(u)
eth2(u)
```

CHAPTER 7 802.1X Configuration

IEEE 802.1x restricts unauthenticated devices from connecting to a switch. Only after authentication is successful, traffic is allowed through the switch.

Topology

In this example, a radius server keeps the client information, validating the identity of the client and updating the switch about the authentication status of the client. The switch is the physical access between the two clients and the server. It requests information from the client, relays information to the server and then back to the client. To configure 802.1x authentication, enable authentication on ports eth1 and eth and specify the radius server IP address and port.

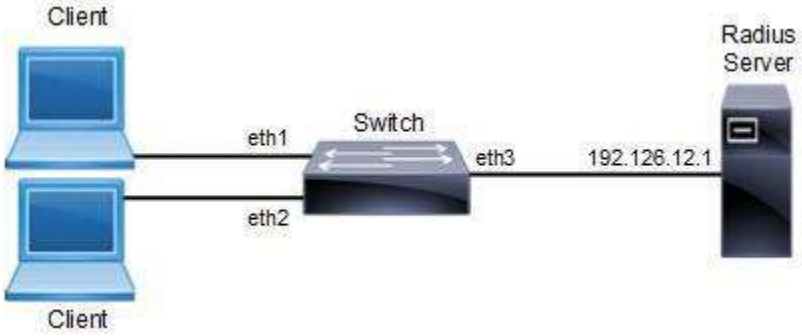


Figure 7-56: 802.1x Topology

Switch Configuration

`Switch#configure terminal`	Enter configure mode.
`Switch(config)#dot1x system-auth-ctrl`	Enable authentication globally.
`Switch(config)#interface eth2`	Enter interface mode.
`Switch(config-if)#dot1x port-control auto`	Enable authentication (via Radius) on port (`eth2`).
`Switch(config-if)#exit`	Exit interface mode.
`Switch(config)#interface eth1`	Enter interface mode.
`Switch(config-if)#dot1x port-control auto`	Enable authentication (via Radius) on port (`eth1`).
`Switch(config-if)#exit`	Exit interface mode.
`Switch(config)#radius-server host 192.126.12.1 auth-port 1812`	Specify the Radius Server address (`192.126.12.1`) and port.
`Switch(config)#radius-server key myKey`	Specify the shared key `myKey` between the radius server and the client.
`Switch(config)#interface eth3`	Enter interface mode.
`Switch(config-if)#ip address 192.126.12.0/24`	Set the IP address on interface `eth3`.

Validation

show dot1x, show dot1x all

```
#show dot1x all
802.1X Port-Based Authentication Enabled
```

802.1X Configuration

```
  RADIUS server address: 192.126.12.1:1812
  Next radius message id: 0
  RADIUS client address: not configured

802.1X info for interface ge1   Supplicant address:
0000.0000.0000 portEnabled: false - portControl: Auto
portStatus: Unauthorized - currentId: 1 protocol
version: 2 reAuthenticate: disabled reAuthPeriod: 3600

  abort:F fail:F start:F timeout:F success:F
  PAE: state: Connected - portMode: Auto
  PAE: reAuthCount: 0 - rxRespId: 0
  PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
  BE: state: Invalid - reqCount: 0 - idFromServer: 0
  BE: suppTimeout: 30 - serverTimeout: 30
  CD: adminControlledDirections: in - operControlledDirections: in
  CD: bridgeDetected: false
  KR: rxKey: false
  KT: keyAvailable: false - keyTxEnabled: false


#show dot1x
802.1X Port-Based Authentication Enabled
  RADIUS server address: 192.126.12.1:1812
  Next radius message id: 0
  RADIUS client address: not configured
```

CHAPTER 8 LACP Configuration

This chapter contains a complete sample Link Aggregation Control Protocol (LACP) configuration.

LACP is based on the 802.3ad IEEE specification. It allows bundling of several physical interfaces to form a single logical channel providing enhanced performance and redundancy. The aggregated interface is viewed as a single link to each switch. The spanning tree views it as one interface and not as two or three interfaces. When there is a failure in one physical interface, the other interfaces stay up and there is no disruption. The SWMRE LACP implementation support physical Ethernet links into a single logical channel is depend on Hardware support.

Topology

In this example, 3 links are configured between the two switches S1 and S2. These three links are assigned the same administrative key (1) so that they aggregate to form a single channel 1. They are viewed by the STP as one interface.

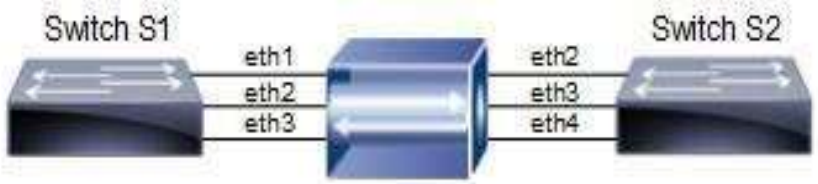


Figure 8-57: LACP Topology

Note: Run the `switchport` command on each port to change to Layer-2 mode.

Configuration

S1

`S1#configure terminal`	Enter configure mode.
`S1(config)#lacp system-priority 20000`	Set the system priority of this switch. This priority is used for determining the system that is responsible for resolving conflicts in the choice of aggregation groups. A lower numerical value has a higher priority.
`S1(config)#interface eth1`	Enter interface mode.
`S1(config-if)#channel-group 10 mode active`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`S1(config-if)#exit`	Exit interface mode.
`S1(config)#interface eth2`	Enter interface mode.
`S1(config-if)#channel-group 10 mode active`	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
`S1(config-if)#exit`	Exit interface mode.

S1(config)#interface eth3	Enter interface mode.
S1(config-if)#channel-group 10 mode active	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.

LACP Configuration

S2

S2#configure terminal	Enter configure mode.
S2(config)#lacp system-priority 20000	Set the system priority of this switch. This priority is used for determining the system that is responsible for resolving conflicts in the choice of aggregation groups. A lower numerical value has a higher priority.
S2(config)#interface eth2	Enter interface mode.
S2(config-if)#channel-group 10 mode active	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
S2(config-if)#exit	Exit interface mode.
S2(config)#interface eth3	Enter interface mode.
S2(config-if)#channel-group 10 mode active	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
S2(config-if)#exit	Exit interface mode.
S2(config)#interface eth4	Enter interface mode.
S2(config-if)#channel-group 10 mode active	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.

Validation

show etherchannel detail, show etherchannel summary

```
#show etherchannel detail
% Aggregator po10 7
%  Mac address: 08:00:27:50:6a:9b
%  Admin Key: 0010 - Oper Key 0010
%  Actor LAG ID- 0x4e20,08-00-27-ab-ea-38,0x000a
%  Receive link count: 3 - Transmit link count: 3
%  Individual: 0 - Ready: 1
%  Partner LAG ID- 0x4e20,08-00-27-f8-3c-30,0x000a
%   Link: eth1 (3) sync: 1
%   Link: eth2 (4) sync: 1
%   Link: eth3 (5) sync: 1

#show etherchannel summary
% Aggregator po10 7
% Admin Key: 0010 - Oper Key 0010
```

```
%   Link: eth1 (3) sync: 1
%   Link: eth2 (4) sync: 1
%   Link: eth3 (5) sync: 1
```

CHAPTER 9 MC-LAG Configuration

This chapter contains a complete example of Multi-Chassis Link Aggregation (MC-LAG) configuration.

MC-LAG (also called DRNI, Distributed Resilient Network Interconnect) expands the concept of link aggregation so that it provides node-level redundancy by allowing two or more nodes to share a common LAG endpoint. It emulates multiple nodes to represent as a single logical node to the remote node running Link aggregation. As a result even if one of the nodes is down there exists a path to reach the destination through the other nodes.

Note: MC-LAG is only compatible with RSTP.

Topology

In the below example Switch 3 and Switch 4 forms a MLAG domain.

As shown in Figure 9-58, switch 3 and switch 4 are a single logical switches to switch 1 and switch 2. Even if either switch 3 or switch 4 is down, there exists a path to reach other destinations.

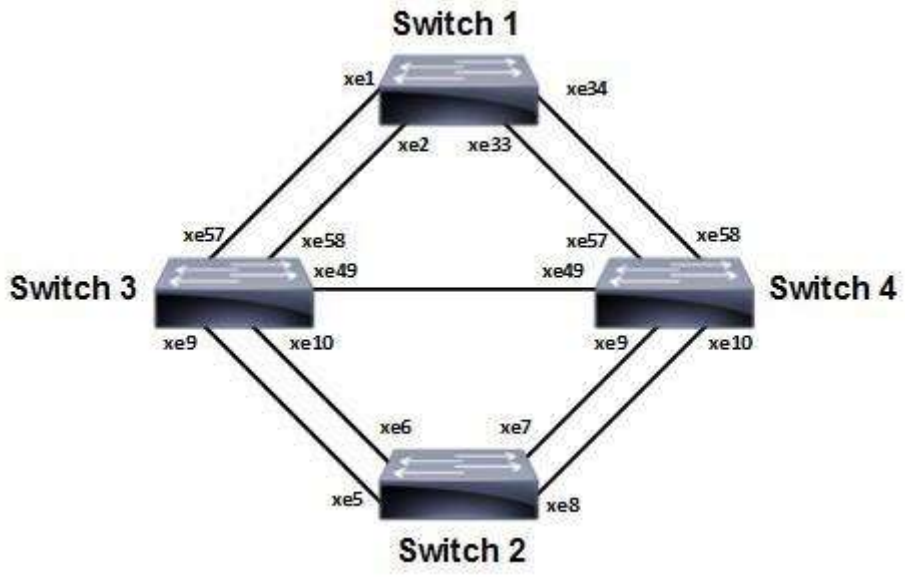


Figure 9-58: MC-LAG Topology

Configuration

Switch 1

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol rstp vlan-bridge`	Create RSTP bridge 1.
`(config)#vlan 2 bridge 1 state enable`	Create VLAN 2.
`(config)#interface xe1`	Enter interface mode.
`(config-if)#switchport`	Configure the interface as Layer 2
`(config-if)#bridge-group 1`	Associate the interface with bridge group 1.

(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe33	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe34	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface po2	Enter interface mode.
(config-if)#exit	Exit interface mode.

Switch 2

#configure terminal	Enter configure mode.

(config)#bridge 1 protocol rstp vlan-bridge	Create RSTP bridge 1.
(config)#vlan 2 bridge 1 state enable	Create VLAN 2.
(config)#interface xe5	Enter interface mode.

(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe6	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe7	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe8	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.

(config-if)#exit	Exit interface mode.
(config)#interface po1	Enter interface mode.
(config-if)#exit	Exit interface mode.

Switch 3

#configure terminal	Enter configure mode.
(config)#bridge 1 protocol rstp vlan-bridge	Create RSTP bridge 1.
(config)#vlan 2 bridge 1 state enable	Create VLAN 2.
(config)#interface xe9	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe57	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe58	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe10	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.

(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#channel-group 1 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface po1	Enter interface mode.
(config-if)#mlag 1	Enabling Mlag group number
(config-if)#exit	Exit interface mode.
(config)#interface po2	Enter interface mode.
(config-if)#mlag 2	enabling Mlag group number
(config-if)#exit	Exit interface mode.
(config)#mcec domain configuration	Entering MCEC mode
(config-mcec-domain)#domain-address 1111.2222.3333	Domain address for the mlag domain
(config-mcec-domain)#intra-domain link xe49	Intra domain line between mlag domain
(config-mcec-domain)#domain-system-number 1	Number to identify the node in a domain
(config-mcec-domain)#exit	Exit MCEC mode

Switch 4

#configure terminal	Enter configure mode.
(config)#bridge 1 protocol rstp vlan-bridge	Create RSTP bridge 1.
(config)#vlan 2 bridge 1 state enable	Create VLAN 2.
(config)#interface xe9	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe10	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.

(config-if)#channel-group 1 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe57	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface xe58	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this interface.
(config-if)#channel-group 2 mode active	Add this interface to channel group 2 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface po1	Enter interface mode.
(config-if)#mlag 1	Enabling Mlag group number
(config-if)#exit	Exit interface mode.
(config)#interface po2	Enter interface mode.
(config-if)#mlag 2	Enabling Mlag group number
(config-if)#exit	Exit interface mode.
(config)#mcec domain configuration	Entering MCEC mode
(config-mcec-domain)#domain-address 1111.2222.3333	Domain address for the Mlag domain
(config-mcec-domain)#intra-domain link xe49	Intra domain Link between Mlag domains
(config-mcec-domain)#domain-system-number 2	Number to identify the node in domain
(config-mcec-domain)#exit	Exit MCEC mode

Validation

Switch 3

```
#sh mlag domain details
```

```
    ------------------------------------
    Domain Configuration
    ------------------------------------

    Domain System Number           : 1
    Domain Address                 : 1111.2222.3333
    Domain Priority                : 1000
    Intra Domain Interface         : xe49

    Hello RCV State                : Current
    Hello Periodic Timer State     : Fast Periodic
    Domain Sync                    : IN_SYNC
    Neigh Domain Sync              : IN_SYNC
    Domain Adjacency               : UP ------------------------------------
MLAG Configuration
------------------------------------

MLAG-1
  Mapped Aggregator           : po1
  Admin Key                   : 16385
  Oper Key                    : 16385
  Physical properties Digest  : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82

  Neigh Admin Key             : 32769
  Neigh Physical Digest       : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
  Info RCV State              : Current
  Info Periodic Time State    : Standby
  Mlag Sync                   : IN_SYNC

MLAG-2
  Mapped Aggregator           : po2
  Admin Key                   : 16386
  Oper Key                    : 16386
  Physical properties Digest  : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82

  Neigh Admin Key             : 32770
  Neigh Physical Digest       : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
  Info RCV State              : Current
  Info Periodic Time State    : Standby
  Mlag Sync                   : IN_SYNC

#sh etherchannel summary
% Aggregator po1 0
% Admin Key: 16385 - Oper Key 16385
%   Link: xe57 (5057) sync: 1
%   Link: xe58 (5058) sync: 1
% Aggregator po2 0
% Admin Key: 16386 - Oper Key 16386
%   Link: xe9 (5009) sync: 1
%   Link: xe10 (5010) sync: 1
```

```
#sh mlag 1 detail

MLAG-1
  Mapped Aggregator           : po1
  Admin Key                   : 16385
  Oper Key                    : 16385
  Physical properties Digest  : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82

  Neigh Admin Key             : 32769
  Neigh Physical Digest       : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
  Info RCV State              : Current
  Info Periodic Time State    : Standby   Mlag
Sync                    : IN_SYNC sh mcec
statistics

Unknown MCCPDU received on the system            : 0

-------------------------------------
IDP xe49
-------------------------------------
   Valid RX Hello PDUs                           : 398
   Valid TX Hello PDUs                           : 417
   Valid RX Info PDUs                            : 16
   Valid TX Info PDUs                            : 6

   Valid RX Mac Sync PDUs                        : 3
   Valid TX Mac Sync PDUs                        : 4

MLAG 1
  Valid RX Info PDUs                             : 8
  Valid TX Info PDUs                             : 3

MLAG 2
  Valid RX Info PDUs                             : 8   Valid
TX Info PDUs                             : 3 sh mlag domain
summary

-------------------------------------
Domain Configuration
-------------------------------------

Domain System Number            : 1
Domain Address                  : 1111.2222.3333
Domain Priority                 : 1000
Intra Domain Interface          : xe49
Domain Adjacency                : UP

-------------------------------------
MLAG Configuration
-------------------------------------

MLAG-1
```

```
  Mapped Aggregator           : po1
  Physical properties Digest  : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
  Total Bandwidth             : 40g
  Mlag Sync                   : IN_SYNC


MLAG-2
  Mapped Aggregator           : po2
  Physical properties Digest  : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
  Total Bandwidth             : 40g
  Mlag Sync                   : IN_SYNC
```

CHAPTER 10 Traffic Mirroring Configuration

This chapter contains a sample Local and Remote switched port analyzer feature configuration.

SPAN Overview

Switched Port Analyzer (SPAN) refers to selecting network traffic for analysis by a network analyzer. SPAN feature is introduced on switches as the switch forwards traffic that is destined for a MAC address directly to the corresponding port leaving no scope to analyze the traffic.

SPAN monitors the traffic on source port and sends a copy of the traffic to a destination port. The network analyzer, which is attached to the destination port, analyzes the received traffic. Source port can be a single port or multiple ports. A replication of the packets is sent to the destination port for analysis

SPAN is originally referred to port mirroring or port monitoring where all the network traffic on the source port is mirrored to destination port. Port mirroring has three subdivisions.

- Ingress mirroring - Traffic received on the source port will be monitored
- Egress mirroring - Traffic transmitted from the source port will be monitored
- Ingress and egress mirroring - Both received and transmitted traffic on the source port will be monitored. With enhancement to SPAN, mirroring can be classified into three categories

Port Mirroring

In port mirroring, source will be a port which could be a physical interface or a port channel. All the traffic on the source port will be mirrored to destination port. Either traffic received on the source port or traffic transmitted from the source port or both can be monitored.

VLAN Mirroring

In vlan mirroring, source will be a vlan ID and the traffic received on all ports with the vlan ID matching source vlan ID will be mirrored to destination port.

Rule Based Mirroring

In rule based mirroring, there will be a set of matching criteria for the ingress traffic such as matching destination mac address or matching frame type, etc. The traffic matching the rules will be mirrored to the destination port

Topology

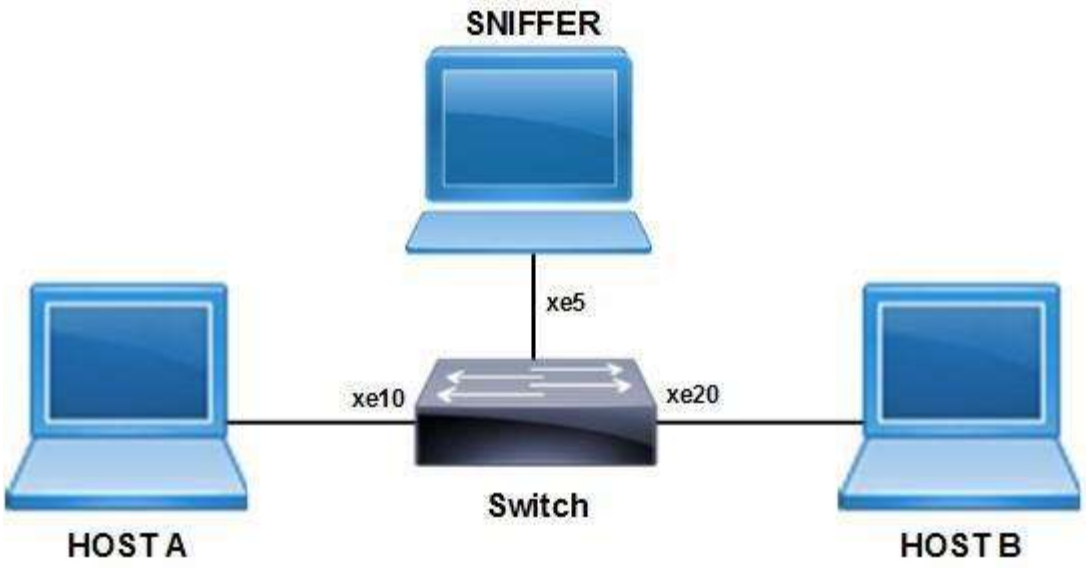


Figure 10-59: SPAN Topology

Port Mirroring Configuration

This example shows detailed configuration of port mirroring.

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge.
`(config)# vlan 101-110 bridge 1 state enable`	Configure VLANs.
`(config)#interface xe10`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.
`(config-if)# switchport trunk allowed vlan add 101-110`	Allow VLANs 101-110 on the interface.
`(config-if)# no shutdown`	Make interface admin up.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe20`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.
`(config-if)# switchport trunk allowed vlan add 101-110`	Allow VLANs 101-110 on the interface.
`(config-if)# no shutdown`	Make interface admin up.
`(config-if)#exit`	Exit interface mode.

(config)#interface xe5	Enter interface mode.
(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)#exit	Exit interface mode.
(config)# monitor session 1	Enter monitor session configuration mode
(config-monitor)# destination interface xe5	Configure the interface as destination port
(config-monitor)# source interface xe10 both	Configure the source interface to mirror ingress as well as egress direction traffic
(config-monitor)# no shut	Activate monitor session
(config-monitor)#end	Exit monitor session configuration mode

Validation

Enter the below commands to confirm the configurations.

```
#show running-config monitor ! monitor session 1  source
interface xe10 both  destination interface xe5  no shut

#show monitor session all    session 1 --------------type
: local state             : up source intf       :     tx
: xe10     rx            : xe10     both          : xe10
source VLANs      :     rx            : destination ports :
xe5 filter count      :

Legend: f = forwarding enabled, l = learning enabled
```

VLAN and Rule Based Mirroring

This example shows detailed configuration of VLAN with rule based mirroring.

#configure terminal	Enter configure mode.
(config)# bridge 1 protocol mstp	Configure bridge 1 as MSTP bridge.
(config)# vlan 101-110 bridge 1 state enable	Configure VLANs
(config)#interface xe10	Enter interface mode.
(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)# bridge-group 1	Associate bridge to an interface.
(config-if)# switchport mode trunk	Configure port as a trunk.
(config-if)# switchport trunk allowed vlan add 101-110	Allow VLANs 101-110 on the interface.
(config-if)# no shutdown	Make interface admin up
(config-if)#exit	Exit interface mode.
(config)#interface xe20	Enter interface mode.
(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)# bridge-group 1	Associate bridge to an interface.

(config-if)# switchport mode trunk	Configure port as a trunk.
(config-if)# switchport trunk allowed vlan add 101-110	Allow VLANs 101-110 on the interface.
(config-if)# no shutdown	Make interface admin up
(config-if)#exit	Exit interface mode.
(config)#interface xe5	Enter interface mode.
(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)#exit	Exit interface mode.
(config)# monitor session 1	Enter monitor session configuration mode
(config-monitor)# destination interface xe5	Configure the interface as destination port
(config-monitor)# source vlan 101	Configure source VLAN to be mirrored
(config-monitor)# filter src-mac host 0000.0000.0005	Configure the rule to match the source MAC
(config-monitor)# no shut	Activate monitor session
(config-monitor)#end	Exit monitor session configuration mode

Validation

Enter the below commands to confirm the configurations.

```
#show running-config monitor ! monitor session 1 source
vlan 101 destination interface xe5 filter src-mac host
0000.0000.0005 no shut
```

```
#show  monitorsession all     session 1 -------------    type                : local state
: up source intf        :     tx              :     rx            :     both          :
source VLANs      :     rx            : 101 destination ports : xe5 filter count      :
1 Legend: f = forwarding enabled, l = learning enabled
```

```
#show monitor session 1 filter    session 1 -------------- filter
count      : 1

--------------    match set 1    ---------------
  source mac address : 0000.0000.0005 (host)
```

RSPAN Overview

When several switches need to be analyzed with a single centralized sniffer, remote switched port analyzer (RSPAN) is used. In RSPAN, all the mirrored traffic will be tagged with a RSPAN VLAN ID and forwarded to remote destination via a port called reflector port. Reflector port will have the same characteristics of a local destination port. RSPAN VLAN ID will be a dedicated VLAN for the monitoring purpose and will not participate in bridging. RSPAN destination switch will strip the RSPAN VLAN tag and send it the sniffer for analysis. RSPAN will have the same sub-categories as SPAN except that the mirrored traffic will be tagged with RSPAN VLAN header and forwarded to destination switch for analysis.

Topology

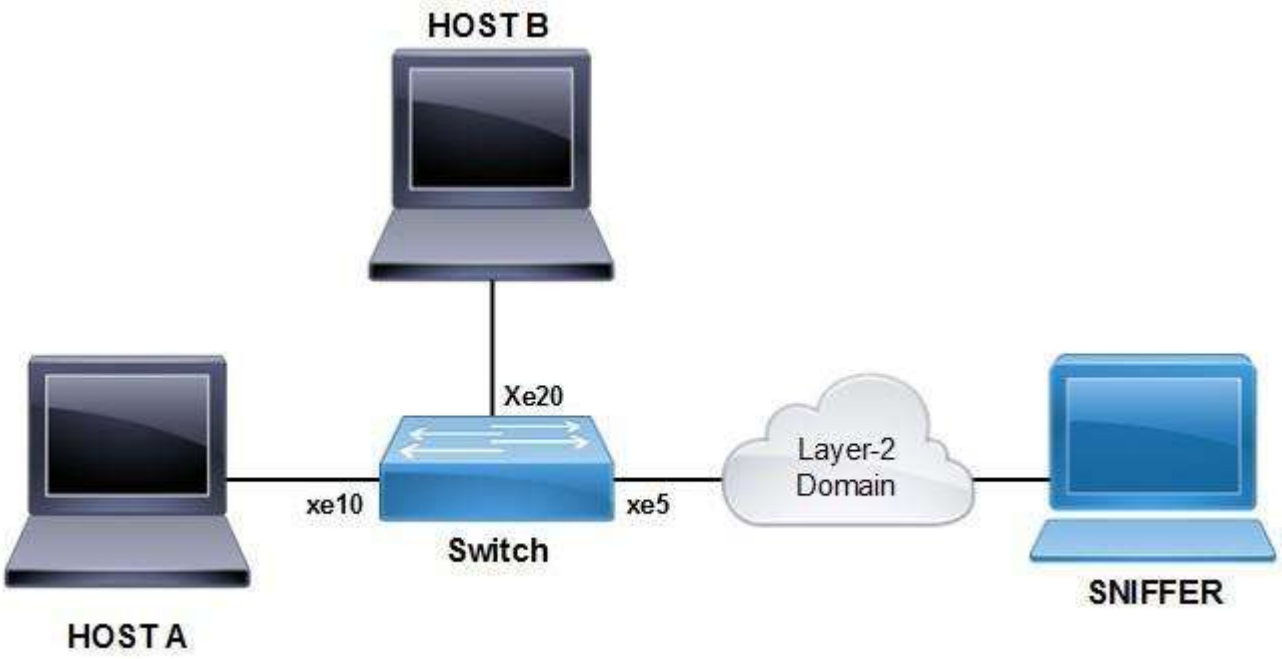


Figure 10-60: RSPAN Topology

Port Mirroring Configuration

This example shows detailed configuration of port mirroring.

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge.
`(config)# vlan 101-110 bridge 1 state enable`	Configure VLANs.
`(config)#interface xe10`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.
`(config-if)# switchport trunk allowed vlan add 101-110`	Allow VLANs 101-110 on the interface.
`(config-if)# no shutdown`	Make interface admin up.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe20`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.

(config-if)# switchport trunk allowed vlan add 101-110	Allow VLANs 101-110 on the interface.
(config-if)# no shutdown	Make interface admin up.
(config-if)#exit	Exit interface mode.
(config)#interface xe5	Enter interface mode.
(config-if)# switchport	Configure interface as a layer 2 port.
(config-if)#exit	Exit interface mode.
(config)# monitor session 1 type remote	Enter monitor session configuration mode.
(config-monitor)# destination remote vlan 100 reflector-port xe5	Configure the interface as remote destination port
(config-monitor)# source interface xe10 both	Configure the source interface to mirror ingress as well as egress direction traffic.
(config-monitor)# no shut	Activate monitor session.
(config-monitor)#end	Exit monitor session configuration mode.

Validation

Enter the commands below to confirm the configurations

```
#show running-config monitor ! monitor session 1 type remote source interface xe10
both destination remote vlan 100 reflector-port xe5 no shut
```

```
#show monitor session all     session 1 ---------------type
: remote state              : up source  intf       :     tx
: xe10     rx            : xe10      both          : xe10 source
VLANs      :     rx             : rspan  VLAN        : 100
reflector ports   : xe5 filter count       :

Legend: f = forwarding enabled, l = learning enabled
```

VLAN and Rule Based Mirroring Configuration

This example shows detailed configuration of VLAN with rule based mirroring.

`#configure terminal`	Enter configure mode.
`(config)# bridge 1 protocol mstp`	Configure bridge 1 as MSTP bridge.
`(config)# vlan 101-110 bridge 1 state enable`	Configure VLANs.
`(config)#interface xe10`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.
`(config-if)# switchport trunk allowed vlan add 101-110`	Allow VLANs 101-110 on the interface.
`(config-if)# no shutdown`	Make interface admin up.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe20`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)# bridge-group 1`	Associate bridge to an interface.
`(config-if)# switchport mode trunk`	Configure port as a trunk.
`(config-if)# switchport trunk allowed vlan add 101-110`	Allow VLANs 101-110 on the interface.
`(config-if)# no shutdown`	Make interface admin up.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe5`	Enter interface mode.
`(config-if)# switchport`	Configure interface as a layer 2 port.
`(config-if)#exit`	Exit interface mode.
`(config)# monitor session 1 type remote`	Enter monitor session configuration mode.
`(config-monitor)# destination remote vlan 100 reflector-port xe5`	Configure the interface as remote destination port.
`(config-monitor)# source vlan 101`	Configure source VLAN to be mirrored.
`(config-monitor)# filter src-mac host 0000.0000.0005`	Configure the rule to match the source MAC.
`(config-monitor)# no shut`	Activate monitor session.
`(config-monitor)#end`	Exit monitor session configuration mode.

Validation

Enter the commands below to confirm the configuration.

```
#show running-config monitor !
monitor session 1 type remote  source vlan 101
```

```
 destination remote vlan 100 reflector-port xe5 filter src-mac host
0000.0000.0005 no shut


#show monitor session all     session 1 --------------    type                : remote state
: up source intf        :     tx              :     rx              :     both          :
source VLANs      :     rx            : 101 rspan VLAN        : 100 reflector ports   :
xe5 filter count      : 1 Legend: f = forwarding enabled, l = learning enabled


#show monitor session 1 filter    session 1 --------------  filter
count       : 1

  --------------  match set 1    ---------------
  source mac address : 0000.0000.0005 (host)
```

CHAPTER 11 Maximum MST Instances Configuration

This chapter describes the configuration support for extending the maximum number of Multiple Spanning Tree instances from 16 to 64.

Topology

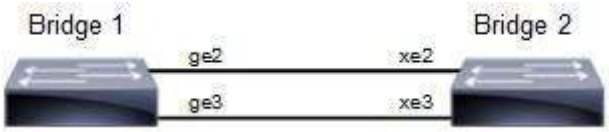


Figure 12-64: Maximum Spanning Tree Topology

Note: This configuration sample assumes that you are running the SWMRE Layer-2 module. If you are using the SWMRE Hybrid Layer-2/Layer-3 module, run the `switchport` command on each port to change to Layer-2 mode.

Configuration

Bridge 1

`Bridge1#configure terminal`	Enter configure mode.
`Bridge1(config)#bridge 1 protocol mstp`	Add `bridge (1)` to the multiple spanning tree table.
`Bridge1(config)#vlan database`	Enter the `VLAN configuration` mode.
`Bridge1(config-vlan)#vlan 2 bridge 1 state enable`	Enable the state of VLAN 2 on bridge 1. This allows forwarding of frames over VLAN 2 on bridge 1.
`Bridge1(config-vlan)#exit`	Exit the VLAN configuration mode.
`Bridge1(config)#spanning-tree mst configuration`	Enter the Multiple Spanning Tree Configuration mode.
`Bridge1(config-mst)#bridge 1 instance 63 vlan 2`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified, the MSTI is not created.
`Bridge1(config-te-msti)#exit`	Exit `te-msti configuration` mode.
`Bridge1(config)#interface eth1`	Enter the `Interface` mode for `eth1`.
`Bridge1(config-if)#bridge-group 1`	Associate the interface with `bridge-group 1`
`Bridge1(config-if)#switchport mode access`	Set the switching characteristics of this interface to `access` mode.
`Bridge1(config-if)#switchport access vlan 2`	Enable VLAN port access by specifying VLAN ID 2 on this interface.
`Bridge1(config-if)#bridge-group 1 instance 63`	Assign `bridge-group 1` to this instance.

`Bridge1(config-if)#exit`	Exit interface mode.
`Bridge1(config)#interface eth2`	Enter the `Interface` mode for `eth2`
`Bridge1(config-if)#bridge-group 1`	Associate the interface with `bridge-group 1`
`Bridge1(config-if)#switchport mode access`	Set the switching characteristics of this interface to `access` mode.

Maximum MST Instances Configuration

`Bridge1(config-if)#switchport access vlan 2`	Enable VLAN port access by specifying VLAN ID 2 on this interface.
`Bridge1(config-if)#bridge-group 1 instance 63`	Assign `bridge-group 1` to this instance.
`Bridge1(config-if)#exit`	Exit interface mode.

Bridge 2

`Bridge2#configure terminal`	Enter configure mode.
`Bridge2(config)#bridge 1 protocol mstp`	Add `bridge 1` to the multiple spanning tree table.
`Bridge2(config)#vlan database`	Enter the `VLAN configuration` mode.
`Bridge2(config-vlan)#vlan 2 bridge 1 state enable`	Enable the state of VLAN 2 on `bridge 1`. This allows forwarding of frames over `VLAN 2` on `bridge 1`.
`Bridge2(config-vlan)#exit`	Exit the `VLAN configuration` mode.
`Bridge2(config)#spanning-tree mst configuration`	Enter the Multiple Spanning Tree Configuration mode.
`Bridge2(config-mst)#bridge 1 instance 63 vlan 2`	Create an instance of VLAN. The VLANs must be created before being associating with an MST instance (MSTI). If the VLAN range is not specified, the MSTI is not created.
`Bridge2(config-te-msti)#exit`	Exit `te-msti configuration` mode.
`Bridge2(config)#interface eth1`	Enter the `Interface` mode for `eth1`.
`Bridge2(config-if)#bridge-group 1`	Associate the interface with `bridge-group 1`.
`Bridge2(config-if)#switchport mode access`	Set the switching characteristics of this interface to access mode.
`Bridge2(config-if)#switchport access vlan 2`	Enable VLAN port access by specifying the VLAN ID 2 on this interface.
`Bridge2(config-if)#bridge-group 1 instance 63`	Assign `bridge-group 1` to this instance.
`Bridge2(config-if)#exit`	Exit interface mode.
`Bridge2(config)#interface eth2`	Enter the `Interface` mode for `eth2`.
`Bridge2(config-if)#bridge-group 1`	Associate the interface with `bridge-group 1`.
`Bridge2(config-if)#switchport mode access`	Set the switching characteristics of this interface to `access` mode.
`Bridge2(config-if)#switchport access vlan 2`	Enable VLAN port access by specifying the VLAN ID 2 on this interface.
`Bridge2(config-if)#bridge-group 1 instance 63`	Assign `bridge-group 1` to this instance.

`Bridge2(config-if)#exit`	Exit interface mode.

Validation

show spanning-tree, show spanning-tree mst detail Layer 2 Gateway Port Configuration

CHAPTER 12 MC-LAG Configuration

This chapter contains a complete example of Multi-Chassis Link Aggregation (MC-LAG) configuration.

MC-LAG (also called DRNI, Distributed Resilient Network Interconnect) expands the concept of link aggregation so that it provides node-level redundancy by allowing two or more nodes to share a common LAG endpoint. It emulates multiple nodes to represent as a single logical node to the remote node running Link aggregation. As a result even if one of the nodes is down there exists a path to reach the destination via other nodes.

Topology

As shown in Figure 14-66, switch s1 and switch s2 share a common endpoint in switch s3. Switches s1 and s2 are a single logical switch to switch s3. Even if switch s1 or switch s2 is down, there exists a path from switch s3 to reach other destinations.

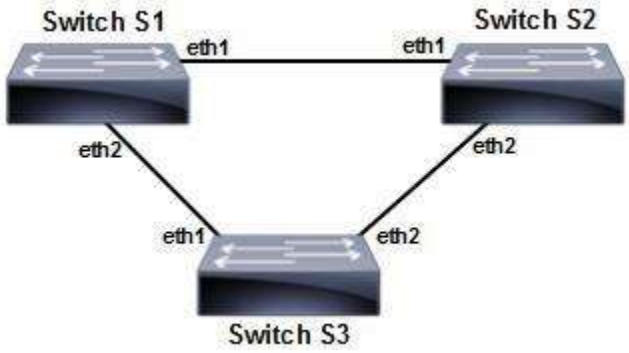


Figure 14-66: MC-LAG Topology

Configuration

S1

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Create STP bridge 1.
`(config)#vlan 2-100 bridge 1 state enable`	Create VLANs 2 to 100.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#switchport`	Configure the interface as Layer 2
`(config-if)#bridge-group 1`	Associate the interface with bridge group 1.
`(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to access mode.
`(config-if)#switchport trunk allowed vlan all`	Enable all VLAN identifiers on this interface.
`(config-if)#channel-group 1 mode active`	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
`(config-if)#exit`	Exit interface mode.

(config)#interface po1	Enter interface mode.
(config-if)#mlag 1	Assign an MLAG-ID to the port channel. One port-channel interface can be bound with an MLAG instance.
(config-if)#exit	Exit interface mode.
(config)#mlag configuration 1	Enters MLAG configuration mode to configure Multi chassis Link aggregation features.
(config-mlag)#portal-system-number 1	Assign the portal system number used to configure portal address, which helps to identify the MLAG domain.
(config-mlag)#portal-name test1	Specify a locally significant name for distributed relay.
(config-mlag)#portal-priority 1	Specify the priority value associated with the portal system.
(config-mlag)#portal-address 0000.0000.0001	Set the portal address, which helps to identify the MLAG domain.
(config-mlag)#portal-topology 2-portal	Set the portal topology.
(config-mlag)#conversation alloc-mode auto	Set5 the conversation allocation mode to automatic.
(config-mlag)#intra-portal-link eth1 neighbor-portal-system 2	Configure the interface that connects two portal systems and a neighbor portal system connected through the IPP.
(config-mlag)#exit	Enter configure mode.

S2

#configure terminal	Enter configure mode.
(config)#bridge 1 protocol ieee vlan-bridge	Create STP bridge 1.
(config)#vlan 2-100 bridge 1 state enable	Create VLANs 2 to 100.
(config)#interface eth2	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to access mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this port.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface po1	Enter interface mode.
(config-if)#mlag 1	Assigns an MLAG-ID to a port channel. One port-channel interface can be bound with an MLAG instance.
(config-if)#exit	Exit interface mode.
(config)#mlag configuration 1	Enters MLAG configuration mode to configure Multi chassis Link aggregation features.
(config-mlag)#portal-system-number 2	Assigns portal system number used to configure portal address, which helps to identify the MLAG domain
(config-mlag)#portal-name test1	Set a locally significant name for distributed relay.

(config-mlag)#portal-priority 1	Set the priority value associated with the portal system.
(config-mlag)#portal-address 0000.0000.0001	Set the portal address, which helps to identify the MLAG domain.
(config-mlag)#portal-topology 2-portal	Set the portal topology.
(config-mlag)#conversation alloc-mode auto	Set the conversation allocation mode to automatic.
(config-mlag)#intra-portal-link eth1 neighbor-portal-system 1	Configure the interface that connects two portal systems and neighbor portal system connected through the IPP.
(config-mlag)#exit	Enter configure mode.

S3

#configure terminal	Enter configure mode.
(config)#bridge 1 protocol ieee vlan-bridge	Create STP bridge 1.
(config)#vlan 2-100 bridge 1 state enable	Create VLANs 2 to 100.
(config)#interface eth1	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to access mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this port.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2.
(config-if)#bridge-group 1	Associate the interface with bridge group 1.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to access mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this port.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it may be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.

Validation

S1

```
#show mlag 1 summary MLAG Configuration :
MLAG-ID             : 1
-------------------------------------

Portal-System-Number : 1
```

```
Portal-Address       : 0000.0000.0001
Portal-Priority      : 1
Mapped Aggregator    : po1
Gateway-Algorithm    : Distribution based on C-VIDs
Port-Algorithm       : Distribution based on C-VIDs
Gateway-Digest       : 799710171191251261187516818511878126107 21
Port-Digest           : 123103220137132113180167127532251208115821838 Dest Mac address
: non-TPMR-group-address

Topology             : Two portal system connected by 1 IPL
Conv Alloc Mode      : Automatic

Master Portal System
Mlag Bandwidth       : 250000000

#show mlag 1 gateway-conversation-id

Gateway Conversation  Portal-System Priority
1      - 50               1               1 1     - 50
2              2 51   - 100             2             1
51    - 100           1              2

#show mlag 1 port-conversation-id

Port Conversation    Port-priority    Port-number Portal-System Priority
1     - 50            32768           6           1            1 1     - 50
32768            3          2              2 51   - 100            32768
3            2            1
51    - 100          32768            6          1             2

#show mlag 1 detail

Portal-System-Number : 1
Portal-Address       : 0000.0000.0001
Portal-Priority      : 1
Mapped Aggregator    : po1
Gateway-Algorithm    : Distribution based on C-VIDs
Port-Algorithm       : Distribution based on C-VIDs
Gateway-Digest       : 799710171191251261187516818511878126107 21
Port-Digest          : 123103220137132113180167127532251208115821838
Dest Mac address     : non-TPMR-group-address

Topology             : Two portal system connected by 1 IPL
Conv Alloc Mode      : Automatic

Master Portal System
Mlag Bandwidth       : 250000000

Intra Portal Interface          : eth1
```

```
Intra Portal Operational Status : Active Intra Portal Admin
Status       : Enabled
Home DRCP State:
 Home Gateway      : Operational
 Neighbor Gateway  : Operational
 Other Gateway     : Non-Operational
 IPP Activity      : Active
 DRCP Timeout      : Long Timeout
 Gateway Sync      : IN_SYNC
 Port Sync         : IN_SYNC
 Expired           :
Neighbour DRCP State:
 Home Gateway      : Operational
 Neighbor Gateway  : Operational
 Other Gateway     : Non-Operational
 IPP Activity      : Active
 DRCP Timeout      : Long Timeout
 Gateway Sync      : IN_SYNC
 Port Sync         : IN_SYNC
 Expired           :
State Machine States
 Receive state     : Current
 Periodic Tx state : Slow Periodic
 IPP Gateway State : IPP Gateway Update
 IPP Port State    : IPP Port Update

 Gateway Conversations Direction:
 51-100

 Port Conversations Passes:  51-100

Portal State Machine State
 Portal System State : Portal System Update
 Gateway State       : Gateway Update
 Port State          : DRNI Port Update

Gateway Conversation  Portal-System Priority
1     -  50              1               1 1      - 50
2              2 51   - 100            2              1
51   - 100             1             2

Port Conversation    Port-priority   Port-number Portal-System Priority
1    - 50            32768           6           1              1
1    - 50            32768           3           2              2
51   - 100           32768           3           2              1
51   - 100           32768           6           1              2

Portal Gateway Conversation  1-50
```

```
Portal Port conversation  1-50

#show drcpdu statistics
Unknown DRCPDU received on the system : 0
Unknown DRCPDU frames received on portal :0
Intra Portal Interface  eth1
Number of valid DRCPDU Received    : 28
Number of invalid DRCPDU Received  : 0
Number of DRCPDU Transmitted       : 29
```

S2

```
#show  mlag 1 summary MLAG  Configuration
:
MLAG-ID             : 1
-------------------------------------

Portal-System-Number : 2
Portal-Address       : 0000.0000.0001
Portal-Priority      : 1
Mapped Aggregator    : po1
Gateway-Algorithm    : Distribution based on C-VIDs
Port-Algorithm       : Distribution based on C-VIDs
Gateway-Digest       : 799710171191251261187516818511878126107 21
Port-Digest          : 123103220137132113180167127532251208115821838
Dest Mac address     : non-TPMR-group-address

Topology             : Two portal system connected by 1 IPL
Conv Alloc Mode      : Automatic

Slave Portal System
Ipp Connecting to Master : eth1
Mlag Bandwidth       : 250000000

#show mlag 1 gateway-conversation-id

Gateway Conversation  Portal-System Priority
1      - 50              1                1 1     - 50
2              2 51   - 100             2             1
51    - 100           1              2

#show mlag 1 port-conversation-id

Port Conversation    Port-priority    Port-number Portal-System Priority
1     - 50           32768            6           1            1 1    - 50
32768            3           2             2 51   - 100            32768
3           2             1
51    - 100          32768            6          1             2

#show   mlag 1 detail
```

```
Portal-System-Number : 2
Portal-Address       : 0000.0000.0001
Portal-Priority      : 1
Mapped Aggregator    : po1
Gateway-Algorithm    : Distribution based on C-VIDs
Port-Algorithm       : Distribution based on C-VIDs
Gateway-Digest       : 799710171191251261187516818511878126107 21
Port-Digest          : 123103220137132113180167127532251208115821838
Dest Mac address     : non-TPMR-group-address

Topology             : Two portal system connected by 1 IPL
Conv Alloc Mode      : Automatic

Slave Portal System
Ipp Connecting to Master : eth1
Mlag Bandwidth       : 250000000

Intra Portal Interface          : eth1
Intra Portal Operational Status : Active Intra Portal Admin Status
: Enabled
Home DRCP State:
Home Gateway      : Operational
Neighbor Gateway  : Operational
Other Gateway     : Non-Operational
IPP Activity      : Active
DRCP Timeout      : Long Timeout
Gateway Sync      : IN_SYNC
Port Sync         : IN_SYNC
Expired           :
Neighbour DRCP State:
Home Gateway      : Operational
Neighbor Gateway  : Operational
Other Gateway     : Non-Operational
IPP Activity      : Active
DRCP Timeout      : Long Timeout
Gateway Sync      : IN_SYNC
Port Sync         : IN_SYNC
Expired           :
State Machine States
Receive state     : Current
Periodic Tx state : Periodic Tx
IPP Gateway State : IPP Gateway Update
IPP Port State    : IPP Port Update

Gateway Conversations Direction:
1-50

Port Conversations Passes: 1-50
```

```
Portal State Machine State
Portal System State : Portal System Update
Gateway State       : Gateway Update
Port State          : DRNI Port Update

Gateway Conversation  Portal-System Priority
1     - 50               1               1 1     - 50
2             2 51   - 100             2             1
51   - 100            1              2

Port Conversation    Port-priority    Port-number Portal-System Priority
1    - 50             32768           6           1             1 1    - 50
32768           3            2             2 51   - 100            32768
3           2             1
51   - 100           32768            6          1             2

Portal Gateway Conversation  51-100

Portal Port conversation  51-100

#show drcpdu statistics
Unknown DRCPDU received on the system : 0
Unknown DRCPDU frames received on portal :0
Intra Portal Interface  eth1
Number of valid DRCPDU Received    : 21
Number of invalid DRCPDU Received  : 0
Number of DRCPDU Transmitted       : 28
```

LACPv2 Configuration

Topology

S1

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Create STP bridge 1.
`(config)#vlan 2-40 bridge 1 state enable`	Create VLANs 2 to 40.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#switchport`	Configure the interface as Layer 2.
`(config-if)#switchport mode trunk`	Set the switching characteristics of this interface to access mode.

(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this port.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to access mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this port.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it may be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface po1	Enter interface mode.
HOST-1(config-if)#no switchport	Configure the interface as Layer 3.
(config-if)#bridge-group 1	Associate the interface po1 with bridge group 1.
(config-if)#port-conv-id 1 20 port-priority 32768 port-number 7 portal-system 0 priority 1 port-priority 32768 port-number 8 portalsystem 0 priority 2	Configure port conversation identifiers 1 to 20 to the aggregation port which has port 7 and set the priority as 1. Assign the same port conversation identifiers to port 8 with the priority as 2.
(config-if)#port-conv-id 21 40 port-priority 32768 port-number 8 portal-system 0 priority 1 port-priority 32768 port-number 7 portalsystem 0 priority 2	Configure port conversation identifiers 21 to 40 to the aggregation port which has port 8 and set the priority as 1. Assign the same port conversation identifiers to port 7 with the priority as 2.

S2

#configure terminal	Enter configure mode.
(config)#bridge 1 protocol ieee vlan-bridge	Create STP bridge 1.
(config)#vlan 2-40 bridge 1 state enable	Create VLANs 2 to 40.
(config)#interface eth1	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2.
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to access mode.
(config-if)#switchport trunk allowed vlan all	Enable all VLAN identifiers on this port.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode.
(config-if)#switchport	Configure the interface as Layer 2
(config-if)#switchport mode trunk	Set the switching characteristics of this interface to trunk mode.

(config-if)#switchport trunk allowed vlan all	Enable all VLAN IDs on this port.
(config-if)#channel-group 1 mode active	Add this interface to channel group 1 and enable link aggregation so that it can be selected for aggregation by the local system.
(config-if)#exit	Exit interface mode.
(config)#interface po1	Enter interface mode.
HOST-1(config-if)#no switchport	Configure the interface as Layer 3.
(config-if)#bridge-group 1	Associate the interface po1 with bridge group 1.
(config-if)#port-conv-id 1 20 port-priority 32768 port-number 2 portal-system 0 priority 1 port-priority 32768 port-number 3 portalsystem 0 priority 2	Configure port conversation identifiers 1 to 20 to the aggregation port which has port 2 and set the priority as 1. Assign the same port conversation identifiers to port 3 with the priority as 2.
(config-if)#port-conv-id 21 40 port-priority 32768 port-number 3 portal-system 0 priority 1 port-priority 32768 port-number 2 portalsystem 0 priority 2	Configure port conversation identifiers 21 to 40 to the aggregation port which has port 3 and set the priority as 1. Assign the same port conversation identifiers to port 2 with the priority as 2.

Validation

S1

```
#show etherchannel summary
% Aggregator po1 1000000
% Admin Key: 0001 - Oper Key 0001
% Discard Wrong Conversation: FALSE
% Port Algo: C-VID
% Port Digest: 218237207806918962135145211157882476223 8
%   Link: p1p2 (8) sync: 1
%   Link: p1p1 (7) sync: 1

#show etherchannel 1
% Aggregator po1 1000000 Admin Key: 0001 - Oper Key 0001
% Actor Port Algorithm: C-VID
% Actor Conversation Port List Digest: 218237207806918962135145211157882476223 8
Port Conversation    Port-priority   Port-number Priority
1     - 20           32768           7           1
1     - 20           32768           8           2
21   -  40           32768           8           1
21   -  40           32768           7           2
% Partner LAG: 0x8000,00-02-a5-4e-d4-8c,0x0001
% Partner Oper Key 0001
% Partner Oper Port Algorithm: C-VID
% Partner Oper Conversation Port List Digest:
832085321121547205217158225222801827824 1157
% Partner Admin Conversation Port List Digest: 0000000000000000
% Differ Port Algorithm: FALSE
% Differ Port Conversation ID Digest: TRUE
```

```
#show etherchannel 1 port-conversation-id
% p1p1
% Conversation ID :  1-20
% p1p2
% Conversation ID :  21-40


#show port etherchannel p1p1
% LACP link info: p1p1 - 7
% LAG ID: 0x8000,00-07-e9-a5-1f-76,0x0001
% Partner oper LAG ID: 0x8000,00-02-a5-4e-d4-8c,0x0001
% Actor Port priority: 0x8000 (32768)
% Admin key: 0x0001 (1) Oper key: 0x0001 (1)
% Physical admin key:(4)
% Receive machine state : Current
% Periodic Transmission machine state : Slow periodic
% Mux machine state : Collecting/Distributing
% Oper state: ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
% Destination Mac: Multicast-group-address [01-80-c2-00-00-02]
% Actor version: 2
% ActPar Sync: 1
% Long LACPDU Transmit: FALSE
% Partner oper state: ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
% Partner link info: admin port 0
% Partner oper port: 2
% Partner admin LAG ID: 0x0000-00:00:00:00:0000
% Admin state: ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
% Partner admin state: ACT:0 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
% Partner version : 2
% Partner ActPar Sync: 1
% Partner system priority - admin:0x0000 - oper:0x8000
% Partner port priority - admin:0x0000 - oper:0x8000 %
Aggregator ID: 1000000
```

S2

```
#show etherchannel summary
% Aggregator po1 1000000
% Admin Key: 0001 - Oper Key 0001
% Discard Wrong Conversation: FALSE
% Port Algo: C-VID
% Port Digest: 832085321121547205217158225222801827824 1157
%   Link: p1p1 (2) sync: 1
%   Link: p1p2 (3) sync: 1


#show etherchannel 1
% Aggregator po1 1000000 Admin Key: 0001 - Oper Key 0001
% Actor Port Algorithm: C-VID
% Actor Conversation Port List Digest: 832085321121547205217158225222801827824 1157
```

```
Port Conversation    Port-priority   Port-number Priority
1     - 20           32768           2            1 1
- 20            32768            3           2 21   - 40
32768           3            1 21   - 40           32768
2           2
% Partner LAG: 0x8000,00-07-e9-a5-1f-76,0x0001
% Partner Oper Key 0001
% Partner Oper Port Algorithm: C-VID
% Partner Oper Conversation Port List Digest: 218237207806918962135145211157882476223 8
% Partner Admin Conversation Port List Digest: 0000000000000000
% Differ Port Algorithm: FALSE
% Differ Port Conversation ID Digest: TRUE


#show etherchannel 1 port-conversation-id
% p1p1
% Conversation ID :  1-20
% p1p2
% Conversation ID :  21-40


#show port etherchannel p1p1
% LACP link info: p1p1 - 2
% LAG ID: 0x8000,00-02-a5-4e-d4-8c,0x0001
% Partner oper LAG ID: 0x8000,00-07-e9-a5-1f-76,0x0001
% Actor Port priority: 0x8000 (32768)
% Admin key: 0x0001 (1) Oper key: 0x0001 (1)
% Physical admin key:(4)
% Receive machine state : Current
% Periodic Transmission machine state : Slow periodic
% Mux machine state : Collecting/Distributing
% Oper state: ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
% Destination Mac: Multicast-group-address [01-80-c2-00-00-02]
% Actor version: 2
% ActPar Sync: 1
% Long LACPDU Transmit: FALSE
% Partner oper state: ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
% Partner link info: admin port 0
% Partner oper port: 7
% Partner admin LAG ID: 0x0000-00:00:00:00:0000
% Admin state: ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
% Partner admin state: ACT:0 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
% Partner version : 2
% Partner ActPar Sync: 1
% Partner system priority - admin:0x0000 - oper:0x8000
% Partner port priority - admin:0x0000 - oper:0x8000
% Aggregator ID: 1000000
```

Layer 2 Command Reference

Contents

This document contains these chapters:

- Chapter 1, *Common Commands*
- Chapter 2, *Bridge Commands*
- Chapter 3, *Spanning Tree Protocol Commands*
- Chapter 5, *Link Aggregation Commands*
- Chapter 6, *Multi-Chassis Link Aggregation Commands*
- Chapter 7, *Traffic Mirroring Commands*
- Chapter 8, *VLAN and Private VLAN Commands*
- Chapter 9, *DHCP Snooping Commands*
- Appendix A, *spanning-tree Commands*

© Symanitron

CHAPTER 1 Common Commands

This chapter provides a description, the syntax, and examples of common Layer 2 commands.

- flowcontrol
- hardware register get
- hardware register set
- show flowcontrol
- show interface capabilities
- snmp restart mstp

flowcontrol

Use this command to enable or disable flow control.

Flow control enables connected Ethernet ports to control traffic rates during periods of congestion by allowing congested nodes to pause link operations at the other end. If one port experiences congestion and cannot receive any more traffic, it notifies the other port to stop sending until the condition clears. When a local device detects congestion at its end, it notifies the remote device by sending a pause frame. On receiving a pause frame, the remote device stops sending data packets, which prevents loss of data packets during the period of congestion.

Use the `no` parameter with this command to disable flow control.

Command Syntax `flowcontrol`

```
both flowcontrol send
on flowcontrol send off
flowcontrol receive on
flowcontrol receive off
no flowcontrol
```

Parameters `both` Specify flow control mode for sending or receiving.

`send` Specify flow control mode for sending. `receive`

Specify the flow control mode for receiving. `off` Turn off flow control.

`on` Turn on flow control.

Default

The flow control is enabled globally and auto-negotiation is on, flow control is enabled and advertised on 10/100/1000M ports. If auto-negotiation is off or if the port speed was configured manually, flow control is neither negotiated with nor advertised to the peer.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
    #configure terminal
    (config)#interface eth1
    (config-if)#flowcontrol receive off

    #configure terminal
    (config)#interface eth1
    (config-if)#flowcontrol receive on
(config)#interface eth1
(config-if)#no flowcontrol
```

hardware register get

Use this command to get the value of a chip register.

Command Syntax `hardware register get ADDR`

Parameters

`ADDR`	Register address in 0xhhhh format

Default

By default, hello time is 2 seconds

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#hardware register get 0x3000
```

hardware register set

Use this command to set the value of a chip register.

Command Syntax `hardware register set ADDR VALUE`

Parameters

`ADDR`	Register address in 0xhhhh format
`VALUE`	Value

Default

By default, hello time is 2 seconds

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#hardware register set 0x3000 10
```

show flowcontrol

Use this command to display flow control information.

Command Syntax `show flowcontrol`

`show flowcontrol interface IFNAME`

Parameters

`interface IFNAME` Specify the name of the interface to be displayed.

Command Mode

Exec mode and Privileged Exec mode

Applicability

Entry	Description
Port	Interface being checked for flowcontrol.
Send admin	Displays whether the flowcontrol send process is administratively on or off.
FlowControl oper	Displays whether send flowcontrol is on or off on this interface.
Received admin	Displays whether the flowcontrol receive process is administratively on or off.
FlowControl oper	Displays whether receive flowcontrol is on or off on this interface.

RxPause	Number of received pause frames.
TxPause	Number of transmitted pause frames.

This command was introduced before SWMRE version 1.3.

Example

The following is a sample output of the `show flowcontrol interface` command displaying flow control information:

```
#show flowcontrol interface ge1
Port     Send FlowControl     Receive FlowControl RxPause TxPause

admin    oper         admin     oper

-----    ------- --------     ------- --------      ------- ------ge1
on        on            on        on             0       0 #
```

Table 1-69 explains the show command output fields.

Table 1-69: show flow control output

show interface capabilities

Use this command to display interface capabilities

Command Syntax `show interface (IFNAME|) capabilities`

Parameters

`IFNAME`	Displays the name of a specific interface for which status and configuration data is desired.

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show interface xe1/1 capabilities
xe1/1
Speed(FD) : 10MB,100MB,1000MB,10GB,20GB,40GB
Interface : xgmii
Medium : copper
Loopback : none,MAC,PHY
```

```
Pause : pause_tx,pause_rx,pause_asymm
Flags : autoneg
Encap : IEEE,HIGIG,HIGIG2
```

Table 1-70 explains the show command output fields.

Table 1-70: show interface capabilities output details

Field	Description
Interface number	The identifying ID number of the interface – eht0, xe1, etc.
Speed (FD)	The Flexible Data-Rates (FD) of the interface
interface	XAUI is a standard for extending the XGMII (10 Gigabit Media Independent Interface) between the MAC and PHY layer of Gigabit Ethernet.
Medium	Members have to have the same medium type configured. This only applies to Ethernet port-channel. Copper, fiber optics, etc.
Loop back	The loop back between the MAC and PHY layers.
Pause	Pause transmit, pause receive, pause asymmetrically.

Table 1-70: show interface capabilities output details

Field	Description
Flags	Interface flags set for Auto-negotiation.
Encap	Encapsulation – IEEE, HIGIG, and HIGIG2 specifications – HIGIG is a proprietary protocol that is implemented by Broadcom. The HIGIG protocol supports various switching functions. The physical signaling across the interface is XAUI, four differential pairs for receive and transmit (SerDes), each operating at 3.125 Gbit/s.

snmp restart mstp

Use this command to restart SNMP in Multiple Spanning Tree Protocol (MSTP).

Command Syntax `snmp`

```
restart mstp
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#snmp restart mstp
```

CHAPTER 2 Bridge Commands

This chapter provides a description, syntax, and examples of the bridge commands. It includes the following commands:

- bridge acquire
- bridge address
- bridge ageing
- bridge forward-time
- bridge hello-time
- bridge mac-priority-override
- bridge max-age
- bridge max-hops
- bridge priority
- bridge shutdown
- bridge transmit-holdcount
- bridge-group
- bridge-group path-cost
- bridge-group priority
- clear allowed-ethertype
- clear mac address-table
- show allowed-ethertype
- show bridge
- show interface switchport
- show mac address-table count bridge
- show mac address-table bridge
- switchport
- switchport allowed ethertype

bridge acquire

Use this command to enable a bridge to learn station location information for an instance. This helps in making forwarding decisions.

Use the `no` parameter with this command to disable learning.

Command Syntax `bridge <1-32> acquire`

`no bridge <1-32> acquire`

Parameter

<1-32>	Specify the bridge group ID.

Default

By default, learning is enabled for all instances.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#bridge 3 acquire
(config)#no bridge 3 acquire
```

bridge address

Use this command to add a static forwarding table entry for the bridge. Use the no parameter with this command to remove the entry for the bridge

Command Syntax `bridge <1-32> address XXXX.XXXX.XXXX (forward|discard) IFNAME bridge <1-32> address XXXX.XXXX.XXXX (forward|discard) IFNAME vlan <2-4094> bridge <1-32> address XXXX.XXXX.XXXX (forward|discard) IFNAME vlan <2-4094> svlan <2-4094> no bridge <1-32> address XXXX.XXXX.XXXX (forward|discard) IFNAME no bridge <1-32> address XXXX.XXXX.XXXX (forward|discard) IFNAME vlan <2-4094> no bridge <1-32> address XXXX.XXXX.XXXX (forward|discard) IFNAME vlan <2-4094> svlan <2-4094>`

Parameters

<1-32>	Bridge identifier
XXXX.XXXX.XXXX	Media Access Control (MAC) address in HHHH.HHHH.HHHH format.
forward	Forward matching frames.
discard	Discard matching frames.
IFNAME	Interface on which the frame comes out.
vlan	Identity of the VLAN in the range of <2-4094>.
svlan	Identity of the SVLAN in the range of <2-4094>.

Defaul

By default, bridge address is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#bridge 1 address 0000.000a.0021 forward eth0
(config)#no bridge 1 address 0000.000a.0021 forward eth0
```

bridge ageing

Use this command to specify the aging-out time for a learned MAC address. The learned MAC address persists until this specified time.

Use the `no` parameter with this command to disable this command.

Command Syntax `bridge <1-32> ageing-time <10-1000000> bridge <1-32> ageing`

`disable no bridge <1-32> ageing-time`

Parameters

`<1-32>`	Specify the bridge group ID.
`<10-1000000>`	Specify the aging time in seconds.

Default

By default, aging time is 300 seconds

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#bridge 3 ageing-time 1000
(config)#no bridge 3 ageing-time
```

bridge forward-time

Use this command to set the time (in seconds) after which (if this bridge is the root bridge) each port changes states to learning and forwarding. This value is used by all instances.

Use the `no` parameter with this command to restore the default value of 15 seconds.

Command Syntax `bridge <1-32> forward-time <4-30> no bridge <1-32> forward-time`

Parameters

`<1-32>`	Specify the bridge group ID.
`<4-30>`	Specify the forwarding time delay in seconds.

Note: Care should be exercised if the value is to be made below 7 seconds.

Default

By default, value is 15 seconds

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#bridge 3 forward-time 6
(config)#no bridge 3 forward-time
```

bridge hello-time

Use this command to set the hello-time, the time in seconds after which (if this bridge is the root bridge) all the bridges in a bridged LAN exchange Bridge Protocol Data Units (BPDUs). A very low value of this parameter leads to excessive traffic on the network, while a higher value delays the detection of topology change.This value is used by all instances.

Configure the bridge instance name before using this command. The allowable range of values is 1-10 seconds. However, make sure that the value of hello time is always greater than the value of hold time (2 seconds by default).

Use the `no` parameter to restore the default value of the hello time.

Note:A Bridge shall enforce the following relationships for Hello-time, Max-age and Forward-delay.

- 2 × (Bridge_Forward_Delay – 1.0 seconds) >= Bridge_Max_Age
- Bridge_Max_Age >= 2 × (Bridge_Hello_Time + 1.0 seconds)

Command Syntax `bridge <1-32> hello-time <1-10> no bridge <1-32> hello-time`

Parameters

`<1-32>`	Specify the bridge group ID.
`<1-10>`	Specify the hello BPDU interval in seconds.

Default

By default, value is 2 seconds

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#bridge 3 hello-time 3

(config)#no bridge 3 hello-time
```

bridge mac-priority-override

Use this command to set a MAC priority override.

Use the `no` parameter with this command to unset a MAC priority override.

Command Syntax

```
bridge <1-32> mac-priority-override mac-address MAC interface IFNAME vlan VLANID
  (static|static-priority-override|static-mgmt|static-mgmt-priority-overide)
  priority <0-7>
no bridge <1-32> mac-priority-override mac-address MAC interface IFNAME vlan VLANID
```

Parameters

`<1-32>`	Specify the bridge group ID.
`mac-address`	Enter a MAC address in HHHH.HHHH.HHHH format.
`interface`	Interface information
`vlan`	Add the values associated with a single VLAN
`static`	The MAC is a static entry
`static-mgmt`	The MAC is a Static Management
`static-mgmt-priority-overide`	The MAC is a Static Management with priority override

`static-priority-override`

The MAC is a static with priority override

`priority`

priority <0-7> priority value

Default

No default address is specified

Command Mode

Configuration Mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#bridge 1 mac-priority-override mac-address 1111.1111.1111
interface eth1 vlan 2 static priority 2

(config)#no bridge 1 mac-priority-override mac-address
1111.1111.1111 interface eth1 vlan 2
```

bridge max-age

Use this command to set the maximum age for a bridge. This value is used by all instances.

Maximum age is the maximum time in seconds for which (if a bridge is the root bridge) a message is considered valid. This prevents the frames from looping indefinitely. The value of maximum age should be greater than twice the value of hello time plus 1, but less than twice the value of forward delay minus 1. The allowable range for max-age is 6-40 seconds. Configure this value sufficiently high, so that a frame generated by root can be propagated to the leaf nodes without exceeding the maximum age.

Use the `no` parameter with this command to restore the default value of the maximum age.

Note:A Bridge shall enforce the following relationships for Hello-time, Max-age and Forward-delay.

- 2 × (Bridge_Forward_Delay – 1.0 seconds) >= Bridge_Max_Age
- Bridge_Max_Age >= 2 × (Bridge_Hello_Time + 1.0 seconds)

Command Syntax `bridge <1-32> max-age <6-40> no bridge <1-32> max-age`

Parameters

`<1-32>`	Specify the bridge group ID.
`<6-40>`	Specify the maximum time, in seconds, to listen for the root bridge <6-40>.

Default

By default, bridge maximum age is 20 seconds

Command Mode

Configure Mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 max-age 12

(config)#no bridge 2 max-age
```

bridge max-hops

Use this command to specify the maximum allowed hops for a BPDU in an MST region. This parameter is used by all the instances of the MST. Specifying the maximum hops for a BPDU prevents the messages from looping indefinitely in the network. When a bridge receives an MST BPDU that has exceeded the allowed maximum hops, it discards the BPDU.

Use the `no` parameter with this command to restore the default value.

Command Syntax `bridge <1-32> max-hops <1-40> no bridge <1-32> max-hops`

Parameters

`<1-32>`	Specify the bridge-group ID.
`<1-40>`	Specify the maximum hops for which the BPDU will be valid <1-40>.

Default

By default, maximum hops in an MST region are 20

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#bridge 3 max-hops 25

#configure terminal
(config)#no bridge 3 max-hops
```

bridge priority

Use this command to set the bridge priority for the common instance. Using a lower priority indicates a greater likelihood of the bridge becoming root. The priority values can be set only in increments of 4096.

Use the `no` form of the command to reset it to the default value.

Command Syntax `bridge (<1-32> | ) priority <0-61440> no bridge (<1-32> | )priority`

Parameters

`<1-32>`	Specify the bridge group ID.
`<0-61440>`	Specify the bridge priority in the range of <0-61440>.

Default

By default, priority is 32768 (or hex 0x8000).

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 priority 4096

(config)#no bridge 2 priority
```

bridge shutdown

Use this command to disable a bridge.

Use the `no` parameter to reset the bridge.

Command Syntax `bridge shutdown <1-32> bridge shutdown <1-32> bridge-forward no bridge shutdown <1-32>`

Parameters

`<1-32>`	Specify the bridge group ID.	
	`bridge-forward`	Put all ports of the bridge into forwarding state

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#bridge shutdown 4
(config)#no bridge shutdown 4
```

bridge transmit-holdcount

Use this command to set the maximum number of transmissions of BPDUs by the transmit state machine.

Use the `no` parameter with this command to restore the default transmit hold-count value.

Command Syntax `bridge <1-32> transmit-holdcount <1-10> no bridge <1-32> transmit-holdcount`

Parameters

`<1-32>`	Specify the bridge group ID.
`<1-10>`	Transmit hold-count value.

Default

By default, transmit hold-count is 6

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#bridge 1 transmit-holdcount 5

(config)#no bridge 1 transmit-holdcount
```

bridge-group

Use this command to bind an interface with a bridge specified by the parameter.

Use the `no` parameter with this command to disable this command.

Command Syntax `bridge-group (<1-32>) no bridge-group (<1-32>)`

Parameters

`<1-32>` Specify the bridge group ID.

Default

By default, bridge-group is disabled

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#bridge-group 2

(config)#interface eth1
(config-if)#no bridge-group 2
```

bridge-group path-cost

Use this command to set the cost of a path associated with a bridge group. The lower the path cost, the greater the likelihood of the bridge becoming root.

Use the `no` parameter with this command to restore the default priority value.

Command Syntax `bridge-group <1-32> path-cost <1-200000000> no bridge-group <1-32> path-cost`

Parameters

`<1-32>` Specify the bridge group ID. `path-cost`

Specify the path-cost of a port.

`<1-200000000>` Specify the cost to be assigned to the group.

Default

By default, bridge-group is disabled

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#bridge-group 3 path-cost 123

(config-if)#no bridge-group 3 path-cost
```

bridge-group priority

Use this command to set the port priority for a bridge. A lower priority indicates a greater likelihood of the bridge becoming root.

Command Syntax `bridge-group <1-32> priority <0-240>` `no bridge-group <1-32> priority`

Parameters

`<1-32>`	Specify the bridge group ID.
`<0-240>`	Specify the port priority range (a lower priority indicates greater likelihood of the interface becoming a root). The priority values can only be set in increments of 16.

Default

By default, priority is 1

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#bridge-group 4 priority 96

(config)#interface eth1
(config-if)#no bridge-group 4 priority
```

clear allowed-ethertype

Use this command to clear statistics for each ethertype per interfaces. `clear allowed-ethertype statistics (IFNAME|)`

Parameters

`IFNAME`	Interface name.

Command Mode

Exec mode

Applicability

This command was introduced in SWMRE version 1.3.1. Example

```
 #clear allowed-ethertype statistics xe54/1

 #show allowed-ethertype statistics xe54/1  Interface xe54/1  arp: 0
Packets, 0 Bytes  ipv4: 0 Packets, 0 Bytes  ipv6: 0 Packets, 0 Bytes
dropped: 0 Packets, 0 Bytes
```

clear mac address-table

Use this command to clear the filtering database for the bridge. This command can be issued to do the following:

- clear the filtering database
- clear all filtering database entries configured through CLI (static)
- clear all multicast filtering database entries
- clear all multicast filtering database entries for a given VLAN or interface
- clear all static or multicast database entries based on a mac address

Command Syntax `clear mac address-table (dynamic|static|multicast) bridge <1-32>`

`clear mac address-table (dynamic|static|multicast) (address MACADDR | interface IFNAME | vlan VID) bridge <1-32> clear mac address-table (dynamic|static|multicast) (address MACADDR | interface IFNAME | vlan VID) (instance INST) bridge <1-32> clear mac address-table (dynamic|static|multicast) cvlan VID svlan VID bridge <1-32>`

Parameters

`dynamic`	Clears all dynamic entries.
`multicast`	Clears all multicast filtering database entries.
`static`	Clears all entries configured through management.
`address`	Clear the specified MAC Address.
`MACADDR`	When filtering database, entries are cleared based on the MAC address.
`bridge`	Clears the bridge group ID. Value range is 1-32.
`bridge`	Clears the bridge group ID. Value range is 1-32.
`cvlan`	Clears all MAC address for the specified CVLAN. Value range is 1-4094.
`svlan`	Clears all mac address for the specified SVLAN. Value range is 1-4094.
`interface`	Clears all MAC address for the specified interface.
`bridge`	Clears the bridge group ID. Value range is 1-32.
`instance`	Clears MSTP instance ID. Value range is <1-63>. `vlan` Clears all MAC address for the specified VLAN. Value range is 1-4094.
`bridge`	Clears the bridge group ID. Value range is 1-32.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

This example shows how to clear all filtering database entries configured through CLI:

```
#clear mac address-table static bridge 1
```

This example shows how to clear multicast filtering database entries:

```
#clear mac address-table multicast bridge 1
```

This example shows how to clear all filtering database entries for a given interface:

```
#clear mac address-table static interface eth0 bridge 1
```

This example shows how to clear multicast filtering database entries for a given VLAN.

```
#clear mac address-table multicast vlan 2 bridge 1
```

This example shows how to clear static filtering database entries for a given MAC address:

```
#clear mac address-table static address 0202.0202.0202 bridge 1
```

This example shows how to clear all filtering database entries learned through bridge operation for a given MAC address.

```
#clear mac address-table dynamic address 0202.0202.0202 bridge 1
```

show allowed-ethertype

Use this command to show allowed and denied traffic statistics.

Note: Dropped slow protocol packets provides the count of slow protocol packets among the total dropped count. Total drop count is fetched from hardware and slow protocol packet count is fetched from software. Hence there can be one or two packet difference.

Command Syntax `show allowed-ethertype statistics (IFNAME|)`

Parameters

`IFNAME` Interface name.

Command Mode

Exec mode

Applicability

This command was introduced in SWMRE version 1.3.1.

Examples

```
#show allowed-ethertype statistics
Interface po1 arp : 0 Packets, 0 Bytes
ipv4 : 511016709 Packets, 184897169366 Bytes
ipv6 : 0 Packets, 0 Bytes dropped : 220
Packets, 28160 Bytes
dropped slow protocol pkts : lacp 220, efm 0, others 0
Interface xe47 arp : 0 Packets, 0 Bytes
ipv4 : 169763534 Packets, 61427990740 Bytes
ipv6 : 0 Packets, 0 Bytes dropped : 0 Packets,
0 Bytes Interface xe48 arp : 0 Packets, 0 Bytes
ipv4 : 0 Packets, 0 Bytes ipv6 : 0 Packets, 0
Bytes dropped : 0 Packets, 0 Bytes
```

show bridge

Use this command to display the filtering database for the bridge. The filtering database is used by a switch to store the MAC addresses that have been learned and which ports that MAC address was learned on.

Command Syntax `show bridge (ieee|rpvst+|mstp|)`

Parameters

`ieee` STP bridges. `rpvst+` RPVST+ bridges. `mstp` MSTP bridges.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show bridge
Ageout time is global and if something is configured for vxlan then it will be affected
here also
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-out
 --------+------+------ +------+-----------+-----------------+-----+---------+
 1         1                   eth1        5254.0029.929c    1     0
 1         2                   eth1        5254.004c.dcc6    1     297
 1         1                   eth1        5254.004c.dcc6    1     291
```

Table 2-71 explains the show command output fields.

Table 2-71: show bridge output fields

Field	Description
Bridge	Bridge identifier.
VLAN, SVLAN, BVLAN	CVLAN, SVLAN, and BVLAN identifiers.
Port	Interface name.
MAC Address	Learned MAC address.
FWD	Whether frames for the MAC addresses are forwarded.
Time-out	How long the learned MAC address persists.

show interface switchport

Use this command to display the characteristics of the interface with the current VLAN.

Command Syntax `show interface switchport bridge <1-32>`

Parameter

`bridge` Bridge name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following is an output of this command displaying the characteristics of this interface on bridge 2.

```
#show interface switchport bridge 2
 Interface name          :  eth5
 Switchport mode         : access
 Ingress filter          : disable
 Acceptable frame types  : all
 Vid swap                : disable
 Default vlan            : 2
 Configured vlans        :    2
 Interface name          :  eth4
 Switchport mode         : access
 Ingress filter          : disable
 Acceptable frame types  : all
 Vid swap                : disable
 Default vlan            : 1
 Configured vlans        :    1
```

Table 2-72 explains the show command output fields.

Table 2-72: show interface switchport output fields

Field	Description
Interface name	Display the name of interface.
Switchport mode	Port that used to connect between switches and access port.
Ingress filter	Ingress filtering examines all inbound packets and then permits or denies entry to the network.
Acceptable frame types	Type of acceptable frame in the interface.
VID swap	Displays the status of the VID swap.

Table 2-72: show interface switchport output fields (Continued)

Field	Description
Default vlan	Default value for the VLAN.
Configured vlans	Displays the information on configured VLANs.

show mac address-table count bridge

Use this command to display a count of MAC entries from the filtering database.

Command Syntax

```
show mac address-table (local|remote|) count bridge <1-32> ({(dynamic | multicast |
  static) | address MAC | interface IFNAME | vlan <1-4094> }|)
```

Parameter

`local`	MAC entries learned locally
`remote`	MAC entries learned from MLAG MAC sync
`<1-32>`	Bridge group
`dynamic`	Dynamic entries
`multicast`	Multicast entries
`static`	Static entries
`MAC`	MAC address in HHHH.HHHH.HHHH format
`IFNAME`	Name of the interface
`<1-4094>`	VLAN identifier

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show mac address-table count bridge 1
MAC Entries for all vlans:
Dynamic Address Count: 3
Static (User-defined) Unicast MAC Address Count: 0
Static (User-defined) Multicast MAC Address Count: 0 Total
MAC Addresses in Use: 3
```

Table 2-73 explains the show command output fields.

Table 2-73: show mac address-table count output fields

Field	Description
Dynamic Address Count	Number of dynamic addresses.
Unicast MAC Address Count	Number of unicast addresses.
Multicast MAC Address Count	Number of multicast addresses.

Total MAC Addresses	Total number of addresses.

show mac address-table bridge

Use this command to display MAC entries from the filtering database.

Command Syntax

```
show mac address-table (local|remote|) bridge <1-32> ({(dynamic | multicast |
  static) | address MAC | interface IFNAME | vlan <1-4094> }|)
```

Parameter

local	MAC entries learned locally
remote	MAC entries learned from MLAG MAC sync
<1-32>	Bridge group
dynamic	Dynamic entries
multicast	Multicast entries
static	Static entries
MAC	MAC address in HHHH.HHHH.HHHH format
IFNAME	Name of the interface
<1-4094>	VLAN identifier

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show mac address-table bridge 1 static interface ge14
VLAN      MAC Address    Type      Ports
 ------ +---------------+--------- +---------+--------------
 1       3333.3333.3333  static    ge14

#show mac address-table bridge 1
VLAN      MAC Address    Type      Ports
 ------ +---------------+--------- +---------+--------------
 1       3417.ebf6.0ace  dynamic   po1
 1       6400.6a8e.48ab  dynamic   po1
 1       a82b.b5b5.c37b  dynamic   po1
 200     0000.5e00.0101  dynamic   po1
 200     3417.ebf6.0ac5  dynamic   po1
 200     3417.ebf6.0ace  dynamic   po1
 200     6400.6a8e.48ab  dynamic   po1
 200    a82b.b5b5.c375   dynamic   po1
 200    a82b.b5b5.c37b   dynamic   po1
```

```
                                                                  800
 0000.5e00.0102   dynamic   po1
    800   3417.ebf6.0ac5   dynamic   po1
    800   3417.ebf6.0ace   dynamic   po1
   800    6400.6a8e.48ab   dynamic   po1
   800    a82b.b5b5.c375   dynamic   po1
```

```
800     a82b.b5b5.c37b   dynamic   po1
```

Table 2-74 explains the show command output fields.

Table 2-74: show mac address-table output fields

Field	Description
VLAN	VLAN identifier.
MAC Address	Media Access Control address.
Type	Dynamic, multicast, or static.
Ports	Interface name.

switchport

Use this command to set the mode of an interface to switched.

All interfaces are configured routed by default. To change the behavior of an interface from switched to routed, you must explicitly give the `no switchport` command.

Note: When you change the mode of an interface from switched to routed and vice-versa, all configurations for that interface are erased.

Use the `no` form of this command to set the mode to routed.

Command Syntax

```
switchport
no
switchport
```

Parameters

None

Default

All interfaces are configured routed by default. To change the behavior of an interface from switched to routed, you must explicitly give the no switchport command.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0 (config-
if)#switchport
```

```
(config)#interface eth0
(config-if)#no switchport
```

switchport allowed ethertype

Use this command to allow a set of ethertype on the access port and deny remaining traffic.

Use the no command to remove ethertype configuration.

Command Syntax `switchport allowed ethertype {arp|ipv4|ipv6|mpls|WORD|log}` `no switchport allowed ethertype ({arp|ipv4|ipv6|mpls|WORD|log}|)`

Parameters

`arp`	Ethertype 0x0806.
`ipv4`	Ethertype 0x0800.
`ipv6`	Ethertype 0x086dd.
`mpls`	Ethertype 0x8847.
`WORD`	Any Ethertype value (0x600 - 0xFFFF).
`log`	Log unwanted ethertype packets.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced in SWMRE version 1.3.1.

Examples

```
#configure terminal
(config)#interface xe1
        (config-if)#switchport allowed ethertype arp ipv4 ipv6 log

(config-if)#no switchport allowed ethertype ipv4
```

CHAPTER 3 Spanning Tree Protocol Commands

This chapter provides a description, syntax, and examples of the Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) commands. It includes the following commands:

- bridge cisco-interoperability
- bridge instance
- bridge instance priority
- bridge instance vlan
- bridge multiple-spanning-tree
- bridge protocol ieee
- bridge protocol mstp
- bridge protocol rstp
- bridge rapid-spanning-tree
- bridge region
- bridge revision
- bridge spanning-tree
- bridge spanning-tree errdisable-timeout
- bridge spanning-tree force-version
- bridge spanning-tree pathcost
- bridge spanning-tree portfast
- bridge te-msti
- bridge te-msti vlan
- bridge-group instance
- bridge-group instance path-cost
- bridge-group instance priority
- bridge-group path-cost
- bridge-group priority
- bridge-group spanning-tree
- clear spanning-tree detected protocols
- clear spanning-tree statistics
- customer-spanning-tree customer-edge path-cost
- customer-spanning-tree customer-edge priority
- customer-spanning-tree forward-time
- customer-spanning-tree hello-time
- customer-spanning-tree max-age
- customer-spanning-tree priority
- customer-spanning-tree provider-edge path-cost

- customer-spanning-tree provider-edge priority
- customer-spanning-tree transmit-holdcount
- debug mstp
- show debugging mstp
- show debugging mstp
- show debugging mstp
- show spanning-tree
- show spanning-tree mst
- show spanning-tree statistics
- spanning-tree autoedge
- spanning-tree edgeport
- spanning-tree edgeport
- spanning-tree guard
- spanning-tree instance restricted-role
- spanning-tree instance restricted-tcn
- spanning-tree link-type
- spanning-tree mst configuration
- spanning-tree restricted-domain-role
- spanning-tree restricted-role
- spanning-tree restricted-tcn
- spanning-tree te-msti configuration
- storm-control

bridge cisco-interoperability

Use this command to enable/disable Cisco interoperability for MSTP (Multiple Spanning Tree Protocol).

If Cisco interoperability is required, all SWMRE devices in the switched LAN must be Cisco-interoperability enabled. When SWMRE inter operates with Cisco, the only criteria used to classify a region are the region name and revision level. VLAN-to-instance mapping is not used to classify regions when interoperating with Cisco.

Command Syntax `bridge <1-32> cisco-interoperability (enable | disable)`

Parameters

`<1-32>`	Specify the bridge group ID
`enable`	Enable Cisco interoperability for MSTP bridge
`disable`	Disable Cisco interoperability for MSTP bridge

Default

By default, cisco interoperability is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

To enable Cisco interoperability on a switch for a bridge:

```
#configure terminal
(config)#bridge 2 cisco-interoperability enable
```

To disable Cisco interoperability on a switch for a particular bridge:

```
#configure terminal
(config)#bridge 2 cisco-interoperability disable
```

bridge instance

Use this command to add an MST instance to a bridge.

Use the `no` form of this command to delete an MST instance identifier from a bridge.

Command Syntax `bridge (<1-32> | backbone) instance (<1-63>) no bridge (<1-32> | backbone) instance (<1-63>)`

Parameters

`<1-32>`	Bridge identifier.
`backbone`	Backbone bridge.
`<1-63>`	MST instance identifier.

Default

The bridge instance default is 1.

Command Mode

MST configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#bridge 4 protocol mstp
(config)#spanning-tree mst configuration (config-mst)#bridge 4 instance 3
...
(config-mst)#no bridge 4 instance 3
```

bridge instance priority

Use this command to set the bridge instance priority.

Use the `no` form of this command to reset the priority to its default.

Command Syntax `bridge (<1-32> | backbone) instance <1-63> priority <0-61440> no bridge (<1-32> | backbone) instance <1-63> priority`

Parameters

`<1-32>`	Specify the bridge identifier.
`backbone`	Specifies the backbone bridge.
`<1-63>`	Specify the instance identifier.
`priority`	Specify the bridge priority for the instance. The lower the priority of the bridge, the better the chances is of the bridge becoming a root bridge or a designated bridge for the LAN. The priority values can be set only in increments of 4096. The default value is 32768.
`<0-61440>`	Specify the bridge priority.

Default

By default, bridge instance priority is 32768

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#bridge 4 instance 3 priority 1
```

bridge instance vlan

Use this command to simultaneously add multiple VLANs for the corresponding instance of a bridge.The VLANs must be created before being associated with an MST instance (MSTI). If the VLAN range is not specified, the MSTI will not be created.

Use the `no` form of this command to simultaneously remove multiple VLANs for the corresponding instance of a bridge.

Command Syntax `bridge (<1-32> | backbone) instance (<1-63>) vlan VLANID no bridge (<1-32> | backbone) instance (<1-63>) vlan VLANID`

Parameters

`<1-32>`	Bridge identifier.
`backbone`	Backbone bridge.
`<1-63>`	MST instance identifier.
`VLANID`	VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list. For a VLAN range, specify two VLAN identifiers: the lowest and then the highest separated by a hyphen. For a VLAN list, specify the VLAN identifiers separated by commas. Do not enter spaces between the hyphens or commas.

Default

The bridge instance VLAN ID Interfaces default-switch is VLAN100 100 ae0.0 ae1.0 ae2.0.

Command Mode

MST configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

To associate multiple VLANs, in this case VLANs 10 and 20 to instance 1 of bridge 1:

```
#configure terminal
(config)#bridge 1 protocol mstp
(config)#spanning-tree mst configuration
```

```
(config-mst)#bridge 1 instance 1 vlan 10,20
```

To associate multiple VLANs, in this case, VLANs 10, 11, 12, 13, 14, and 15 to instance 1 of bridge 1:

```
#configure terminal
(config)#bridge 1 protocol mstp
(config)#spanning-tree mst configuration
(config-mst)#bridge 1 instance 1 vlan 10-15
```

To delete multiple VLANs, in this case, VLANs 10 and 11 from instance 1 of bridge 1:

```
#configure terminal
(config)#bridge 1 protocol mstp
(config)#spanning-tree mst configuration
(config-mst)#no bridge 1 instance 1 vlan 10,11
```

bridge multiple-spanning-tree

Use this command to enable MSTP on a bridge.

Use the `no` form of this command to disable MSTP on the bridge.

Command Syntax `bridge <1-32> multiple-spanning-tree enable`

`no bridge <1-32> multiple-spanning-tree enable (bridge-forward|)`

Parameters

`<1-32>` Specify the bridge-group ID. `enable` Enables the spanning tree protocol. `bridge-forward` Puts all ports of the specified bridge into forwarding state.

Default

If the bridge-forward option is entered when using the `no` parameter, the default behavior is to put all bridge ports in forwarding state.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 multiple-spanning-tree enable
```

```
#configure terminal
(config)#no bridge 2 multiple-spanning-tree enable bridge-forward
```

bridge protocol ieee

Use this command to add a IEEE 802.1d Spanning Tree Protocol bridge.

After creating a bridge instance, add interfaces to the bridge using the `bridge-group` command. Bring the bridge instance into operation with the `no shutdown` command in interface mode.

Use the `no` parameter with this command to remove the bridge.

Command Syntax `bridge <1-32> protocol ieee`

`(vlan-bridge|) no bridge <1-32>`

Parameters

`<1-32>` Specify the bridge group ID. `vlan-bridge`

Specify this as a VLAN-aware bridge.

Default

The bridge protocol default value is 2 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#bridge 3 protocol ieee

(config)#bridge 4 protocol ieee vlan-bridge
```

bridge protocol mstp

Use this command to create a multiple spanning-tree protocol (MSTP) bridge of a specified parameter. This command creates an instance of the spanning tree and associates the VLANs specified with that instance.

The MSTP bridges can have different spanning-tree topologies for different VLANs inside a region of “similar” MSTP bridges. The multiple spanning tree protocol, like the rapid spanning tree protocol, provides rapid reconfiguration capability, while providing load balancing ability. A bridge created with this command forms its own separate region unless it is added explicitly to a region using the `region name` command.

Use the `no` parameter with this command to remove the bridge.

Command Syntax `bridge <1-32> protocol`

`mstp (ring|) no bridge <1-32>`

Parameters

`<1-32>`	Specify the bridge group ID.
`ring`	(Optional) Enable rapid ring spanning-tree.

Default

The bridge protocol mstp default value is 50 seconds

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 protocol mstp

#configure terminal
(config)#bridge 2 protocol mstp ring
```

bridge protocol rstp

Use this command to add an IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) bridge.

After creating a bridge instance, add interfaces to the bridge using the `bridge-group` command. Bring the bridge instance into operation with the `no shutdown` command in Interface mode.

Use the `no` parameter with this command to remove the bridge.

Command Syntax `bridge <1-32> protocol rstp bridge <1-32> protocol rstp (vlan-bridge|)(ring|) no bridge <1-32>`

Parameters

`<1-32>` Specify the bridge group ID. `ring` (Optional) Add an RSTP bridge for a ring topology. `vlan-bridge` (Optional) Adds a VLAN-aware bridge.

Default

By default, bridge protocol rstp is enabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 protocol rstp
```

```
#configure terminal
(config)#bridge 3 protocol rstp vlan-bridge
```

bridge rapid-spanning-tree

Use this command to enable or disable RSTP on a specific bridge. Use the `bridge-forward` option with the `no` form of the command to place all ports on the specified bridge into the forwarding state. Use the `no` form of the command to disable the Rapid Spanning Tree protocol on a bridge.

Command Syntax `bridge <1-32> rapid-spanning-tree enable`

`no bridge <1-32> rapid-spanning-tree enable (bridge-forward|)`

Parameters

`<1-32>` Specify the bridge group ID.

`enable` Enables the spanning tree protocol. `bridge-forward` (Optional) Puts all ports of the specified bridge into forwarding state.

Default

When the `bridge-forward` option is used with the `no` parameter, the default behavior puts all bridge ports in the forwarding state.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples `configure terminal`

```
(config)#bridge 2 rapid-spanning-tree enable
```

```
 configure terminal
(config)#no bridge 2 rapid-spanning-tree enable bridge-forward
```

bridge region

Use this command to create an MST region and specify its name. MST bridges of a region form different spanning trees for different VLANs.

Use the `no` form of the command to disable the Rapid Spanning Tree protocol on a region.

Command Syntax `bridge <1-32> region REGION_NAME no bridge <1-32> region`

Parameters

`<1-32>` Specify the bridge group ID.

REGION_NAME	Specify the name of the region.

Default

By default, each MST bridge starts with the region name as its bridge address. This means each MST bridge is a region by itself, unless specifically added to one.

Command Mode

MST configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree mst configuration (config-mst)#bridge
3 region myRegion

(config)#spanning-tree mst configuration
(config-mst)#no bridge 3 region
```

bridge revision

Use this command to specify the number for configuration information.

Command Syntax `bridge <1-32> revision <0-65535>`

Parameters

<1-32>	Specify the bridge group ID in the range of <1-32>.
<0-65535>	Specify a revision number in the range of <0-65535>.

Default

By default, revision number is 0

Command Mode

MST configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#spanning-tree mst configuration
(config-mst)#bridge 3 revision 25
```

bridge spanning-tree

Use this command to enable the Spanning Tree Protocol on a bridge.

Use the `no` parameter to disable the Spanning Tree Protocol on the bridge.

Command Syntax `bridge <1-32> spanning-tree enable`

`no bridge <1-32> spanning-tree enable (bridge-forward|)`

Parameters

`<1-32>` Specify the bridge group ID. `enable` Enables the spanning tree protocol on this bridge. `bridge-forward` Puts all ports of the specified bridge into the forwarding state.

Default

If the bridge-forward option is entered when using the `no` parameter, the default behavior is to put all bridge ports in forwarding state.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#bridge 2 spanning-tree enable

#configure terminal
(config)#no bridge 2 spanning-tree enable bridge-forward
```

bridge spanning-tree errdisable-timeout

Use this command to enable the error-disable-timeout facility, which sets a timeout for ports that are disabled due to the BPDU guard feature.

The BPDU guard feature shuts down the port on receiving a BPDU on a BPDU-guard enabled port. This command associates a timer with the feature such that the port gets enabled back without manual intervention after a set interval.

Use the `no` parameter to disable the error-disable-timeout facility.

Command Syntax `bridge <1-32> spanning-tree errdisable-timeout enable`

`bridge <1-32> spanning-tree errdisable-timeout interval <10-1000000> no bridge <1-32> spanning-tree errdisable-timeout enable`

`no bridge <1-32> spanning-tree errdisable-timeout interval`

Parameters

`<1-32>`	Specify the bridge group ID.
`enable`	Enable the timeout mechanism for the port to be enabled back
`interval`	Specify the interval after which port shall be enabled.

`<10-1000000>`

Specify the error-disable-timeout interval in seconds.

Default

By default, the port is enabled after 300 seconds

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#bridge 1 spanning-tree errdisable-timeout enable

#configure terminal
(config)#bridge 4 spanning-tree errdisable-timeout interval 34
```

bridge spanning-tree force-version

Use this command to set the version for the bridge. A version identifier of less than a value of 2 enforces the spanning tree protocol. Although the command supports an input range of 0-4, for RSTP, the valid range is 0-2. When the forceversion is set for a bridge, all ports of the bridge have the same spanning tree version set.

Use the `show spanning tree` command to display administratively configured and currently running values of the BPDU filter parameter for the bridge and port (see show spanning-tree).

Use the no parameter with this command to disable the version for the bridge.

Command Syntax `bridge <1-32> spanning-tree force-version <0-4> no bridge <1-32> spanning-tree force-version`

Parameters

`<1-32>` Specify the bridge group ID. `force-version`

Specify a force version identifier:

`0`	STP
`1`	Not supported
`2`	RSTP
`3`	MSTP

Default

By default, spanning tree force version is 0

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

Set the value to enforce the spanning tree protocol:

```
#configure terminal
(config)#bridge 1 spanning-tree force-version 0

(config)#no bridge 1 spanning-tree force-version
```

bridge spanning-tree pathcost

Use this command to set a spanning-tree path cost method.

If the short parameter is used, the switch uses a value for the default path cost a number in the range 1 through 65,535.
If the long parameter is used, the switch uses a value for the default path cost a number in the range 1 through 200,000,000. Refer to the show spanning-tree to view the administratively configured and current running pathcost method running on a bridge.

Use the no option with this command to return the path cost method to the default setting.

Command Syntax `bridge <1-32> spanning-tree pathcost method`

`(short|long) no bridge <1-32> spanning-tree pathcost method`

Parameters

`<1-32>`	Specify the bridge group ID.
`method`	Method used to calculate default port path cost.
`long`	Use 16-bit based values for default port path costs.
`short`	Use 32-bit based values for default port path costs.

Default

By default, path cost method for STP is short and for MSTP/RSTP is long.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#bridge 1 spanning-tree pathcost method short

(config)#no bridge 1 spanning-tree pathcost method
```

bridge spanning-tree portfast

Use this command to set the portfast BPDU (Bridge Protocol Data Unit) guard or filter for the bridge.

Use the `show spanning tree` command to display administratively configured and currently running values of the BPDU filter parameter for the bridge and port (see show spanning-tree).

Use the `no` parameter with this command to disable the BPDU filter for the bridge.

BPDU Filter

All ports that have their BPDU filter set to default take the same value of BPDU filter as that of the bridge. The Spanning Tree Protocol sends BPDUs from all ports. Enabling the BPDU Filter feature ensures that PortFast-enabled ports do not transmit or receive any BPDUs.

BPDU Guard

When the BPDU guard feature is set for a bridge, all portfast-enabled ports of the bridge that have the BPDU guard set to default shut down the port on receiving a BPDU. In this case, the BPDU is not processed. You can either bring the port back up manually by using the `no shutdown` command, or configure the errdisable-timeout feature to enable the port after the specified time interval.

Command Syntax `bridge <1-32> spanning-tree portfast bpdu-guard` `bridge <1-32> spanning-tree portfast bpdu-filter` `no bridge <1-32> spanning-tree portfast bpdu-guard` `no bridge <1-32> spanning-tree portfast bpdu-filter`

Parameters

`<1-32>` Specify the bridge group ID. `bpdu-filter` Specify to filter the BPDUs on portfast enabled ports. `bpdu-guard` Specify to guard the portfast ports against BPDU receive.

Default

By default, portfast for STP is enabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#bridge 3 spanning-tree portfast bpdu-filter

#configure terminal
(config)#bridge 1 spanning-tree portfast bpdu-guard
```

bridge te-msti

Use this command to enable or disable a Multiple Spanning Tree Instance (MSTI).

The te-msti always refers to the MST instance indexed by the pre-defined macro constant MSTP_TE_MSTID internally. This is the only MST instance which supports the disabling of spanning trees.

Use the no form of this command to remove the configuration.

Command Syntax bridge (<1-32> | backbone) te-msti no bridge (<1-32> | backbone) te-msti

Parameters

<1-32>	Specify the bridge group ID.
backbone	Identity of the backbone bridge group.
te-msti	MSTI to be the traffic engineering MSTI instance.

Default

By default, bridge te-msti is disabled

Command Mode

TE-MSTI Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree te-msti configuration
(config-te-msti)#bridge 2 te-msti

(config-te-msti)#no bridge 2 te-msti
```

bridge te-msti vlan

Use this command to enable or disable a Multiple Spanning Tree Instance (MSTI). When an MSTI is shutdown (disabled) each VLAN in the MSTI is set to the forwarding state on all bridge ports which the VLAN as a member of. When and MSTI is enabled (no shutdown), normal MSTP operation is started for the MSTI.

The te-msti always refers to the MST instance indexed by the pre-defined macro constant MSTP_TE_MSTID internally. This is the only MST instance which supports the disabling of spanning trees. All VLANs that do not want spanning tree topology computation need to be assigned to this te-msti instance.

This command is intended for supporting Traffic Engineering (TE) Ethernet tunnels. All VLANs allocated for traffic engineering should be assigned to one MSTI. That MSTI can in turn shutdown the spanning tree operation so that each VLAN path through the network can be manually provisioned.

Use the no form of this command to remove the configuration.

Command Syntax `bridge (<1-32> | backbone) te-msti vlan <1-4094>` `no bridge (<1-32> | backbone) te-msti vlan <1-4094>`

Parameters

`<1-32>` Specify the bridge group ID. `backbone` Identity of the backbone bridge group. `vlan` Specify a VLAN.

`<1-4094>` Specify a VLAN identifier to be associated.

Note: This designated instance is defined in 802.1Qay clause 8.9 to be 0xFFE.

Default

By default, te-msti vlan is vlan1.

Command Mode

TE-MSTI Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree te-msti configuration
(config-te-msti)#bridge 2 te-msti vlan 10
(config-te-msti)#no bridge 2 te-msti vlan 10
```

bridge-group instance

Use this command to assign a Multiple Spanning Tree (MST) instance to a port.

Use the `no` form of this command to remove the interface from the MST instance.

Command Syntax `bridge-group (<1-32> | backbone) instance (<1-63> | te-msti)` `no bridge-group (<1-32> | backbone) instance (<1-63> | te-msti)`

Parameters

`<1-32>`	Bridge identifier.
`backbone`	Backbone bridge.
`<1-63>`	Multiple spanning tree instance identifier.
`te-msti`	Traffic engineering MSTI instance.

For Provider Backbone Bridging (PBB), bridge-group <1-32> refers to the I-component or PB bridge while the <backbone> bridge group refers to the B-component. Usually for a BEB (Backbone Edge Bridge) device, the backbone bridge-group is used for traffic engineering.

For a PB (Provider Bridge) device used as BCB (Backbone Core Bridge), bridge group <132> is used for traffic engineering.

Default

By default, the bridge port remains in the listening and learning states for 15 seconds before transitional to the forwarding state.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#bridge-group 1
(config-if)#bridge-group 1 instance te-msti
```

bridge-group instance path-cost

Use this command to set a path cost for a multiple spanning tree instance.

Before you can give this command, you must explicitly add an MST instance to a port using the `bridge-group instance` command.

Use the `no` form of this command to set the path cost to its default which varies depending on bandwidth.

Command Syntax `bridge-group (<1-32> | backbone) instance <1-63> path-cost <1-200000000> no bridge-group ( <1-32> | backbone) instance <1-63> path-cost`

Parameters

`<1-32>` Bridge identifier. `backbone`

Specify the backbone bridge.

`<1-63>` Set the MST instance identifier.

`<1-200000000>` Path cost for a port (a lower path cost means greater likelihood of becoming root).

Default

Assuming a 10 Mb/s link speed, the default value is 200,000.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#spanning-tree mst configuration
(config-mst)#bridge 4 instance 3 vlan 3
(config-mst)#exit
(config)#interface eth1
(config-if)#bridge-group 4 instance 3
(config-if)#bridge-group 4 instance 3 path-cost 1000
```

bridge-group instance priority

Use this command to set the priority of a multiple spanning tree instance.

The Multiple Spanning Tree Protocol uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies a better priority. In the case of the same priority, the interface index will serve as the tiebreaker, with the lower-numbered interface being preferred over others.

Command Syntax `bridge-group (<1-32>) instance (<1-63>) priority <0-240> no bridge-group (<1-32>) instance (<1-63>) priority`

Parameters

`<1-32>`	Bridge identifier.
`backbone`	Backbone bridge.
`<1-63>`	Multiple spanning tree instance identifier.
`<0-240>`	Port priority. A lower value means greater likelihood of becoming root. Set the port priority in increments of 16.

Default

By default, the port priority is 128

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
(config)#interface eth2
(config-if)#bridge-group 2
(config-if)#bridge-group 2 instance 4
(config-if)#bridge-group 2 instance 4 priority 64
```

bridge-group path-cost

Use this command to set the cost of a path. Before you can use this command to set a path-cost in a VLAN configuration, you must explicitly add an MST instance to a port using the `bridge-group instance` command.

Use the `no` parameter with this command to restore the default cost value of the path which varies depending on the bandwidth.

Command Syntax `bridge-group <1-32> path-cost <1-200000000> no bridge-group <1-32> path-cost`

Parameters

`<1-32>`	Specify the bridge group ID.
`path-cost`	Specify the cost of path for a port.
`<1-200000000>`	Specify the cost of the path (a lower cost means a greater likelihood of the interface becoming root).

Default

Assuming a 10 Mb/s link speed, the default value is 200,000.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree mst configuration
(config-mst)#bridge 4 instance 3 vlan 3
(config-mst)#exit
(config)#interface eth1
(config-if)#bridge-group 4
(config-if)#bridge-group 4 path-cost 1000
```

bridge-group priority

Use this command to set the port priority for a bridge group.

The Multiple Spanning Tree Protocol uses port priority as a tiebreaker to determine which port should forward frames for a particular instance on a LAN, or which port should be the root port for an instance. A lower value implies a better priority. In the case of the same priority, the interface index will serve as the tiebreaker, with the lower-numbered interface being preferred over others.

Command Syntax `bridge-group (<1-32> | backbone) priority <0-240> no bridge-group (<1-32> | backbone) priority`

Parameters

`<1-32>`	Specify the bridge group ID.
`backbone`	Backbone bridge.

`<0-240>` Specify the port priority (a lower priority indicates greater likelihood of the interface becoming a root). The priority values can only be set in increments of 16.

Default

By default, port priority for each instance is 128

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#bridge-group 4 priority 80
```

bridge-group spanning-tree

This command is used to enable or disable the spanning-tree on a configured bridge.

Command Syntax `bridge-group <1-32> spanning-tree (disable|enable)`

Parameters

`<1-32>` Specify the bridge group ID.

`disable` Disable spanning tree on the interface. `enable` Enable spanning tree on the interface.

Default

By default, spanning-tree is enabled

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
(config)#interface eth1
(config-if)#bridge-group 1 spanning-tree enable
```

clear spanning-tree detected protocols

Use this command to clear the detected protocols for a specific bridge or interface. This command begins the port migration as per IEEE 802.1w-2001, Section 17.26. After issuing this command, the migration timer is started on the port, only if the force version is RSTP or MSTP (greater versions of RSTP).

Command Syntax `clear spanning-tree detected protocols bridge <1-32>`

Parameters

`<1-32>`	Specify the bridge group ID.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear spanning-tree detected protocols bridge 2
```

clear spanning-tree statistics

Use this command to clear all STP BPDU statistics.

Command Syntax `clear spanning-tree statistics bridge <1-32> clear spanning-tree statistics interface IFNAME (instance (<1-63>)| vlan <1-4094>) bridge <1-32>`

`clear spanning-tree statistics (interface IFNAME| (instance (<1-63>)| vlan <24094>)) bridge <1-32>`

Parameters

`<1-32>`	Specify the bridge identifier.
`IFNAME`	Specify the name of the interface on which protocols have to be cleared.
`<1-63>`	MST instance ID.
`<1-4094>`	VLAN identifier where spanning tree is located <2-4094>

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear spanning-tree statistics bridge 32
```

customer-spanning-tree customer-edge path-cost

Use this command to set the cost of a path associated with a customer edge port on a customer edge spanning tree.

Use the `no` form of this command to remove the cost of a path associated with a customer edge port on a customer edge spanning tree.

Command Syntax `customer-spanning-tree customer-edge path-cost <1-200000000> no customer-spanning-tree customer-edge path-cost`

Parameters `path-cost` Specify the path-cost of a port.

`<1-200000000>` Specify the cost to be assigned to the group.

Default

Assuming a 10 Mb/s link speed, the default value is 200,000

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree customer-edge path-cost 1000
```

customer-spanning-tree customer-edge priority

Use this command to set the port priority for a customer-edge port in the customer spanning tree.

Command Syntax `customer-spanning-tree customer-edge priority <0-240>`

Parameters

`priority`	Specify the port priority.
`<0-240>`	Specify the port priority range (a lower priority indicates greater likelihood of the interface becoming a root). The priority values can only be set in increments of 16.

Default

By default, priority is 1

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree customer-edge priority 100
```

customer-spanning-tree forward-time

Use this command to set the time (in seconds) after which (if this bridge is the root bridge) each port changes states to learning and forwarding. This value is used by all instances.

Use the `no` form of this command to restore the default value of 15 seconds.

Command Syntax `customer-spanning-tree forward-time <4-30> no customer-spanning-tree forward-time`

Parameters

`<4-30>`	Specify the forwarding time delay in seconds.

Note: Care should be exercised if the value is set to less than 7 seconds.

Default

By default, priority is 15 seconds

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree forward-time 6

(config-if)#no customer-spanning-tree forward-time
```

customer-spanning-tree hello-time

Use this command to set the hello-time, the time in seconds after which (if this bridge is the root bridge) all the bridges in a bridged LAN exchange Bridge Protocol Data Units (BPDUs). Avoid a very low value of this parameter as this can lead to excessive traffic on the network; a higher value delays the detection of topology change. This value is used by all instances.

Use the `no` option with this command to restore the default value of the hello-time.

Command Syntax `customer-spanning-tree hello-time <1-10> no customer-spanning-tree hello-time`

Parameters

`<1-10>`	Specify the hello BPDU interval in seconds.

Default

By default, level is 2 seconds

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree hello-time 3

(config-if)#no customer-spanning-tree hello-time
```

customer-spanning-tree max-age

Use this command to set the max-age for a bridge.

Max-age is the maximum time in seconds for which (if a bridge is the root bridge) a message is considered valid. This prevents the frames from looping indefinitely. The value of max-age should be greater than twice the value of hello-time plus one, but less than twice the value of forward delay minus one. The allowable range for max-age is 6-40 seconds. Configure this value sufficiently high, so that a frame generated by a root can be propagated to the leaf nodes without exceeding the max-age.

Use the `no` parameter with this command to restore the default value of max-age.

Command Syntax `customer-spanning-tree max-age <6-40> no customer-spanning-tree max-age`

Parameters

`<6-40>`	Specify the maximum time in seconds to listen for the root bridge.

Default

By default, bridge max-age is 20 seconds

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree max-age 12 (config-if)#no customer-spanning-tree max-age
```

customer-spanning-tree priority

Use this command to set the bridge priority for the spanning tree on a customer edge port. Using a lower priority indicates a greater likelihood of the bridge becoming root. This command must be used to set the priority of the customer spanning tree running on the customer edge port. Use the `no` form of the command to reset it to the default value.

Command Syntax `customer-spanning-tree priority <0-61440> no customer-spanning-tree priority`

Parameters

`<0-61440>`	Specify the bridge priority in the range <0-61440>. Priority values can be set only in increments of 4096.

Default

By default, priority is 61440

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree priority 4096

(config-if)#no customer-spanning-tree priority
```

customer-spanning-tree provider-edge path-cost

Use this command to set the cost of a path associated with a provider edge port on a customer edge spanning tree.

Use the `no` form of this command to remove the cost of a path associated with a provider edge port on a customer edge spanning tree.

Command Syntax `customer-spanning-tree provider-edge svlan <1-4094> path-cost <1-200000000> no customer-spanning-tree provider-edge svlan <1-4094> path-cost`

Parameters

`<1-4094>` Specify the SVLAN identifier of provider edge port.

`<1-200000000>` Specify the cost to be assigned to the group.

Default

Assuming a 10 Mb/s link speed, the default value is 200,000

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree provider-edge svlan 2 path-cost 1000

(config-if)#no customer-spanning-tree provider-edge svlan 2 path-cost
```

customer-spanning-tree provider-edge priority

Use this command to set the port priority for a provider-edge port in the customer spanning tree.

Command Syntax `customer-spanning-tree provider-edge svlan <1-4094> priority <0-240>`

Parameters

<1-4094>	Specify the SVLAN identifier of provider edge port.
<0-240>	Specify the port priority (a lower priority means greater likelihood of the interface becoming root). The priority values can only be set in increments of 16.

Default

By default, priority is 1

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree provider-edge svlan 2 priority 0
```

customer-spanning-tree transmit-holdcount

Use this command to set the transmit-holdcount for a bridge.

Use the `no` parameter with this command to restore the default value of `transmit-holdcount`.

Command Syntax `customer-spanning-tree transmit-holdcount <1-10> no customer-spanning-tree transmit-holdcount`

Parameters

<1-10>	Specify the maximum number that can be transmitted per second.

Default

By default, bridge transmit hold count is 6

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#customer-spanning-tree transmit-holdcount 3

(config-if)#no customer-spanning-tree transmit-holdcount
```

debug mstp

Use this command to turn on, and turn off, debugging and echoing data to the console, at various levels.

Note: This command enables MSTP, RSTP, and STP debugging.

Use the `no` parameter with this command to turn off debugging.

Command Syntax `debug mstp all debug mstp cli debug mstp packet rx debug mstp packet tx debug mstp protocol debug mstp protocol detail debug mstp timer debug mstp timer detail no debug mstp all no debug mstp cli no debug mstp packet rx no debug mstp packet tx no debug mstp protocol no debug mstp protocol detail no debug mstp timer no debug mstp timer detail`

Parameters

`all`	Echoes all spanning-tree debugging levels to the console.
`cli`	Echoes spanning-tree commands to the console.
`packet`	Echoes spanning-tree packets to the console.
`rx`	Received packets.
`tx`	Transmitted packets.
`protocol`	Echoes protocol changes to the console.
`detail`	Detailed output.
`timer`	Echoes timer start to the console.
`detail`	Detailed output.

Command Mode

Exec, Privileged Exec, and Configure modes

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#debug mstp all
(config)#debug mstp cli
(config)#debug mstp packet rx
(config)#debug mstp protocol detail
(config)#debug mstp timer
```

show debugging mstp

Use this command to display the status of debugging of the MSTP system.

Command Syntax `show debugging mstp`

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show debugging mstp
MSTP debugging status:
MSTP debugging status:
 MSTP timer debugging is on
 MSTP protocol debugging is on
 MSTP detailed protocol debugging is on
 MSTP cli echo debugging is on
 MSTP transmitting packet debugging is on
 MSTP receiving packet debugging is on
#
```

show spanning-tree

Use this command to show the state of the spanning tree for all STP or RSTP bridge-groups, including named interface and VLANs.

Command Syntax `show spanning-tree show spanning-tree interface IFNAME show spanning-tree mst show spanning-tree mst config show spanning-tree mst interface IFNAME show spanning-tree mst detail show spanning-tree mst detail interface IFNAME show spanning-tree mst instance (<1-63>) interface IFNAME show spanning-tree mst instance (<1-63> | te-msti) show spanning-tree statistics bridge <1-32> show spanning-tree statistics interface IFNAME (instance (<1-63>)| vlan <2-4094>)`

`bridge <1-32>`

`show spanning-tree statistics (interface IFNAME | (instance (<1-63>) | vlan <1-4094>)) bridge <1-32> show`

`spanning-tree vlan range-index`

Parameters `interface` Display interface

information `mst` Display MST information

`statistics` Display statistics of the BPDUs `vlan`

`range-index`

Display a VLAN range-index value

`config` Display configuration information `detail`

Display detailed information `instance` Display

instance information `<1-63>` Specify the instance identifier

`te-msti` Display Traffic Engineering MSTI instance

`<1-32>` Specify the bridge identifier

`IFNAME` Display the interface name

`<2-4094>` Specify a VLAN identifier, associated with the instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following is a sample output of this command displaying spanning tree information.

```
#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20
% 1: Root Id 80000002b328530a
% 1: Bridge Id 80000002b328530a
% 1: last topology change Wed Nov 19 22:39:18 2008
% 1: 11 topology change(s) - last topology change Wed Nov 19 22:39:18 2008
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%eth2: Ifindex 5 - Port Id 8005 - Role Designated - State Forwarding
%eth2: Designated Path Cost 0
%eth2: Configured Path Cost 200000 - Add type Explicit ref count 1
%eth2: Designated Port Id 8005 - Priority 128 -
%eth2: Root 80000002b328530a
%eth2: Designated Bridge 80000002b328530a
%eth2: Message Age 0 - Max Age 20
%eth2: Hello Time 2 - Forward Delay 15
%eth2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%eth2: forward-transitions 4
%eth2: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
%eth2: No portfast configured - Current portfast off
%eth2: portfast bpdu-guard default - Current portfast bpdu-guard off
%eth2: portfast bpdu-filter default - Current portfast bpdu-filter off
%eth2: no root guard configured- Current root guard off
%eth2: Configured Link Type point-to-point - Current point-to-point
%eth1: Ifindex 4 - Port Id 8004 - Role Designated - State Forwarding
%eth1: Designated Path Cost 0
%eth1: Configured Path Cost 200000 - Add type Explicit ref count 1
%eth1: Designated Port Id 8004 - Priority 128 -
%eth1: Root 80000002b328530a
%eth1: Designated Bridge 80000002b328530a
%eth1: Message Age 0 - Max Age 20
%eth1: Hello Time 2 - Forward Delay 15
%eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%eth1: forward-transitions 4
%eth1: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
%eth1: No portfast configured - Current portfast off
%eth1: portfast bpdu-guard default - Current portfast bpdu-guard off
%eth1: portfast bpdu-filter default - Current portfast bpdu-filter off
```

```
%eth1: no root guard configured- Current root guard off
%eth1: Configured Link Type point-to-point - Current point-to-point
%
%
```

The following is a sample output of this command displaying the state of the spanning tree for interface `eth1`.

```
#show spanning-tree interface eth1
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20
% 1: Root Id 80000002b328530a
% 1: Bridge Id 80000002b328530a
% 1: last topology change Wed Nov 19 22:39:18 2008
% 1: 11 topology change(s) - last topology change Wed Nov 19 22:39:18 2008
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% eth1: Ifindex 4 - Port Id 8004 - Role Designated - State Forwarding
% eth1: Designated Path Cost 0
% eth1: Configured Path Cost 200000 - Add type Explicit ref count 1
% eth1: Designated Port Id 8004 - Priority 128 -
% eth1: Root 80000002b328530a
% eth1: Designated Bridge 80000002b328530a
% eth1: Message Age 0 - Max Age 20
% eth1: Hello Time 2 - Forward Delay 15
% eth1: forward-transitions 4
% eth1: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
% eth1: No portfast configured - Current portfast off
% eth1: portfast bpdu-guard default - Current portfast bpdu-guard off
% eth1: portfast bpdu-filter default - Current portfast bpdu-filter off
% eth1: no root guard configured- Current root guard off
```

Table 3-75 Explains the show command output fields.

Table 3-75: show spanning-tree interface output fields

Field	Description
Bridge up	A network bridge is a computer networking device that creates a single aggregate network from multiple communication networks or network segments.
Root Path Cost	Root cost for the interface.
Root Port	Interface that is the current elected root port for this bridge.

Bridge Priority	Used for the common instance.
Forward Delay	Configured time an STP bridge port remains in the listening and learning states before transitioning to the forwarding state.
Hello Time	Configured number of seconds between transmissions of configuration BPDUs.
Max Age	Maximum age of received protocol BPDUs.
Port Id	Logical interface identifier configured to participate in the MSTP instance.
Role Designated	Designated role for the packets in the interface.
State Forwarding	State of the forwarding packets in the interface.

Field	**Description**
Designated Path Cost	Designated cost for the interface.
Configured Path Cost	Configured cost for the interface.
Designated Port Id	Port ID of the designated port for the LAN segment this interface is attached to.
Priority	Specify the port priority.
Message Age	Number of seconds elapsed since the most recent BPDU was received.
Forward Timer	The forward delay timer is the time interval that is spent in the listening and learning state.
Msg Age Timer	The message age contains the length of time that has passed since the root bridge initially originated the BPDU.
Received RSTP	Number of times the received the RSTP.
Send RSTP	Number of times transmitted the RSTP.

show spanning-tree mst

Use this command to display the filtering database values. This command displays the number of instances created, and VLANs associated with it.

Command Syntax `show spanning-tree mst show spanning-tree mst config show spanning-tree mst detail show spanning-tree mst detail interface IFNAME show spanning-tree mst instance (<1-63>) interface IFNAME show spanning-tree mst instance (<1-63> | te-msti) show spanning-tree mst interface IFNAME`

Parameters

`config`	Display configuration information.
`detail`	Display detailed information.
`interface`	Display interface information.
`instance`	Display instance information.
`<1-63>`	Specify the instance identifier.
`te-msti`	Traffic Engineering MSTI instance.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show spanning-tree mst
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge
Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 80000002b328530a
% 1: CIST Reg Root Id 80000002b328530a
% 1: CIST Bridge Id 80000002b328530a
% 1: 2 topology change(s) - last topology change Wed Nov 19 22:43:21 2008
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec%
% Instance VLAN
 % 0:       1
 % 2:       3-4
```

Table 3-76 Explains the show command output fields.

Table 3-76: show spanning-tree mst output fields

Field	Description
Bridge up	A network bridge is networking process that creates a single aggregate network from multiple communication networks or network segments.
CIST Root Path Cost	Calculated cost to reach the regional root bridge from the bridge where the command is entered.
CIST Root Port	Interface that is the current elected CIST root port for this bridge.
CIST Bridge	A CIST bridge is networking process that creates a single aggregate network from multiple communication networks.
Priority	Specify the port priority.
Forward Delay	Configured time an STP bridge port remains in the listening and learning states before transitioning to the forwarding state.
Hello Time	Configured number of seconds between transmissions of configuration BPDUs.
Max Age	Maximum age of received protocol BPDUs.
Max-hops	Configured maximum number of hops a BPDU can be forwarded in the MSTP region.

show spanning-tree statistics

Use this command to display detailed BPDU statistics for a spanning tree instance.

Command Syntax `show spanning-tree statistics bridge <1-32> show spanning-tree statistics interface IFNAME (instance (<1-63>)| vlan <2-4094>) bridge <1-32>`

`show spanning-tree statistics (interface IFNAME | (instance (<1-63>) | vlan <14094>)) bridge <1-32>`

Parameters

`<1-32>`	Bridge identifier.
`<1-63>`	MST instance identifier.
`IFNAME`	Displays the interface name.
`<2-4094>`	Specify a VLAN identifier, associated with the instance.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

In the following example, bridge-group 1 is configured for IEEE on the eth2 interface.

```
#show spanning-tree statistics interface eth2 bridge 1

% BPDU Related Parameters
% ----------------------
% Port Spanning Tree                : Enable
% Spanning Tree Type                : Spanning Tree Protocol
% Current Port State                : Learning
% Port ID                           : 8004
% Port Number                       : 4
% Path Cost                         : 200000
% Message Age                       : 0
% Designated Root                   : 00:02:b3:d5:91:ec
% Designated Cost                   : 0
% Designated Bridge                 : 00:02:b3:d5:91:ec
% Designated Port Id                : 8005
% Top Change Ack                    : FALSE
% Configure Pending                    : FALSE

% PORT Based Information & Statistics
% ----------------------------------
% Configure Bpdu's xmitted             : 0
% Configure Bpdu's received            : 22
% TCN Bpdu's xmitted                : 0
% TCN Bpdu's received               : 8
% Forward Trans Count               : 0

% STATUS of Port Timers
% ---------------------
% Hello Time Configured             : 2
% Hello timer                       : ACTIVE
% Hello Time Value                  : 1
% Forward Delay Timer               : ACTIVE
% Forward Delay Timer Value         : 1
% Message Age Timer                 : ACTIVE
% Message Age Timer Value           : 19
% Topology Change Timer             : INACTIVE
% Topology Change Timer Value       : 0
% Hold Timer                        : INACTIVE
% Hold Timer Value                  : 0

% Other Port-Specific Info
  ------------------------
```

```
% Max Age Transitions                : 1
% Msg Age Expiry                     : 0
% Similar BPDUS Rcvd                 : 14
% Src Mac Count                      : 0
% Total Src Mac Rcvd                 : 15
% Next State                         : Blocked
% Topology Change Time               : 0


% Other Bridge information & Statistics
  ---------------------------------------
% STP Multicast Address              : 01:80:c2:00:00:00
% Bridge Priority                    : 32768
% Bridge Mac Address                 : 00:02:b3:d5:98:3f
% Bridge Hello Time                  : 2
% Bridge Forward Delay               : 15
% Topology Change Initiator          : 0
% Last Topology Change Occurred       : Wed Dec 31 16:00:00 1969
% Topology Change                    : FALSE
% Topology Change Detected           : FALSE
% Topology Change Count              : 0
% Topology Change Last Recvd from    : 00:00:00:00:00:00
```

Table 3-77 Explains the show command output fields.

Table 3-77: show spanning-tree statistics output fields

Field	Description
BPDU Related Parameters	Details of the BPDU related parameters.
PORT Based Information & Statistics	Information of the port and interface for which the statistics are being displayed.

Field	Description
STATUS of Port Timers	Status of the port timers.
Other Port-Specific Info	Specific information about the port.

Other Bridge information & Statistics	Information about bridge and statistics being displayed.

spanning-tree autoedge

Use this command to assist in automatic identification of the edge port.

Use the `no` parameter with this command to disable this feature.

Command Syntax `spanning-tree autoedge no spanning-tree autoedge`

Default

By default, spanning-tree autoedge is disabled

Parameters

None

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree autoedge
```

spanning-tree edgeport

Use this command to set a port as an edge-port and to enable rapid transitions.

Use the `no` parameter with this command to set a port to its default state (not an edge-port) and to disable rapid transitions.

Note: This command is an alias to the `spanning-tree portfast` command. Both commands can be used interchangeably.

Command Syntax `spanning-tree`

`edgeport no spanning-tree`

`edgeport`

Default

By default, spanning-tree edgeport is disabled

Parameters

None

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree edgeport
```

spanning-tree guard

Use this command to enable the root guard feature for the port. This feature disables reception of superior BPDUs.

The root guard feature makes sure that the port on which it is enabled is a designated port. If the root guard enabled port receives a superior BPDU, it goes to a Listening state (for STP) or discarding state (for RSTP and MSTP).

Use the `no` parameter with this command to disable the root guard feature for the port.

Command Syntax `spanning-tree guard root` `no spanning-tree guard root`

Parameters `root` Set to disable reception of superior BPDUs

Default

By default, spanning-tree guard root is enabled

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree guard root
```

spanning-tree instance restricted-role

Use this command to set the restricted role value for the instance to TRUE.

Use the `no` parameter with this command to set the restricted role value for the instance to FALSE.

Command Syntax `spanning-tree instance <1-63> restricted-role` `no spanning-tree instance <1-63> restricted-role`

Parameters

`<1-63>` Specify the instance ID range.

Default

By default, restricted-role value is FALSE

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree instance 2 restricted-role
```

spanning-tree instance restricted-tcn

Use this command to set the restricted TCN value for the instance to TRUE.

Command Syntax `spanning-tree instance <1-63> restricted-tcn no spanning-tree instance <1-63> restricted`

Parameters

`<1-63>`	Specify the instance ID range.

Default

By default, restricted TCN value is FALSE

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
                              (config-if)#spanning-tree instance 2 restricted-tcn
```

spanning-tree link-type

Use this command to enable or disable point-to-point or shared link types.

RSTP has a backward-compatible STP mode, `spanning-tree link-type shared`. An alternative is the `spanning-tree force-version 0`.

Use the `no` parameter with this command to disable rapid transition.

Command Syntax `spanning-tree link-type auto spanning-tree link-type point-to-point spanning-tree link-type shared no spanning-tree link-type`

Parameters `auto` Sets to either point-to-point or shared based on duplex state. `point-to-point` Enables rapid transition. `shared` Disables rapid transition.

Default

By default, spanning-tree link-type is enabled.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree link-type point-to-point

(config-if)#no spanning-tree link-type
```

spanning-tree mst configuration

Use this command to enter the Multiple Spanning Tree Configuration mode.

Command Syntax `spanning-tree mst configuration`

Parameters

None

Default

No default value is specified.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree mst configuration
(config-mst)#
```

spanning-tree bpdu-filter

Use this command to set the BPDU filter value for individual ports. When the `enable` or `disable` parameter is used with this command, this configuration takes precedence over bridge configuration. However, when the `default` parameter is used with this command, the bridge level BPDU filter configuration takes effect for the port.

Use the `show spanning tree` command to display administratively configured and currently running values of the BPDU filter parameter for the bridge and port (see show spanning-tree).

Use the `no` parameter with this command to revert the port BPDU filter value to default.

Command Syntax `spanning-tree bpdu-filter (enable|disable|default) no spanning-tree bpdu-filter`

Parameters

`default`	Sets the bpdu-filter to the default level.
`disable`	Disables the BPDU-filter.
`enable`	Enables the BPDU-filter.

Default

By default, spanning-tree bpdu-filter is default option

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree bpdu-filter enable

(config-if)#no spanning-tree bpdu-filter
```

spanning-tree bpdu-guard

Use this command to enable or disable the BPDU Guard feature on a port.

This command supersedes the bridge level configuration for the BPDU Guard feature. When the `enable` or `disable` parameter is used with this command, this configuration takes precedence over bridge configuration. However, when the `default` parameter is used with this command, the bridge-level BPDU Guard configuration takes effect.

Use the `show spanning tree` command to display administratively configured and currently running values of the BPDU filter parameter for the bridge and port (see show spanning-tree).

Use the no parameter with this command to set the BPDU Guard feature on a port to default.

Command Syntax `spanning-tree bpdu-guard (enable|disable|default) no spanning-tree bpdu-guard`

Parameters

`default`	Sets the BPDU-guard to the default level.

`disable`	Disables the BPDU-guard.
`enable`	Enables the BPDU-guard.

Default

By default, spanning-tree bpdu-guard is default

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree bpdu-guard enable

(config-if)#no spanning-tree bpdu-guard
```

spanning-tree restricted-domain-role

Use this command to set the restricted-domain-role value of the port to TRUE.

Use the `no` parameter with this command to set the restricted-domain-role value of the port to FALSE.

Command Syntax `spanning-tree restricted-domain-role no`

```
spanning-tree restricted-domain-role
```

Parameters

None

Default

By default, restricted-role value is FALSE

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree restricted-domain-role
```

spanning-tree restricted-role

Use this command to set the restricted-role value of the port to TRUE.

Use the `no` parameter with this command to set the restricted-role value of the port to FALSE.

Command Syntax `spanning-tree restricted-role no spanning-tree restricted-role`

Parameters

None

Default

By default, restricted-role value is FALSE

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree restricted-role
```

spanning-tree restricted-tcn

Use this command to set the restricted TCN value of the port to TRUE.

Use the `no` parameter with this command to set the restricted TCN value of the port to FALSE.

Command Syntax `spanning-tree restricted-tcn no spanning-tree restricted-tcn`

Parameters

None

Default

By default, restricted TCN value is FALSE

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree restricted-tcn
```

spanning-tree te-msti configuration

This command is used to put the terminal into the `te-msti` configuration mode.

After creating a bridge instance and adding VLAN to that bridge instance, use this command to enter `te-msti` configuration mode.

Command Syntax `spanning-tree te-msti configuration`

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#spanning-tree te-msti configuration
(config-te-msti)#
```

storm-control

Use this command to set the rising threshold level for broadcast, multicast, or destination lookup failure traffic. The storm control action occurs when traffic utilization reaches this level.

Storm control is used to block the forwarding of unnecessary flooded traffic. A packet storm occurs when a large number of broadcast packets are received on a port. Forwarding these packets can cause the network to slow down or time out.

Use the `no` form of this command to disable storm control.

Note:Minimum granularity for storm-control is 64kbps.

Command Syntax

```
storm-control (broadcast|multicast|dlf) (level LEVEL | <0-1000000000>
  (kbps|mbps|gbps)) no storm-control
(broadcast|multicast|dlf)
```

Parameters `broadcast` Broadcast rate limiting.

`multicast` Multicast rate limiting. `dlf`

Destination lookup failure limiting.

`level` Sets the percentage of the threshold.

LEVEL The percentage of the threshold; percentage of the maximum speed (pps) of the interface <0.0000-1000.0000>.

<0-1000000000> Sets absolute threshold value <0-1000000000> kbps specifies the units of Kilobits per second. mbps specifies the units of Megabits per second.

gbps specifies the units of Gigabits per second.

Default

By default, storm control is disabled

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#storm-control broadcast level 30

(config)#interface eth0 (config-if)#storm-
control multicast level 30

(config)#interface eth0
```

```
(config-if)#storm-control multicast 300 mbps

(config)#interface eth0
(config-if)#no storm-control multicast
```

CHAPTER 4 RPVST+ Commands

This chapter contains the commands used for Rapid Per VLAN Spanning Tree (RPVST+). RPVST+ enables a bridge to inter-operate with Cisco RPVST+ switches.

RPVST+ uses the Multiple Spanning Tree Protocol (MSTP) with a single VLAN for each Multiple Spanning Tree instance (MSTI). The MST bridges can have different spanning-tree topologies for different VLANs inside a region of similar MST bridges. MSTP, like the Rapid Spanning Tree Protocol (RSTP), provides rapid reconfiguration capabilities and supports load balancing.

This chapter includes the following commands:

- bridge vlan
- bridge vlan priority
- bridge-group vlan
- bridge protocol rpvst+
- bridge rapid-pervlan-spanning-tree
- show spanning-tree rpvst+
- spanning-tree rpvst+ configuration

- spanning-tree vlan restricted-role
- spanning-tree vlan restricted-tcn

bridge vlan

This command creates or deletes a mapping between an MSTI (Multiple Spanning Tree Instance) and a VLAN for RPVST+ operation. There can be only one VLAN per MST instance if the bridge is configured to run in RPVST+ mode.

The VLAN must have already been created. Spanning tree is enabled on each configured VLAN, and one instance of spanning-tree runs on each configured VLAN.

Use the `no` form of the command to disable this functionality.

Command Syntax `bridge <1-32> vlan <2-4094> no bridge <1-32> vlan <2-4094>`

Parameters

`<1-32>`	Bridge identifier.
`<2-4094>`	VLAN identifier.

Command Mode

RPVST+ configure mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Examples

```
#configure terminal
(config)#spanning-tree rpvst+ configuration
(config-rpvst+)#bridge 1 vlan 2
(config-rpvst+)#no bridge 1 vlan 2
```

bridge vlan priority

This command sets the priority value for the spanning-tree on the bridge. The lower the priority of the VLAN on a bridge, the better the chances of the bridge becoming a root bridge, or a designated bridge for the VLAN.

Use the `no` form of this command to set the priority to its default (32,768).

Command Syntax `bridge <1-32> vlan <2-4094> priority <0-61440> no bridge <1-32> vlan <2-4094> priority`

Parameters

`<1-32>`	Bridge identifier.
`<2-4094>`	VLAN identifier.
`<0-61440>`	Bridge priority for the common instance. Set the priority in increments of 4096. A lower priority indicates greater likelihood of becoming root.

Default

By default, priority for each VLAN is 32,768

Command Mode

Configure mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Examples

```
#configure terminal
(config)#bridge 1 vlan 2 priority 80
(config)#no bridge 1 vlan 10 priority
```

bridge-group vlan

Use this command to assign a Rapid Per-VLAN Spanning Tree (RPVST+) instance to a port.

RPVST+ uses port priority as a tiebreaker to determine which port should forward frames for a particular LAN, or which port should be the root port for a VLAN. A lower value implies a better priority. In the case of the same priority, the interface index serves as the tiebreaker, with a lower-numbered interface being preferred over others.

Use the `no` parameter with this command to remove an RPVST+ instance from this port.

Command Syntax `bridge-group <1-32> vlan <2-4094> bridge-group <1-32> vlan <2-4094> path-cost <1-200000000> bridge-group <1-32> vlan <2-4094> priority <0-240> no bridge-group <1-32> vlan <2-4094> no bridge-group <1-32> vlan <2-4094> path-cost no bridge-group <1-32> vlan <2-4094> priority`

Parameters

`<1-32>`	Bridge group identifier.
`<2-4094>`	VLAN identifier.
`<1-200000000>`	Cost of a path associated with the interface.
`<0-240>`	Port priority. A lower priority indicates greater likelihood of the interface becoming a root. Set the priority only in increments of 16.

Command Mode

Interface mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#bridge-group 1 vlan 10

(config)#interface eth1
(config-if)#bridge-group 1 vlan 10 path-cost 1000
```

```
(config-if)#no bridge-group 1 vlan 10 path-cost

(config)#interface eth1
(config-if)#bridge-group 1 vlan 10 priority 240

(config-if)#no bridge-group 1 vlan 10 priority
```

bridge protocol rpvst+

Use this command to enable Rapid Per-VLAN Spanning Tree on a bridge.

Command Syntax `bridge <1-32> protocol rpvst+`

Parameter

`<1-32>`	Bridge identifier.

Command Mode

Configure mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#configure terminal
(config)#bridge 1 protocol rpvst+
```

bridge rapid-pervlan-spanning-tree

Use this command to enable RPVST+ functionality on a bridge.

Use the `no` form of this command to disable RPVST+ functionality on a bridge.

Command Syntax:

```
bridge <1-32> rapid-pervlan-spanning-tree enable
no bridge <1-32> rapid-pervlan-spanning-tree enable (bridge-forward|)
```

Parameters

`<1-32>` Bridge identifier. `enable` Enable the spanning tree protocol. `bridge-forward` Put all ports of the specified bridge into forwarding state.

Default

When the `bridge-forward` option is used with the `no` parameter, the default behavior is to put all bridge ports in the blocking state.

Command Mode

Configure mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Examples

```
#configure terminal
(config)#bridge 1 rapid-pervlan-spanning-tree enable

(config)#no bridge 1 rapid-pervlan-spanning-tree enable bridge-forward
```

show spanning-tree rpvst+

Use this command to display RPVST information.

Command Syntax `show spanning-tree rpvst+ show spanning-tree rpvst+ config show spanning-tree rpvst+ detail show spanning-tree rpvst+ detail interface IFNAME show spanning-tree rpvst+ interface IFNAME show spanning-tree rpvst+ vlan <1-4094>`

`show spanning-tree rpvst+ vlan <1-4094> interface IFNAME`

Parameters

`config`	Display configuration information.
`detail`	Display detailed information.
`IFNAME`	Display interface information.

<1-4094>	Display VLAN information

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

The following displays output of this command without any parameters.

```
#show spanning-tree rpvst+
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 8001525400b092de
% 1: Bridge Id 8001525400b092de
% 1: last topology change Wed Mar 28 02:31:50 2018
% 1: 1 topology change(s)  - last topology change Wed Mar 28 02:31:50 2018

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State Forwarding
%    eth1: Designated External Path Cost 0 -Internal Path Cost 0
%    eth1: Configured Path Cost 200000  - Add type Explicit ref count 2
%    eth1: Designated Port Id 0x8003 - Priority 128  -
```

```
%   eth1: Root 8001525400b092de
%   eth1: Designated Bridge 8001525400b092de
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 3 - topo change timer 0
%   eth1: forward-transitions 1
%   eth1: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
%    eth1: Configured Link Type point-to-point - Current point-to-point
%   eth1: No auto-edge configured - Current port Auto Edge off
%
%
%   Instance        VLAN
%   0:              1, 4-10
%   1:                2
%   2:              3
```

The following displays output of this command with the `config` parameter.

```
#show spanning-tree rpvst+ config
%
%  RPVST Configuration Information for bridge 1 :
%-------------------------------------------------------
%  Format Id      : 0
%  Name           : Default
%  Revision Level : 0
%  Digest         : 0xB41829F9030A054FB74EF7A8587FF58D
%-------------------------------------------------------

#show spanning-tree rpvst+ detail
% 1: Bridge up - Spanning Tree Enabled  - topology change detected
% 1: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Transmit Hold Count 6
% 1: Root Id 8001525400b092de
% 1: Bridge Id 8001525400b092de
% 1: last topology change Wed Mar 28 02:31:50 2018
% 1: 1 topology change(s)  - last topology change Wed Mar 28 02:31:50 2018

% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated -
State Forwarding
%   eth1: Designated External Path Cost 0 -Internal Path Cost 0
%   eth1: Configured Path Cost 200000  - Add type Explicit ref count 2
%   eth1: Designated Port Id 0x8003 - Priority 128  -
```

```
%   eth1: Root 8001525400b092de
%   eth1: Designated Bridge 8001525400b092de
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change timer 0
%   eth1: forward-transitions 1
%   eth1: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
%   eth1: No portfast configured - Current  portfast off
%   eth1: bpdu-guard  default  - Current bpdu-guard off
%   eth1: bpdu-filter default  - Current bpdu-filter off
%   eth1: no root guard configured     - Current root guard off
%   eth1: Configured Link Type point-to-point - Current point-to-point
%   eth1: No auto-edge configured - Current port Auto Edge off %

% Instance  1:  Vlans: 2
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated -
State Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 200000
%   eth1: Configured External Path cost 200000
%   eth1: Configured Internal Priority 128
%   eth1: Configured External Priority 128
%   eth1: Designated Root 8002525400b092de
%   eth1: Designated Bridge 8002525400b092de
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1

#show spanning-tree rpvst+ vlan 2
% vlan 2 Instance 1 configured
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Root Id 8002525400b092de
% 1: Bridge Id 8002525400b092de
%   eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated -
State Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 200000
%   eth1: Configured External Path cost 200000
%   eth1: Configured Internal Priority 128
%   eth1: Configured External Priority 128
%   eth1: Designated Root 8002525400b092de
%   eth1: Designated Bridge 8002525400b092de
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
%

%
#show spanning-tree rpvst+ vlan 2 interface eth1
```

```
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Root Id 8002525400b092de
% 1: Bridge Id 8002525400b092de
%    eth1: Port Number 3 - Ifindex 3 - Port Id 0x8003 - Role Designated - State
Forwarding
%   eth1: Designated Internal Path Cost 0  - Designated Port Id 0x8003
%   eth1: Configured Internal Path Cost 200000
%   eth1: Configured External Path cost 200000
%   eth1: Configured Internal Priority 128 %
eth1: Configured External Priority 128 %
eth1: Designated Root 8002525400b092de
%   eth1: Designated Bridge 8002525400b092de
%   eth1: Message Age 0 - Max Age 20
%   eth1: Hello Time 2 - Forward Delay 15
%   eth1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 %
```

spanning-tree rpvst+ configuration

Use this command to enter RPVST+ configuration mode after creating a bridge and adding a VLAN to that bridge.

Internally, an RSTP Instance is created for each configured VLAN.

Command Syntax `spanning-tree rpvst+ configuration`

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#configure terminal
(config)#spanning-tree rpvst+ configuration
(config-rpvst+)#
```

spanning-tree vlan restricted-role

Use this command to restrict the role of the interface.

Use the `no` form of this command to not restrict the role of the interface.

Command Syntax `spanning-tree vlan <2-4094> restricted-role no spanning-tree vlan <2-4094> restricted-role`

Parameters

`<2-4094>` VLAN identifier.

Default

The default is to not restrict the role of the interface

Command Mode

Interface mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#configure terminal
(config)#interface eth0
                        (config-if)#spanning-tree vlan 10 restricted-role
```

spanning-tree vlan restricted-tcn

Use this command to restrict propagating topology change notifications (TCNs) from the interface.

Use the `no` form of this command to not restrict propagating TCNs from the interface.

Command Syntax `spanning-tree vlan <2-4094> restricted-tcn no spanning-tree vlan <2-4094> restricted_tcn`

Parameters

`<2-4094>` VLAN identifier.

Default

The default is to not restrict propagating TCNs

Command Mode

Interface mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#spanning-tree vlan 10 restricted-tcn
(config-if)#no spanning-tree vlan 10 restricted_tcn
```

CHAPTER 5 Link Aggregation Commands

This chapter describes the link aggregation commands.

- channel-group mode
- clear lacp
- debug lacp
- interface po
- interface sa
- lacp destination-mac
- lacp discard wrong conversation
- lacp port-priority
- lacp system-priority
- lacp timeout
- port-channel load-balance
- port-channel min-bandwidth
- port-channel min-links
- show debugging lacp
- show etherchannel
- show lacp sys-id
- show lacp-counter
- show port etherchannel
- show static-channel-group
- show static-channel load-balance
- snmp restart lacp
- static-channel-group

channel-group mode

Use this command to add an interface to an existing link aggregation group.

After you execute this command, the interface loses its properties and takes the properties of the aggregated interface.

Use the `no` parameter with this command to remove an interface from a dynamic link aggregation group. When you remove an interface from a LAG, the interface acquires the default interface properties.

Command Syntax `channel-group <1-65535> mode (active|passive)`

`channel-group <1-16383> mode (active|passive)`

`no channel-group`

Parameters

`<1-65535>` Specify a channel group number (without DRNI).

<1-16383>	Specify a channel group number (with DRNI).
mode	Specify a channel mode.
active	Enable LACP negotiation.
passive	Disable LACP negotiation.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#switchport
(config-if)#channel-group 1 mode active
(config-if)#exit

#sh run in po1
!
interface po1
switchport
 port-channel load-balance src-dst-mac
```

The is an example of `no channel-group`:

```
#configure terminal
(config)#interface xe1
(config-if)#switchport
(config-if)#no channel-group
(config-if)#exit

#sh run in xe1
!
interface xe1
!
#sh run in po1
!
interface po1  switchport  port-channel load-balance src-dst-mac !
```

clear lacp

Use this command to clear the counters of all LACP aggregators or a given LACP aggregator.

Command Syntax `clear lacp <1-65535> counters clear lacp counters`

Parameters

`<1-65535>`	Clears a channel-group number.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear lacp 2 counters
```

debug lacp

Use this command to enable LACP debugging.

Use the `no` parameter with this command to disable debugging.

Command Syntax `debug lacp (event|cli|timer|packet|sync|ha|all|rx|tx) no debug lacp (event|cli|timer|packet|sync|ha|allrx|tx) undebug all`

Parameters

`all`	Enables all LACP debugging.
`cli`	Echo commands to console.
`event`	Sets the debug options for LACP events.
`ha`	Echo High availability events to console.
`packet`	Sets the debug option for LACP packets.
`sync`	Echo synchronization to console.
`timer`	Echo timer expiry to console.
`rx`	Echo receiving of lacpdus to console.
`tx`	Echo transmission of lacpdus to console.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#debug lacp all
```

interface po

Use this command to create a dummy dynamic link aggregate interface (by default an L3 LAG interface).

Use the `no` form of this command to remove a dynamic link aggregate group and also it remove the properties of the po from all member ports.

Note:Switchport/routed mode needs to be set for the PO before adding member ports to it.

Command Syntax `interface po<1-16383> no interface po<1-16383>`

Parameters

`<1-16383>`	LACP port priority.

Default

By default, interface po is L3 LAG interface

Command Mode

Configuration mode

Applicability

This command was introduced before SWMRE version 1.3.4.

Example

```
#configure terminal
(config)#interface po1
(config-if)#switchport
(config-if)#exit
```

interface sa

Use this command to create a dummy static link aggregate interface (by default an L3 LAG interface) and to add an interface to an existing static link aggregation group.

Use the `no` form of this command to remove a static link aggregate group and also remove the properties of the po from all member ports.

Command Syntax

`interface sa<1-12>`

`no interface sa<1-12>`

Parameters

`<1-12>`	Channel group number.

Default

By default, interface sa is L3 LAG interface

Command Mode

Configuration mode

Applicability

This command was introduced in SWMRE version 1.3.4.

Example

```
#configure terminal
(config)#interface sa1
(config-if)#switchport
(config-if)#exit
```

lacp destination-mac

Use this command to set the address type to use for sending LACPDUs (Link Aggregation Control Protocol Data Units).

Note:The interface must be an aggregation port.

Use the `no` form of this command to set the address type to its default (multicast group address).

Command Syntax

```
lacp destination-mac (customer-bridge-group-address | multicast-group-address |
  non-tmpr-group-address)
no lacp destination-mac
```

Parameters `customer-bridge-group-address`

Customer bridge group address

`multicast-group-address`

Multicast group address (default)

`non-TPMR-group-address`

Non-Two-Port Media Access Control Relay (TPMR) group address

Default

By default, lacp destination-mac is multicast-group-address

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#config terminal
(config)#interface eth1
(config-if)#lacp destination-mac customer-bridge-group-address
```

lacp discard wrong conversation

Use this command to enable or disable discarding frames with an incorrect port conversation identifier.

Note: The interface must be a dynamic port-channel.

Command Syntax `lacp discard wrong conversation (disable|enable)`

Parameters

`disable`	Do not discard frames with an incorrect port conversation identifier
`enable`	Discard frames with an incorrect port conversation identifier

Default

By default, lacp discard wrong conversation is disabled

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#config terminal
(config)#interface po1
(config-if)#lacp discard wrong conversation enable
```

lacp port-priority

Use this command to set the priority of a channel. Channels are selected for aggregation based on their priority with the higher priority (numerically lower) channels selected first.

Use the `no` parameter with this command to set the priority of port to the default value (32768).

Command Syntax `lacp port-priority <1-65535>`

`no lacp port-priority`

Parameters

`<1-65535>`	Specify the LACP port priority.

Default

By default, lacp port priority is 32768

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#lacp port-priority 34
```

lacp system-priority

Use this command to set the LACP system priority. This priority determines the system responsible for resolving conflicts in the choice of aggregation groups.

Note: A lower numerical value has a higher priority.

Use the `no` parameter with this command to set the system priority to its default value (32768).

Command Syntax `lacp system-priority <1-65535> no lacp system-priority`

Parameters

`<1-65535>`	System priority.

Default

By default, system priority is 32768

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#lacp system-priority 6700
```

lacp timeout

Use this command to set either a short or long timeout value on a port. The timeout value is the number of seconds before invalidating a received LACP data unit (DU).

Command Syntax `lacp timeout (short|long)`

Parameters

`short`	LACP short timeout. 3 seconds.
`long`	LACP long timeout. 90 seconds.

Default

By default, lacp timeout is long

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following sets the LACP short timeout on a port.

```
#configure terminal
(config)#interface eth0
(config-if)#lacp timeout short
```

port-channel load-balance

Use this command to configure LACP port-channel load-balancing and set port-selection criteria (PSC) for an interface.

Use the `no` option with this command to remove the load-balancing configuration and unset PSC.

Command Syntax

```
port-channel load-balance (dst-mac|src-mac|src-dst-mac|dst-ip|src-ip|src-dst-ip|dst-port|src-port|src-dst-port|rtag7)
no port-channel load-balance
```

Parameters

`dst-ip`	Destination IP address-based load balancing.
`dst-mac`	Destination MAC address-based load balancing.
`dst-port`	Destination TCP/UDP address-based load balancing.
`src-dst-ip`	Source and Destination IP address-based load balancing.
`src-dst-mac`	Source and Destination MAC address-based load balancing.
`src-dst-port`	Source and Destination TCP/UDP address-based load balancing.
`src-ip`	Source IP address-based load balancing.
`src-mac`	Source MAC address-based load balancing.
`src-port`	Source port address-based load balancing.
`rtag7`	Hashing based on packet type. IP - IP/Layer4 header, L2 - Layer2 header, TRILL - TRILL packet.

Default

By default, load balance is src-dst-port

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface po1
(config-if)#port-channel load-balance src-dst-mac
```

port-channel min-bandwidth

Use this command to set the minimum active bandwidth of aggregated links.

Note: The port-channel min-links feature and this feature are mutually exclusive. Both configurations cannot exist at the same time.

Use the `no` form of this command to set the bandwidth to the collective bandwidth of the LACP member ports.

Command Syntax `port-channel min-bandwidth BANDWIDTH` `no port-channel min-bandwidth`

Parameters

`BANDWIDTH` <1-999>k for 1 to 999 kilobits/s

<1-999>m for 1 to 999 megabits/s

<1-1000>g for 1 to 1000 gigabits/s

Default

The default is the collective bandwidth of the LACP member ports.

Command Mode

Interface mode

Applicability

This command was introduced in SWMRE version 1.3.5.

Example

```
#configure terminal
(config)#interface po1
(config-if)#port-channel min-bandwidth 999m
```

port-channel min-links

Use this command to set the minimum number of aggregated links that need to be up in the LAG interface.

When a the minimum number of links are configured for a LAG, if the active links for that interface become less than the configured value, then the whole LAG is brought down. When the number of active links become the same or more than the configured value, then the whole LAG is restored.

Note: The port-channel min-bandwidth feature and this feature are mutually exclusive. Both configurations cannot exist at the same time.

Use the `no` form of this command to remove the minimum number of aggregated links that need to be up in the LAG interface.

Note: The minimum number of aggregated links should be same across both ends of an aggregation interface. If not configured, then on one of the nodes the LAG port will be treated as up and on the other as down and traffic will be discarded.

Note: When a LAG port is moved to the down state because it does not have the minimum number of required links up and running, then the traffic on the remaining interfaces in the LAG arecounted as port-block discards.

Command Syntax `port-channel min-links <2-32> no port-channel min-links`

Parameters

`<2-32>`	Minimum number of links

Default

By default, port channel min-link is disabled.

Command Mode

Interface mode

Applicability

This command was introduced in SWMRE version 1.3.4.

Example

```
#configure terminal
(config)#interface po1
(config-if)#port-channel min-links 10
(config-if)#exit
```

show debugging lacp

Use this command to display the status of the debugging of the LACP system.

Command Syntax `show debugging lacp`

Parameters

None

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show debugging lacp

LACP debugging status:
LACP timer debugging is on
```

show etherchannel

Use this command to display information about link aggregation groups.

Command Syntax `show etherchannel show etherchannel <1-65535>` With MLAG:

`show etherchannel (<1-16383>|) detail show etherchannel (<1-16383>|) load-balance show etherchannel (<1-16383>|) summary` Without MLAG:

`show etherchannel (<1-65535>|) detail show etherchannel (<1-65535>|) load-balance show etherchannel (<1-65535>|) summary`

Parameters

`<1-65535>`	Specify channel-group number.
`<1-16383>`	Specify channel-group number.
`detail`	Specify detailed etherchannel information.
`load-balance`	Specify load balancing.
`summary`	Specify Etherchannel summary information.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show etherchannel summary
% Aggregator po1 185
% Aggregator Type: Layer3
% Admin Key: 0001 - Oper Key 0001
%   Link: eth3 (5) sync: 0
-------------------------------------
% Aggregator po4 186
% Admin Key: 0004 - Oper Key 0004
%   Link: eth2 (4) sync: 0
-------------------------------------
% Aggregator po5 187
% Admin Key: 0005 - Oper Key 0005
%   Link: eth1 (3) sync: 0
```

```
#show etherchannel detail
% Aggregator po1 185
% Aggregator Type: Layer3
%  Mac address: 08:00:27:36:f5:7d
%  Admin Key: 0001 - Oper Key 0001
%  Actor LAG ID- 0x8000,08-00-27-fa-4b-0e,0x0001
%  Receive link count: 0 - Transmit link count: 0
%  Individual: 0 - Ready: 0
%  Partner LAG ID- 0x0000,00-00-00-00-00-00,0x0000
%   Link: eth3 (5) sync: 0
%  Collector max delay: 5
------------------------------------------------
% Aggregator po4 186
%  Mac address: 08:00:27:76:0c:57
%  Admin Key: 0004 - Oper Key 0004
%  Actor LAG ID- 0x8000,08-00-27-fa-4b-0e,0x0004
%  Receive link count: 0 - Transmit link count: 0
%  Individual: 0 - Ready: 1
%  Partner LAG ID- 0x0000,00-00-00-00-00-00,0x0000
%   Link: eth2 (4) sync: 0
%  Collector max delay: 5
------------------------------------------------
% Aggregator po5 187
%  Mac address: 08:00:27:2f:d5:ae
%  Admin Key: 0005 - Oper Key 0005
%  Actor LAG ID- 0x8000,08-00-27-fa-4b-0e,0x0005
%  Receive link count: 0 - Transmit link count: 0
%  Individual: 0 - Ready: 0
%  Partner LAG ID- 0x0000,00-00-00-00-00-00,0x0000
%   Link: eth1 (3) sync: 0
%  Collector max delay: 5
```

Table 5-78 explains the show command output fields.

Table 5-78: show etherchannel detail output

Field	Description
Aggregator	Link aggregators name and ID number.
Mac address	Unique MAC address for link identification.
Admin Key	LACP administrative key – automatically configured value on each port configured to use LACP.
Oper Key	LACP operator key on Partner – automatically configured value on each port configured to use LACP.

Actor LAG ID	LAG ID consisting of MAC address plus aggregator ID number for this Actor.
Receive link count	The number of link received from the peer LAG.
Transmit link count	The number of links contained transmitted to the peer LAG.
Individual	The individual physical network interfaces or ports contained in the LAG.
Ready	The number of links in the active state on this Actor.
Partner LAG ID	Partner LAG ID consisting of MAC address plus aggregator ID number.

Table 5-78: show etherchannel detail output (Continued)

Description
Interface and ID number of the link.
MAC address synchronization enables a MC-LAG Partner to forward Layer 3 packets arriving on this interfaces with either its own MAC address or its Partner's.
Maximum period of wait time between sending of two subsequent Ethernet frames on a link.

show lacp sys-id

Use this command to display the LACP system identifier and priority.

Command Syntax `show lacp sys-id`

Parameters `sys-id` Display LACP system ID and priority

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show lacp sys-id
% System 8000,00-0e-0c-83-37-27
```

show lacp-counter

Use this command to display the packet traffic on all ports of all present LACP aggregators, or a given LACP aggregator.

Command Syntax `show lacp-counte show lacp-counter <1-65535>`

Parameters

`<1-65535>`	Channel-group number

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show lacp-counter 555

Port      LACPDUs          Marker          Pckt err
        Sent    Recv    Sent    Recv    Sent    Recv
```

show port etherchannel

Use this command to display details about a PO and its members' interfaces or to display details of a single member interface of a PO.

Command Syntax `show port etherchannel IFNAME`

Parameters

`IFNAME`	Interface name

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show port etherchannel ce29/1
LAG ID                        : 0x8000,cc-37-ab-a0-89-ca,0x0002
Partner oper LAG ID           : 0x8000,a8-2b-b5-38-1e-48,0x0004
Aggregator ID                 : 100002
```

```
  LACP link info             : ce29/1 - 10001
Periodic Transmission
  machine state              : Slow periodic
  Receive machine state      : Current
  Mux machine state          : Collecting/Distributing
  Actor Info :
  ===========
  Actor Port priority        : 0x8000 (32768)
  Admin key                  : 0x0002 (2) Oper key: 0x0002 (2)
  Physical admin key         : (2)
  Actor Oper state           : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
  Actor Admin state          : ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
  Partner Info:
  ============
  Partner oper port          : 10009
  Partner link info          : admin port 0
  Partner admin LAG ID       : 0x0000-00:00:00:00:0000
  Partner system priority    : admin:0x0000 - oper:0x8000
  Partner port priority      : admin:0x0000 - oper:0x8000
  Partner oper state         : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
  Partner admin state        : ACT:0 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0


#show port etherchannel po2
LAG ID                       : 0x8000,cc-37-ab-a0-89-ca,0x0002
Partner oper LAG ID          : 0x8000,a8-2b-b5-38-1e-48,0x0004
Aggregator ID                : 100002
  LACP link info             : ce29/1 - 10001
Periodic Transmission
  machine state              : Slow periodic
  Receive machine state      : Current
  Mux machine state          : Collecting/Distributing
  Actor Info :
  ===========
  Actor Port priority        : 0x8000 (32768)
  Admin key                  : 0x0002 (2) Oper key: 0x0002 (2)
  Physical admin key         : (2)
  Actor Oper state           : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
  Actor Admin state          : ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
  Partner Info:
  ============
  Partner oper port          : 10009
  Partner link info          : admin port 0
  Partner admin LAG ID       : 0x0000-00:00:00:00:0000
  Partner system priority    : admin:0x0000 - oper:0x8000
  Partner port priority      : admin:0x0000 - oper:0x8000
  Partner oper state         : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
  Partner admin state        : ACT:0 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
```

```
  LACP link info              : ce30/1 - 10005
Periodic Transmission
  machine state               : Slow periodic
  Receive machine state       : Current
  Mux machine state           : Collecting/Distributing
  Actor Info :
  ===========
  Actor Port priority         : 0x8000 (32768)
  Admin key                   : 0x0002 (2) Oper key: 0x0002 (2)
  Physical admin key          : (2)
  Actor Oper state            : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
  Actor Admin state           : ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
  Partner Info:
  ============
  Partner oper port           : 10013
  Partner link info           : admin port 0
  Partner admin LAG ID        : 0x0000-00:00:00:00:0000
  Partner system priority     : admin:0x0000 - oper:0x8000
  Partner port priority       : admin:0x0000 - oper:0x8000
  Partner oper state          : ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
  Partner admin state         : ACT:0 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
```

Note: Most of the output of this command is duplicated in the show etherchannel command (see also the 802.3ad specificiation). The output of the `show port etherchannel` command is primarily a list of state machine values. An explanation of the state machine bits follows. See Figure 5-71.

Table 5-79 explains the show command output fields.

Table 5-79: show port etherchannel detailed output

Entry	Description
Actor/Partner state	The Actor's and Partner's state variables, encoded as individual bits within a single octet.
ACT	LACP_Activity is encoded in bit 0. Active LACP is encoded as a 1; Passive LACP as a 0.

Table 5-79: show port etherchannel detailed output (Continued)

Entry	Description
TIM	LACP_Timeout is encoded in bit 1. Short Timeout is encoded as a 1; Long Timeout as a 0.
AGG	Aggregability is encoded in bit 2. Aggregatable is encoded as a 1; Individual is encoded as a 0.
SYN	Synchronization is encoded in bit 3. In_Sync is encoded as a 1; Out_Of_Sync is encoded as a 0.

COL	Collecting is encoded in bit 4. True is encoded as a 1; False is encoded as a 0.
DIS	Distributing is encoded in bit 5. True is encoded as a 1; False is encoded as a 0.
DEF	Defaulted is encoded in bit 6.
EXP	Defaulted is encoded in bit 7.

Bits 7 and 8 are reserved; these are ignored on receipt and transmitted as zero. However, the received value of these bits is recorded on receipt to accurately reflect the actor's view of the partner's state in outgoing PDUs.

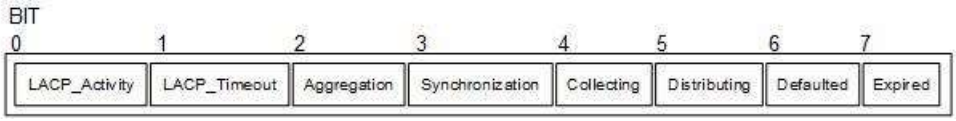


Figure 5-71: Diagram of state machine octet

show static-channel-group

Use this command to display the types of load-balancing port selection criteria (PSC) used on configured static aggregators.

Command Syntax `show static-channel-group (<1-12>|)`

Parameters

`<1-12>`	Specify channel-group number.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following is an example of the output of this command:

```
#show  static-channel-group 1 %
Static Aggregator: sa1
% Member:    eth1
```

show static-channel load-balance

Use this command to display information about static channel groups.

Command Syntax `show static-channel (<1-12>|) load-balance` **Parameters**

`<1-12>`	Specify static-channel-group number.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following is an example of the output of this command:

```
#show static-channel load-balance
% Static Aggregator: sa5
Source and Destination Mac address
-----------------------------------------
% Static Aggregator: sa3
Source and Destination Mac address
-----------------------------------------
```

```
% Static Aggregator: sa1
Source and Destination Mac address

#show static-channel 1 load-balance
% Static Aggregator: sa1
Source and Destination Mac address
```

snmp restart lacp

Use this command to restart SNMP in LACP.

Command Syntax `snmp restart lacp`

Parameters

None

Default

By default, snmp restart lacp is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#snmp restart lacp
```

static-channel-group

Use this command to create a static link aggregation group or to add an interface to an existing link aggregation group.

Use the `no` form of this command to remove an interface from a static link aggregation group without removing the static link aggregation group itself.

Command Syntax `static-channel-group <1-12> no static-channel-group`

Parameter

`<1-12>`	Channel group number.

Default

By default, static channel group is disabled

Command Mode

Interface mode

Applicability

This command was introduced in SWMRE version 1.3.4.

Example

```
#configure terminal
(config)#interface xe1
(config-if)#switchport
(config-if)#static-channel-group 1
(config-if)#exit

#sh run in sa1
! interface
sa1
switchport
 port-channel load-balance src-dst-mac
```

This is an example of `no static-channel-group`:

```
#configure terminal
(config)#interface xe1
(config-if)#switchport
(config-if)#no static-channel-group
(config-if)#exit

#sh run in xe1
!
interface xe1
!
```

```
#sh run in sa1
! interface
sa1
switchport
port-channel
load-balance
src-dst-mac !
```

CHAPTER 6 Multi-Chassis Link Aggregation Commands

This chapter describes the Multi-Chassis Link Aggregation commands.

Multi-Chassis Link Aggregation is also called MC-LAG, MLAG, or Distributed Resilient Network Interconnect (DRNI). In this document, it is called MC-LAG.

- domain-address
- debug mcec
- domain hello timeout
- domain priority
- domain system number
- intra-domain-link
- mlag
- mcec domain configuration
- mode
- show mlag detail
- show mlag summary
- show mcec statistics
- switchover type

domain-address

Use this command to configure domain address, which helps to identify the mcec domain.

Use the `no` form of this command to remove the domain address.

Command Syntax `domain-address <domain-id> no domain-address`

Parameters `domain-id` domain address in HHHH.HHHH.HHHH format

Command Mode

MCEC mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#config terminal
(config)#mcec domain configuration (config-mcec-domain)#domain-address 1111.2222.3333
```

debug mcec

Use this command to view debugging logs for MLAG.

Use the `no` form of this command to remove debugging logs for MLAG.

Command Syntax `debug mcec (timer|event|hello|info|cli|mac-sync|all) no debug mcec (timer|event|hello|info|cli|mac-sync|all)`

Parameters

`all`	ALL
`cli`	CLI
`event`	Event
`hello`	Hello
`info`	Info
`mac-sync`	Mac Sync
`timer`	Timer

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#debug mcec all
#no debug mcec all
```

domain hello timeout

Use this command to specify the domain hello-timeout value.

Command Syntax `domain-hello-timeout (long|short)`

Parameters

`long`	Long Timeout
`short`	Short Timeout

Command Mode

MCEC mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#config terminal
(config)#mcec domain configuration
                                    (config-mcec-domain)#domain-hello-timeout long
```

domain priority

Use this command to specify the priority value associated with mcec domain.

Use the `no` form of this command to remove the priority value associated with mcec domain.

Command Syntax `domain-priority <1-65535> no domain-priority`

Parameters

`<1-65535>` Priority Value

Command Mode

MCEC mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#domain-priority 2
```

domain system number

Use this command to configure domain system number, which uniquely identifies domain system in mcec domain.

Use the `no` form of this command to configure domain system number.

Command Syntax `domain-systm-number <1-2> no domain-systm-number`

Parameters

`<1-2>`	Domain System Number

Command Mode

MLAC mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#config terminal
(config)#mcec domain configuration (config-mcec-domain)#domain-system-number 2
```

intra-domain-link

Use this command to map an interface as intra domain link that connects the domain system with its neighbor in a mcec domain.

Use the no form of this command to unmap the interface configured as intra domain link that connects the domain system with its neighbor in a mcec domain.

Command Syntax `intra-domain-link <IFNAME> no intra-domain-link`

Parameters

`IFNAME`	Interface name

Command Mode

MCEC mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#config terminal
(config)#mcec domain configuration (config-mcec-domain)#intra-domain-link eth2
```

mlag

Use this command to map a port-channel to mlag instance.

Note:The interface must be a dynamic port channel.

Note: All MLAG nodes must use the same MAC table size.

Use the `no` form of this command to un-map the port channel from mlag instance.

Command Syntax `mlag <1-256> no mlag`

Parameters

`<1-256>`	MC-LAG identifier

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#config terminal
```

```
(config)#interface po1
```

```
(config-if)#mlag 1
```

mcec domain configuration

Use this command to enter MCEC Domain configuration mode to configure mcec domain information.

Command Syntax `mcec domain configuration`

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#config terminal
(config)#mcec domain configuration
(config-mcec-domain)#
```

mode

Use this command to set the MC-LAG mode.

Use the no form of this command to turn off this feature.

Command Syntax `mode (active-active | active-standby)` `no mode (active-active | active-standby)`

Parameters

`active-active`	The interface is the active interface that carries the traffic
`active-standby`	The interface is ready to transition to the active-active state should a failure occur in the other node

Default `active-standby`

Command Mode

Interface mode

Applicability

This command was introduced in SWMRE version 1.3.5.

Examples

```
(config)#
(config)#interface mlag1
(config-if)#mode active-active

(config)#
(config)#interface mlag1
(config-if)#mode active-standby
```

show mlag detail

Use this command to display details about MC-LAG configuration and status.

Command Syntax `show mlag <1-256> detail`

Parameters

`<1-256>`	MLAG group number

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#sh mlag 1 detail

MLAG-1
Mapped Aggregator : po1
Admin Key : 32769
Oper Key: 16385
Physical properties Digest : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82

Neigh Admin Key: 16385
Neigh Physical Digest: dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
Info RCV State : Current
Info Periodic Time State : Standby Mlag
Sync: IN_SYNC
```

Table 6-80 Shows the output details.

Table 6-80: Show mlag output details

Entry	Description
Info RCV State	Details of the RCV.
Info Periodic Time State	A simple state space formulation of a general digital periodic time series is constructed.
Mlag Sync	MAC address synchronization enables a MC-LAG Partner to forward Layer 3 packets arriving on this interfaces with either its own MAC address or its Partner's.

Entry	Description
Mapped Aggregator	Map the output of the aggregator in the interface which is active transformation.
Admin Key	MLAG administrative key – automatically configured value on each port configured to use MLAG.
Oper Key	MLAG operator key on Partner – automatically configured value on each port configured to use MLAG.
Physical properties Digest	Physical properties of the digest.
Neigh Admin Key	Neigh administrative key – automatically configured value on each port configured to use MLAG.
Neigh Physical Digest	Neigh physical properties of the digest.

show mlag summary

Use this command to display MC-LAG configuration and status.

Command Syntax `show mlag domain <details|summary>`

Parameters

`details`	details
`summary`	summary

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show mlag domain summary
-----------------------------------
Domain Configuration
-----------------------------------
Domain System Number : 2
Domain Address: 1111.2222.3333
Domain Priority: 1000
Intra Domain Interface: xe49
Domain Adjacency: UP

-----------------------------------
MLAG Configuration
-----------------------------------

MLAG-1
Mapped Aggregator: po1
Physical properties Digest: dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
Total Bandwidth : 40g Mlag
 Sync : IN_SYNC


#sh mlag domain details
-----------------------------------
Domain Configuration
-----------------------------------

Domain System Number: 2
Domain Address: 1111.2222.3333
Domain Priority: 1000
Intra Domain Interface: xe49
```

```
Hello RCV State: Current
Hello Periodic Timer State: Fast Periodic
Domain Sync : IN_SYNC
Neigh Domain Sync : IN_SYNC
Domain Adjacency : UP

-------------------------------------
MLAG Configuration
-------------------------------------

MLAG-1
Mapped Aggregator: po1
Admin Key: 32769
Oper Key: 16385
Physical properties Digest: dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82

Neigh Admin Key: 16385
Neigh Physical Digest : dd 9c f 76 dd b6 5f 2f eb a1 d3 bb 8d 96 fc 82
Info RCV State : Current
Info Periodic Time State : Standby Mlag
Sync : IN_SYNC
```

Table 6-81 Shows the output details.

Table 6-81: Show mlag summary details

Entry	Description
Domain System Number	Number to identify the node in domain.
Domain Address	Domain address for the MLAG domain.
Domain Priority	Domain priority for the MLAG domain.
Intra Domain Interface	Intra domain interface between MLAG domains.
Domain Adjacency	Domain adjacency details and configuration.
Physical properties Digest	physical properties of the digest algorithm.
Total Bandwidth	Total bandwidth available on the interface.
Domain System Number	Number of the domain system.

Domain Address	Domain address for the MLAG domain.
Domain Priority	Domain priority for the MLAG domain.
Intra Domain Interface	Details of the intra domain in the interface.
Hello RCV State	State of the hello RCV in the interface.
Hello Periodic Timer State	State of the hello periodic timer in the interface.
Domain Sync	Detail of the domain configuration synchronization.
Mapped Aggregator	Map the output of the aggregator in the interface which is active transformation.
Admin Key	MLAG administrative key – automatically configured value on each port configured to use MLAG.

Table 6-81: Show mlag summary details

Entry	Description
Oper Key	MLAG operator key on Partner – automatically configured value on each port configured to use MLAG.
Physical properties Digest	Physical properties of the digest.
Neigh Admin Key	Neigh administrative key – automatically configured value on each port configured to use MLAG.
Neigh Physical Digest	Neigh physical properties of the digest.
Info RCV State	Details of the RCV.
Info Periodic Time State	A simple state space formulation of a general digital periodic time series is constructed.
Mlag Sync	MAC address synchronization enables a MC-LAG Partner to forward Layer 3 packets arriving on this interfaces with either its own MAC address or its Partner's.

show mcec statistics

Use this command to display all the statistics related to hello and info pdu's in mcec domain.

Command Syntax `show mcec statistics`

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Entry	Description
RX Hello PDUs	Total number of received hello PDUs.
TX Hello PDUs	Total number of transmitted hello PDUs.
RX Info PDUs	Total number of received Info PDUs.
TX Info PDUs	Total number of transmitted Info PDUs.
RX Mac Sync PDUs	Total number of received Mac Sync PDUs.

TX Mac Sync PDUs	Total number of transmitted Mac Sync PDUs.

Examples

```
#sh mcec statistics
Unknown MCCPDU received on the system : 0

-----------------------------------
IDP xe49
-----------------------------------
Valid RX Hello PDUs : 109
Valid TX Hello PDUs : 201
Valid RX Info PDUs: 23
Valid TX Info PDUs : 28
Valid RX Mac Sync PDUs : 5
Valid TX Mac Sync PDUs : 4

MLAG 1
Valid RX Info PDUs : 5
Valid TX Info PDUs : 7
```

Table 6-80 Shows the output details.

Table 6-82: Show mcec statistics details

switchover type

Use this command to set the MC-LAG switchover type.

Use the `no` form of this command to turn off switchover.

Command Syntax `switchover type revertive <1-255> switchover type non-revertive`

`no switchover type (revertive | non-revertive)`

Parameters

`revertive` If a failure happens that triggers a switchover, after failure recovery the initially-active node becomes active again

`<1-255>` Switch back to the initially-active node this many seconds after failure recovery `non-revertive`

Do not switch back to the initially-active node after failure recovery

Default `revertive` in 10

seconds

Command Mode

Interface mode

Applicability

This command was introduced in SWMRE version 1.3.5.

Examples

```
(config)#
(config)#interface mlag1
(config-if)#switchover type revertive 20
```

```
(config)#
(config)#interface mlag1
(config-if)#switchover type non-revertive
```

CHAPTER 7 Traffic Mirroring Commands

This chapter provides a description of syntax, and examples for Traffic Mirroring. It includes the following commands:

- monitor session
- monitor session shut
- source port
- source vlan
- destination port
- no shut
- shut
- filter
- description
- remote destination
- show monitor
- show monitor session
- show filter
- show monitor running configuration

monitor session

Use this command to create a local or remote monitor session. By default, a local monitor session is created.

A monitor session consists of:

- A single destination interface, referred to as a mirror-to port or a single remote destination
- One or more source interfaces (egress, ingress, or both)
- One or more VLAN sources in the ingress direction
- One or more filters that can be applied to filter the mirrored packets Use the `no` parameter to delete a monitor session.

Command Syntax `monitor session <1-18> ( | type ( local | remote )) no monitor session ( <1-18> | all )`

Parameters

`<1-18>`	Session number
`local`	Create a local session
`remote`	Create a remote source node session
`all`	All sessions

Default

By default, monitor session type is local and will not be active by default

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#monitor session 1
(config-monitor)#exit
(config)#monitor session 3 type remote
(config-monitor)#exit
(config)#no monitor session 1
```

monitor session shut

Use this command to deactivate one or all monitor sessions.

Use the `no` parameter to activate one or all monitor sessions.

Command Syntax `monitor session (<1-18> | all) shut no monitor session (<1-18> | all) shut`

Parameters

<1-18>	Session number
all	All sessions

Default

Monitor session will not be active by default

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#monitor session 3 shut

                    (config)#no monitor session 3 shut
```

source port

Use this command to configure a source port per monitor session in either ingress or egress or both directions. Source port can be physical interface or a trunk port. Use the `no` parameter to remove the source port.

Command Syntax `source interface IFNAME ( rx | tx | both | ) no source interface IFNAME ( rx | tx | both | )`

Parameters

IFNAME	Interface name
rx	Ingress direction
tx	Egress direction
both	Both directions

Default

Source port will be mirrored for both directions if the direction is not specified

Command Mode

Monitor configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#monitor session 1
(config-monitor)#source interface xe1 both
(config-monitor)#no source interface xe1 tx
```

source vlan

Use this command to configure one or more VLANs as source per monitor session. A VLAN as source will be mirrored only in the ingress direction. Up to 32 VLANs can be configured as source per monitor session.

Use the `no` parameter to remove vlan source from monitor session.

Command Syntax `source vlan`

`VLAN_RANGE no source vlan`

`VLAN_RANGE`

Parameters

`VLAN_RANGE`	VLAN identifier or VLAN identifier range

Default

A trunk port is a member of all VLANs by default.

Command Mode

Monitor configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#monitor session 1
(config-monitor)#source vlan 2
(config-monitor)#source vlan 4-10
(config-monitor)#no source vlan 2-5,10
```

destination port

Use this command to configure a mirror-to port per local monitor session. A destination port can be a physical port or a trunk port.

Use the `no` parameter to remove the destination port from a local monitor session.

Command Syntax `destination`

`interface IFNAME no destination`

`interface IFNAME`

Parameters

`IFNAME`	Interface name

Default

The Firewall device uses the outgoing interface by default.

Command Mode

Monitor configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface xe3
(config-if)#switchport
(config-if)#exit
(config)#monitor session 1 (config-
monitor)#destination interface xe3 (config-
monitor)#no destination interface xe3
```

no shut

Use this command to activate a monitor session

Command Syntax `no shut`

Parameters

None

Default

Monitor session will not be active by default.

Command Mode

Monitor configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#monitor session 3
(config-monitor)#no shut
```

shut

Use this command to de-activate a monitor session.

Command Syntax `shut`

Parameters

None

Default

Monitored session is not active by default.

Command Mode

Monitor configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#monitor session 3
(config-monitor)#shut
```

filter

Use this command to add filters to the monitor session. Filters can be applied only in case of ingress mirroring.

Use the `no` parameter to remove the filter from monitor session.

Command Syntax

```
filter {vlan <2-4094> | cos <0-7> | dest-mac (host XXXX.XXXX.XXXX |
  XXXX.XXXX.XXXX XXXX.XXXX.XXXX) | src-mac (host XXXX.XXXX.XXXX | XXXX.XXXX.XXXX
  XXXX.XXXX.XXXX) | frame-type (ETHTYPE | arp (req | resp|) (sender-ip A.B.C.D|)
  (target-ip A.B.C.D|)
  | ipv4 (src-ip (A.B.C.D | A.B.C.D/M)|) (dest-ip (A.B.C.D | A.B.C.D/M)|) |
  ipv6 (src-ip X:X::X:X/M |) (dest-ip X:X::X:X/M |))} no filter {vlan <2-
4094> | cos <0-7> | dest-mac (host XXXX.XXXX.XXXX |
  XXXX.XXXX.XXXX XXXX.XXXX.XXXX) | src-mac (host XXXX.XXXX.XXXX | XXXX.XXXX.XXXX
  XXXX.XXXX.XXXX) | frame-type (ETHTYPE | arp (req | resp|) (sender-ip A.B.C.D|)
  (target-ip A.B.C.D|) | ipv4 (src-ip (A.B.C.D | A.B.C.D/M)|) (dest-ip (A.B.C.D |
  A.B.C.D/M)|) | ipv6 (src-ip X:X::X:X/M |) (dest-ip X:X::X:X/M |))}
```

Parameters

`<2-4094>`	VLAN identifier
`<0-7>`	COS number
`XXXX.XXXX.XXXX`	MAC address
`ETHTYPE`	Ethertype
`arp`	ARP frames
`req`	Request frames `resp` Response frames
`A.B.C.D`	Single IP address
`A.B.C.D/M`	IP addresses with mask
`X:X::X:X/M`	IPv6 addresses with mask

Default

No default value is specified.

Command Mode

Monitor configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#monitor session 3
(config-monitor)#filter dest-mac host 0000.0001.2421 frame-type ipv4
(config-monitor)#filter cos 3 frame-type arp req sender-ip 2.2.2.1
(config-monitor)#no filter dest-mac host 0000.0001.2421 frame-type ipv4
(config-monitor)#no filter cos 3 frame-type arp req sender-ip 2.2.2.1
```

description

Use this command to add a description to the monitor session.

Use the `no` parameter to delete a description of the monitor session.

Command Syntax `description LINE no description`

Parameters

`LINE`	Enter the description string

Default

No default value is specified.

Command Mode

Monitor configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#monitor session 3
                                    (config-monitor)#description "port mirror rx"
(config-monitor)#no description
```

remote destination

Use this command to configure a destination VLAN and the reflector port for the remote monitor session.

Use the `no` parameter to remove a destination from a remote monitor session.

Command Syntax `destination remote vlan <2-4094> reflector-port IFNAME no destination remote`

Parameters

<2-4094>	VLAN identifier
IFNAME	Interface name

Default

By default, all VLANs active on the trunk are monitored.

Command Mode

Monitor configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#no vlan 900 bridge 1
(config)#interface xe3
(config-if)#switchport
(config)#monitor session 1
(config-monitor)#destination remote vlan 900 reflector-port xe3
(config-monitor)#no destination remote
```

show monitor

Use this command to display states of all monitor sessions. If a session is down, the reason is displayed.

Command Syntax `show`

```
monitor
```

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show monitor
Session   State          Reason                Description
------- ----------- --------------------- --------------------------------
1       down        No sources configured
2       down        Dst in wrong mode
```

show monitor session

Use this command to display the configuration details of one or more monitor sessions.

Command Syntax `show monitor session (<1-18>|all|(range RANGE)) (brief|)`

Parameters

`<1-18>`	Session number
`all`	All sessions
`RANGE`	Session number range (n1-n2)
`brief`	Brief information

Command Mode

Exec mode or Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show monitor session 1 session 1 ------------
--- type              : local
state              : down (Session admin shut) source intf        :
tx                  : xe1 xe3 xe4 rx                  : xe2 xe3 xe4
both              : xe3 xe4 source VLANs      : rx                :
2,5-10,15,18-20 destination ports : xe5 filter count       :

Legend: f = forwarding enabled, l = learning enabled #
```

Table 7-83 Explains the show command output fields

Table 7-83: Show monitor session output fields

Field	Description
Type	Type of monitor session.
State	State of the security flow filter.
Rx	Incoming flow (source and destination IP addresses).
Tx	Reverse flow (source and destination IP addresses).

Field	Description
Both	Incoming and reverse flow (source and destination IP address)
Destination Port	Name of the destination port to be matched.
Source intf	Number of maximum intf central source session.
Source VLANs	Number of maximum VLANs central source session.
Filter count	Used to count number of lines in a file or table.

© Symanitron Proprietary

show filter

Use this command to display filters for one or more monitor sessions.

Command Syntax `show monitor session (<1-18>|all|(range RANGE)) filter`

Parameters

`<1-18>` Session number `all` All sessions

`RANGE` Session number range (n1-n2)

Command Mode

Exec mode or Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show monitor session 1 filter
session 1 ---------------
filter count : 3 --------------
-

match set 1 ---------------
destination mac address : 0000.0002.4451 (host) source
mac address : 0000.0012.2288 (host)
---------------

match set 2 ---------------
frame type : arp sender ip
address : 2.2.2.5 target ip
addres : 2.2.2.8 -----------
----

match set 3 ---------------
destination mac address : 0000.0001.1453 (host)
frame type : ipv4 source ip address : 3.3.3.5 #
```

show monitor running configuration

Use this command to display the mirror-related running configuration.

Command Syntax `show running-config monitor (all|)`

Parameters `all` Show running configuration with defaults

Command Mode

Exec mode or Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show running-config monitor
! monitor session 1 source
interface xe10 rx destination
interface po1 no shut #
```

CHAPTER 8 VLAN and Private VLAN Commands

This chapter has the commands used to manage VLANs and private VLANs.

- private-vlan association
- private-vlan community
- private-vlan isolated
- private-vlan primary
- show dtag vlan
- show vlan access-map
- show vlan
- show vlan brief
- show vlan classifier
- switchport access
- switchport hybrid
- switchport mode
- switchport mode access ingress-filter
- switchport mode hybrid acceptable-frame-type
- switchport mode hybrid ingress-filter
- switchport mode trunk ingress-filter
- switchport trunk allowed
- switchport trunk allowed vlan dtag
- switchport trunk native
- switchport mode private-vlan
- switchport private-vlan host-association
- switchport private-vlan mapping
- vlan classifier activate
- vlan classifier group
- vlan classifier rule ipv4
- vlan classifier rule mac
- vlan classifier rule proto
- vlan database
- vlan dtag
- vlan state
- vlan VLAN_RANGE bridge

private-vlan association

Use this command to associate a secondary VLAN to a primary VLAN. Only one isolated VLAN can be associated to a primary VLAN. Multiple community VLANs can be associated to a primary VLAN.

Use the `no` form of this command to remove association of all the secondary VLANs to a primary VLAN.

Command Syntax `private-vlan association add VLAN_RANGE private-vlan association remove VLAN_RANGE no private-vlan association`

Parameters

`add`	Add a VLAN to private VLAN list.
`remove`	Removes values associated with a single VLAN.
`VLAN_RANGE`	Specify VLAN ID 1-4094 or range(s): 1-5, 10 or 2-5,7-19 of the private VLANs to be configured

Default

By default, functionality is disabled

Command Mode

VLAN Configuration mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#vlan database
(config-vlan)#private-vlan association add 3-4
(config-vlan)#private-vlan association remove 3-4
(config-vlan)#no private-vlan association
```

private-vlan community

Use this command to set a VLAN type for a private (community) VLAN.

Use the `no` form of this command to remove the specified private VLAN.

Command Syntax `private-vlan <2-4094> community bridge <1-32> no private-vlan <2-4094> community bridge <1-32>`

Parameters

<2-4094>	Specify a private VLAN identifier.	bridge	Specify the bridge identifier.

Default

By default, private vlan is disabled

Command Mode

VLAN Configuration mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#vlan database
                (config-vlan)#private-vlan 4 community bridge 1
```

private-vlan isolated

Use this command to create an isolated private VLAN.

Use the no form of this command to remove the specified private VLAN.

Command Syntax private-vlan <2-4094> isolated bridge <1-32> no private-vlan <2-4094> isolated bridge <1-32>

Parameters

<2-4094>	Specify a private VLAN identifier.	bridge	Specify the bridge identifier.

Default

By default, private vlan is disabled

Command Mode

VLAN Configuration mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#vlan database
                (config-vlan)#private-vlan 3 isolated bridge 1
```

private-vlan primary

Use this command to create a primary VLAN.

Use the no form of this command to remove the specified private VLAN.

Command Syntax private-vlan <2-4094> primary bridge <1-32> no private-vlan <2-4094> primary bridge <1-32>

Parameters

<2-4094> Specify a private VLAN identifier. bridge Specify the bridge identifier.

Default

By default, private vlan is disabled

Command Mode

VLAN Configuration mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#vlan database
(config-vlan)#private-vlan 2 primary bridge 1
```

show dtag vlan

Use this command to display information about VLAN double tagging.

Command Syntax

```
show dtag
vlan
DTAG_VLAN_I
D
```

Parameters

DTAG-VLAN-IDs Outer-VLAN identifier and inner-VLAN identifier in the format 100.200, where 100 is the outer tag and 200 is the inner tag

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in SWMRE version 1.3.5.

Example

```
#show dtag vlan 2000.3001
```

Table 8-84 explains the output.

Table 8-84: show dtag vlan output

Field	Description
Bridge	Bridge number
VLAN ID	VLAN identifier
Name	Double tag-VLAN identifers
State	VLAN state: ACTIVE, SUSPEND, or INVALID
H/W Status	Hardware status: UP or DOWN
Member ports	Interfaces that are part of the VLAN and whether untagged (u) or tagged (t)

show vlan access-map

Use this command to display information for VLAN access maps.

Command Syntax `show vlan access-map`

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show vlan access-map Vlan access-map myMap 10
match ip: myMap        action: drop
```

show vlan

Use this command to display information about static, dynamic or all VLANs.

Command Syntax `show vlan (all|static|dynamic|auto) bridge <1-32>`

Parameters

`<1-32>`	Displays the bridge group ID.
`all`	Displays all VLANs (static and dynamic).
`static`	Displays static VLANs.
`dynamic`	Displays dynamic VLANs.
`auto`	Displays auto configured VLANs.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#sh vlan all bridge 1
Bridge VLAN ID Name State H/W Status Member ports

                                                                (u)-
Untagged, (t)-Tagged
======= ======= ================ ======= ==========
==========================
1       1       default          ACTIVE  Up         xe2(u)
xe10(u)
1       2       vlan2            ACTIVE  Up         xe10(t)
1       10      VLAN0010         ACTIVE  Up         xe2(t)
xe10(t)
1       20      VLAN0020         ACTIVE  Up         xe2(t)
xe10(t)
1       30      VLAN0030         ACTIVE  Up         xe10(t)
1       40      VLAN0040         ACTIVE  Up         xe10(t)
1       50      VLAN0050         ACTIVE  Up         xe10(t)
1       60      VLAN0060         ACTIVE  Up
xe10(t) #
```

Table 8-85 Explains the show command output fields.

Table 8-85: show vlan output fields

Field	Description
Bridge	Number of bridge in the interface.
VLAN ID	VLAN identifier of the VLAN listed.
Name	Name of the VLAN.
State	Indicates whether the physical link is operational and can pass packets.

Field	Description
H/W Status	Indicates that the hardware is operational.
Member ports	The tagged interfaces to which a VLAN is associated.

show vlan brief

Use this command to display brief VLAN information for all bridges.

Command Syntax `show vlan (brief | <2-4094>)`

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following is a sample output from this command when using the `all` parameter.

```
#show vlan brief

Bridge          VLAN ID  Name            State   Member ports
                                                 (u)-Untagged, (t)-Tagged
=============== ======= ================ ======= ===============================
1               1       default          ACTIVE  eth2(u)


0               1       default          ACTIVE
0               2       new              ACTIVE
```

Table 8-86 Explains the show command output fields.

Table 8-86: show vlan brief output fields

Field	Description
Bridge	Number of bridge in the interface.
VLAN ID	VLAN identifier of the VLAN listed.
Name	Name of the VLAN.
State	Indicates whether the physical link is operational and can pass packets.

H/W Status	Indicates that the hardware is operational.
Member ports	The tagged interfaces to which a VLAN is associated.

show vlan classifier

Use this command to display information on configured VLAN classifier groups, interfaces configured for a VLAN group or all the groups, or all configured VLAN classifier rules.

If either a group ID or rule ID is not specified, all configured VLAN classifier rules are shown. If either a group ID or rule ID is specified, a specific configured VLAN classifier rule is shown.

Command Syntax `show vlan classifier group interface`

```
IFNAME  show  vlan  classifier  group  (<1-16>|)
show vlan classifier rule(<1-256>|)
```

Parameters

`group`	Displays group activated information.
`<1-16>`	Displays the group ID
`interface`	Displays interface information.
`interface`	Displays interface group information.
`group`	Displays group activated information.
`<1-16>`	Displays the group ID.
`rule`	Displays VLAN classifier rule ID.
`<1-256>`	Displays rule ID information.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

This example displays groups for VLAN classifier groups:

```
#show vlan classifier group 1 vlan
classifier group 1 add rule 1
```

This example displays interfaces for all VLAN classifier groups:

```
#show vlan classifier interface group vlan
classifier group 1 interface fe2 vlan
classifier group 1 interface fe3 vlan
classifier group 2 interface fe5 vlan
classifier group 3 interface fe7
```

This example displays interfaces for VLAN classifier group 1:

```
#show vlan classifier interface group 1
vlan classifier group 1 interface fe2 vlan
classifier group 1 interface fe3
```

This example displays interfaces for VLAN classifier rule 1:

```
#show vlan classifier rule 1 vlan classifier rule 1 mac 222.2222.2222 vlan 2
```


© Symanitron Proprietary

switchport access

Use this command to change the default VLAN on the current interface.

Note: Symanitron does not recommend using VLAN identifier 1 because of interoperability issues with other vendors' equipment.

Use the `no` parameter to remove an existing VLAN.

Command Syntax `switchport access vlan <2-4094> no switchport access vlan`

Parameter

`<2-4094>`	Specify the VLAN identifier.

Default

The switchport access vlan default value is 3968.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

This example shows the steps of a typical VLAN session, creating and destroying a VLAN.

```
#configure terminal
(config)#interface eth0
(config-if)#switchport access vlan 3

(config)#interface eth0
(config-if)#no switchport access vlan
```

switchport hybrid

Use this command to set the switching characteristics of the interface to hybrid. Both tagged and untagged frames will be classified over hybrid interfaces.

For a VLAN range, specify two VLAN identifiers: the lowest and then the highest separated by a hyphen. For a VLAN list, specify the VLAN identifiers separated by commas. Do not enter spaces between the hyphens or commas.

Use the `no` parameter to turn off allowed hybrid switching.

Command Syntax `switchport hybrid allowed vlan all switchport hybrid vlan <2-4094> switchport hybrid allowed vlan none switchport hybrid allowed vlan except VLAN_ID switchport hybrid allowed vlan remove VLAN_ID switchport hybrid allowed vlan add VLAN_ID egress-tagged (enable|disable) no switchport hybrid no switchport hybrid vlan`

Parameters

`all`	Allow all VLANs to transmit and receive through the interface.
`none`	Allow no VLANs to transmit and receive through the interface.
`except`	Allow all VLANs except these VLANs to transmit and receive through the interface.
`VLAN_ID`	VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.
`remove`	Remove these VLANs from the member set.
`VLAN_ID`	VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.
`add`	Add these VLANs to the member set.
`VLAN_ID`	VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.
`egress-tagged`	Whether to tag outgoing frames.
`enable`	Enable egress tagging for outgoing frames.
`disable`	Disable egress tagging for outgoing frames.

Default

By default, switchport hybrid is enabled.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following shows adding a single VLAN to the member set.

```
(config-if)#switchport hybrid allowed vlan add eg switchport hybrid allowed
vlan add 2 egress-tagged enable
```

The following shows adding a range of VLANs to the member set.

```
(config-if)#switchport hybrid allowed vlan add eg switchport hybrid allowed
vlan add 2-4 egress-tagged enable
```

switchport mode

Use this command to set the switching characteristics of the Layer 2 interface.

Command Syntax `switchport mode (access|hybrid|trunk|provider-network|customer-edge |customer-network|private-vlan)`

Parameters

`access`	Access.
`hybrid`	Hybrid.
`trunk`	Trunk.
`provider-network`	Provider network.
`customer-network`	Customer network.

Default

By default, switchport hybrid is enabled

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode access
```

switchport mode access ingress-filter

Use this command to set the switching characteristics of the interface to access mode, and classify untagged frames only. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

Command Syntax `switchport mode access ingress-filter (enable|disable)`

Parameters

`ingress-filter` Set the ingress filtering for the received frames.

`enable` Set the ingress filtering for received frames. Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded. This is the default value.

`disable` Turn off ingress filtering to accept frames that do not meet the classification criteria.

Default

Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/ trunk) are discarded.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode access ingress-filter enable
```

switchport mode hybrid acceptable-frame-type

Use this command to set the interface acceptable frame types. This processing occurs after VLAN classification.

Command Syntax `switchport mode hybrid acceptable-frame-type (all|vlan-tagged)`

Parameters `all` Set all frames can be received `vlan-tagged` Accept only classified frames that belong to the port's member set.

Default

Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/ trunk) are discarded.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode hybrid acceptable-frame-type vlan-tagged
```

switchport mode hybrid ingress-filter

Use this command to set the switching characteristics of the interface as hybrid, and classify both tagged and untagged frames. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

Command Syntax `switchport mode hybrid ingress-filter (enable|disable)`

Parameters

`enable`	Set the ingress filtering for received frames. Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded. This is the default value.
`disable`	Turn off ingress filtering to accept frames that do not meet the classification criteria.

Default

Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/ trunk) are discarded.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode hybrid ingress-filter enable
```

switchport mode trunk ingress-filter

Use this command to set the switching characteristics of the interface as trunk, and specify only tagged frames. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

Command Syntax `switchport mode trunk ingress-filter (enable|disable)`

Parameters

ingress-filter	Set the ingress filtering for the received frames.
enable	Set the ingress filtering for received frames. Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded. This is the default value.
disable	Turn off ingress filtering to accept frames that do not meet the classification criteria.

Default

Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/ trunk) are discarded.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#switchport mode trunk ingress-filter enable
```

switchport trunk allowed

Use this command to set the switching characteristics of the interface to trunk.

For a VLAN range, specify two VLAN identifiers: the lowest and then the highest separated by a hyphen. For a VLAN list, specify the VLAN identifiers separated by commas. Do not enter spaces between the hyphens or commas.

Use the `no` parameter to remove all VLAN identifiers configured on this port.

Command Syntax `switchport trunk allowed vlan all`

`switchport trunk allowed vlan none switchport trunk allowed vlan add VLAN_ID switchport trunk allowed vlan except VLAN_ID switchport trunk allowed vlan remove VLAN_ID no switchport trunk`

Parameters

all	Allow all VLANs to transmit and receive through the interface.
none	Allow no VLANs to transmit and receive through the interface.
add	Add these VLANs to the member set.
VLAN_ID	VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.
except	All VLANs except these VLANs are part of the member set.
VLAN_ID	VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.
remove	Remove these VLANs from the member set.

VLAN_ID	VLAN identifier(s) <2-4094>. You can specify a single VLAN, a VLAN range, or a VLAN list.

Default

Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/ trunk) are discarded.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following shows adding a single VLAN to the port's member set.

```
(config)#interface eth0
(config-if)#switchport trunk allowed vlan add 2
```

The following shows adding a range of VLANs to the port's member set.

```
(config)#interface eth0
(config-if)#switchport trunk allowed vlan add 2-4
```


© Symanitron Proprietary

switchport trunk allowed vlan dtag

Use this command to maintain a mapping between the double-tagged logical interfaces with the physical interfaces for the purpose of enabling VLAN-translation on the port alone.

An example of when to use this command is in a GPON application, where an S-tag uniquely identifies an OLT channel partition and a C-tag uniquely identifies a subscriber/service on that channel partition.

Command Syntax `switchport trunk allowed vlan add dtag DTAG-VLAN-IDs switchport trunk allowed vlan remove dtag DTAG-VLAN-IDs`

Parameters

`add`	Add a mapping
`remove`	Remove a mapping
`DTAG-VLAN-IDs`	Outer-VLAN identifier and inner-VLAN identifier in the format 100.200, where 100 is the outer tag and 200 is the inner tag

Default

None

Command Mode

Interface mode

Applicability

This command was introduced in SWMRE version 1.3.5.

Examples

```
(config)#int mlag1
(config-if)#switchport
(config-if)#bridge-group 1
(config-if)#switchport mode trunk (config-if)#switchport
trunk allowed vlan add 100,2000 (config-if)#switchport trunk
allowed vlan add dtag 2000.3001
```

switchport trunk native

Use this command to configure native VLANs for this port. The native VLAN is used for classifying the incoming untagged packets.

Use the `no` parameter to revert the native VLAN to the default VLAN identifier 1.

Command Syntax `switchport trunk native vlan VLAN_ID no switchport trunk native vlan`

Parameter

`VLAN_ID`	VLAN identifier(s) <1-4094>. You can specify a single VLAN, or a VLAN list.

For a VLAN list, specify the VLAN identifiers separated by commas. Do not enter spaces in between the hyphens or commas.

Default

The default is that ingress filtering is off and all frame types are classified and accepted.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#switchport trunk native vlan 2

(config)#interface eth0 (config-if)#no
switchport trunk native vlan
```

switchport mode private-vlan

Use this command to make a layer2 port as a host port or promiscuous port.

Use the `no` form of this command to remove the configuration.

Command Syntax `switchport mode private-vlan (host | promiscuous)` `no switchport mode private-vlan (host | promiscuous)`

Parameters

`host` This port type can communicate with all other host ports assigned to the same community VLAN, but it cannot communicate with the ports in the same isolated VLAN. All communications outside of this VLAN must pass through a promiscuous port in the associated primary VLAN.

`promiscuous` A promiscuous port can communicate with all interfaces, including the community and isolated ports within a private VLAN

Default

By default, switchport mode private-vlan is host.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0 (config-if)#switchport mode private-vlan host
(config)#interface eth1
(config-if)#switchport mode private-vlan promiscuous
(config)#interface eth2
(config-if)#no switchport mode private-vlan promiscuous
```

switchport private-vlan host-association

Use this command to associate a primary VLAN and a secondary VLAN to a host port. Only one primary and secondary VLAN can be associated to a host port.

Use the `no` form of this command to remove the association.

Command Syntax `switchport private-vlan host-association <2-4094> add <2-4094> no switchport private-vlan host-association`

Parameters

`<2-4094>` VLAN identifier of the primary VLAN. `add` Adds the secondary VLAN.

`<2-4094>` VLAN identifier of the secondary VLAN (either isolated or community).

Default

By default, switchport mode private-vlan value is 1

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport private-vlan host-association 2 add 3

#configure terminal
(config)#interface eth0
(config-if)#no switchport private-vlan host-association
```

switchport private-vlan mapping

Use this command to associate a primary VLAN and a set of secondary VLANs to a promiscuous port.

Use the `no` form of this to remove all the association of secondary VLANs to primary VLANs for a promiscuous port.

Command Syntax `switchport private-vlan mapping <2-4094> add VLAN_ID switchport private-vlan mapping <2-4094> remove VLAN_ID no switchport private-vlan mapping`

Parameters

`<2-4094>`	VLAN identifier of the primary VLAN.
`add`	Adds the secondary VLAN.
`remove`	Removes the secondary VLAN.
`VLAN_ID`	VLAN identifier <2-4094> of the secondary VLAN (either isolated or community).

Default

By default, switchport mode private-vlan mapping value is 1

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#switchport private-vlan mapping 2 add 3-4
(config-if)#switchport private-vlan mapping 2 remove 3-4

(config-if)#no switchport private-vlan mapping
```

vlan classifier activate

Use this command to activate the VLAN classifier.

Use no form of this command to deactivate the VLAN classifier.

Command Syntax `vlan classifier activate <1-16> vlan <2-4096> no vlan classifier activate <1-16>`

Parameters

`<1-16>`	Indicates the VLAN classifier activate identifier.
`<2-4094>`	VLAN identifier of the primary VLAN.

Default

By default, vlan classifier activate value is 1

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth2
                (config-if)#vlan classifier activate 1 vlan 2

(config-if)#no vlan classifier activate 1
```

vlan classifier group

Use this command to create a subnet-based VLAN classifier group. A group indicates a VLAN classifier group ID.

Command Syntax `vlan classifier group <1-16> (add | delete) rule <1-256> no vlan classifier group <1-16>`

Parameters

`add`	Adds a rule to a group.
`delete`	Deletes a rule from a group.
`rule`	Indicates the VLAN classifier rule identifier `<1-256>`.

Default

By default, vlan classifier group value is 1

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#vlan classifier group 1 delete rule 1
(config)#no vlan classifier group 2
```

vlan classifier rule ipv4

Use this command to create a subnet-based VLAN classifier rule and map it to a specific VLAN. If the source IP address matches the IP subnet specified in the VLAN classifier rule, received packets are mapped to the designated VLAN.

Command Syntax `vlan classifier rule <1-256> ipv4 A.B.C.D/M no vlan classifier rule <1-256>`

Parameters

`A.B.C.D/M`	Indicates the IPv4 address classification. Enter the address in A.B.C.D/M format.

Default

By default, vlan classifier rule is VLAN1

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#vlan classifier rule 2 ipv4
20.20.20.2/24 (config)#no vlan classifier rule 2
```

vlan classifier rule mac

Use this command to create a subnet-based VLAN classifier rule and map it to a specific VLAN.

If the source IP address matches the IP subnet specified in the VLAN classifier rule, received packets are mapped to the designated VLAN.

Command Syntax `vlan classifier rule <1-256>`

`mac WORD no vlan classifier rule <1-256>`

Parameters

`WORD`	Indicate the Mac address classification. Enter the address in HHHH.HHHH.HHHH format.

Default

By default, vlan classifier rule value is VLAN1

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#vlan classifier rule 2 mac fe80::22e::b5ff:fee8:6/64
(config)#no vlan classifier rule 2
```

vlan classifier rule proto

Use this command to create a subnet-based VLAN classifier rule for a protocol and map it to a specific VLAN. If the source IP address matches the IP subnet specified in the VLAN classifier rule, received packets are mapped to the designated VLAN.

Command Syntax

```
vlan classifier rule <1-256> proto (ip|ipv6|ipx|x25|arp|rarp|atalkddp|atalkaarp|
```

```
atmmulti|atmtransport|pppdiscovery|pppsession|xeroxpup|xeroxaddrtrans|g8bpqx25|
ieeepup|ieeeaddrtrans|dec|decdnadumpload|decdnaremoteconsole|decdnarouting
| declat|decdiagnostics|deccustom|decsyscomm|<0-65535>)
no vlan classifier rule <1-256>
```

Parameters

`<0-65535>`	Ethernet decimal
`arp`	Address Resolution Protocol
`atalkaarp`	Appletalk AARP
`atalkddp`	Appletalk DDP
`atmmulti`	MultiProtocol Over ATM
`atmtransport`	Frame-based ATM Transport
`dec`	DEC Assigned
`deccustom`	DEC Customer use
`decdiagnostics`	EC Diagnostics
`decdnadumpload`	DEC DNA Dump/Load
`decdnaremoteconsole`	DEC DNA Remote Console
`decdnarouting`	DEC DNA Routing
`declat`	DEC LAT
`decsyscomm`	DEC Systems Comms Arch
`g8bpqx25`	G8BPQ AX.25
`ieeeaddrtrans`	Xerox IEEE802.3 PUP Address Translation
`ieeepup`	Xerox IEEE802.3 PUP
`ip`	IP address
`ipv6`	IPv6 address
`ipx`	IPX address
`pppdiscovery`	PPPoE discovery
`pppsession`	PPPoE session
`rarp`	Reverse Address Resolution
`x25`	CCITT X.25
`xeroxaddrtrans`	Xerox PUP Address Translation
`xeroxpup`	Xerox PUP

ethv2	Ethernet v2
nosnapllc	Indicates LLC without snap encapsulation snapllcIndicates LLC snap encapsulation

Default

By default, vlan classifier rule value is VLAN1

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
                  (config)#vlan classifier rule 2 proto
ip (config)#no vlan classifier rule 2
```

vlan database

Use this command to enter the VLAN configuration mode to add, delete, or modify values associated with a single VLAN.

Command Syntax `vlan`

```
database
```

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

In the following example, note the change to VLAN configuration mode from Configure mode:

```
#configure terminal
(config)#vlan database
(config-vlan)#
```

vlan dtag

Use this command to enable or disable double tagging packets with an outer-VLAN identifier and an inner-VLAN identifier.

An example of when to use this command is in a GPON application, where an S-tag uniquely identifies an OLT channel partition and a C-tag uniquely identifies a subscriber/service on that channel partition.

Use the `no` form of this command to not double tag packets.

Command Syntax `vlan dtag DTAG-VLAN-IDs bridge <1-32> state (enable|disable)`
`subscriber no vlan dtag DTAG-VLAN-IDs bridge <1-32>`

Parameters

`DTAG-VLAN-IDs` Outer-VLAN identifier and inner-VLAN identifier in the format 100.200, where 100 is the outer tag and 200 is the inner tag

`<1-32>` Bridge number `enable` Enable

double tagging `disable` Suspend

double tagging

Default

No default value is specified

Command Mode

VLAN database mode

Applicability

This command was introduced inSWMRE version 1.3.5.

Example

```
(config)#vlan database
(config-vlan)#vlan dtag 2000.3001 bridge 1 state enable subscriber
```

vlan state

This command enables or disables the state of a particular VLAN on the bridge.

Command Syntax `vlan <2-4094> bridge <1-32> (state (enable|disable)|)`

Parameters

`<1-32>`	Specify bridge group ID
`state`	Indicates the operational state of the VLAN

`enable`	Sets VLAN into a enable state.
`disable`	Sets VLAN into a disable state.
`name`	The VLAN name
`WORD`	The name of the VLAN

Default

By default, vlan bridge state is disabled.

Command Mode

VLAN Configuration mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#vlan database
(config-vlan)#vlan 45 bridge 1 state enable
```

vlan VLAN_RANGE bridge

.This command allows you to create a single/range of VLAN’s on the VLAN aware bridges.

Use the no form of this command to delete the VLAN.

Command Syntax `vlan VLAN_RANGE bridge <1-32> vlan VLAN_RANGE bridge <1-32> (name WORD|) state (enable | disable) no vlan VLAN_RANGE bridge <1-32>`

Parameters

`VLAN_RANGE`	The vlan-id or range of vlan-id's separated by ','&'-'
`bridge`	Specify the bridge group ID in the range <1-32>.
`state`	Indicates the operational state of the VLAN.
`enable`	Sets VLAN into an enable state.

`disable`	Sets VLAN into a disable state.

Default

By default, vlan bridge state is disabled

Command Mode

Configuration Mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#vlan 3-40,56 bridge 4
(config)#no vlan 2-5 bridge 2
```

© Symanitron Proprietary

CHAPTER 9 DHCP Snooping Commands

This chapter provides a description of the syntax and examples DHCP snooping. It includes the following commands:

- clear ip dhcp snooping binding
- debug ip dhcp snooping
- ip dhcp packet strict-validation
- ip dhcp snooping
- ip dhcp snooping binding
- ip dhcp snooping database
- ip dhcp snooping information option
- ip dhcp snooping ratelimit
- ip dhcp snooping trust
- ip dhcp snooping verify mac-address
- ip dhcp snooping vlan
- renew ip dhcp snooping binding database
- show debugging ip dhcp snooping
- show ip dhcp snooping
- show ip dhcp snooping binding

- show ip dhcp arp-inspection statistics

clear ip dhcp snooping binding

Use this command to remove all entries from the binding table.

Command Syntax `clear ip dhcp snooping (source|) binding bridge <1-32>`

Parameters

`<1-32>`	Bridge number
`source`	IP source guard

Default

No default value is specified.

Command Mode

Privileged Exec Mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear ip dhcp snooping binding bridge 1
```

debug ip dhcp snooping

Use this command to enable the debugging DHCP snooping.

Use the `no` parameter to disable the debug options.

Command Syntax `debug ip dhcp snooping (event|rx|tx|packet|all) no debug ip dhcp snooping (event|rx|tx|packet|all)`

Parameters

`event`	Enable event debugging
`rx`	Enable receive debugging
`tx`	Enable transmit debugging
`packet`	Enable packet debugging
`all`	Enable all debugging

Default

By default all debugging options are disabled.

Command Mode

Exec mode and configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#debug ip dhcp snooping all
#no debug ip dhcp snooping packet
```

ip dhcp packet strict-validation

Use this command to enable strict validation of DHCP packets. Strict validation of the DHCP packet checks that the DHCP option field in the packet is valid including the magic cookie value in the first four bytes of the options field. The device drops the packet if validation fails. Use the `no` parameter to disable strict validation.

Command Syntax `ip dhcp packet strict-validation`

`bridge <1-32> no ip dhcp packet strict-validation`

`bridge <1-32>`

Parameters

`<1-32>`	Bridge number

Default

By default strict validation of the DHCP packets is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#conf term
(conf)#ip dhcp packet strict-validation bridge 1
(conf)#no ip dhcp packet strict-validation bridge 1
```

ip dhcp snooping

Use this command to enable DHCP snooping on the bridge level.

Use the `no` parameter to remove the entire DHCP snooping configuration.

Command Syntax `ip dhcp snooping bridge <1-32> no ip dhcp snooping bridge <1-32>`

Parameters

`<1-32>`	Bridge number

Default

By default dhcp snooping will be disabled on the bridge.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ip dhcp snooping bridge 1
(config)#no ip dhcp snooping bridge 1
```

ip dhcp snooping binding

Use this command to create a static binding entry in the binding table. All the DHCP responses will be validated against the static entries. If the response does not match the entry in the binding table, the response packet is dropped.

Use the `no` parameter to remove an entry from the binding table.

Command Syntax

```
ip dhcp snooping binding bridge <1-32> XXXX.XXXX.XXXX <1-4094> (ipv4 A.B.C.D | ipv6
```

X:X::X:X) IFNAME no ip dhcp snooping binding bridge <1-32> XXXX.XXXX.XXXX <1-4094> (ipv4 | ipv6)

Parameters

<1-32>	Bridge number
XXXX.XXXX.XXXX	MAC address
<1-4094>	VLAN identifier
A.B.C.D	IPv4 address
X:X::X:X	IPv6 address
IFNAME	Interface name

Default

By default binding table will not have any entry

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ip dhcp snooping binding bridge 1 0001.0002.0003 2 ipv4 12.0.0.1 xe1
(config)#no ip dhcp snooping binding bridge 1 0001.0002.0003 2 ipv4
```

ip dhcp snooping database

Use this command to write the entries in the binding table to persistent storage.

Command Syntax ip dhcp snooping database bridge <1-32> **Parameters**

<1-32>	Bridge number

Default

No default value is specified.

Command Mode

Privileged Exec Mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#ip dhcp snooping database bridge 1
```

ip dhcp snooping information option

Use this command to insert option 82 information into DHCP packets.

Use the `no` parameter to disable inserting option 82.

Command Syntax `ip dhcp snooping information option bridge <1-32> no ip dhcp snooping information option bridge <1-32>`

Parameters

`<1-32>`	Bridge number

Default

By default address option 82 information insertion is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#conf term
            (conf)#ip dhcp snooping information option bridge 1
                        (conf)#no ip dhcp snooping information option bridge 1
```

ip dhcp snooping ratelimit

Use this command to limit the rate of DHCP packets per second.

Use the no parameter to set the rate limit to its default value (100 pps).

Command Syntax `ip dhcp snooping ratelimit RATELIMIT bridge <1-32> no ip dhcp snooping ratelimit bridge <1-32>`

Parameters

`RATELIMIT`	Packets per second <0-2048>
`<1-32>`	Bridge number

Default

The default rate limit value is 100 packets per second.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#conf term
                                    (conf)#ip dhcp snooping ratelimit 2000 bridge 1
                    (conf)#no ip dhcp snooping ratelimit bridge 1
```

ip dhcp snooping trust

Use this command to mark an interface as trusted. All DHCP servers must be connected to the trusted interface.

Use the `no` parameter to remove an interface from the list of trusted interfaces.

Command Syntax `ip dhcp snooping trust`

`no ip dhcp snooping trust`

Parameters

None

Default

By default all interfaces are untrusted.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface xe1
(config-if)#ip dhcp snooping trust
(config-if)#no ip dhcp snooping trust
```

ip dhcp snooping verify mac-address

Use this command to enable the DHCP snooping MAC address verification. If the device receives a DHCP request packet on an untrusted interface and the source MAC address and the DHCP client hardware address do not match, the device drops the packet.

Use the `no` parameter to disable the address verification.

Command Syntax `ip dhcp snooping verify mac-address bridge <1-32>`

`no ip dhcp snooping verify mac-address bridge <1-32>`

Parameters

<1-32>	Bridge number

Default

By default address verification is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#conf term
(conf)#ip dhcp snooping verify mac-address bridge 1
(conf)#no ip dhcp snooping verify mac-address bridge 1
```

ip dhcp snooping vlan

Use this command to enable DHCP snooping for the given VLAN.

Use the no parameter to disable the DHCP snooping on the VLAN.

Command Syntax ip dhcp snooping vlan VLAN_RANGE2 bridge <1-32> no ip dhcp snooping vlan VLAN_RANGE2 bridge <1-32>

Parameters

VLAN_RANGE2	VLAN identifier <1-4094>
<1-32>	Bridge number

Default

By default DHCP snooping will be disabled on all the vlans

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ip dhcp snooping vlan 10 bridge 1
                (config)#no ip dhcp snooping vlan 10 bridge 1
```

renew ip dhcp snooping binding database

Use this command to populate the binding table by fetching the binding entries from persistent storage.

Command Syntax `renew ip dhcp snooping (source|) binding database bridge <1-32>`

Parameters

`<1-32>`	Bridge number
`source`	IP source guard

Default

No default value is specified.

Command Mode

Privileged Exec Mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#renew ip dhcp snooping binding database bridge 1
```

show debugging ip dhcp snooping

Use this command to display the enabled debugging options.

Command Syntax `show debugging ip dhcp snooping`

Parameters

None

Command Mode

Privileged Exec Mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show debugging ip dhcp snooping
DHCP snoop debugging status:
DHCP snoop event debugging is on
DHCP snoop tx debugging is on
```

show ip dhcp snooping

Use this command to display the DHCP configuration, including trusted ports, rate limit, configured VLAN, active VLAN, and strict validation status.

Command Syntax `show ip dhcp snooping bridge <1-32>`

Parameters

`<1-32>`	Bridge number

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#sh ip dhcp snooping bridge 1

Bridge Group                                          : 1
DHCP snooping is                                      : Enabled
DHCP snooping option82 is                             : Disabled
Verification of hwaddr field is                       : Disabled
Rate limit(pps)                                       : 100

DHCP snooping trust is configured on the following Interfaces

Interface               Trusted ---
------------          ------xe1/4
Yes

DHCP snooping IP Source Guard is configured on the following Interfaces

Interface               Source Guard
---------------         ------------
```

show ip dhcp snooping binding

Use this command to display the dhcp snooping binding table.

Command Syntax `show ip dhcp snooping (source|) binding bridge <1-32>`

Parameters

`<1-32>`	Bridge number
`source`	DHCP snooping IP source guard

Command Mode

Privileged Exec Mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
# show ip dhcp snooping binding bridge 1

Total number of static IPV4 entries                : 1
Total number of dynamic IPV4 entries               : 0
Total number of static IPV6 entries                : 0
Total number of dynamic IPV6 entries               : 0

MacAddress          IpAddress      Lease(sec)     Type       VLAN    Interface
--------------    -------------   ----------  -----------   ----    ----------
0001.0002.0003       12.0.0.1          0         static       2      xe2
```

Table 9-87 explains the show command output fields.

Table 9-87: show ip dhcp snooping binding output details

Entry	Description
Total number of static IPV4 entries	Number of static IPV4 entries in the interface.
Total number of dynamic IPV4 entries	Number of dynamic IPV4 entries in the interface.
Total number of static IPV6 entries	Number of static IPV6 entries in the interface.
Total number of dynamic IPV6 entries	Number of dynamic IPV6 entries in the interface.
Mac Address	MAC address forwards the packet into a given dhcp instance.
IP Address	IP address of the peer device.
Lease (sec)	The DHCP lease time in seconds provided to untrusted IP addresses.
Type	Configured either statically or dynamically by the DHCP server.

Table 9-87: show ip dhcp snooping binding output details (Continued)

	Description
	Identifier of the number.
	Interface is being snooped.

show ip dhcp arp-inspection statistics

Use this command to display the dhcp snooping dynamic ARP inspection statistics information.

Command Syntax `show ip dhcp snooping arp-inspection statistics bridge <1-32>`

Parameters

`<1-32>`	Bridge number

Command Mode

Privileged Exec Mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip dhcp snooping arp-inspection statistics bridge 1

bridge     forwarded  dai dropped ------     ---------
-----------
1          0          0
```

Table 9-88 explains the show command output fields.

Table 9-88: show ip dhcp snooping arp-inspection statistics output

Field	Description
bridge	The bridge identifier (number) on which snooping is being used.
forward	The number of packets forwarded to neighbor.
dai dropped	The number of packets that have been dropped because they did not pass dynamic arp inspection (DIA).

Appendix A spanning-tree Commands

The following lists the spanning-tree command aliases for the SWMRE `bridge` and `bridge-group` commands.

- spanning-tree ageing-time <10-1000000>
- no spanning-tree ageing-time
- spanning-tree cisco-interoperability (enable | disable)
- spanning-tree enable
- spanning-tree errdisable-timeout enable
- no spanning-tree errdisable-timeout enable
- spanning-tree errdisable-timeout interval <10-1000000>
- no spanning-tree errdisable-timeout interval
- spanning-tree force-version <0-3>
- no spanning-tree force-version
- spanning-tree forward-time <4-30>
- no spanning-tree forward-time
- spanning-tree hello-time <1-10>
- no spanning-tree hello-time
- spanning-tree instance <1-63>
- no spanning-tree instance <1-63>
- spanning-tree instance <1-63> path-cost <1-200000000>
- no spanning-tree instance <1-63> path-cost
- spanning-tree instance <1-63> priority <0-240>
- spanning-tree instance <1-63> priority <0-61440>
- no spanning-tree instance <1-63> priority
- spanning-tree max-age <6-40>
- no spanning-tree max-age
- spanning-tree max-hops <1-40>
- no spanning-tree max-hops <1-40>
- spanning-tree path-cost <1-200000000>
- no spanning-tree path-cost
- spanning-tree portfast bpdu-filter
- no spanning-tree portfast bpdu-filter
- spanning-tree portfast bpdu-guard
- no spanning-tree portfast bpdu-guard
- spanning-tree priority <0-61440>
- no spanning-tree priority
- spanning-tree shutdown

- no spanning-tree shutdown
- spanning-tree transmit-holdcount <1-10>

spanning-tree Commands

- no spanning-tree transmit-holdcount
- spanning-tree vlan <2-4094>
- no spanning-tree vlan <2-4094>
- spanning-tree vlan <2-4094> path-cost <1-200000000>
- no spanning-tree vlan <2-4094> path-cost
- spanning-tree vlan <2-4094> priority <0-240>
- spanning-tree vlan <2-4094> priority <0-61440>
- no spanning-tree vlan <2-4094> priority

SECTION 6

Layer 3

Layer 3 Unicast Configuration Guide

Contents

This guide contains these chapters:

- Chapter 1, *BGP*
- Chapter 2, *BGP4+*
- Chapter 3, *OSPFv2*
- Chapter 4, *OSPFv3*
- Chapter 5, *IS-IS IPv4*
- Appendix 5, *IS-IS IPv6*
- Chapter 6, *VLAN Interfaces*
- Chapter 7, *Layer 3 Link Aggregation*
- Chapter 8, *Static Routes*
- Chapter 9, *RIP*

© Symanitron

CHAPTER 1 BGP

This chapter contains basic Border Gateway Protocol configuration examples.

For details about the commands used in these examples, see the *Border Gateway Protocol Command Reference*.

Enable BGP Routers in the Same Autonomous System

Figure 1-72 shows the minimum configuration required to enable BGP on an interface. R1 and R2 are two routers belonging to the same AS, AS200, connecting to network 10.10.10.0/24. First, define the routing process and the AS number to which the routers belong. Then, define BGP neighbors to start exchanging routing updates.

Topology

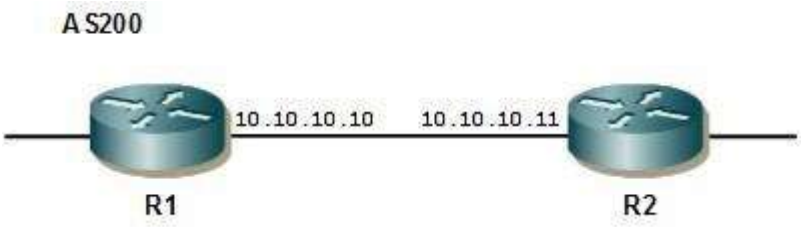


Figure 1-72: Routers in the Same Autonomous System

R1

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 200`	Define the routing process. The number `200` specifies the AS number of R1.
`(config-router)#neighbor 10.10.10.11 remoteas 200`	Define BGP neighbors, and establish a TCP session. `10.10.10.11` is the IP address of the neighbor (R2), and `200` is the neighbor's AS number.

R2

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 200`	Define the routing process. The number `200` specifies the AS number of `R2`.
`(config-router)#neighbor 10.10.10.10 remoteas 200`	Define BGP neighbors, and establish a TCP session. `10.10.10.10` is the IP address of the neighbor (`R1`), and `200` is the neighbor's AS number.

Validation

```
#sh ip bgp summary
BGP router identifier 192.168.56.101, local AS number 200
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries
```

```
Neighbor                 V    AS    MsgRcv     MsgSen TblVer    InQ    OutQ    Up/
 Down    State/PfxRcd
10.10.10.11               4    200   387         390       1       0       0
00:00:04                0

Total number of neighbors 1

Total number of Established sessions 1

#sh ip bgp neighbors
BGP neighbor is 10.10.10.11, remote AS 200, local AS 200, internal link
  BGP version 4, remote router ID 192.168.56.102
  BGP state = Established, up for 00:01:01
  Last read 00:01:01, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 389 messages, 0 notifications, 0 in queue
  Sent 391 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 2; dropped 1 Local
host: 10.10.10.10, Local port: 50322 Foreign
host: 10.10.10.11, Foreign port: 179
Nexthop: 10.10.10.10
Nexthop global: fe80::a00:27ff:fe21:7ed2
Nexthop local: ::
BGP connection: non shared network
Last Reset: 02:23:59, due to BGP Notification sent
Notification Error Message: (Hold Timer Expired/Unspecified Error Subcode)
```

Enable BGP Between Different Autonomous Systems

This example shows the minimum configuration required for enabling BGP on an interface, when the routers belong to different autonomous systems. R1 and R2 are two routers in different autonomous system, AS200 and AS300, connecting to network 10.10.10.0/24.

Topology

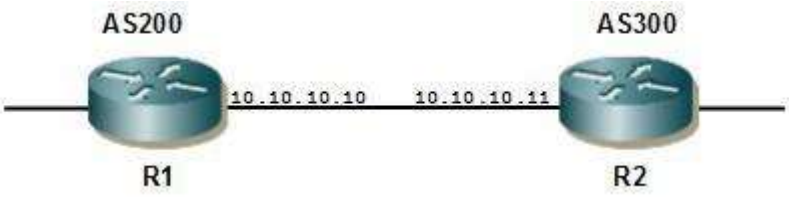


Figure 1-73: Routers in Different Autonomous Systems

R1

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 200`	Define the routing process. The number `200` specifies the AS number of R1.
`(config-router)#neighbor 10.10.10.11 remoteas 300`	Define BGP neighbors, and establish a TCP session. `10.10.10.11` is the IP address of the neighbor (R2), and `300` is the neighbor's AS number.

R2

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 300`	Define the routing process. The number `300` specifies the AS number of `R2`.
`(config-router)#neighbor 10.10.10.10 remoteas 200`	Define BGP neighbors, and establish a TCP session. `10.10.10.10` is the IP address of the neighbor (R1), and `200` is the neighbor's AS number.

Validation

```
#sh ip bgp neighbors
BGP neighbor is 10.10.10.10, remote AS 200, local AS 300, external link
  BGP version 4, remote router ID 192.168.56.101
  BGP state = Established, up for 00:00:13
  Last read 00:00:13, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 2 messages, 0 notifications, 0 in queue
  Sent 2 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30
 seconds For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0 Local
host: 10.10.10.11, Local port: 53545 Foreign
host: 10.10.10.10, Foreign port: 179
Nexthop: 10.10.10.11
```

```
Nexthop global: fe80::a00:27ff:fe50:6a9b
Nexthop local: ::
BGP connection: non shared network

#sh ip bgp summary
BGP router identifier 192.168.56.102, local AS number 300
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries
Neighbor                 V    AS    MsgRcv    MsgSen TblVer    InQ    OutQ    Up/
Down   State/PfxRcd
10.10.10.10               4   200     3          3       1       0       0
00:00:50                0

Total number of neighbors 1

Total number of Established sessions 1
```

Route-Map

Use route maps to filter incoming updates from a BGP peer. In this example, the prefix-list `ABC` on R1 is configured to deny entry of any routes with the IP address 1.1.1.0/M (M = 26, 27, 28). To test the filter, R2 is configured to generate network addresses 1.1.1.0/27 and 1.1.2.0/24. To verify, use the `show ip bgp` command on R1; it displays R1 receiving updates from only 1.1.2.0/24.

Topology

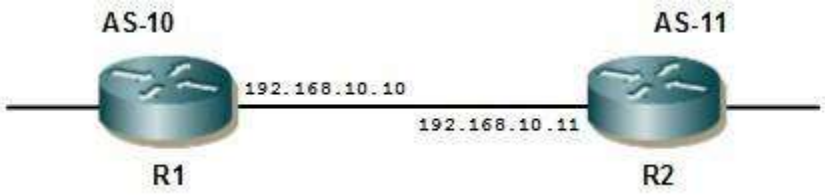


Figure 1-74: Configure Route-Map

R1

`#configure terminal`	Enter Configure mode.
`(config)#ip prefix-list ABC seq 5 deny 1.1.1.0/24 ge 26 le 28`	Create an entry in the prefix-list. The `ABC` parameter is the name of the map that is created above. `5` specifies the sequence number or position of this specific route map. `deny` specifies the packets are to be rejected. `26` and `28` are the minimum and maximum prefix lengths to be matched.
`(config)#ip prefix-list ABC seq 10 permit any`	Create another entry in the `ABC` map. `10` specifies the sequence number or position of this specific route map. The `permit` parameter `any` specifies accept all packets of any length.
`(config)#route-map ABC permit 1`	Enter Route-map mode to set the match operation.

(config-route-map)#match ip address prefixlist ABC	Set the match criteria. In this case, if the route-map name matches ABC, the packets from the first sequence are denied.
(config-route-map)#exit	Exit Route-map mode, and return to Configure mode.
(config)#router bgp 10	Define the routing process, and establish a TCP session. The number 10 specifies the AS number of R1.
(config-router)#neighbor 192.168.10.11 remote-as 11	Define BGP neighbors, and establish a TCP session. 192.168.10.11 is the IP address of the neighbor (R2), and 11 is the neighbor's AS number.
#configure terminal	Enter Configure mode.
(config)#ip prefix-list ABC seq 5 deny 1.1.1.0/24 ge 26 le 28	Create an entry in the prefix-list. The ABC parameter is the name of the map that is created above. 5 specifies the sequence number or position of this specific route map. deny specifies the packets are to be rejected. 26 and 28 are the minimum and maximum prefix lengths to be matched.
(config)#ip prefix-list ABC seq 10 permit any	Create another entry in the ABC map. 10 specifies the sequence number or position of this specific route map. The permit parameter any specifies accept all packets of any length.
(config)#route-map ABC permit 1	Enter Route-map mode to set the match operation.
(config-route-map)#match ip address prefixlist ABC	Set the match criteria. In this case, if the route-map name matches ABC, the packets from the first sequence are denied.
(config-route-map)#exit	Exit Route-map mode, and return to Configure mode.
(config-router)#neighbor 192.168.10.11 routemap ABC in	Apply a route map to routes. 192.168.10.11 specifies the IP address of BGP neighbor. The ABC parameter is the name of the route map, and in specifies that the access list applies to incoming advertisements.
(config-router)#exit	Exit router mode.

R2

#configure terminal	Enter Configure mode.
(config)#interface lo	Enter loopback interface mode.
(config-if)#ip address 1.1.1.1/27	Specify the interface address.
(config-if)#ip address 1.1.2.1/24	Specify the interface address.
(config-if)#exit	Exit loopback interface mode.
(config)#router bgp 11	Define the routing process, and establish a TCP session. The number 11 specifies the AS number of R2.
(config-router)#neighbor 192.168.10.10 remote-as 10	Define BGP neighbors, and establish a TCP session. 192.168.10.10 is the IP address of the neighbor (R1), and 10 is the neighbor's AS number.
(config-router)#network 1.1.1.0/27	Specify the network to be advertised by the BGP routing process.
(config-router)#network 1.1.2.0/24	Specify the network to be advertised by the BGP routing process.

`(config-router)#exit`	Exit router mode.

Validation

```
#sh ip bgp
BGP table version is 9, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
l - labeled               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network          Next Hop            Metric     LocPrf      Weight Path *>
1.1.2.0/24        10.20.30.2           0        100          0      11 i

Total number of prefixes 1
```

Route Reflector

The configurations in this section apply to BGP Route Reflectors (RR).

Reduce the iBGP Mesh Inside an Autonomous System

Use Route Reflectors to reduce the iBGP mesh inside an Autonomous System (AS).

Topology

In this example, R2, R5, and R4 would have to maintain a full mesh among themselves, but by making R5 the Route Reflector, R2 (Client1) has an iBGP session with the RR only, but not with R4 (Client 2). The routes learned from R2 are advertised to the other clients, and to iBGP peers outside the cluster; the iBGP routes learned from iBGP peers outside the cluster are advertised to R2. This reduces the iBGP peer connections in AS1.

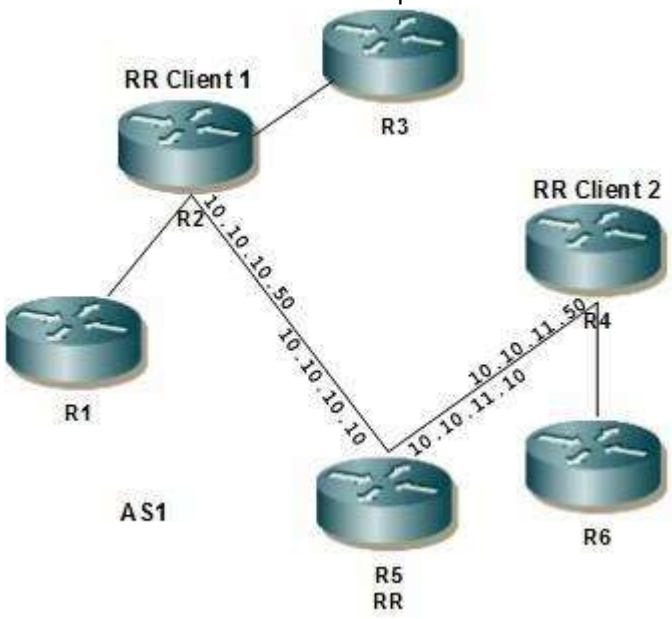


Figure 1-75: BGP Route Reflector

RR (R5)

#configure terminal	Enter Configure mode.
(config)#router bgp 1	Define the routing process. The number 1 identifies the AS number of R5.
(config-router)#neighbor 10.10.10.50 remoteas 1	Define the BGP neighbor, and establish a TCP session. 10.10.10.50 is the IP address of one of the neighbors (R2), and 1 is the neighbor's AS number.
(config-router)#neighbor 10.10.10.50 routereflector-client	Configure R5 as the Route-Reflector (RR) and neighbor R2 as its client.
(config-router)#neighbor 10.10.11.50 remoteas 1	Define the BGP neighbor, and establish a TCP session. 10.10.11.50 is the IP address of one of the neighbors (R4), and 1 is the neighbor's AS number.
(config-router)#neighbor 10.10.11.50 routereflector-client	Configure R5 as the Route-Reflector (RR) and neighbor R4 as its client.
(config-router)#exit	Exit router mode.

RR Client 1 (R2)

(config)#router bgp 1	Define the routing process. The number 1 specifies the AS number of R2.
(config-router)#neighbor 10.10.10.10 remoteas 1	Define the BGP neighbor, and establish a TCP session. 10.10.10.10 is the IP address of the neighbor (R5), and 1 is the neighbor's AS number.
(config-router)#exit	Exit router mode.

RR Client 2 (R4)

(config)#router bgp 1	Define the routing process. The number 1 identifies the AS number of R4.
(config-router)#neighbor 10.10.11.10 remoteas 1	Define BGP neighbor, and establish a TCP session. 10.10.11.10 is the IP address of the neighbor (R5), and 1 is the neighbor's AS number.
(config-router)#exit	Exit router mode.

Validation

R5

```
#sh ip bgp neighbors
BGP neighbor is 10.10.10.50, remote AS 1, local AS 1, internal link
  BGP version 4, remote router ID 10.12.4.152
  BGP state = Established, up for 00:01:04
  Last read 00:01:04, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 4 messages, 0 notifications, 0 in queue
  Sent 4 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv4 IPv4
```

```
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes
 Connections established 1; dropped 0
Local host: 10.10.10.10, Local port: 47983
Foreign host: 10.10.10.50, Foreign port: 179
Nexthop: 10.10.10.10
Nexthop global: fe80::a00:27ff:fe09:fd25
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 10.10.11.50, remote AS 1, local AS 1, internal link
  BGP version 4, remote router ID 10.12.4.197
  BGP state = Established, up for 00:01:04
  Last read 00:01:04, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 4 messages, 0 notifications, 0 in queue
  Sent 4 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0 Local
host: 10.10.11.10, Local port: 39851 Foreign
host: 10.10.11.50, Foreign port: 179
Nexthop: 10.10.11.10
Nexthop global: fe80::a00:27ff:fe52:45f6
Nexthop local: ::
BGP connection: non shared network
```

R3

```
#sh ip bgp neighbors
BGP neighbor is 10.10.11.10, remote AS 1, local AS 1, internal link
  BGP version 4, remote router ID 10.12.4.185
  BGP state = Established, up for 00:00:56
  Last read 00:00:56, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
```

```
  Received 3 messages, 0 notifications, 0 in queue
  Sent 3 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.11.50, Local port: 179
Foreign host: 10.10.11.10, Foreign port: 39851
Nexthop: 10.10.11.50
Nexthop global: fe80::a00:27ff:fe42:fb7a
Nexthop local: ::
BGP connection: non shared network
```

R2

```
#sh ip bgp neighbors
BGP neighbor is 10.10.10.10, remote AS 1, local AS 1, internal link
  BGP version 4, remote router ID 10.12.4.185
  BGP state = Established, up for 00:01:23
  Last read 00:01:23, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 4 messages, 0 notifications, 0 in queue
  Sent 4 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0 Local
host: 10.10.10.50, Local port: 179 Foreign
host: 10.10.10.10, Foreign port: 47983
Nexthop: 10.10.10.50
Nexthop global: fe80::a00:27ff:fe9c:f35d
Nexthop local: ::
BGP connection: non shared network
```

Multiple Route Reflectors

The basic rule of BGP is that a BGP speaker cannot advertise a route to an iBGP neighbor if that route was learned from another iBGP neighbor. Configuring a route reflector provides a means to circumvent this rule. The entire route reflector process is transparent to the clients, and no configuration is necessary on these clients.

Whenever an iBGP-speaking router receives a route update, it forwards the route to the neighbor without changing the nexthop IP address, thus making it an unreachable route, unless verified by an iGP (for example, neighbor x.x.x.x route-reflector-client).

- If a router is configured as a Route Reflector, it forwards the routes received by changing the nexthop address as itself, thus making the nexthop reachable.
- If a route is received from a client, the route is forwarded to the clients.
- If a route is received from a non-client, the route is forwarded to the clients and non-clients.

Topology

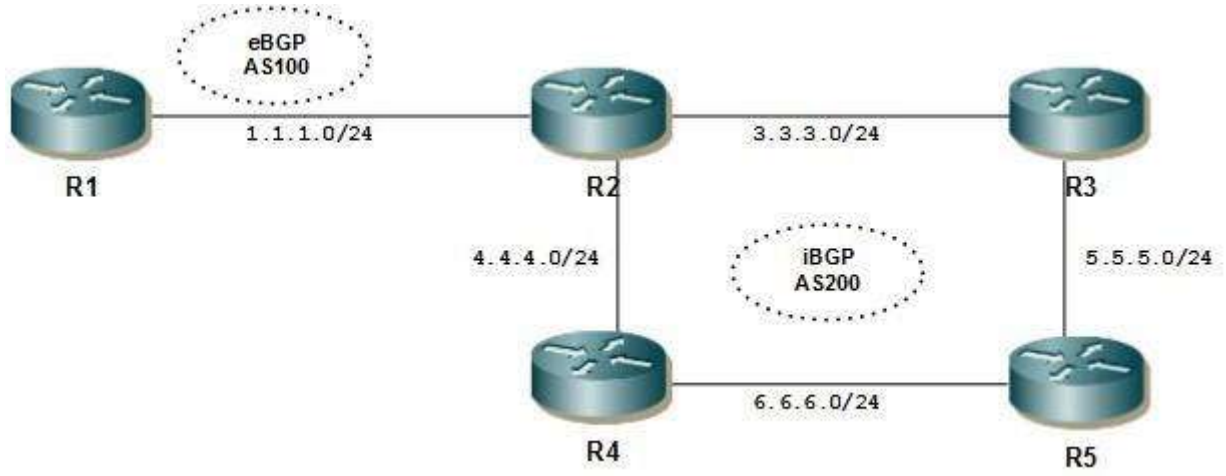


Figure 1-76: eBGP and iBGP Route Reflector Topology

R1

`#configure terminal`	Enter Configure mode.
`(config)#interface lo`	Enter loopback interface mode.
`(config-if)#ip address 100.100.100.100/32`	Specify IP address for the interface.
`(config-if)#exit`	Exit loopback interface mode.
`(config)#router bgp 100`	Define the routing process with AS number `100`.
`(config-router)#neighbor 1.1.1.2 remote-as 200`	Define the eBGP neighbor (R2).
`(config-router)#network 100.100.100.100/32`	Advertise a route via eBGP connection to R2.
`(config-router)#exit`	Exit router mode.

R2

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 200`	Define the routing process with AS number `200`.

(config-router)#neighbor 1.1.1.1 remote-as 100	Define the eBGP neighbor (R1).
(config-router)#neighbor 4.4.4.1 remote-as 200	Define the iBGP neighbor (R4).
(config-router)#neighbor 3.3.3.1 remote-as 200	Define the iBGP neighbor (R3).
(config-router)#bgp cluster-id 4	Define a cluster ID (4) when multiple Route Reflectors exist.
(config-router)#neighbor 3.3.3.1 routereflector-client	Configure R2 as the Route-Reflector and neighbor R3 as its client.
(config-router)#neighbor 4.4.4.1 routereflector-client	Configure R2 as the Route-Reflector and neighbor R4 as its client.
(config-router)#exit	Exit router mode.

R3

#configure terminal	Enter Configure mode.
(config)#router bgp 200	Define the routing process with AS number 200.
(config-router)#neighbor 3.3.3.2 remote-as 200	Define the iBGP neighbor (R2).
(config-router)#neighbor 5.5.5.2 remote-as 200	Define the iBGP neighbor (R5).
(config-router)#neighbor 5.5.5.2 routereflector-client	Configure R3 as the Route-Reflector and neighbor R5 as its client.
(config-router)#exit	Exit router mode.

R4

#configure terminal	Enter Configure mode.
(config)#router bgp 200	Define the routing process with AS number 200.
(config-router)#neighbor 4.4.4.2 remote-as 200	Define the iBGP neighbor (R2).
(config-router)#neighbor 6.6.6.2 remote-as 200	Define the iBGP neighbor (R5).
(config-router)#exit	Exit router mode.

R5

#configure terminal	Enter Configure mode.
(config)#router bgp 200	Define the routing process with AS number 200.
(config-router)#neighbor 5.5.5.1 remote-as 200	Define the iBGP neighbor (R3).
(config-router)#neighbor 6.6.6.1 remote-as 200	Define the iBGP neighbor (R4).
(config-router)#exit	Exit router mode.

Validation

R2

```
    #sh ip bgp neighbors
    BGP neighbor is 1.1.1.1, remote AS 100, local AS 200, external link
      BGP version 4, remote router ID 10.12.4.142
      BGP state = Established, up for 00:00:17
      Last read 00:00:17, hold time is 90, keepalive interval is 30 seconds
      Neighbor capabilities:
        Route refresh: advertised and received (old and new)
        Address family IPv4 Unicast: advertised and received
      Received 2 messages, 0 notifications, 0 in queue
      Sent 2 messages, 0 notifications, 0 in queue
      Route refresh request: received 0, sent 0
      Minimum time between advertisement runs is 30
     seconds For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 1.1.1.2, Local port: 45966
Foreign host: 1.1.1.1, Foreign port: 179
Nexthop: 1.1.1.2
Nexthop global: fe80::a00:27ff:fecf:3354
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 3.3.3.1, remote AS 200, local AS 200, internal
  link BGP version 4, remote router ID 10.12.4.197
  BGP state = Established, up for 00:00:03
  Last read 00:00:03, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 2 messages, 0 notifications, 0 in queue
  Sent 2 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 3, Offset 0, Mask 0x8
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 3.3.3.2, Local port: 179
Foreign host: 3.3.3.1, Foreign port: 54514
Nexthop: 3.3.3.2
```

```
Nexthop global: fe80::a00:27ff:fee1:4b5f
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 4.4.4.1, remote AS 200, local AS 200, internal
  link BGP version 4, remote router ID 10.12.4.185
  BGP state = Established, up for 00:09:48
  Last read 00:09:48, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 21 messages, 0 notifications, 0 in queue
  Sent 22 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 4.4.4.2, Local port: 179
Foreign host: 4.4.4.1, Foreign port: 39999
Nexthop: 4.4.4.2
Nexthop global: fe80::a00:27ff:fe02:9f2a
Nexthop local: ::
BGP connection: non shared network
#sh ip bgp summary
BGP router identifier 10.12.4.196, local AS number
200 BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                  V   AS    MsgRcv    MsgSen TblVer    InQ   OutQ   Up/ Down
State/PfxRcd
1.1.1.1                   4   100     4          4       1      0      0
00:01:07               0
3.3.3.1                   4   200     3          3       1      0      0
00:00:53               0
4.4.4.1                   4   200    23         24       1      0      0
00:10:38               0

Total number of neighbors 3


Total number of Established sessions 3
#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
```

```
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2        E1
- OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 10.12.4.1 to network 0.0.0.0

K*      0.0.0.0/0 [0/0] via 10.12.4.1, eth0
C       1.1.1.0/24 is directly connected, eth1
C3.3.3.0/24 is directly connected, eth3
C4.4.4.0/24 is directly connected, eth2
C10.12.4.0/24 is directly connected, eth0
C 127.0.0.0/8 is directly connected, lo #sh
ip bgp
BGP table version is 2, local router ID is 10.12.4.196
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network           Next Hop           Metric     LocPrf      Weight Path
*>   100.100.100.100/32
                     1.1.1.1             0         100         0       100 i Total
number of prefixes 1
```

R1

```
    #sh bgp neighbors
    BGP neighbor is 1.1.1.2, remote AS 200, local AS 100, external link
      BGP version 4, remote router ID 10.12.4.196
      BGP state = Established, up for 00:04:18
      Last read 00:04:18, hold time is 90, keepalive interval is 30 seconds
      Neighbor capabilities:
        Route refresh: advertised and received (old and new)
        Address family IPv4 Unicast: advertised and received
      Received 10 messages, 0 notifications, 0 in queue
      Sent 10 messages, 0 notifications, 0 in queue
      Route refresh request: received 0, sent 0
      Minimum time between advertisement runs is 30
     seconds For address family: IPv4 IPv4
      BGP table version 6, neighbor version 6
      Index 1, Offset 0, Mask 0x2
      Community attribute sent to this neighbor (both)
      0 accepted prefixes
    0 announced prefixes

     Connections established 1; dropped 0
    Local host: 1.1.1.1, Local port: 179
    Foreign host: 1.1.1.2, Foreign port: 45966
    Nexthop: 1.1.1.1
    Nexthop global: fe80::a00:27ff:feca:b09a
```

```
Nexthop local: ::
BGP connection: non shared network

#sh ip bgp summary
BGP router identifier 10.12.4.142, local AS number 100
BGP table version is 6
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS    MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
 Down   State/PfxRcd
1.1.1.2                  4   200   11          11       6      0      0
00:04:41              0

Total number of neighbors 1

Total number of Established sessions 1
```

R3

```
#sh ip bgp
BGP table version is 2, local router ID is 10.12.4.197
Status codes: s suppressed, d damped, h history, * valid, > best, i -
 internal, l - labeled               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network          Next Hop            Metric    LocPrf       Weight Path
*>i  100.100.100.100/32
                     1.1.1.1              0        100          0       100 i
Total number of prefixes 1
#sh ip bgp neighbors
BGP neighbor is 3.3.3.2, remote AS 200, local AS 200, internal
  link BGP version 4, remote router ID 10.12.4.196
  BGP state = Established, up for 00:08:38
  Last read 00:08:38, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 20 messages, 0 notifications, 0 in queue
  Sent 19 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv4 IPv4
  BGP table version 2, neighbor version 2
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 3.3.3.1, Local port: 54514
Foreign host: 3.3.3.2, Foreign port: 179
```

```
Nexthop: 3.3.3.1
Nexthop global: fe80::a00:27ff:fe9b:d954
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 5.5.5.2, remote AS 200, local AS 200, internal
  link BGP version 4, remote router ID 10.12.4.152
  BGP state = Established, up for 00:11:57
  Last read 00:11:57, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 25 messages, 0 notifications, 0 in queue
  Sent 26 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv4 IPv4
  BGP table version 2, neighbor version 2
  Index 2, Offset 0, Mask 0x4
  Route-Reflector Client
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 5.5.5.1, Local port: 179
Foreign host: 5.5.5.2, Foreign port: 34757
Nexthop: 5.5.5.1
Nexthop global: fe80::a00:27ff:fe42:fb7a
Nexthop local: ::
BGP connection: non shared network

#sh ip bgp summary
BGP router identifier 10.12.4.197, local AS number
    200 BGP table version is 2
  1 BGP AS-PATH entries
    0 BGP community entries

    Neighbor                 V   AS    MsgRcv    MsgSen TblVer   InQ   OutQ   Up/
    Down   State/PfxRcd
    3.3.3.2                   4   200    21          20       2       0       0
    00:09:03                 1
    5.5.5.2                   4   200    26          27       2       0       0
    00:12:22                 0

    Total number of neighbors 2

    Total number of Established sessions 2
```

R4

```
    #sh ip bgp
```

```
BGP table version is 2, local router ID is 10.12.4.185
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric     LocPrf      Weight Path
*>i  100.100.100.100/32
                    1.1.1.1             0         100          0       100 i

Total number of prefixes 1
#sh ip bgp neighbors
BGP neighbor is 4.4.4.2, remote AS 200, local AS 200, internal link
  BGP version 4, remote router ID 10.12.4.196
  BGP state = Established, up for 00:19:52
  Last read 00:19:52, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 42 messages, 0 notifications, 0 in queue
  Sent 41 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv4 IPv4
  BGP table version 2, neighbor version 2
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 4.4.4.1, Local port: 39999
Foreign host: 4.4.4.2, Foreign port: 179
Nexthop: 4.4.4.1
Nexthop global: fe80::a00:27ff:fe09:fd25
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 6.6.6.2, remote AS 200, local AS 200, internal link
  BGP version 4, remote router ID 10.12.4.152
  BGP state = Established, up for 00:10:45
  Last read 00:10:45, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 23 messages, 0 notifications, 0 in queue
  Sent 24 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv4 IPv4
  BGP table version 2, neighbor version 2
```

```
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
0 announced prefixes

 Connections established 1; dropped 0
Local host: 6.6.6.1, Local port: 179
Foreign host: 6.6.6.2, Foreign port: 51885
Nexthop: 6.6.6.1
Nexthop global: fe80::a00:27ff:fe52:45f6
Nexthop local: ::
BGP connection: non shared network

#sh ip bgp summary
BGP router identifier 10.12.4.185, local AS number 200
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS    MsgRcv    MsgSen TblVer   InQ   OutQ   Up/
Down   State/PfxRcd
4.4.4.2                   4   200    42         41       2      0      0
00:19:58                1
6.6.6.2                   4   200    23         24       2      0      0
00:10:51                0

Total number of neighbors 2

Total number of Established sessions 2
```

R5

```
#sh ip bgp
BGP table version is 2, local router ID is 10.12.4.152
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network           Next Hop            Metric     LocPrf      Weight Path
*>i  100.100.100.100/32
                     1.1.1.1              0         100          0       100 i

Total number of prefixes 1
#sh ip bgp neighbors
BGP neighbor is 5.5.5.1, remote AS 200, local AS 200, internal link
  BGP version 4, remote router ID 10.12.4.197
BGP state = Established, up for 00:13:59
Last read 00:13:59, hold time is 90, keepalive interval is 30 seconds
Neighbor capabilities:
  Route refresh: advertised and received (old and new)
  Address family IPv4 Unicast: advertised and received
Received 30 messages, 0 notifications, 0 in queue
```

```
  Sent 29 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv4 IPv4
  BGP table version 2, neighbor version 2
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 5.5.5.2, Local port: 34757
Foreign host: 5.5.5.1, Foreign port: 179
Nexthop: 5.5.5.2
Nexthop global: fe80::a00:27ff:fe9c:f35d
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 6.6.6.1, remote AS 200, local AS 200, internal
  link BGP version 4, remote router ID 10.12.4.185
  BGP state = Established, up for 00:11:19
  Last read 00:11:19, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 24 messages, 0 notifications, 0 in queue
  Sent 24 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv4 IPv4
  BGP table version 2, neighbor version 2
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
0 announced prefixes

 Connections established 1; dropped 0
Local host: 6.6.6.2, Local port: 51885
Foreign host: 6.6.6.1, Foreign port: 179
Nexthop: 6.6.6.2
Nexthop global: fe80::a00:27ff:fe6d:d83e
Nexthop local: ::
BGP connection: non shared network

#sh ip bgp summary
BGP router identifier 10.12.4.152, local AS number
200 BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries
```

```
Neighbor                 V    AS    MsgRcv    MsgSen TblVer    InQ    OutQ    Up/
 Down    State/PfxRcd
5.5.5.1                   4    200    31         30       2       0       0
00:14:05                 1
6.6.6.1                   4    200    24         24       2       0       0
00:11:25                 0

Total number of neighbors 2

Total number of Established sessions 2
```

BGP Confederations

In BGP, nodes running iBGP protocols must be interconnected forming a full mesh. Confederation solves the iBGP fullmesh network complexity and inefficiency by splitting a large autonomous system domain into smaller autonomous system domains, called member autonomous systems. Member autonomous systems can form eBGP connections among themselves, to prevent full-mesh connections among each iBGP-running node.

The `bgp confederation identifier` command tells the router that it is a member of a confederation and the confederation ID. The `bgp confederation peers` command lists the member AS to which the router is connected.

In the following example, R1, R2, and R3 are members of the same confederation with different AS numbers.

Topology

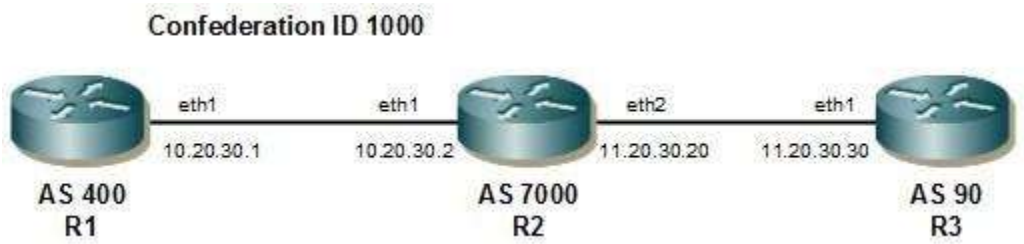


Figure 1-77: BGP Confederation

R1

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 400`	Assign the ASN value (`400`) to the router.
`(config-router)#bgp confederation identifier 1000`	Specify the BGP confederation ID, the externally visible autonomous system number that identifies the BGP confederation as a whole.
`(config-router)#bgp confederation peers 7000`	Specify the neighbor ASN value for confederation membership.
`(config-router)#neighbor 10.20.30.2 remote-as 7000`	Specify the neighbor's IP address (`10.20.30.2`) and the ASN value of the neighbor (`7000`).
`(config-router)#end`	Exit router and configure mode

R2

`#configure terminal`	Enter Configure mode.

(config)#router bgp 7000	Assign the ASN value (7000) to the router.
(config-router)#bgp confederation identifier 1000	Specify the BGP confederation ID.
(config-router)#bgp confederation peers 400 90	Specify the neighbor ASN values for confederation membership.
(config-router)#neighbor 10.20.30.1 remote-as 400	Specify the neighbor's IP address (10.20.30.1) and the ASN value of the neighbor (400).
(config-router)#neighbor 11.20.30.30 remoteas 90	Specify the neighbor's IP address (11.20.30.30) and the ASN value of the neighbor (90).
(config-router)#end	Exit router and configure mode

R3

#configure terminal	Enter Configure mode.
(config-router)#router bgp 90	Assign the ASN value (90) to the router.
(config-router)#bgp confederation identifier 1000	Specify the BGP confederation ID.
(config-router)#bgp confederation peers 7000	Specify the neighbor ASN value for confederation membership.
(config-router)#neighbor 11.20.30.20 remote-as 7000	Specify the neighbor's IP address (11.20.30.20) and the ASN value of the neighbor (7000).
(config-router)#end	Exit router and configure mode

Validation:

```
#sh ip bgp summary
BGP router identifier 192.168.56.101, local AS number 7000
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V    AS   MsgRcv    MsgSen TblVer   InQ   OutQ   Up/
Down   State/PfxRcd
10.20.30.1               4    400    5          5       1      0      0
00:01:36                0
11.20.30.30              4     90    2          3       1      0      0
00:00:24                0

Total number of neighbors 2

Total number of Established sessions 2

#sh ip bgp neighbors
BGP neighbor is 10.20.30.1, remote AS 400, local AS 7000, external link
  BGP version 4, remote router ID 1.1.1.1
  Neighbor under common administration
  BGP state = Established, up for 00:01:25
  Last read 00:01:25, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
```

```
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 4 messages, 0 notifications, 0 in queue
  Sent 4 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30
 seconds For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.20.30.2, Local port: 35108
Foreign host: 10.20.30.1, Foreign port: 179
Nexthop: 10.20.30.2
Nexthop global: fe80::a00:27ff:fe21:7ed2
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 11.20.30.30, remote AS 90, local AS 7000, external link
  BGP version 4, remote router ID 192.168.56.103
  Neighbor under common administration
  BGP state = Established, up for 00:00:13
  Last read 00:00:13, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 2 messages, 0 notifications, 0 in queue
  Sent 3 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30
 seconds For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0 Local
host: 11.20.30.20, Local port: 179 Foreign
host: 11.20.30.30, Foreign port: 33465
Nexthop: 11.20.30.20
Nexthop global: fe80::a00:27ff:fed0:57d1
Nexthop local: ::
BGP connection: non shared network
```

R1

```
#sh ip bgp neighbors
BGP neighbor is 10.20.30.2, remote AS 7000, local AS 400, external link
  BGP version 4, remote router ID 192.168.56.101
  Neighbor under common administration
  BGP state = Established, up for 00:01:51
  Last read 00:01:51, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 5 messages, 0 notifications, 0 in queue
  Sent 6 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30
 seconds For address family: IPv4 IPv4
  BGP table version 3, neighbor version 3
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
0 announced prefixes

 Connections established 1; dropped 0 Local
host: 10.20.30.1, Local port: 179 Foreign
host: 10.20.30.2, Foreign port: 35108
Nexthop: 10.20.30.1
Nexthop global: fe80::a00:27ff:fe50:6a9b
Nexthop local: ::
BGP connection: non shared network


#sh ip bgp summary
BGP router identifier 1.1.1.1, local AS number
400 BGP table version is 3
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS    MsgRcv    MsgSen TblVer   InQ   OutQ   Up/
Down   State/PfxRcd
10.20.30.2               4   7000    5          6       3      0      0
00:01:57                0

Total number of neighbors 1

Total number of Established sessions 1
```

R3

```
#sh ip bgp neighbors
BGP neighbor is 11.20.30.20, remote AS 7000, local AS 90, external link
  BGP version 4, remote router ID 192.168.56.101
  Neighbor under common administration
  BGP state = Established, up for 00:00:04
```

```
  Last read 00:00:04, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 2 messages, 0 notifications, 0 in queue
  Sent 2 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30
 seconds For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 11.20.30.30, Local port: 33465
Foreign host: 11.20.30.20, Foreign port: 179
Nexthop: 11.20.30.30
Nexthop global: fe80::a00:27ff:fe24:5dc9
Nexthop local: ::
BGP connection: non shared network

#sh ip bgp summary
BGP router identifier 192.168.56.103, local AS number 90
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS    MsgRcv    MsgSen TblVer   InQ   OutQ   Up/
Down   State/PfxRcd
11.20.30.20               4   7000    3          3       1      0      0
00:00:55               0

Total number of neighbors 1

Total number of Established sessions 1
```

Multiple Autonomous Systems

In the following example, R1 and R2 are members of the same confederation with the same AS numbers, and R3 is a member of the same confederation with a different AS number.

Topology

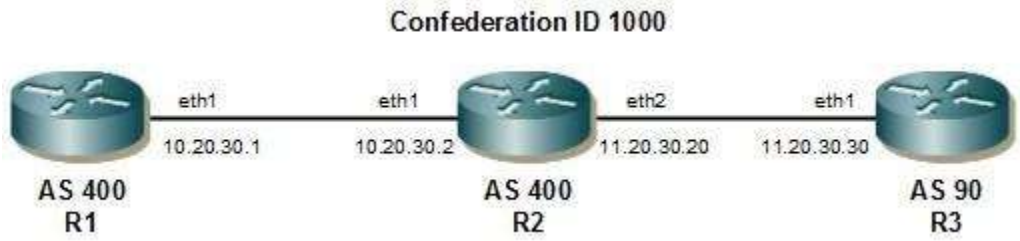


Figure 1-78: BGP Confederation with Multiple AS

R1

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 400`	Assign the ASN value (`400`) to the router.
`(config-router)#bgp confederation identifier 1000`	Specify the BGP confederation ID.
`(config-router)#neighbor 10.20.30.2 remote-as 400`	Specify the neighbor's IP address (`10.20.30.2`) and the ASN value of the neighbor (`400`).

R2

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 400`	Assign the ASN value (`400`) to the router.
`(config-router)#bgp confederation identifier 1000`	Specify the BGP confederation ID.
`(config-router)#bgp confederation peers 90`	Specify the neighbor ASN value for confederation membership.
`(config-router)#neighbor 10.20.30.1 remote-as 400`	Specify the neighbor's IP address (`10.20.30.1`) and the ASN value of the neighbor (`400`).
`(config-router)#neighbor 11.20.30.30 remoteas 90`	Specify the neighbor's IP address (`11.20.30.30`) and the ASN value of the neighbor (`90`).

R3

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 90`	Assign the ASN value (`90`) to the router.
`(config-router)#bgp confederation identifier 1000`	Specify the BGP confederation ID.
`(config-router)#bgp confederation peers 400`	Specify the neighbor ASN value for confederation membership.
`(config-router)#neighbor 11.20.30.20 remoteas 400`	Specify the neighbor's IP address (`11.20.30.20`) and the ASN value of the neighbor (`400`).

Validation:

R2

```
#sh ip bgp summary
BGP router identifier 192.168.56.101, local AS number 400
BGP table version is 1
```

```
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V    AS   MsgRcv    MsgSen TblVer   InQ   OutQ   Up/
Down   State/PfxRcd
10.20.30.1               4    400   16         16       1      0      0
00:07:27                0
11.20.30.30              4     90   32         42       1      0      0
00:00:27                0

Total number of neighbors 2

Total number of Established sessions 2
#sh ip bgp neighbors
BGP neighbor is 10.20.30.1, remote AS 400, local AS 400, internal
  link BGP version 4, remote router ID 1.1.1.1
  BGP state = Established, up for 00:08:10
  Last read 00:08:10, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 18 messages, 0 notifications, 0 in queue
  Sent 18 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 10.20.30.2, Local port: 35214
Foreign host: 10.20.30.1, Foreign port: 179
Nexthop: 10.20.30.2
Nexthop global: fe80::a00:27ff:fe21:7ed2
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 11.20.30.30, remote AS 90, local AS 400, external
  link BGP version 4, remote router ID 192.168.56.103
  Neighbor under common administration
  BGP state = Established, up for 00:01:10
  Last read 00:01:10, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 20 messages, 14 notifications, 0 in queue
  Sent 42 messages, 2 notifications, 0 in queue
  Route refresh request: received 0, sent 0
```

```
  Minimum time between advertisement runs is 30
 seconds For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 11.20.30.20, Local port: 179
Foreign host: 11.20.30.30, Foreign port: 33623
Nexthop: 11.20.30.20
Nexthop global: fe80::a00:27ff:fed0:57d1
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:01:36, due to BGP Notification sent
Notification Error Message: (OPEN Message Error/Bad Peer AS.)
```

R1

```
#sh ip bgp neighbors
BGP neighbor is 10.20.30.2, remote AS 400, local AS 400, internal
  link BGP version 4, remote router ID 192.168.56.101
  BGP state = Established, up for 00:08:41
  Last read 00:08:41, hold time is 90, keepalive interval is 30 seconds
Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 34 messages, 0 notifications, 0 in queue
  Sent 35 messages, 3 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv4 IPv4
  BGP table version 16, neighbor version 16
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 2; dropped 1
Local host: 10.20.30.1, Local port: 179
Foreign host: 10.20.30.2, Foreign port: 35214
Nexthop: 10.20.30.1
Nexthop global: fe80::a00:27ff:fe50:6a9b
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:09:03, due to BGP Notification sent
Notification Error Message: (OPEN Message Error/Bad Peer AS.)

#sh ip bgp summary
```

```
BGP router identifier 1.1.1.1, local AS number
400 BGP table version is 16
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS    MsgRcv    MsgSen TblVer   InQ   OutQ   Up/
Down   State/PfxRcd
10.20.30.2               4   400    34         38      16      0      0
00:08:44                0

Total number of neighbors 1

Total number of Established sessions 1
```

R3

```
#sh ip bgp summary
BGP router identifier 192.168.56.103, local AS number 90
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS    MsgRcv    MsgSen TblVer   InQ   OutQ   Up/
Down   State/PfxRcd
11.20.30.20              4   400     2          2       1      0      0
00:00:15                0

Total number of neighbors 1

Total number of Established sessions 1
#sh ip bgp summary
BGP router identifier 192.168.56.103, local AS number 90
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS    MsgRcv    MsgSen TblVer   InQ   OutQ   Up/
Down   State/PfxRcd
11.20.30.20              4   400     6          6       1      0      0
00:02:19                0

Total number of neighbors 1

Total number of Established sessions 1 x86_64-
debian#sh ip bgp neighbors
BGP neighbor is 11.20.30.20, remote AS 400, local AS 90, external
  link BGP version 4, remote router ID 192.168.56.101
  Neighbor under common administration
  BGP state = Established, up for 00:02:24
  Last read 00:02:24, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
```

```
  Received 6 messages, 0 notifications, 0 in queue
  Sent 6 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30
 seconds For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 11.20.30.30, Local port: 33623
Foreign host: 11.20.30.20, Foreign port: 179
Nexthop: 11.20.30.30
Nexthop global: fe80::a00:27ff:fe24:5dc9
Nexthop local: ::
BGP connection: non shared network
```

Outside Autonomous System

In the following example, R1 and R2 are members of the same confederation with different AS numbers, and R3 is a member outside the confederation.

Topology

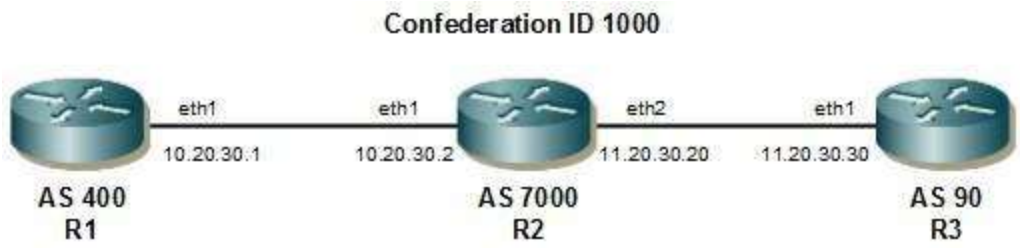


Figure 1-79: Single Confederation with Outside AS

R1

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 400`	Assign the ASN value (`400`) to the router.
`(config-router)#bgp confederation identifier 1000`	Specify the BGP confederation ID.
`(config-router)#bgp confederation peers 7000`	Specify the neighbor ASN value for confederation membership.
`(config-router)#neighbor 10.20.30.2 remote-as 7000`	Specify the neighbor's IP address (`10.20.30.2`) and the ASN value of the neighbor (`7000`).

R2

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 7000`	Assign the ASN value (`7000`) to the router.

`(config-router)#bgp confederation identifier 1000`	Specify the BGP confederation ID.
`(config-router)#bgp confederation peers 400`	Specify the neighbor ASN value for confederation membership.
`(config-router)#neighbor 10.20.30.1 remote-as 400`	Specify the neighbor's IP address (`10.20.30.1`) and the ASN value of the neighbor (`400`).
`(config-router)#neighbor 11.20.30.30 remoteas 90`	Specify the neighbor's IP address (`11.20.30.30`) and the ASN value of the neighbor (`90`).

R3

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 90`	Assign the ASN value (`90`) to the router.
`(config-router)#neighbor 11.20.30.20 remote-as 1000`	Specify the neighbor's IP address (`11.20.30.20`) and the BGP confederation ID (`1000`).

Validation

R3

```
#sh ip bgp neighbors
BGP neighbor is 11.20.30.20, remote AS 1000, local AS 90, external link
  BGP version 4, remote router ID 192.168.56.101
  BGP state = Established, up for 00:01:10
  Last read 00:01:10, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 112 messages, 1 notifications, 0 in queue
  Sent 142 messages, 88 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30
 seconds For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 2; dropped 1
Local host: 11.20.30.30, Local port: 33951
Foreign host: 11.20.30.20, Foreign port: 179
Nexthop: 11.20.30.30
Nexthop global: fe80::a00:27ff:fe24:5dc9
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:01:26, due to BGP Notification sent
Notification Error Message: (OPEN Message Error/Bad Peer AS.)

#sh ip bgp summary
```

```
BGP router identifier 192.168.56.103, local AS number 90
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS    MsgRcv     MsgSen TblVer   InQ   OutQ   Up/
Down   State/PfxRcd
11.20.30.20               4   1000 113         230       1      0      0
00:01:13                0

Total number of neighbors 1

Total number of Established sessions 1
```

R2

```
#sh ip bgp summary
BGP router identifier 192.168.56.101, local AS number 7000
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V    AS   MsgRcv    MsgSen TblVer   InQ   OutQ   Up/
Down   State/PfxRcd
10.20.30.1                4    400   22          22       1      0      0
00:10:04                0
11.20.30.30               4     90  179         202       1      0      0
00:00:42                0

Total number of neighbors 2

Total number of Established sessions 2
#sh ip bgp neighbors
BGP neighbor is 10.20.30.1, remote AS 400, local AS 7000, external link
  BGP version 4, remote router ID 1.1.1.1
  Neighbor under common administration
  BGP state = Established, up for 00:11:06
  Last read 00:11:06, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 24 messages, 0 notifications, 0 in queue
  Sent 24 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30
 seconds For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes
```

```
 Connections established 1; dropped 0 Local
host: 10.20.30.2, Local port: 35444 Foreign
host: 10.20.30.1, Foreign port: 179
Nexthop: 10.20.30.2
Nexthop global: fe80::a00:27ff:fe21:7ed2
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 11.20.30.30, remote AS 90, local AS 1000, external link
  BGP version 4, remote router ID 192.168.56.103
  BGP state = Established, up for 00:01:44
  Last read 00:01:44, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 93 messages, 88 notifications, 0 in queue
  Sent 204 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30
 seconds For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 11.20.30.20, Local port: 179
Foreign host: 11.20.30.30, Foreign port: 33951
Nexthop: 11.20.30.20
Nexthop global: fe80::a00:27ff:fed0:57d1
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:02:00, due to BGP Notification received
Notification Error Message: (OPEN Message Error/Bad Peer AS.)
```

R1

```
#sh ip bgp summary
BGP router identifier 1.1.1.1, local AS number
400 BGP table version is 34
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS    MsgRcv    MsgSen TblVer   InQ   OutQ   Up/
Down   State/PfxRcd
10.20.30.2               4   7000   77         91      34      0      0
00:10:18               0

Total number of neighbors 1
```

```
Total number of Established sessions 1
#sh ip bgp neighbors
BGP neighbor is 10.20.30.2, remote AS 7000, local AS 400, external link
  BGP version 4, remote router ID 192.168.56.101
  Neighbor under common administration
  BGP state = Established, up for 00:11:40
  Last read 00:11:40, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 80 messages, 0 notifications, 0 in queue
  Sent 82 messages, 12 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30
 seconds For address family: IPv4 IPv4
  BGP table version 35, neighbor version 35
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 3; dropped 2
Local host: 10.20.30.1, Local port: 179
Foreign host: 10.20.30.2, Foreign port: 35444
Nexthop: 10.20.30.1
Nexthop global: fe80::a00:27ff:fe50:6a9b
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:12:47, due to BGP Notification sent
Notification Error Message: (OPEN Message Error/Bad Peer AS.)
```

BGP Authentication

BGP authentication allows users to receive selected routing information, enhancing security of their network traffic. When BGP authentication is enabled on a router, the router verifies routing packets it receives by exchanging a password that is configured on both the sending and receiving routers.

In this example, both R1 and R2 have `ABC` as the password. Configure the same password on all routers that are to communicate using BGP in a network.

Topology

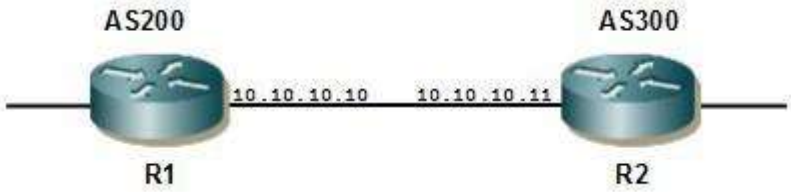


Figure 1-80: BGP Authentication

R1

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 200`	Define the routing process. The number `200` specifies the AS number of R1.
`(config-router)#neighbor 10.10.10.11 remoteas 300`	Define BGP neighbors, and establish a TCP session. `10.10.10.11` is the IP address of the neighbor (R2), and `300` is the neighbor's AS number.
`(config-router)#neighbor 10.10.10.11 password ABC`	Specify the password.

R2

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 300`	Define the routing process. The number `300` specifies the AS number of R2.
`(config-router)#neighbor 10.10.10.10 remoteas 200`	Define BGP neighbors, and establish a TCP session. `10.10.10.10` is the IP address of the neighbor (R1), and `200` is the neighbor's AS number.
`(config-router)#neighbor 10.10.10.10 password ABC`	Specify the password.

Validation

```
#sh ip bgp neighbors
BGP neighbor is 10.10.10.10, remote AS 200, local AS 300, external link
  BGP version 4, remote router ID 192.168.56.101
  BGP state = Established, up for 00:09:18
  Last read 00:09:18, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 20 messages, 0 notifications, 0 in queue
  Sent 20 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30
 seconds For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0 Local
host: 10.10.10.11, Local port: 53545 Foreign
host: 10.10.10.10, Foreign port: 179
Nexthop: 10.10.10.11
Nexthop global: fe80::a00:27ff:fe50:6a9b
Nexthop local: ::
```

```
BGP connection: non shared network
```

Dynamic BGP Peering

BGP Dynamic Neighbors is a quick way of setting up BGP on device like a Hub router where user is expecting numerous BGP neighbors. Before dynamic neighbors, user had to provide a large amount of configuration to work with all these neighbors. This new feature dramatically reduces the amount and complexity of CLI configuration on the router and save CPU and memory usage.

BGP dynamic neighbor support allows BGP peering to a group of remote neighbors that are defined by a range of IP addresses. Each range can be configured as a subnet IP address. BGP dynamic neighbors are configured using a range of IP addresses and BGP peer groups.

After a subnet range is configured for a BGP peer group and a TCP session is initiated by another router for an IP address in the subnet range, a new BGP neighbor is dynamically created as a member of that group. After the initial configuration of subnet ranges and activation of the peer group, dynamic BGP neighbor creation does not require any further CLI configuration on the initial router. Other routers can establish a BGP session with the initial router, but the initial router need not establish a BGP session to other routers if the IP address of the remote peer used for the BGP session is not within the configured range.

A dynamic BGP neighbor will inherit any configuration for the peer group. In larger BGP networks, implementing BGP dynamic neighbors can reduce the amount and complexity of CLI configuration and save CPU and memory usage. Both IPv4 and IPV6 peering is supported.

IPv4 IBGP Configuration

Below figure displays the minimum configuration required to enable BGP on an interface. R1 and R2 are two routers belonging to the same AS, AS100, connecting to network 11.11.11.0/24 and 11.11.12.0/24. First, define the routing process and the AS number to which the routers belong. Then, define BGP neighbors to start exchanging routing updates.

Topology

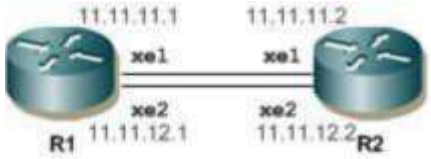


Figure 1-81: IPv4 IBGP Peering

R1

`#configure terminal`	Enter Configure mode.
`(config)#interface lo`	Enter Interface mode for loopback.
`(config-if)#ip address 33.33.33.33/32 secondary`	Assign a secondary IP address.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe1`	Enter Interface mode for xe1.
`(config-if)#ip address 11.11.11.1/24`	Assign IP address to the interface.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe2`	Enter Interface mode for xe2.

(config-if)#ip add 11.11.12.1/24	Assign IP address to the interface.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router bgp 100	Enter Router BGP mode.
(config-router)#bgp router-id 1.1.1.1	Assign a BGP router ID.
(config-router)#neighbor IPV4_IBGP_PEER peergroup range 11.11.0.0/16	Create a dynamic peer-group, IPV4_IBGP_PEER with a dynamic range 11.11.0.0/16
(config-router)#neighbor IPV4_IBGP_PEER remote-as 100	Assign a remote AS for the peer-group, IPV4_IBGP_PEER.
(config-router)#network 33.33.33.33/32	Advertise the loopback network into BGP.
(config-router)#end	Exit from Router BGP mode.

R2

#configure terminal	Enter Configure mode.
(config)#interface lo	Enter Interface mode for loopback.
(config-if)#ip address 22.22.22.22/32	Assign a secondary IP address.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe1	Enter Interface mode for xe1.
(config-if)#ip address 11.11.11.2/24	Assign IP address to the interface.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe2	Enter Interface mode for xe2.
(config-if)#ip add 11.11.12.2/24	Assign IP address to the interface.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router bgp 100	Enter Router BGP mode.
(config-router)#bgp router-id 2.2.2.2	Assign a BGP router ID.
(config-router)#neighbor 11.11.11.1 remote-as 100	Create a static BGP neighbor 11.11.11.1 in remote AS 100.
(config-router)#neighbor 11.11.12.1 remote-as 100	Create a static BGP neighbor 11.11.12.1 in remote AS 100.
(config-router)#network 22.22.22.22/32	Advertise the loopback network into BGP.
(config-router)#end	Exit from Router BGP mode.

Validation

R1

```
#show ip bgp summary

BGP router identifier 1.1.1.1, local AS number
100 BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries
```

```
Neighbor                 V    AS    MsgRcv    MsgSen TblVer    InQ    OutQ    Up/
Down   State/PfxRcd
*11.11.11.2               4   100     42         43       2       0       0
00:20:25                 1
*11.11.12.2               4   100     42         43       2       0       0
00:20:25                 1
* Dynamically created based on a listen range command

BGP dynamic peer-group: IPV4_IBGP_PEER
listen range:  11.11.0.0/16
  Total number of dynamically created neighbors/limit: 2/(200)

Total number of dynamically created neighbors: 2
Total number of activated dynamic peer-groups for IPv4 Unicast address-family:
1

Total number of neighbors 2
Total number of Established sessions 2


#show ip bgp neighbors

BGP neighbor is 11.11.11.2, remote AS 100, local AS 100, internal
 link Member of peer-group IPV4_IBGP_PEER for session parameters
  BGP version 4, local router ID 1.1.1.1, remote router ID
  2.2.2.2 BGP state = Established, up for 00:21:56
  Last read 00:00:27, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 46 messages, 0 notifications, 0 in queue
  Sent 46 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 0, Offset 0, Mask 0x1
  IPV4_IBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0 Local
host: 11.11.11.1, Local port: 40361 Foreign
host: 11.11.11.2, Foreign port: 179
Nexthop: 11.11.11.1
Nexthop global: :: Nexthop local:
::
BGP connection: non shared network

BGP neighbor is 11.11.12.2, remote AS 100, local AS 100, internal link
```

```
 Member of peer-group IPV4_IBGP_PEER for session parameters
  BGP version 4, local router ID 1.1.1.1, remote router ID
  2.2.2.2 BGP state = Established, up for 00:21:56
  Last read 00:00:27, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 46 messages, 0 notifications, 0 in queue
  Sent 46 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 1, Offset 0, Mask 0x2
  IPV4_IBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0 Local
host: 11.11.12.1, Local port: 33478 Foreign
host: 11.11.12.2, Foreign port: 179 Nexthop:
11.11.12.1 Nexthop global: :: Nexthop local:
::
BGP connection: non shared network

#show running-config bgp

router bgp 100  bgp router-id
1.1.1.1  network 33.33.33.33/32
 neighbor IPV4_IBGP_PEER peer-group range 11.11.0.0/16 neighbor
IPV4_IBGP_PEER remote-as 100


#show ip bgp
BGP table version is 3, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric     LocPrf      Weight Path
*>i   22.22.22.22/32   11.11.11.2             0         100           0       i
* i                    11.11.12.2             0         100           0       i *>
33.33.33.33/32    0.0.0.0             0         100           32768   i

Total number of prefixes 2
```

R2

```
    #show ip bgp summary
    BGP router identifier 2.2.2.2, local AS number 100
    BGP table version is 3
    1 BGP AS-PATH entries
```

```
0 BGP community entries

Neighbor                 V   AS    MsgRcv    MsgSen TblVer   InQ   OutQ   Up/
 Down   State/PfxRcd
11.11.11.1                4   100    55         56       3      0      0
00:26:21                 1
11.11.12.1                4   100    55         56       3      0      0
00:26:21                 1

Total number of neighbors 2
Total number of Established sessions 2


#show bgp neighbors
BGP neighbor is 11.11.11.1, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 2.2.2.2, remote router ID 1.1.1.1
  BGP state = Established, up for 00:26:43
  Last read 00:00:14, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 56 messages, 0 notifications, 0 in queue
  Sent 57 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 0, Offset 0, Mask 0x1
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0 Local
host: 11.11.11.2, Local port: 179 Foreign
host: 11.11.11.1, Foreign port: 40361 Nexthop:
11.11.11.2 Nexthop global: :: Nexthop local:
::
BGP connection: non shared network

BGP neighbor is 11.11.12.1, remote AS 100, local AS 100, internal link
  BGP version 4, local router ID 2.2.2.2, remote router ID 1.1.1.1
  BGP state = Established, up for 00:26:43
  Last read 00:00:14, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 56 messages, 0 notifications, 0 in queue
  Sent 57 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv4 Unicast
```

```
  BGP table version 3, neighbor version 3
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0 Local
host: 11.11.12.2, Local port: 179 Foreign
host: 11.11.12.1, Foreign port: 33478 Nexthop:
11.11.12.2 Nexthop global: :: Nexthop local:
::
BGP connection: non shared network

#show ip bgp
BGP table version is 3, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i -
              internal, l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network          Next Hop            Metric    LocPrf      Weight Path
*>    22.22.22.22/32  0.0.0.0              0         100            32768    i
*>i   33.33.33.33/32  11.11.11.1             0         100            0        i
* i                    11.11.12.1             0         100            0        i

Total number of prefixes 2
```

IPv4 IBGP VRF Configuration

Below figure displays the minimum configuration required to enable BGP on an interface with vrf enabled on the device and interface being part of vrf. R1 and R2 are two routers belonging to the same AS, AS100, connecting to network 11.11.11.0/24 and 11.11.12.0/24. First, define the routing process and the AS number to which the routers belong. Then, define BGP neighbors to start exchanging routing updates.

Topology

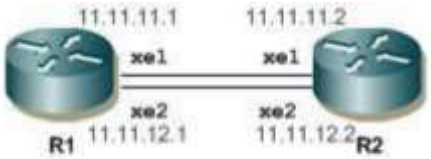


Figure 1-82: IPv4 VRF IBGP Peering

R1

#Configure terminal	Enter Configuration mode.
(config)#ip vrf vrfA	Create a VRF, vrfA on the router.
(config-vrf)#rd 1:1	Assign a route distinguisher to VRF.
(config-if)#exit	Exit VRF mode and return to Configure mode.
(config)#interface xe1	Enter Interface mode for xe1.
(config-if)# ip vrf forwarding vrfA	Assign IP address to VRF.

(config-if)#ip address 11.11.11.1/24	Assign IP address to the interface.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe2	Enter Interface mode for xe2.
(config-if)# ip vrf forwarding vrfA	Assign IP address to VRF.
(config-if)#ip add 11.11.12.1/24	Assign IP address to the interface.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router bgp 100	Enter Router BGP mode.
(config-router)#bgp router-id 1.1.1.1	Assign a BGP router ID.
(config-router)#address-family ipv4 vrf	Enter IPv4 VRF Address Family.
(config-router)#neighbor IPV4_IBGP_PEER peergroup range 11.11.0.0/16	Create a dynamic peer-group, IPV4_IBGP_PEER with a dynamic range 11.11.0.0/16.
(config-router)#neighbor IPV4_IBGP_PEER remote-as 100	Assign a remote AS for the peer-group, IPV4_IBGP_PEER.
(config-router)#network 33.33.33.33/32	Advertise the loopback network into BGP
(config-router)#end	Exit from Router BGP mode.

R2

#configure terminal	Enter Configure mode.
(config)#ip vrf vrfA	Create a VRF, vrfA on router.
(config-vrf)#rd 2:1	Assign a route distinguisher to VRF.
(config-if)#exit	Exit VRF mode and return to Configure mode.
(config)#interface xe1	Enter Interface mode for xe1.
(config-if)# ip vrf forwarding vrfA	Assign IP address to VRF.
(config-if)#ip address 11.11.11.2/24	Assign IP address to the interface.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe2	Enter Interface mode for xe2.
(config-if)# ip vrf forwarding vrfA	Assign IP address to VRF.
(config-if)#ip add 11.11.12.2/24	Assign IP address to the interface.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router bgp 100	Enter Router BGP mode.
(config-router)#bgp router-id 2.2.2.2	Assign a BGP router ID.
(config-router)#address-family ipv4 vrf vrfA	Enter IPv4 VRF Address Family.
(config-router)#neighbor 11.11.11.1 remote-as 100	Create a static BGP neighbor 11.11.11.1 in remote AS 100.
(config-router)#neighbor 11.11.12.1 remote-as 100	Create a static BGP neighbor 11.11.12.1 in remote AS 100
(config-router)#network 22.22.22.22/32	Advertise the loopback network into BGP.
(config-router)#end	Exit from Router BGP mode.

Validation

R1

```
#show running-config bgp
! router bgp 100 bgp
router-id 1.1.1.1
 !  address-family ipv4
vrf vrfA
 neighbor IPV4_VRF_IBGP_PEER peer-group range
11.11.0.0/16 neighbor IPV4_VRF_IBGP_PEER remote-as 100
neighbor IPV4_VRF_IBGP_PEER activate
 neighbor IPV4_VRF_IBGP_PEER send-community
extended exit-address-family !

#show ip bgp summary vrf vrfA
BGP router identifier 11.11.11.1, local AS number 100
BGP VRF vrfA Route Distinguisher: 1:1
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS    MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
*11.11.11.2              4   100    50         50       1      0      0
00:24:06               0
*11.11.12.2              4   100    50         50       1      0      0 00:24:06
0

* Dynamically created based on a listen range command

BGP dynamic peer-group: IPV4_VRF_IBGP_PEER
listen range:  11.11.0.0/16
  Total number of dynamically created neighbors/limit: 2/(200)

Total number of dynamically created neighbors: 1
Total number of activated dynamic peer-groups for IPv4 Unicast address-family:
1

Total number of neighbors 2
Total number of Established sessions 2


#show bgp neighbors
BGP neighbor is 11.11.11.2, vrf vrfA, remote AS 100, local AS 100, internal link
 Member of peer-group IPV4_VRF_IBGP_PEER for session parameters
  BGP version 4, local router ID 11.11.11.1, remote router ID
  11.11.11.2 BGP state = Established, up for 00:26:24
  Last read 00:00:25, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
```

```
  Received 54 messages, 0 notifications, 0 in queue
  Sent 54 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  IPV4_VRF_IBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0 Local
host: 11.11.11.1, Local port: 38517 Foreign
host: 11.11.11.2, Foreign port: 179 Nexthop:
11.11.11.1 Nexthop global: :: Nexthop local:
::
BGP connection: non shared network
```

IPv4 EBGP Configuration

Below figure displays the minimum configuration required to enable BGP on an interface. R1, R2 and R3 are three routers belonging to the different AS, AS100 AS200 and AS300, connecting to network 11.11.11.0/24 and 11.11.12.0/ 24. First, define the routing process and the AS number to which the routers belong. Then, define BGP neighbors to start exchanging routing updates.

Topology

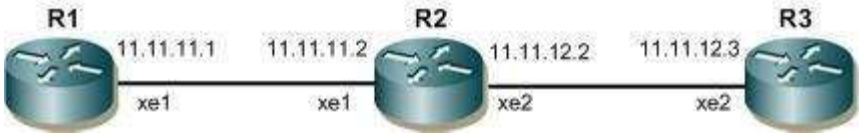


Figure 1-83: IPv4 EBGP Peering

R1

`#configure terminal`	Enter Configure mode.
`(config)#interface lo`	Enter Interface mode for loopback.
`(config-if)#ip address 33.33.33.33/32 secondary`	Assign a secondary IP address.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe1`	Enter Interface mode for xe1.
`(config-if)#ip address 11.11.11.1/24`	Assign IP address to the interface.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#router bgp 100`	Enter Router BGP mode.
`(config-router)#bgp router-id 1.1.1.1`	Assign a BGP router ID.
`(config-router)#neighbor 11.11.11.2 remote-as 200`	Create a static neighbor 11.11.11.2 with remote AS 200.

(config-router)#network 33.33.33.33/32	Advertise the loopback network into BGP.
(config-router)#end	Exit from Router BGP mode.

R2

#configure terminal	Enter Configure mode.
(config)#interface lo	Enter Interface mode for loopback.
(config-if)#ip address 22.22.22.22/32	Assign a secondary IP address.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe1	Enter Interface mode for xe1.
(config-if)#ip address 11.11.11.2/24	Assign IP address to the interface.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe2	Enter Interface mode for xe2.
(config-if)#ip add 11.11.12.2/24	Assign IP address to the interface.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router bgp 200	Enter Router BGP mode.
(config-router)#bgp router-id 2.2.2.2	Assign a BGP router ID.
(config-router)#neighbor IPV4_EBGP_PEER peer-group range 11.11.0.0/16	Create a dynamic peer-group, IPV4_EBGP_PEER.
(config-router)#neighbor IPV4_EBGP_PEER remote-as 100	Assign remote AS with the peer-group IPV4_EBGP_PEER.
(config-router)#neighbor IPV4_EBGP_PEER optional-as 300	Assign optional AS with the peer-group IPV4_EBGP_PEER
(config-router)#network 22.22.22.22/32	Advertise the loopback network into BGP.
(config-router)#end	Exit from Router BGP mode.

R3

#configure terminal	Enter Configure mode.
(config)#interface lo	Enter Interface mode for loopback.
(config-if)#ip address 44.44.44.44/32	Assign a secondary IP address.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe2	Enter Interface mode for xe2.
(config-if)#ip add 11.11.12.3/24	Assign IP address to the interface.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router bgp 300	Enter Router BGP mode.
(config-router)#bgp router-id 3.3.3.3	Assign a BGP router ID.
(config-router)#neighbor 11.11.12.2 remote-as 200	Create a static BGP neighbor 11.11.12.2 with remote AS 200.
(config-router)#network 44.44.44.44/32	Advertise the loopback network into BGP.
(config-router)#end	Exit from Router BGP mode.

Validation

R2

```
#show ip bgp summary
BGP router identifier 2.2.2.2, local AS number
200 BGP table version is 3
2 BGP AS-PATH entries
0 BGP community entries
Neighbor                 V   AS    MsgRcv    MsgSen TblVer   InQ   OutQ   Up/
Down   State/PfxRcd
*11.11.11.1               4   100    29         29       3      0      0
00:13:10                1
*11.11.12.3               4   300    27         27       3      0      0
00:12:20                1
* Dynamically created based on a listen range command

BGP dynamic peer-group: IPV4_EBGP_PEER
listen range:  11.11.0.0/16
  Total number of dynamically created neighbors/limit: 2/(200)
Total number of dynamically created neighbors: 2
Total number of activated dynamic peer-groups for IPv4 Unicast address-family:
1
Total number of neighbors 2
Total number of Established sessions 2

#show running-config bgp
! router bgp 200 bgp
router-id 2.2.2.2
 neighbor IPV4_EBGP_PEER peer-group range 11.11.0.0/16
neighbor IPV4_EBGP_PEER remote-as 100 neighbor
IPV4_EBGP_PEER optional-as 300


#show bgp neighbors
BGP neighbor is 11.11.11.1, remote AS 100, local AS 200, external
 link Member of peer-group IPV4_EBGP_PEER for session parameters
  BGP version 4, local router ID 2.2.2.2, remote router ID
  1.1.1.1 BGP state = Established, up for 00:15:30
  Last read 00:00:01, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 34 messages, 0 notifications, 0 in queue
  Sent 34 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30
 seconds For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 1, Offset 0, Mask 0x2
  IPV4_EBGP_PEER peer-group member
```

```
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0 Local
host: 11.11.11.2, Local port: 56027 Foreign
host: 11.11.11.1, Foreign port: 179 Nexthop:
11.11.11.2 Nexthop global: :: Nexthop local:
::
BGP connection: non shared network

BGP neighbor is 11.11.12.3, remote AS 300, local AS 200, external
 link Member of peer-group IPV4_EBGP_PEER for session parameters
  BGP version 4, local router ID 2.2.2.2, remote router ID
  3.3.3.3 BGP state = Established, up for 00:14:40
  Last read 00:00:12, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 32 messages, 0 notifications, 0 in queue
  Sent 32 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30
 seconds For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 2, Offset 0, Mask 0x4
  IPV4_EBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0 Local
host: 11.11.12.2, Local port: 50963 Foreign
host: 11.11.12.3, Foreign port: 179 Nexthop:
11.11.12.2 Nexthop global: :: Nexthop local:
::
BGP connection: non shared network
```

IPv6 IBGP Configuration

Below figure displays the minimum configuration required to enable BGP on an interface. R1 and R2 are two routers belonging to the same AS, AS100, connecting to network 11:11:11::1/64 and 11:11:12::1/64. First, define the routing process and the AS number to which the routers belong. Then, define BGP neighbors to start exchanging routing updates.

Topology

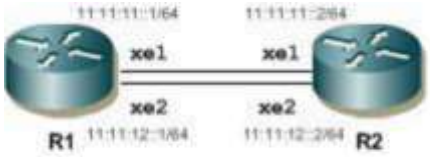


Figure 1-84: IPv6 IBGP Peering

R1

#configure terminal	Enter Configure mode.
(config)#interface lo	Enter Interface mode for loopback.
(config-if)#(config-if)#ipv6 address 33::1/128	Assign an IPv6 address.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe1	Enter Interface mode for xe1.
(config-if)#(config-if)#ipv6 address 11:11:11::1/64	Assign an IPv6 address to the interface.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe2	Enter Interface mode for xe2.
(config-if)#ipv6 address 11:11:12::1/64	Assign an IPv6 address to the interface.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router bgp 100	Enter Router BGP mode.
(config-router)#bgp router-id 1.1.1.1	Assign a BGP router ID.
(config-router)#neighbor IPV6_IBGP_PEER peergroup range 11:11::/16	Create a dynamic peer-group, IPV6_IBGP_PEER with a dynamic range 11:11::/16
(config-router)#neighbor IPV6_IBGP_PEER remote-as 100	Configure a remote AS with the peer group, IPV6_IBGP_PEER.
(config-router)#neighbor IPV6_IBGP_PEER limit 1	Set peer group neighbors limit to 1. Only one BGP session will be up.
(config-router)#address-family ipv6 unicast	Enter the IPv6 Unicast Address Family.
(config-router-af)#neighbor IPV6_IBGP_PEER activate	Activate the peer group, IPV6_IBGP_PEER in the IPv6 address family.
(config-router-af)#network 33::1/128	Advertise the loopback network into the BGP IPv6 address family.
(config-router-af)#end	Exit from Router BGP address family mode.

R2

#Configure terminal	Enter Configuration mode.
(config)#interface lo	Enter Interface mode for loopback.
(config-if)#ipv6 address 22::2/128	Assign an IPv6 address.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe1	Enter Interface mode for xe1.

(config-if)#ipv6 address 22::2/128	Assign an IPv6 address to the interface.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe1	Enter Interface mode for xe1.
(config-if)#ipv6 address 11:11:11::2/64	Assign an IPv6 address to the interface.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe2	Enter Interface mode for xe2.
(config-if)#ipv6 address 11:11:12::2/64	Assign an IPv6 address to the interface.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router bgp 100	Enter Router BGP mode.
(config-router)#bgp router-id 2.2.2.2	Assign a BGP router ID.
(config-router)#neighbor 11:11:11::1 remoteas 100	Configure BGP neighbor by specifying the neighbor IP address.
(config-router)#neighbor 11:11:12::1 remoteas 100	Configure BGP neighbor by specifying the neighbor IP address.
(config-router)#address-family ipv6 unicast	Enter the IPv6 Unicast Address Family.
(config-router-af)#network 22::2/128	Advertise the loopback network into BGP.
(config-router-af)#neighbor 11:11:12::1 activate	Activate the neighbor in the IPv6 address family.
(config-router-af)#neighbor 11:11:11::1 activate	Activate the neighbor in the IPv6 address family.
(config-router-af)#end	Exit from Router BGP address family mode.

Validation

R1

```
#show ipv6 bgp summary
BGP router identifier 1.1.1.1, local AS number
100 BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS    MsgRcv    MsgSen TblVer   InQ   OutQ   Up/
Down   State/PfxRcd
*11:11:11::2             4   100     6          6       2      0      0
00:01:41               1
* Dynamically created based on a listen range command

BGP dynamic peer-group: IPV6_IBGP_PEER
listen range:  11::/16
  Total number of dynamically created neighbors/limit: 1/(1)

Total number of dynamically created neighbors: 1
Total number of activated dynamic peer-groups for IPv6 Unicast address-family:
1
```

```
    Total number of neighbors 1

    Total number of Established sessions 1

    #show ip bgp peer-group IPV6_IBGP_PEER

    BGP dynamic peer-group is IPV6_IBGP_PEER, IBGP, remote AS 100
      BGP dynamic peer-group IPV6_IBGP_PEER listen range group members:
      11::/16
      BGP version 4
    Minimum time between advertisement runs is 5 seconds
    For address family: IPv4 Unicast   Peer-group member:
  *11:11:11::2
  Index 1, Offset 0, Mask 0x2
0 accepted prefixes, 0 announced prefixesFor address family:
  IPv6 Unicast
  Peer-group member:
  *11:11:11::2
  Index 0, Offset 0, Mask 0x0
1 accepted prefixes, 1 announced prefixes


#show bgp ipv6
BGP table version is 2, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop             Metric    LocPrf      Weight Path
*>i  22::2/128         11:11:11::2(fe80::5054:ff:fe95:85ec)
                                          0         100           0       i *>
33::1/128         ::                   0         100           32768   i

Total number of prefixes 2

#show running-config bgp
! router bgp 100 bgp router-
id 1.1.1.1
 neighbor IPV6_IBGP_PEER peer-group range 11::/16
neighbor IPV6_IBGP_PEER remote-as 100 neighbor
IPV6_IBGP_PEER limit 1
 !  address-family ipv6 unicast
network 33::1/128
 neighbor IPV6_IBGP_PEER activate  exit-address-family


#show bgp neighbors
BGP neighbor is 11:11:11::2, remote AS 100, local AS 100, internal link
 Member of peer-group IPV6_IBGP_PEER for session parameters
  BGP version 4, local router ID 1.1.1.1, remote router ID
  2.2.2.2 BGP state = Established, up for 00:04:17
  Last read 00:00:18, hold time is 90, keepalive interval is 30 seconds
```

```
 Neighbor capabilities:
   Route refresh: advertised and received (old and new)
   Address family IPv4 Unicast: advertised and received
   Address family IPv6 Unicast: advertised and received
 Received 11 messages, 0 notifications, 0 in queue
 Sent 11 messages, 0 notifications, 0 in queue
 Route refresh request: received 0, sent 0
 Minimum time between advertisement runs is 5
seconds For address family: IPv4 Unicast
 BGP table version 1, neighbor version 1
 Index 0, Offset 0, Mask 0x1
 IPV6_IBGP_PEER peer-group member
 Community attribute sent to this neighbor (both)
     0 accepted prefixes
   0 announced prefixes

    For address family: IPv6 Unicast
     BGP table version 2, neighbor version 2
     Index 0, Offset 0, Mask 0x0
     IPV6_IBGP_PEER peer-group member
     Community attribute sent to this neighbor (both)
   1 accepted prefixes
     1 announced prefixes

    Connections established 1; dropped 0
   Local host: 11:11:11::1, Local port: 42410
   Foreign host: 11:11:11::2, Foreign port: 179
   Nexthop: 1.1.1.1
   Nexthop global: 11:11:11::1
   Nexthop local: fe80::5054:ff:fe51:f74
   BGP connection: shared network
```

IPV6 IBGP VRF Configuration

Below figure displays the minimum configuration required to enable BGP on an interface with VRF enabled on the device and interface being part of VRF. R1 and R2 are two routers belonging to the same AS, AS100, connecting to network 11:11:11::1 and 11:11:12::1. First, define the routing process and the AS number to which the routers belong. Then, define BGP neighbors to start exchanging routing updates.

Topology

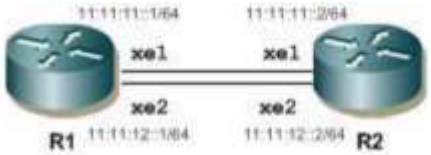


Figure 1-85: IPv6 VRF IBGP peering

R1

`#Configure terminal`	Enter Configuration mode.

(config)#ip vrf vrfA	Configure a VRF, vrfA.
(config-vrf)#rd 1:1	Configure a route distinguisher to VRF.
(config-vrf)#router-id 7.7.7.7	Configure a router ID.
(config-vrf)#exit	Exit from VRF mode and return to Configuration mode.
(config)#interface xe1	Enter Interface mode for xe1.
(config-if)# ip vrf forwarding vrfA	Assign IP address to VRF.
(config-if)#ipv6 address 11:11:11::1/64	Assign an IPv6 address to the interface.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe2	Enter Interface mode for xe2.
(config-if)# ip vrf forwarding vrfA	Assign IP address to VRF.
(config-if)#ipv6 address 11:11:12::1/64	Assign an IPv6 address to the interface.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router bgp 100	Enter Router BGP mode.
(config-router)#address-family ipv6 vrf	Enter IPv6 VRF Address Family.
(config-router-af)#neighbor IPV6 VRF IBGP PEER peer-group range 11:11::1/16	Configure a dynamic peer group, IPV6_IBGP_PEER with a dynamic range value.
(config-router-af)#neighbor IPV6 VRF IBGP PEER remote-as 100	Configure a remote AS with the peer group, IPV6_IBGP_PEER.
(config-router)#end	Exit from Router BGP mode.

R2

#configure terminal	Enter Configure mode.
(config)#ip vrf vrfA	Configure a VRF, vrfA.
(config-vrf)#rd 2:1	Configure a route distinguisher to VRF.
(config-vrf)#router-id 1.1.1.1	Configure a router ID.
(config-vrf)#exit	Exit from VRF mode and return to Configuration mode.
(config)#interface xe1	Enter Interface mode for xe1.
(config-if)# ip vrf forwarding vrfA	Assign IP address to VRF.
(config-if)#ipv6 address 11:11:11::2/64	Assign an IPv6 address to the interface.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe2	Enter Interface mode for xe2.
(config-if)# ip vrf forwarding vrfA	Assign IP address to vrf.
(config-if)#ipv6 address 11:11:12::2/64	Assign an IPv6 address to the interface.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router bgp 100	Enter Router BGP mode
(config-router)#address-family ipv6 vrf vrfA	Enter IPv6 VRF Address Family.
(config-router-af)#neighbor 11:11:12::1 remote-as 100	Configure BGP neighbor by specifying the neighbor IP address.

(config-router-af)#neighbor 11:11:11::1 remote-as 100	Configure BGP neighbor by specifying the neighbor IP address.
(config-router)#end	Exit from Router BGP mode.

Validation

R1

```
    #show ipv6 bgp summary vrf vrfA
    BGP router identifier 7.7.7.7, local AS number 100
    BGP VRF vrfA Route Distinguisher: 1:1
    BGP table version is 1
    0 BGP AS-PATH entries
    0 BGP community entries

    Neighbor                 V    AS   MsgRcv    MsgSen TblVer    InQ   OutQ    Up/
    Down    State/PfxRcd
*11:11:11::2              4  100     6          6       1      0      0
00:00:17                0
*11:11:12::2              4  100     7         10       1      0      0
00:00:15                0
* Dynamically created based on a listen range command

BGP dynamic peer-group: IPV6_VRF_IBGP_PEER    listen
range:   11::/16
  Total number of dynamically created neighbors/limit: 2/(200)

Total number of dynamically created neighbors: 2
Total number of activated dynamic peer-groups for IPv6 Unicast address-family:
1

Total number of neighbors 2

Total number of Established sessions 2


#show running-config bgp
!
router bgp 100
 !  address-family ipv6 vrf vrfA
 neighbor IPV6_VRF_IBGP_PEER peer-group range 11::/16
neighbor IPV6_VRF_IBGP_PEER remote-as 100 neighbor
IPV6_VRF_IBGP_PEER activate
 neighbor IPV6_VRF_IBGP_PEER send-community extended
exit-address-family !

#show ip bgp peer-group vrf vrfA

BGP dynamic peer-group is IPV6_VRF_IBGP_PEER, IBGP, remote AS 100
  BGP dynamic peer-group IPV6_VRF_IBGP_PEER listen range group members:
  11::/16
  BGP version 4
```

```
Minimum time between advertisement runs is 5 seconds For
address family: IPv6 Unicast
  Peer-group member:
  *11:11:12::2
  Index 1, Offset 0, Mask 0x2
  0 accepted prefixes, 0 announced prefixes
  Peer-group member:
  *11:11:11::2
  Index 2, Offset 0, Mask 0x4
  0 accepted prefixes, 0 announced prefixes

#show running-config bgp
!
router bgp 100
 !
 address-family ipv6 vrf vrfA
 neighbor IPV6_VRF_IBGP_PEER peer-group range 11::/16
neighbor IPV6_VRF_IBGP_PEER remote-as 100 neighbor
IPV6_VRF_IBGP_PEER activate
 neighbor IPV6_VRF_IBGP_PEER send-community extended
 exit-address-family !

#show ip bgp peer-group vrf vrfA

BGP dynamic peer-group is IPV6_VRF_IBGP_PEER, IBGP, remote AS 100
  BGP dynamic peer-group IPV6_VRF_IBGP_PEER listen range group members:
  11::/16
  BGP version 4
Minimum time between advertisement runs is 5 seconds For
address family: IPv6 Unicast
  Peer-group member:
  *11:11:12::2
  Index 1, Offset 0, Mask 0x2
  0 accepted prefixes, 0 announced prefixes
  Peer-group member:
  *11:11:11::2
  Index 2, Offset 0, Mask 0x4
  0 accepted prefixes, 0 announced prefixes

#show bgp ipv6 neighbors
BGP neighbor is 11:11:11::2, vrf vrfA, remote AS 100, local AS 100, internal link
 Member of peer-group IPV6_VRF_IBGP_PEER for session parameters
  BGP version 4, local router ID 7.7.7.7, remote router ID
  1.1.1.1 BGP state = Established, up for 00:02:13
  Last read 00:00:14, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv6 Unicast: advertised and received
  Received 8 messages, 2 notifications, 0 in queue
  Sent 10 messages, 0 notifications, 0 in queue
```

```
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv6 Unicast
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  IPV6_VRF_IBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0 Local
host: 11:11:11::1, Local port: 179 Foreign
host: 11:11:11::2, Foreign port: 48206
Nexthop: 7.7.7.7
Nexthop global: 11:11:11::1
Nexthop local: fe80::5054:ff:fe51:f74
BGP connection: shared network
Last Reset: 00:02:18, due to BGP Notification received
Notification Error Message: (OPEN Message Error/Bad BGP Identifier.)

BGP neighbor is 11:11:12::2, vrf vrfA, remote AS 100, local AS 100, internal link
 Member of peer-group IPV6_VRF_IBGP_PEER for session parameters
  BGP version 4, local router ID 7.7.7.7, remote router ID
  1.1.1.1 BGP state = Established, up for 00:02:11
      Last read 00:00:12, hold time is 90, keepalive interval is 30 seconds
      Neighbor capabilities:
        Route refresh: advertised and received (old and new)
        Address family IPv6 Unicast: advertised and received
      Received 8 messages, 3 notifications, 0 in queue
      Sent 13 messages, 1 notifications, 0 in queue
      Route refresh request: received 0, sent 0
      Minimum time between advertisement runs is 5
     seconds For address family: IPv6 Unicast
      BGP table version 1, neighbor version 1
      Index 1, Offset 0, Mask 0x2
      IPV6_VRF_IBGP_PEER peer-group member
      Community attribute sent to this neighbor (both)
      0 accepted prefixes
      0 announced prefixes

     Connections established 1; dropped 0 Local
    host: 11:11:12::1, Local port: 179 Foreign
    host: 11:11:12::2, Foreign port: 49010
    Nexthop: 7.7.7.7
    Nexthop global: 11:11:12::1
    Nexthop local: fe80::5054:ff:fe8b:8f5c
    BGP connection: shared network
    Last Reset: 00:02:16, due to BGP Notification received
    Notification Error Message: (OPEN Message Error/Bad BGP Identifier.)
```

IPv6 EBGP Configuration

Below figure displays the minimum configuration required to enable BGP on an interface. R1, R2 and R3 are three routers belonging to the different AS, AS100 AS200 and AS300, connecting to network 11:11:11::/64 and 11:11:12::/64. First, define the routing process and the AS number to which the routers belong. Then, define BGP neighbors to start exchanging routing updates.

Topology

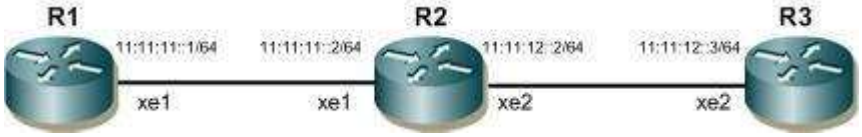


Figure 1-86: IPv6 EBGP peering

R1

`#configure terminal`	Enter Configuration mode.
`(config)#interface lo`	Enter Interface mode for loopback.
`(config-if)#ipv6 address 33::1/128`	Assign an IPv6 address.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe1`	Enter Interface mode for xe1.
`(config-if)#ipv6 address 11:11:11::1/64`	Assign an IPv6 address to the interface.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#router bgp 100`	Enter Router BGP mode.
`(config-router)#bgp router-id 1.1.1.1`	Assign a BGP router ID.
`(config-router)#neighbor 11:11:11::2 remoteas 200`	Configure BGP neighbor by specifying the neighbor IP address.
`(config-router)#address-family ipv6 unicast`	Enter the IPv6 Unicast Address Family.
`(config-router-af)#neighbor 11:11:11::2 activate`	Activate the neighbor in the address family.
`(config-router-af)#network 33::1/128`	Advertise the loopback network into BGP.
`(config-router)#end`	Exit from Router BGP mode.

R2

`#configure terminal`	Enter Configure mode.
`(config)#interface lo`	Enter Interface mode for loopback.
`(config-if)#ipv6 address 22::1/128`	Assign an IPv6 address.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe1`	Enter Interface mode for xe1
`(config-if)#ipv6 address 11:11:11::2/64`	Assign an IPv6 address to the interface.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface xe2`	Enter Interface mode for xe2.

(config-if)#ipv6 address 11:11:12::2/64	Assign an IPv6 address to the interface.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router bgp 200	Enter Router BGP mode.
(config-router)#bgp router-id 2.2.2.2	Assign a BGP router ID.
(config-router)#neighbor IPV6_EBGP_PEER peer-group range 11::1/16	Configure a dynamic peer group, IPV6_EBGP_PEER.
(config-router)#neighbor IPV6_EBGP_PEER remote-as 100	Configure remote AS with peer group, IPV6_EBGP_PEER.
(config-router)#neighbor IPV6_EBGP_PEER optional-as 300	Configure optional AS with peer group, IPV6_EBGP_PEER.
(config-router)#address-family ipv6 unicast	Enter IPv6 Unicast Address Family.
(config-router-af)#neighbor IPV6_EBGP_PEER activate	Activate peer group in the address family.
(config-router-af)#network 22::1/128	Advertise the loopback network into BGP.
(config-router)#end	Exit from Router BGP mode.

R3

#Configure terminal	Enter Configuration mode.
(config)#interface lo	Enter Interface mode for loopback.
(config-if)#ipv6 address 44::1/128	Assign an IPv6 address.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe2	Enter Interface mode for xe2
(config-if)#ipv6 address 11:11:12::3/64	Assign an IPv6 address.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router bgp 300	Enter Router BGP mode.
(config-router)#bgp router-id 3.3.3.3	Assign a BGP router ID.
(config-router)#neighbor 11:11:12::2 remoteas 200	Configure the BGP neighbor by specifying the neighbor IP address.
(config-router)#address-family ipv6 unicast	Enter the IPv6 Unicast Address Family.
(config-router-af)#neighbor 11:11:12::2 activate	Activate the neighbor in address family.
(config-router-af)#network 44::1/128	Advertise the loopback network into BGP.
(config-router)#end	Exit from Router BGP mode.

Validation

R2

```
#show ipv6 bgp sum
BGP router identifier 2.2.2.2, local AS number
200 BGP table version is 5
3 BGP AS-PATH entries
0 BGP community entries
```

```
Neighbor                 V    AS    MsgRcv    MsgSen TblVer    InQ    OutQ    Up/
Down   State/PfxRcd
*11:11:11::1              4   100     9         11       5       0       0
00:01:28                 1
*11:12::3                 4   300     6          6       5       0       0
00:01:14                 1
* Dynamically created based on a listen range command

BGP dynamic peer-group: IPV6_EBGP_PEER
listen range:  11::/16
  Total number of dynamically created neighbors/limit: 2/(200)
Total number of dynamically created neighbors: 2
Total number of activated dynamic peer-groups for IPv6 Unicast address-family:
1
Total number of neighbors 2
Total number of Established sessions 2


#show running-config bgp
! router bgp 200 bgp
router-id 2.2.2.2
 neighbor IPV6_EBGP_PEER peer-group range
11::/16 neighbor IPV6_EBGP_PEER remote-as 100
neighbor IPV6_EBGP_PEER optional-as 300
 !  address-family ipv6 unicast
network 22::1/128 neighbor
IPV6_EBGP_PEER activate exit-
address-family !
#show bgp ipv6 neighbors
BGP neighbor is 11:11:11::1, remote AS 100, local AS 200, external link
 Member of peer-group IPV6_EBGP_PEER for session parameters
  BGP version 4, local router ID 2.2.2.2, remote router ID
  1.1.1.1 BGP state = Established, up for 00:02:15
  Last read 00:00:16, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv6 Unicast: advertised and received
  Received 11 messages, 0 notifications, 0 in queue
  Sent 12 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 0, Offset 0, Mask 0x1
  IPV6_EBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
0 announced prefixes
```

```
 For address family: IPv6 Unicast
  BGP table version 5, neighbor version 5
  Index 0, Offset 0, Mask 0x0
  IPV6_EBGP_PEER peer-group member
  Community attribute sent to this neighbor (both)
1 accepted prefixes
2 announced prefixes

 Connections established 2; dropped 1
Local host: 11:11:11::2, Local port: 53043
Foreign host: 11:11:11::1, Foreign port: 179
Nexthop: 2.2.2.2
Nexthop global: 11:11:11::2
Nexthop local: fe80::5054:ff:fe95:85ec
BGP connection: shared network
Last Reset: 00:02:20, due to BGP Notification sent
Notification Error Message: (Cease/Other Configuration Change.)

BGP neighbor is 11:11:12::3, remote AS 300, local AS 200, external link
 Member of peer-group IPV6_EBGP_PEER for session parameters
  BGP version 4, local router ID 2.2.2.2, remote router ID
  3.3.3.3 BGP state = Established, up for 00:02:01
  Last read 00:00:02, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv6 Unicast: advertised and received
  Received 8 messages, 0 notifications, 0 in queue
  Sent 8 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
 Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 0, Offset 0, Mask 0x1
  IPV6_EBGP_PEER peer-group member
      Community attribute sent to this neighbor (both)
      0 accepted prefixes
    0 announced prefixes

     For address family: IPv6 Unicast
      BGP table version 5, neighbor version 5
      Index 0, Offset 0, Mask 0x0
      IPV6_EBGP_PEER peer-group member
      Community attribute sent to this neighbor (both)
    1 accepted prefixes
    2 announced prefixes

     Connections established 1; dropped 0
    Local host: 11:11:12::2, Local port: 47743
    Foreign host: 11:11:12::3, Foreign port: 179
```

```
Nexthop: 2.2.2.2
Nexthop global: 11:11:12::2
Nexthop local: fe80::5054:ff:fee5:b088
BGP connection: shared network
```

VPNV4 Configuration

Below mentioned topology displays bgp vpnv4 configuration on PE nodes, R1 and R3. IBGP peering will be formed on the loopback interface of R1 and R3; also IGP is running between all the routers.

Topology

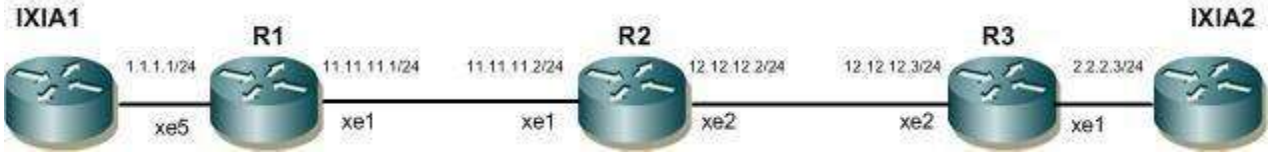


Figure 1-87: IPv4 IBGP VPNv4 Configuration

R1

`#Configure terminal`	Enter Configuration mode.
`(config)#ip vrf vrf1`	Create a VRF, vrf1.
`(config-vrf)#rd 100:1`	Configure a route distinguisher value.
`(config-vrf)#route-target export 100:1`	Configure a route target export value to VRF.
`(config-vrf)#route-target import 200:1`	Configure a route target import value to VRF.
`(config-vrf)#exit`	Exit from VRF configuration mode.
`(config)#router ldp`	Enter Router LDP mode.
`(config-router)#router-id 3.3.3.3`	Configure an LDP router ID.
`(config-router)#exit`	Exit from Router LDP mode.
`(config)#interface xe5`	Enter Interface configuration mode.
`(config-if)#ip vrf forwarding vrf1`	Configure the interface to a VRF.
`(config-if)#ip address 1.1.1.1/24`	Assign an IP address to the interface.
`(config-if)#exit`	Exit from Interface configuration mode.
`(config-if)#interface xe1`	Enter another interface.
`(config-if)#ip address 11.11.11.1/24`	Assign an IP address to the interface.
`(config-if)#label-switching`	Enable label switching on interface.
`(config-if)#enable-ldp ipv4`	Enable IPv4 LDP configuration on interface.
`(config-if)#exit`	Exit from Interface configuration mode.
`(config-if)#interface lo`	Enter the loopback interface.
`(config-if)#ip address 20.20.20.20/32 secondary`	Assign a secondary IP address to the interface.
`(config-if)#exit`	Exit from Interface Configuration mode.

(config)#router ospf 100	Enter Router OSPF mode.
(config-router)#network 11.11.11.0/24 area 0	Configure the interface on which OSPF runs, and associate the area ID.
(config-router)#network 20.20.20.20/32 area 0	Configure the interface on which OSPF runs, and associate the area ID.
(config-router)#exit	Exit from Router OSPF mode.
(config)#router ospf 200 vrf1	Create an OSPF process on VRF.
(config-router)#network 1.1.1.1/24 area 0	Configure the interface on which OSPF runs, and associate the area ID.
(config-router)#redistribute bgp	Redistribute BGP into OSPF.
(config-router)#exit	Exit from Router OSPF mode.
(config)#router bgp 100	Create a BGP process.
(config-router)#neighbor lo_peer peer-group range 30.30.30.30/32	Configure a dynamic peer group with the range command.
(config-router)#neighbor lo_peer remote-as 100	Configure remote AS to the peer group.
(config-router)#neighbor lo_peer updatesource lo	Configure BGP neighbors to update the source routes.
(config-router)#address-family vpnv4 unicast	Enter the VPNv4 Address Family.
(config-router-af)#neighbor lo_peer activate	Activate the peer group in VPNv4 address family.
(config-router-af)#exit-address-family	Exit from VPNv4 address family.
(config-router)#address-family ipv4 vrf vrf1	Enter IPv4 VRF address family.
(config-router-af)#redistribute ospf 200	Redistribute OSPF into the IPv4 VRF address family.
(config-router)#end	Exit from the Router BGP mode.

R2

#Configure terminal	Enter Configuration mode.
(config)#router ldp	Enter Router LDP mode.
(config-router)#router-id 4.4.4.4	Configure an LDP router ID.
(config-router)#exit	Exit from Router LDP mode.
(config-if)#interface xe2	Enter Interface Configuration mode.
(config-if)#ip address 12.12.12.2/24	Assign an IP address to the interface.
(config-if)#label-switching	Enable label switching on the interface.
(config-if)#enable-ldp ipv4	Enable IPv4 LDP configuration on the interface.
(config-if)#exit	Exit from Interface configuration mode.
(config-if)#interface xe1	Enter another Interface.
(config-if)#ip address 11.11.11.2/24	Assign an IP address to the interface.
(config-if)#label-switching	Enable label switching on the interface.
(config-if)#enable-ldp ipv4	Enable IPv4 LDP configuration on the interface.
(config-if)#exit	Exit from Interface mode.

(config)#router ospf 100	Create an OSPF process.
(config-router)#network 11.11.11.0/24 area	Define the interface on which OSPF runs, and associate the area ID
(config-router)#network 12.12.12.0/24 area 0	Define the interface on which OSPF runs, and associate the area ID
(config-router)#end	Exit from Router BGP mode.

R3

#Configure terminal	Enter Configuration mode.
(config)#router ldp	Enter Router LDP mode.
(config-router)#router-id 5.5.5.5	Configure an LDP router ID.
(config-router)#exit	Exit from Router LDP mode.
(config)#ip vrf vrf2	Create a VRF, vrf2.
(config-vrf)#rd 200:1	Configure a route distinguisher value.
(config-vrf)#route-target export 200:1	Configure a route target export value to VRF.
(config-vrf)#route-target import 100:1	Configure a route target import value to VRF.
(config-vrf)#exit	Exit from VRF configuration mode.
(config)#interface xe1	Enter Interface configuration mode.
(config-if)#ip vrf forwarding vrf2	Configure an interface to a VRF.
(config-if)#ip address 2.2.2.3/24	Assign an IP address to the interface.
(config-if)#exit	Exit from Interface configuration mode.
(config-if)#interface xe2	Enter another interface.
(config-if)#ip address 12.12.12.3/24	Assign an IP address to the interface.
(config-if)#label-switching	Enable label switching on interface.
(config-if)#enable-ldp ipv4	Enable IPv4 LDP configuration on the interface.
(config-if)#exit	Exit from Interface configuration mode.
(config-if)#interface lo	Enter loopback interface.
(config-if)#ip address 30.30.30.30/32 se	Assign a secondary IP address to the interface.
(config-if)#exit	Exit from Interface mode.
(config)#router ospf 100	Enter Router OSPF mode.
(config-router)#network 12.12.12.0/24 area 0	Define the interface on which OSPF runs, and associate the area ID
(config-router)#network 30.30.30.30/32 area 0	Define the interface on which OSPF runs, and associate the area ID
(config-router)#exit	Exit from Router OSPF mode.
(config)#router ospf 200 vrf2	Create an OSPF process on VRF.
(config-router)#network 2.2.2.3/24 area 0	Define the interface on which OSPF runs, and associate the area ID.
(config-router)#redistribute bgp	Redistribute BGP into OSPF.

(config-router)#exit	Exit from Router OSPF mode.
(config)#router bgp 100	Create a BGP process.
(config-router)#neighbor 20.20.20.20 remoteas 100	Configure BGP neighbor by specifying a neighbor IP address.
(config-router)#neighbor 20.20.20.20 update-slo	Define the BGP neighbors to update the source routes.
(config-router)#address-family vpnv4 unicast	Enter VPNv4 Address Family.
(config-router-af)#neighbor 20.20.20.20 act	Activate the neighbor in VPNv4 address family.
(config-router-af)#exit-address-family	Exit from VPNv4 address family.
(config-router)#address-family ipv4 vrf vrf2	Enter IPv4 VRF address family.
(config-router-af)#redistribute ospf 200	Redistribute OSPF into the IPv4 address family.
(config-router)#end	Exit from Router BGP mode.

Validation

R1

```
    #show running-config router bgp router bgp
    100
     neighbor      lo_peer      peer-group      range
    30.30.30.30/32  neighbor  lo_peer  remote-as  100
    neighbor lo_peer update-source lo
     !  address-family vpnv4 unicast
    neighbor lo_peer activate exit-
    address-family
!
     address-family ipv4 vrf
    vrf1 redistribute ospf 200
    exit-address-family !

    #show ip  bgp vpnv4 all summary
    BGP router identifier 10.12.29.115, local AS number 100
    BGP table version is 2
    1 BGP AS-PATH entries
    0 BGP community entries

    Neighbor                 V    AS    MsgRcv    MsgSen TblVer    InQ    OutQ    Up/
    Down    State/PfxRcd
    *30.30.30.30             4    100     3          3       2       0       0
    00:00:30                1
    * Dynamically created based on a listen range command

    BGP  dynamic  peer-group:  lo_peer     listen
    range:   30.30.30.30/32    Total  number of
    dynamically    created    neighbors/limit:
    1/(200)

Total number of dynamically created neighbors: 1
```

```
Total number of activated dynamic peer-groups for VPNv4 Unicast addressfamily: 1

Total number of neighbors 1

Total number of Established sessions 1


#show ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled S Stale Origin codes: i
- IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 100:1 (Default for VRF vrf1)
*> l 1.1.1.0/24       0.0.0.0               1         100           32768    ?
 Announced routes count = 1  Accepted
routes count = 0

#show ip  bgp vpnv4 all neighbors
BGP neighbor is 30.30.30.30, remote AS 100, local AS 100, internal link
 Member of peer-group lo_peer for session parameters
  BGP version 4, local router ID 10.12.29.115, remote router ID
  10.12.29.117 BGP state = Established, up for 00:02:11
  Last read 00:00:12, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family VPNv4 Unicast: advertised and received
  Received 7 messages, 0 notifications, 0 in queue
  Sent 7 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
  seconds Update source is lo
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2   lo_peer
peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
0 announced prefixes

 For address family: VPNv4 Unicast
  BGP table version 2, neighbor version 2
  Index 0, Offset 0, Mask 0x0   lo_peer
peer-group member
  Community attribute sent to this neighbor (both)
1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 20.20.20.20, Local port: 50898
```

```
Foreign host: 30.30.30.30, Foreign port: 179
    Nexthop: 20.20.20.20
    Nexthop global: :: Nexthop
    local: ::
    BGP connection: non shared network

    #show ip bgp peer-group

    BGP dynamic peer-group is lo_peer, IBGP, remote AS 100
      BGP dynamic peer-group lo_peer listen range group members:
      30.30.30.30/32
    BGP version 4
    Minimum time between advertisement runs is 5 seconds
    For address family: IPv4 Unicast
      Peer-group member:
      *30.30.30.30
      Index 1, Offset 0, Mask 0x2
    0 accepted prefixes, 0 announced prefixesFor address family:
      VPNv4 Unicast
      Peer-group member:
      *30.30.30.30
      Index 0, Offset 0, Mask 0x0
    1 accepted prefixes, 1 announced prefixes
```

Enable eBGP Multihop

This example shows the minimum configuration required for enabling eBGP multihop on peers speaking BGP. eBGP multihop is used for routers that are not directly connected to each other. Typically, eBGP peers are directly connected, but if there is a requirement that necessitates this scenario, this configuration can be used.

Note: The IP addresses used in the configuration should be accessible through an IGP or static routing.

Topology

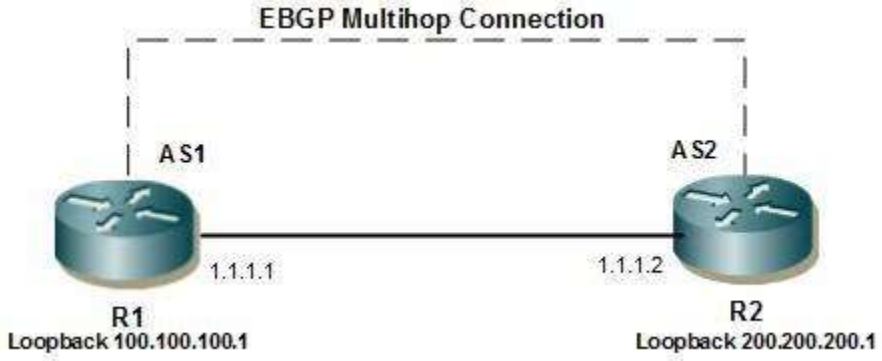


Figure 1-88: eBGP Multihop Connection

R1

#configure terminal	Enter Configure mode.
(config)#interface lo	Enter loopback interface mode.
(config-if)#ip address 100.100.100.1/24	Specify IP address to the interface.
(config-if)#exit	Exit loopback interface mode.
(config)#ip route 200.200.200.0/24 1.1.1.2	Specify route IP address.
(config)#router bgp 1	Define the routing process. The number 1 specifies the AS number of R1.
(config-router)#neighbor 200.200.200.1 remote-as 2	Define BGP neighbors, and establish a TCP session. 200.200.200.1 is the IP address of the neighbor (R2), and 100 is the neighbor's AS number.
(config-router)#neighbor 200.200.200.1 update-source lo	Define BGP neighbors, to update the source routes.
(config-router)#neighbor 200.200.200.1 ebgpmultihop	Define the neighbor 200.200.200.1 for eBGP multihops.
(config-router)#end	Exit BGP router mode.

R2

#configure terminal	Enter Configure mode.
(config)#interface lo	Enter loopback interface mode.
(config-if)#ip address 200.200.200.1/24	Specify IP address to the interface.
(config-if)#exit	Exit loopback interface mode.
(config)#ip route 100.100.100.0/24 1.1.1.1	Specify route IP address.
(config)#router bgp 2	Define the routing process. The number 2 specifies the AS number of R1.
(config-router)#neighbor 100.100.100.1 remote-as 1	Define BGP neighbors, and establish a TCP session. 100.100.100.1 is the IP address of the neighbor (R2), and 100 is the neighbor's AS number.
(config-router)#neighbor 100.100.100.1 update-source lo	Define BGP neighbors, to update the source routes.
(config-router)#neighbor 100.100.100.1 ebgpmultihop	Define the neighbor 100.100.100.1 for eBGP multihops.
(config-router)#end	Exit BGP router mode.

Validation

show ip bgp, show ip bgp neighbors

Enable Peer Groups

A BGP speaker might have the same update policies for a set of its peers. This is very useful if you have to change the update policies for all of the peers: Changing individual routers for separate policies can be very time-consuming, thus, peer groups play an important role in creating and assigning policies to a group of routers.

In the following scenario, R1, R2, and R3 belong to the same peer group. R4 and R1 are eBGP peers. R1 is the route reflector (configuration not shown), and R2 and R3 are in AS 200. R4 is in AS 100.

Topology

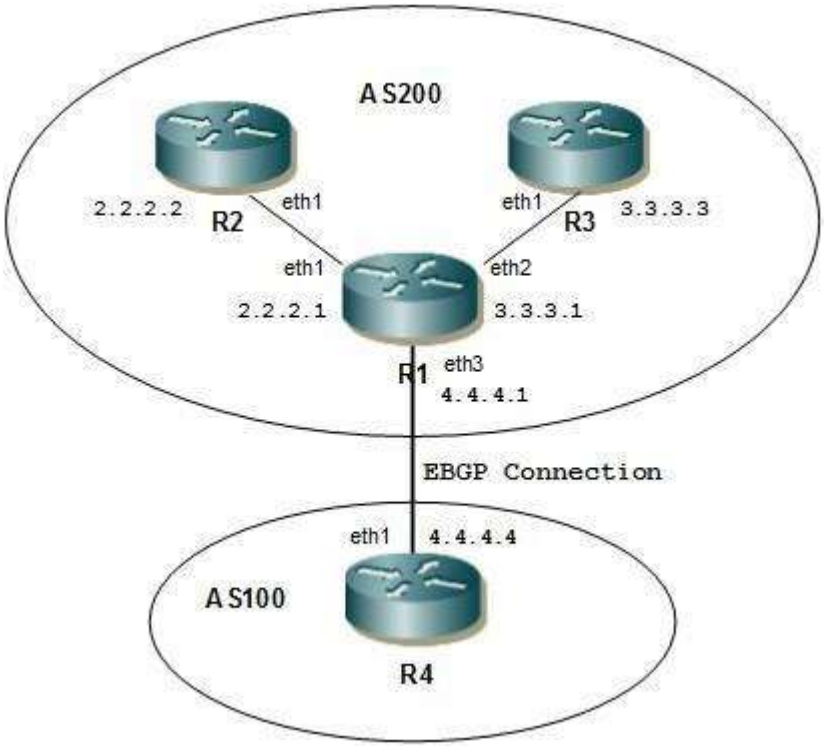


Figure 1-89: BGP Peer Groups

R1

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 200`	Define the routing process. The number `200` specifies the AS number of R1.
`(config-router)#neighbor ABC peer-group`	Create a peer group named `ABC`.
`(config-router)#neighbor ABC remote-as 200`	Assign options to the peer group named `ABC`.
`(config-router)#neighbor 2.2.2.2 peer-group ABC`	Define neighbor `2.2.2.2` (`R2`) as a peer group member.
`(config-router)#neighbor 3.3.3.3 peer-group ABC`	Define neighbor `3.3.3.3` (`R3`) as a peer group member.
`(config-router)#neighbor 4.4.4.4 remote-as 100`	Define neighbor `4.4.4.4` (`R4`) is the IP address of R4 and 100 is the AS number.

R2

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 200`	Define the routing process. The number `200` specifies the AS number of R2.
`(config-router)#neighbor 2.2.2.1 remote-as 200`	Create a TCP connection with neighbor `2.2.2.1` of AS `200`.

R3

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 200`	Define the routing process. The number `200` specifies the AS number of R3.
`(config-router)#neighbor 3.3.3.1 remote-as 200`	Create a TCP connection with neighbor `3.3.3.1` of AS `200`.

R4

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 100`	Define the routing process. The number `100` specifies the AS number of R4.
`(config-router)#neighbor 4.4.4.1 remote-as 200`	Create a TCP connection with neighbor 4.4.4.1 of AS 200.

Validation

show ip bgp, show ip bgp neighbors

R1

```
R1#show ip bgp neighbors
BGP neighbor is 2.2.2.2, remote AS 200, local AS 200, internal link
 Member of peer-group ABC for session parameters
  BGP version 4, remote router ID 10.12.7.155
  BGP state = Established, up for 00:04:55
  Last read 00:04:55, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 11 messages, 0 notifications, 0 in queue
  Sent 11 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  ABC peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 2.2.2.1, Local port: 33865
Foreign host: 2.2.2.2, Foreign port: 179
Nexthop: 2.2.2.1
Nexthop global: 1111::1
Nexthop local: fe80::a00:27ff:fecc:47a6
BGP connection: non shared network

BGP neighbor is 3.3.3.3, remote AS 200, local AS 200, internal link
```

```
    Member of peer-group ABC for session parameters
  BGP version 4, remote router ID 10.12.7.153
  BGP state = Established, up for 00:04:55
  Last read 00:04:55, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 11 messages, 0 notifications, 0 in queue
  Sent 11 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  ABC peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 3.3.3.1, Local port: 44280
Foreign host: 3.3.3.3, Foreign port: 179
Nexthop: 3.3.3.1
Nexthop global: fe80::a00:27ff:fe85:25d4
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 4.4.4.4, remote AS 100, local AS 200, external
  link BGP version 4, remote router ID 10.12.7.120
  BGP state = Established, up for 00:04:55
  Last read 00:04:55, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 11 messages, 0 notifications, 0 in queue
  Sent 11 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 3, Offset 0, Mask 0x8
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 4.4.4.1, Local port: 55493
Foreign host: 4.4.4.4, Foreign port: 179
Nexthop: 4.4.4.1
Nexthop global: fe80::a00:27ff:fe7e:674a
```

```
Nexthop local: ::
BGP connection: non shared network

R1#show ip bgp summary
BGP router identifier 10.12.7.174, local AS number 200
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries
    Neighbor                 V   AS    MsgRcv    MsgSen TblVer   InQ   OutQ   Up/
    Down   State/PfxRcd
    2.2.2.2                  4   200    12         12       1      0      0
    00:05:02              0
    3.3.3.3                  4   200    12         12       1      0      0
    00:05:02              0
    4.4.4.4                  4   100    12         12       1      0      0
    00:05:02              0

    Total number of neighbors 3

    Total number of Established sessions 3
```

Route Redistribution in BGP

If there are routers that run both OSPF and BGP, certain OSPF routes might have to be sent to other eBGP peers. This can be achieved using the redistribution feature. Consider the following topology, in which R1 and R2 are eBGP peers, and R2 and R3 are OSPF peers. R2 is redistributing OSPF routes into BGP. The OSPF routes are sent to the R1 BGP routing table. This configuration assumes that all OSPF and eBGP sessions are up and running, and that only the redistribution must be configured.

Topology

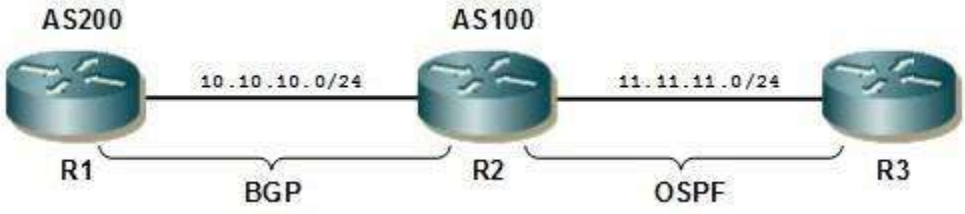


Figure 1-90: Redistribute with OSPF

R2

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 100`	Define the routing process. The number `100` specifies the AS number of R2.
`(config-router)#redistribute ospf`	Redistribute OSPF routes in the R2 routing table into the R1 BGP routing table.
`(config-router)#exit`	Exit Router-BGP mode.

Validation

```
#show ip bgp
BGP table version is 33, local router ID is 10.12.7.155
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled                S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric   LocPrf       Weight Path
*>   3.3.3.0/24       10.10.10.2            2        100          0      100 ?
*>   10.10.10.0/24    0.0.0.0               0        100          32768    i
    *                    10.10.10.2            0        100          0      100 i

Total number of prefixes 2
```

Add Multiple Instances of the Same Autonomous System

BGP supports adding the same AS number multiple times to influence the route selection process. This can be done using route maps, as described below.

Under normal circumstances, any route advertised by R1 is sent to R4 via two different routes, and then R4 selects the path from R2. This decision can be influenced by adding multiple instances of AS number 200 at R2.

Topology

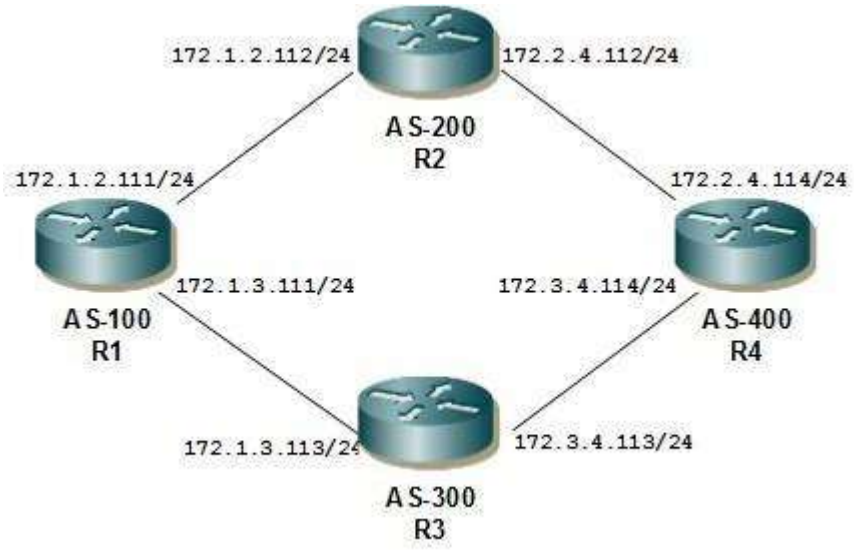


Figure 1-91: Multiple Instances of Same AS

R1

`#configure terminal`	Enter Configure mode.
`(config)#interface lo`	Enter loopback interface mode.
`(config-if)#ip address 44.44.44.1/24`	Specify the IP address for the interface.
`(config-if)#exit`	Exit loopback interface mode.
`(config)#router bgp 100`	Define the routing process with AS number `100`.

(config-router)#neighbor 172.1.2.112 remoteas 200	Define neighbor R2. 172.1.2.112 is the IP address of R2, and 200 is the AS number.
(config-router)#neighbor 172.1.3.113 remoteas 300	Define neighbor R3. 172.1.3.113 is the IP address of R2, and 300 is the AS number.
(config-router)#network 44.44.44.0/24	Advertise network 44.44.44.0/24 through BGP. This route reaches R4 via R2 and R3.

R2

#configure terminal	Enter Configure mode.
(config)#route-map mul_inst permit 10	Define the route-map multiple instance with permit definition sequence number 10.
(config-route-map)#set as-path prepend 200 200	Prepend AS number 200 two times to the AS_PATH attribute in the BGP Update message.
(config-route-map)#exit	Exit Route-map mode, and return to Configure mode.
(config)#router bgp 200	Define the routing process with AS number 200.
(config-router)#neighbor 172.1.2.111 remoteas 100	Define neighbor R1. 172.1.2.111 is the IP address of R1, and 100 is the AS number.
(config-router)#neighbor 172.2.4.114 remoteas 400	Define neighbor R4. 172.2.4.114 is the IP address of R2, and 400 is the AS number.
(config-router)#neighbor 172.2.4.114 routemap mul_inst out	Apply route-map multi inst to all outbound routes to R4.

R3

#configure terminal	Enter Configure mode.
(config)#router bgp 300	Define the routing process with AS number 300.
(config-router)#neighbor 172.1.3.111 remoteas 100	Define neighbor R1. 172.1.3.111 is the IP address of R1, and 100 is the AS number.
(config-router)#neighbor 172.3.4.114 remoteas 400	Define neighbor R4. 172.3.4.114 is the IP address of R4, and 400 is the AS number.

R4

#configure terminal	Enter Configure mode.
(config)#router bgp 400	Define the routing process with AS number 400.
(config-router)#neighbor 172.2.4.112 remoteas 200	Define neighbor R2. 172.2.4.112 is the IP address of R2, and 200 is the AS number.
(config-router)#neighbor 172.3.4.113 remoteas 300	Define neighbor R3. 172.3.4.113 is the IP address of R3, and 300 is the AS number.

Validation

```
#show ip bgp
BGP table version is 1, local router ID is 44.44.44.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - interna l,
l - labeled
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
Network Next Hop Metric LocPrf Weight Path
*> 44.44.44.0/24 0.0.0.0 0 100 32768 i
Total number of prefixes 1
```

Remove the Multi-Exit Disc Attribute from Update Messages

You can remove the Multi-Exit Disc (MED) attribute values from received update messages.

Topology

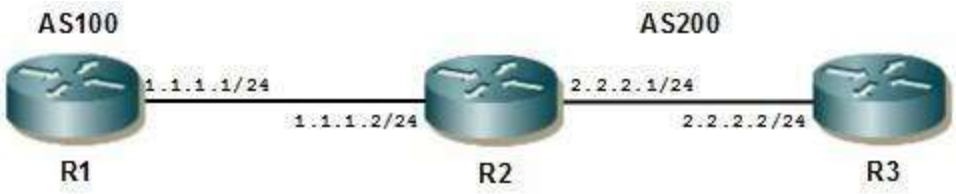


Figure 1-92: Remove MED Attribute

R1

`#configure terminal`	Enter Configure mode.
`(config)#route-map med permit 1`	Define the route-map MED with permit definition sequence number `1`.
`(config-route-map)#set metric 400`	Set the metric value.
`(config-route-map)#exit`	Exit Route-map mode, and return to Configure mode.
`(config)#router bgp 100`	Define the routing process with AS number `100`.
`(config-router)#neighbor 1.1.1.2 remote-as 200`	Define neighbor R2. `1.1.1.2` is the IP address of R2, and `200` is the AS number.
`(config-router)#neighbor 1.1.1.2 route-map med out`	Apply the route-map MED to all outbound routes to R2.

R3

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 200`	Define the routing process with AS number `200`.
`(config-router)#neighbor 2.2.2.1 remote-as 200`	Define neighbor R2. `2.2.2.1` is the IP address of R2, and `200` is the AS number.

Removing Sent and Received MED values

The following describes how to remove the received and sent MED values, respectively.

R2 - Remove Received MED Value

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 200`	Define the routing process with AS number `200`.
`(config-router)#neighbor 1.1.1.1 remote-as 100`	Define neighbor R1. `1.1.1.1` is the IP address of R1, and `100` is the AS number.

(config-router)#neighbor 2.2.2.2 remote-as 200	Define neighbor R3. 2.2.2.2 is the IP address of R3, and 200 is the AS number.
(config-router)#bgp bestpath med remove-recvmed	Enable the remove received MED value option.
R2 - Remove Send MED Value	
#configure terminal	Enter Configure mode.
(config)#router bgp 200	Define the routing process with AS number 200.
(config-router)#neighbor 1.1.1.1 remote-as 100	Define neighbor R1. 1.1.1.1 is the IP address of R1, and 100 is the AS number.
(config-router)#neighbor 2.2.2.2 remote-as 200	Define neighbor R3. 2.2.2.2 is the IP address of R3, and 200 is the AS number.
(config-router)#bgp bestpath med remove-sendmed	Enable the remove sent MED value option.

Validation

show ip bgp

BGP Four-Byte Autonomous System

Extended AS numbers can be mapped to 2-byte AS numbers if the value is less than, or equal to, 65535. If the AS number is higher than 65535, it cannot be mapped to a 2-byte AS number. Therefore, if a BGP speaker is configured with a non-mappable AS number, it must enable the BGP extended ASN capability in SWMRE.

Note: Autonomous System number 23456 is a reserved IANA number for AS transition; thus, it is recommended that no system be configured with 23456 as its AS number.

The extended ASN capability is disabled by default. However, when it is enabled, it is able to interoperate with a 2-byte AS-numbered speaker, in compliance with RFC 4893.

If a 4-byte AS number is configured in the provider's network using BGP MPLS VPN or standard IPv4/IPv6 BGP, it is recommended that the PE routers be 4-byte AS-enabled before connecting to 4-byte AS-enabled customer networks. For implications related to AS number transition issues, refer to RFC 4893.

You can also set up 4-byte AS-specific extended communities and route distinguishers (RDs) with limited capabilities. However, it is recommended that 2-byte AS-specific RDs and extended communities be used for regular deployment.

BGP encodes an ASN into four octets, so that more autonomous systems can be supported. Extended ASN capability is advertised in the Open message capabilities when the 4-octet ASN capability is enabled. When the 4-octet ASN capability is enabled, the valid ASN value range is <1-4294967295>, with the exception discussed in the first Note, above.

Note:Four-octet capability is disabled by default.

4-Octet ASN Capability Enabled on R1 and R2

In this example, 4-Octet ASN capability is enabled on BGP speakers R1 and R2.

Topology

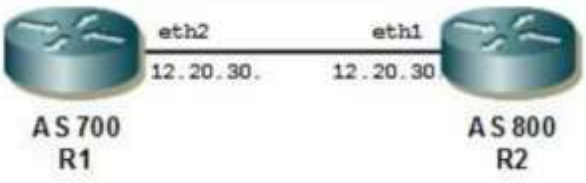


Figure 1-93: 4-Octet ASN on Both Routers

R1

`#configure terminal`	Enter Configure mode.
`(config)#bgp extended-asn-cap`	Enable 4-octet ASN capability.
`(config)#router bgp 400000`	Assign the ASN value (`400000`) to the router.
`(config-router)#neighbor 10.20.30.2 remote-as 7000`	Specify the neighbor's IP address (`10.20.30.2`) and the ASN value of the neighbor (`7000`).

R2

`#configure terminal`	Enter Configure mode.
`(config)#bgp extended-asn-cap`	Enable 4-octet ASN capability.
`(config)#router bgp 7000`	Assign the ASN value (`7000`) to the router.
`(config-router)#neighbor 10.20.30.1 remote-as 400000`	Specify the neighbor's IP address (`10.20.30.1`) and the ASN value of the neighbor (`400000`).

4-Octet ASN Capability Enabled on R1 and Disabled on R2

In the following two examples, 4-Octet ASN capability is enabled on BGP speaker R1 and disabled on R2.

Topology

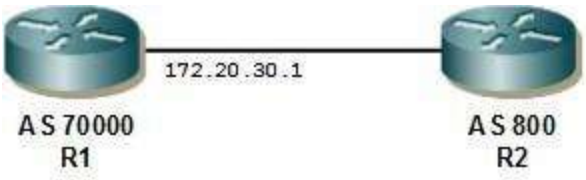


Figure 1-94: 4-Octet ASN on One Router

R1

`#configure terminal`	Enter Configure mode.
`(config)#bgp extended-asn-cap`	Enable 4-octet ASN capability.
`(config)#router bgp 70000`	Assign the ASN value (`70000`) to the router.
`(config-router)#neighbor 172.20.30.20 remoteas 800`	Specify the neighbor's IP address (`172.20.30.20`) and the ASN value of the neighbor (`800`).

R2

`#configure terminal`	Enter Configure mode.
`(config)#no bgp extended-asn-cap`	Disable 4-octet ASN capability.
`(config)#router bgp 800`	Assign the ASN value (`800`) to the router.
`(config-router)#neighbor 172.20.30.10 remoteas 23456`	Specify the neighbor's IP address (`172.20.30.10`) and the ASN value of the neighbor (`23456`).

Topology

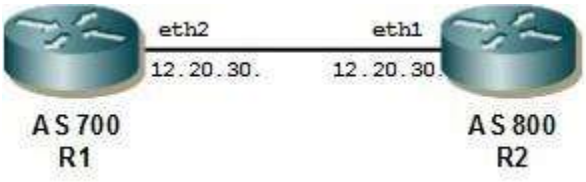


Figure 1-95: 4-Octet ASN

R1

`#configure terminal`	Enter Configure mode.
`(config)#bgp extended-asn-cap`	Enable 4-octet ASN capability.
`(config)#router bgp 700`	Assign the ASN value (`700`) to the router.
`(config-router)#neighbor 172.20.30.20 remoteas 800`	Specify the neighbor's IP address (`172.20.30.20`) and the ASN value of the neighbor (`800`).

R2

`#configure terminal`	Enter Configure mode.
`(config)#no bgp extended-asn-cap`	Disable 4-octet ASN capability.
`(config)#router bgp 800`	Assign the ASN value (`800`) to the router.
`(config-router)#neighbor 172.20.30.10 remoteas 700`	Specify the neighbor's IP address (`172.20.30.10`) and the ASN value of the neighbor (`700`).

Validation

show ip bgp summary, show ip bgp neighbors

BGP Extended Community Attribute

The Extended Community Attribute provides a mechanism for labeling information carried in BGP.

Extended Community with a 2-Byte ASN

In the following example, CE1, PE1, PE2, and CE2 are 2-byte-ASN capable, and do not support 4-byte-ASN capability.

Topology

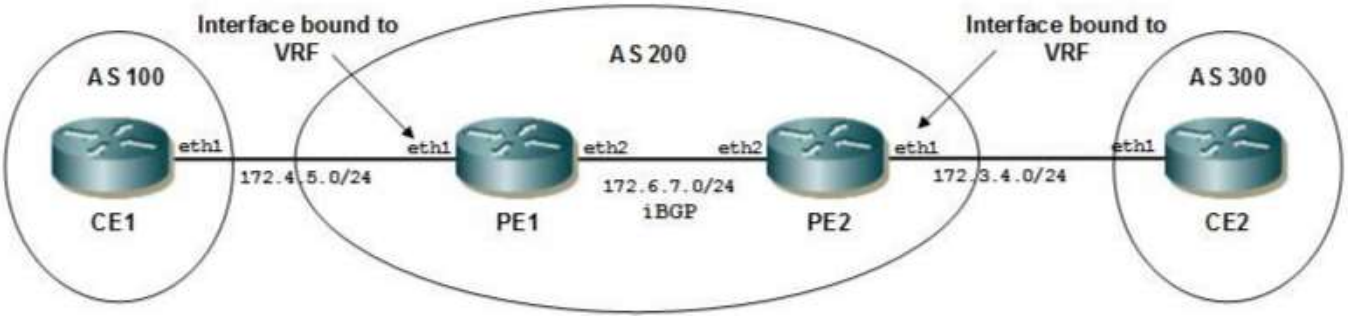


Figure 1-96: Extended Communities — 2-Byte ASN

CE1

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to configure, and enter Interface mode.
`(config-if)#ip address 172.4.5.115/24`	Configure the IP address on this interface
`(config-if)#exit`	Exit Interface mode, and return to Configure mode.
`(config)#router bgp 100`	Assign the ASN value (`100`) to the router. The ASN range is <1-65535>.
`(config-router)#neighbor 172.4.5.116 remoteas 200`	Specify the neighbor's IP address (`172.4.5.116`) and the ASN value of the neighbor (`200`).

CE2

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to configure, and enter Interface mode.
`(config-if)#ip address 172.3.4.114/24`	Configure the IP address on this interface
`(config-if)#exit`	Exit Interface mode, and return to Configure mode.
`(config)#router bgp 300`	Assign the ASN value (`300`) to the router. The ASN range is <1-65535>.
`(config-router)#neighbor 172.3.4.117 remoteas 200`	Specify the neighbor's IP address (`172.3.4.117`) and the ASN value of the neighbor (`200`).

PE1

`#configure terminal`	Enter Configure mode.
`(config)#ip vrf VRF1`	Specify the name of the VRF (`VRF1`) to be created.
`(config-vrf)#rd 100:10`	Assign a route distinguisher (RD) for the VRF, which is a unique value on the router. The RD value can be in ASN:NN or A.B.C.D:NN format.
`(config-vrf)#route-target both 100:10`	Specify the 2-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.

(config-vrf)#exit	Exit VRF mode, and return to Configure mode.
(config)#interface eth1	Specify the interface (eth1) to configure, and enter Interface mode.
(config-if)#ip vrf forwarding VRF1	Bind the interface (eth1) to the VRF (VRF1).
(config-if)#ip address 172.4.5.116/24	Configure the IP address on this interface
(config-if)#exit	Exit Interface mode, and return to Configure mode.
(config)#ip route vrf VRF1 75.1.1.0/24 eth1	Create a VRF static route.
(config)#interface eth2	Specify the interface (eth2) to configure, and enter Interface mode.
(config-if)#ip address 172.6.7.116/24	Configure the IP address on this interface
(config-if)#exit	Exit Interface mode, and return to Configure mode.
(config)#router bgp 200	Assign the ASN value (200) to the router.
(config-router)#neighbor 172.6.7.117 remoteas 200	Specify the neighbor's (PE2) IP address (172.6.7.117) and the ASN value of the neighbor (200). In this case, it is an iBGP connection, so both PE1 and PE2 are in the same AS.
(config-router)#address-family vpnv4 unicast	Enable the exchange of VPNv4 routing information among ISP PE-routers, and enter Address-Family-VPNv4 mode.
(config-router-af)#neighbor 172.6.7.117 activate	Enable the exchange of routing information with a peer router.
(config-router-af)#exit	Exit Address-Family-VPNv4 mode.
(config-router)#address-family ipv4 vrf VRF1	Enable the exchange of VRF routing information among ISP PE-routers, and enter Address-Family-VRF mode.
(config-router-af)#neighbor 172.4.5.115 remote-as 100	Specify the neighbor's (CE1) IP address and ASN value.
(config-router-af)#neighbor 172.4.5.115 sendcommunity both	Enable extended community attribute for the neighbor.
(config-router-af)#redistribute static	Configure static redistribution.
(config-router-af)#end	Exit Address-Family mode

PE2

`#configure terminal`	Enter Configure mode.
`(config)#ip vrf VRF1`	Specify the name of the VRF (`VRF1`) to be created.
`(config-vrf)#rd 100:10`	Assign a route distinguisher (RD) for the VRF.
`(config-vrf)#route-target both 100:10`	Specify the 2-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.
`(config-vrf)#exit`	Exit VRF mode, and return to Configure mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to configure, and enter Interface mode.
`(config-if)#ip vrf forwarding VRF1`	Bind the interface (eth1) to the VRF (`VRF1`).
`(config-if)#ip address 172.3.4.117/24`	Configure the IP address on this interface
`(config-if)#exit`	Exit Interface mode, and return to Configure mode.
`(config)#ip route vrf VRF1 100.1.1.0/24 eth1`	Create a VRF static route.
`(config)#interface eth2`	Specify the interface (`eth2`) to configure, and enter Interface mode.
`(config-if)#ip address 172.6.7.117/24`	Configure the IP address on this interface
`(config-if)#exit`	Exit Interface mode, and return to Configure mode.
`(config)#router bgp 200`	Assign the ASN value (`200`) to the router.
`(config-router)#neighbor 172.6.7.116 remoteas 200`	Specify the neighbor's (PE1) IP address (`172.6.7.116`) and the ASN value of the neighbor (`200`). In this case, it is an iBGP connection, so both PE1 and PE2 are in the same AS.
`(config-router)#address-family vpnv4 unicast`	Enable the exchange of VPNv4 routing information among ISP PE-routers, and enter Address-Family-VPNv4 mode.
`(config-router-af)#neighbor 172.6.7.116 activate`	Enable the exchange of routing information with a peer router.
`(config-router-af)#exit`	Exit Address-Family-VPNv4 mode.
`(config-router)#address-family ipv4 vrf VRF1`	Enable the exchange of VRF routing information among ISP PE-routers, and enter Address-Family-VRF mode.
`(config-router-af)#neighbor 172.3.4.114 remote-as 300`	Specify the neighbor's (CE2) IP address and ASN value.
`(config-router-af)#neighbor 172.3.4.114 sendcommunity both`	Enable extended community attribute for the neighbor.
`(config-router-af)#redistribute static`	Configure static redistribution.
`(config-router-af)#end`	Exit Address-Family mode

Validation

CE1

```
CE1#show ip bgp
BGP table version is 33, local router ID is 10.12.7.174
```

```
    Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
    l - labeled               S Stale
    Origin codes: i - IGP, e - EGP, ? - incomplete
    Network          Next Hop            Metric    LocPrf       Weight Path
 *>  75.1.1.0/24       172.4.5.116           0        100           0      200 ?
 *>  100.1.1.0/24      172.4.5.116           0        100           0      200 ?

Total number of prefixes 2
CE1#show ip bgp neighbors
BGP neighbor is 172.4.5.116, remote AS 200, local AS 100, external link
  BGP version 4, remote router ID 172.6.7.116
  BGP state = Established, up for 00:32:37
  Last read 00:32:37, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 209 messages, 0 notifications, 0 in queue
  Sent 215 messages, 139 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 IPv4
  BGP table version 33, neighbor version 33
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 172.4.5.115, Local port: 179
Foreign host: 172.4.5.116, Foreign port: 53816
Nexthop: 172.4.5.115
Nexthop global: fe80::a00:27ff:fecc:47a6
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:32:48, due to BGP Notification sent
Notification Error Message: (OPEN Message Error/Bad Peer AS.)

CE1#show ip bgp vrf all
BGP table version is 34, local router ID is 10.12.7.174
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled                S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   75.1.1.0/24       172.4.5.116           0        100           0      200 ?
*>   100.1.1.0/24      172.4.5.116           0        100           0      200 ?

Total number of prefixes 2
CE1#show ip bgp summary vrf all
BGP router identifier 10.12.7.174, local AS number 100
BGP table version is 34
```

```
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V    AS   MsgRcv    MsgSen TblVer    InQ    OutQ    Up/ Down
State/PfxRcd
172.4.5.116              4    200 210        355       34       0       0  00:33:11
2
    Total number of neighbors 1

    Total number of Established sessions 1
```

PE1

```
    PE1#show ip bgp vpnv4 all
    Status codes: s suppressed, d damped, h history, * valid, > best, i -
    internal, l - labeled                S Stale
    Origin codes: i - IGP, e - EGP, ? - incomplete

        Network          Next Hop            Metric    LocPrf       Weight Path
    Route Distinguisher: 100:10 (Default for VRF VRF1)
    *> l 75.1.1.0/24      0.0.0.0             0         100          32768    ? *>i
    100.1.1.0/24      172.6.7.117          0       100           0        ?
     Announced routes count = 1
     Accepted routes count = 1
    Route Distinguisher: 100:10
    *>i  100.1.1.0/24     172.6.7.117           0       100           0        ?
    PE1#show ip bgp
    PE1#
    PE1#
    PE1#show ip bgp vrf all
    BGP table version is 1, local router ID is 172.6.7.116
    Status codes: s suppressed, d damped, h history, * valid, > best, i -
    internal, l - labeled                S Stale
    Origin codes: i - IGP, e - EGP, ? - incomplete

        Network          Next Hop            Metric    LocPrf       Weight Path

    BGP Route Table for VRF VRF1
    *> l 75.1.1.0/24      0.0.0.0             0         100          32768    ? *>i
    100.1.1.0/24      172.6.7.117          0       100           0        ?

    Total number of prefixes 2
    PE1#show ip bgp summary vrf all
    BGP router identifier 172.6.7.116, local AS number 200
    BGP VRF VRF1 Route Distinguisher: 100:10
    BGP table version is 1
    1 BGP AS-PATH entries
    0 BGP community entries

    Neighbor                 V   AS    MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
    Down   State/PfxRcd
    172.4.5.115              4   100   87         90       1      0      0
```

```
    00:42:30              0

    Total number of neighbors 1

    Total number of Established sessions 1
    BGP router identifier 172.6.7.116, local AS number 200
    BGP table version is 43
    1 BGP AS-PATH entries
    0 BGP community entries
Neighbor                 V   AS    MsgRcv    MsgSen TblVer    InQ   OutQ   Up/ Down
State/PfxRcd
172.6.7.117               4   200    90          91      43       0       0
00:40:35               0

Total number of neighbors 1

Total number of Established sessions 1
PE1#show ip bgp neighbors
BGP neighbor is 172.6.7.117, remote AS 200, local AS 200, internal link
  BGP version 4, remote router ID 172.6.7.117
  BGP state = Established, up for 00:40:35
  Last read 00:40:35, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family VPNv4 Unicast: advertised and received
  Received 89 messages, 1 notifications, 0 in queue
  Sent 91 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv4 IPv4
  BGP table version 43, neighbor version 43
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
0 announced prefixes

 For address family: VPNv4 IPv4
  BGP table version 4, neighbor version 4
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
1 accepted prefixes
  1 announced prefixes

 Connections established 2; dropped 1
Local host: 172.6.7.116, Local port: 179
Foreign host: 172.6.7.117, Foreign port: 34206
Nexthop: 172.6.7.116
Nexthop global: fe80::a00:27ff:feb1:aa0
Nexthop local: ::
BGP connection: non shared network
```

```
Last Reset: 00:40:36, due to BGP Notification received
Notification Error Message: (Cease/Administratively Shutdown.)

BGP neighbor is 172.4.5.115, vrf VRF1, remote AS 100, local AS 200, external link
  BGP version 4, remote router ID 10.12.7.174
  BGP state = Established, up for 00:42:30
  Last read 00:42:30, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 87 messages, 0 notifications, 0 in queue
  Sent 90 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30
     seconds For address family: IPv4 IPv4
      BGP table version 1, neighbor version 1
      Index 1, Offset 0, Mask 0x2
      Community attribute sent to this neighbor (both)
      0 accepted prefixes
      0 announced prefixes

     Connections established 1; dropped 0
    Local host: 172.4.5.116, Local port: 53816
    Foreign host: 172.4.5.115, Foreign port: 179
    Nexthop: 172.4.5.116
    Nexthop global: fe80::a00:27ff:fef4:8dcf
    Nexthop local: ::
    BGP connection: non shared network
```

PE2

```
    PE2#show ip bgp vrf all
    BGP table version is 1, local router ID is 172.6.7.117
    Status codes: s suppressed, d damped, h history, * valid, > best, i -
    internal, l - labeled                S Stale
    Origin codes: i - IGP, e - EGP, ? - incomplete

        Network          Next Hop            Metric    LocPrf       Weight Path

    BGP Route Table for VRF VRF1
    *>i  75.1.1.0/24       172.6.7.116          0        100          0       ? *> l
    100.1.1.0/24      0.0.0.0             0        100          32768    ?

    Total number of prefixes 2
    PE2#show ip bgp summary vrf all
    BGP router identifier 172.6.7.117, local AS number 200
    BGP VRF VRF1 Route Distinguisher: 100:10
    BGP table version is 1
    1 BGP AS-PATH entries
    0 BGP community entries
```

```
    Neighbor                 V    AS    MsgRcv    MsgSen TblVer    InQ    OutQ    Up/
     Down   State/PfxRcd
    172.3.4.114               4    300    86          87        1       0       0
    00:42:09                 0

    Total number of neighbors 1

    Total number of Established sessions 1
    BGP router identifier 172.6.7.117, local AS number 200
    BGP table version is 43
    1 BGP AS-PATH entries
    0 BGP community entries

    Neighbor                 V    AS    MsgRcv    MsgSen TblVer    InQ    OutQ    Up/
     Down   State/PfxRcd
    172.6.7.116               4    200    87          86       43       0       0
    00:42:10                 0

    Total number of neighbors 1
Total number of Established sessions 1
PE2#show ip bgp neighbors
BGP neighbor is 172.6.7.116, remote AS 200, local AS 200, internal link
  BGP version 4, remote router ID 172.6.7.116
  BGP state = Established, up for 00:42:10
  Last read 00:42:10, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family VPNv4 Unicast: advertised and received
  Received 87 messages, 0 notifications, 0 in queue
  Sent 86 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv4 IPv4
  BGP table version 43, neighbor version 43
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
0 announced prefixes

 For address family: VPNv4 IPv4
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
1 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0 Local
host: 172.6.7.117, Local port: 34206
Foreign host: 172.6.7.116, Foreign port:
179 Nexthop: 172.6.7.117
```

```
Nexthop global: fe80::a00:27ff:fe0b:a48
Nexthop local: ::
BGP connection: non shared network

BGP neighbor is 172.3.4.114, vrf VRF1, remote AS 300, local AS 200, external link
  BGP version 4, remote router ID 10.12.7.120
  BGP state = Established, up for 00:42:09
  Last read 00:42:09, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 86 messages, 0 notifications, 0 in queue
  Sent 87 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (standard)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 172.3.4.117, Local port: 60754
    Foreign host: 172.3.4.114, Foreign port: 179
    Nexthop: 172.3.4.117
    Nexthop global: fe80::a00:27ff:fe9f:b825
    Nexthop local: ::
    BGP connection: non shared network
```

CE2

```
    CE2#show ip bgp vpnv4 all
    CE2#show ip bgp
    BGP table version is 44, local router ID is 10.12.7.120
    Status codes: s suppressed, d damped, h history, * valid, > best, i -
    internal, l - labeled               S Stale
    Origin codes: i - IGP, e - EGP, ? - incomplete

        Network          Next Hop            Metric    LocPrf       Weight Path
    *>   75.1.1.0/24       172.3.4.117          0        100           0      200 ?
    *>   100.1.1.0/24      172.3.4.117          0        100           0      200 ?

    Total number of prefixes 2
    CE2#
    CE2#
    CE2#show ip bgp vrf all
    BGP table version is 44, local router ID is 10.12.7.120
    Status codes: s suppressed, d damped, h history, * valid, > best, i -
    internal, l - labeled               S Stale
    Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
    Network          Next Hop            Metric    LocPrf       Weight Path
 *>  75.1.1.0/24      172.3.4.117           0        100           0      200 ?
 *>  100.1.1.0/24     172.3.4.117           0        100           0      200 ?

  Total number of prefixes 2
  CE2#show ip bgp summary vrf all
  BGP router identifier 10.12.7.120, local AS number 300
  BGP table version is 44
  1 BGP AS-PATH entries
  0 BGP community entries

  Neighbor                 V   AS   MsgRcv     MsgSen TblVer   InQ   OutQ   Up/
   Down   State/PfxRcd
  172.3.4.117              4   200  190         377      44      0      0
  00:42:16                2

  Total number of neighbors 1

  Total number of Established sessions 1
  CE2#show ip bgp neighbors
  BGP neighbor is 172.3.4.117, remote AS 200, local AS 300, external link
    BGP version 4, remote router ID 172.6.7.117
    BGP state = Established, up for 00:42:16
    Last read 00:42:16, hold time is 90, keepalive interval is 30 seconds
    Neighbor capabilities:
      Route refresh: advertised and received (old and new)
      Address family IPv4 Unicast: advertised and received
    Received 190 messages, 0 notifications, 0 in queue
  Sent 274 messages, 103 notifications, 0 in
  queue Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 IPv4
  BGP table version 44, neighbor version 44
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  2 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 172.3.4.114, Local port: 179
Foreign host: 172.3.4.117, Foreign port: 60754
Nexthop: 172.3.4.114
Nexthop global: fe80::a00:27ff:fe65:1973
Nexthop local: ::
BGP connection: non shared network
Last Reset: 00:42:17, due to BGP Notification sent
Notification Error Message: (OPEN Message Error/Bad Peer AS.)
```

Extended Community with a 4-Byte ASN

In the following example, CE1, PE1, PE2, and CE2 support 4-byte ASN capability.

Note: PE1 and PE2 should both either be 4-byte-ASN capable or 2-byte-ASN capable. Support for the combination of one 4-byte-ASN capable PE with one 2-byte-ASN-capable PE is currently unavailable.

Topology

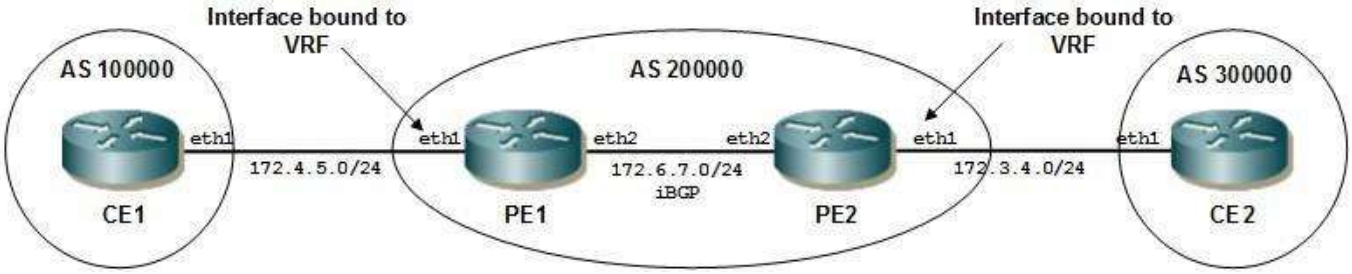


Figure 1-97: Extended Communities — 4-Byte ASN

CE1

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to configure, and enter Interface mode.
`(config-if)#ip address 172.4.5.115/24`	Configure the IP address on this interface
`(config-if)#exit`	Exit Interface mode, and return to Configure mode.
`(config)#bgp extended-asn-cap`	Enable 4-octet ASN capability.
`(config)#router bgp 100000`	Assign the ASN value (`100000`) to the router. The ASN range is <1-4294967295>.
`(config-router)#neighbor 172.4.5.116 remoteas 200000`	Specify the neighbor's IP address (`172.4.5.116`) and the ASN value of the neighbor (`200000`).

PE1

`#configure terminal`	Enter Configure mode.
`(config)#bgp extended-asn-cap`	Enable 4-octet ASN capability. Dynamic change from 2byte to 4-byte capability, or vice versa, is not allowed, unless the VRF is removed.
`(config)#ip vrf VRF1`	Specify the name of the VRF (`VRF1`) to be created.
`(config-vrf)#rd 1.1.1.1:200`	Assign a 4-byte route distinguisher (RD) for the VRF, which is a unique value on the router. The RD value can be in A.B.C.D:NN format.
`(config-vrf)#route-target both 1.1.1.1:200`	Specify the 4-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.
`(config-vrf)#exit`	Exit VRF mode, and return to Configure mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to configure, and enter Interface mode.
`(config-if)#ip vrf forwarding VRF1`	Bind the interface (eth1) to the VRF (`VRF1`).

(config-if)#ip address 172.4.5.116/24	Configure the IP address on this interface
(config-if)#exit	Exit Interface mode, and return to Configure mode.
(config)#ip route vrf VRF1 50.1.1.0/24 eth1	Create a VRF static route.
(config)#interface eth2	Specify the interface (eth2) to configure, and enter Interface mode.
(config-if)#ip address 172.6.7.116/24	Configure the IP address on this interface
(config-if)#exit	Exit Interface mode, and return to Configure mode.
(config)#router bgp 200000	Assign the ASN value (200000) to the router.
(config-router)#neighbor 172.6.7.117 remoteas 200000	Specify the neighbor's (PE2) IP address (172.6.7.117) and the ASN value of the neighbor (200000). In this case, it is an iBGP connection, so both PE1 and PE2 are in the same AS.
(config-router)#address-family vpnv4 unicast	Enable the exchange of VPNv4 routing information among ISP PE-routers, and enter Address-Family-VPNv4 mode.
(config-router-af)#neighbor 172.6.7.117 activate	Enable the exchange of routing information with a peer router.
(config-router-af)#exit	Exit Address-Family-VPNv4 mode.
(config-router)#address-family ipv4 vrf VRF1	Enable the exchange of VRF routing information among ISP PE-routers, and enter Address-Family-VRF mode.
(config-router-af)#neighbor 172.4.5.115 remote-as 100000	Specify the neighbor's (CE1) IP address and ASN value.
(config-router-af)#neighbor 172.4.5.115 sendcommunity both	Enable extended community attribute for the neighbor.
(config-router-af)#redistribute static	Configure static redistribution.
(config-router-af)#end	Exit Address-Family mode

PE2

#configure terminal	Enter Configure mode.
(config)#bgp extended-asn-cap	Enable 4-octet ASN capability. Dynamic change from 2byte to 4-byte capability, or vice versa, is not allowed, unless the VRF is removed.
(config)#ip vrf VRF1	Specify the name of the VRF (VRF1) to be created.
(config-vrf)#rd 1.1.1.1:200	Assign a 4-byte route distinguisher (RD) for the VRF.
(config-vrf)#route-target both 1.1.1.1:200	Specify the 4-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.
(config-vrf)#exit	Exit VRF mode, and return to Configure mode.
(config)#interface eth1	Specify the interface (eth2) to configure, and enter Interface mode.
(config-if)#ip vrf forwarding VRF1	Bind the interface (eth1) to the VRF (VRF1).
(config-if)#ip address 172.3.4.117/24	Configure the IP address on this interface
(config-if)#exit	Exit Interface mode, and return to Configure mode.
(config)#ip route vrf VRF1 200.1.1.0/24 eth1	Create a VRF static route.

(config)#interface eth2	Specify the interface (eth2) to configure, and enter Interface mode.
(config-if)#ip address 172.6.7.117/24	Configure the IP address on this interface
(config-if)#exit	Exit Interface mode, and return to Configure mode.
(config)#router bgp 200000	Assign the ASN value (200000) to the router.
(config-router)#neighbor 172.6.7.116 remoteas 200000	Specify the neighbor's (PE2) IP address (172.6.7.116) and the ASN value of the neighbor (200000). In this case, it is an iBGP connection, so both PE1 and PE2 are in the same AS.
(config-router)#address-family vpnv4 unicast	Enable the exchange of VPNv4 routing information among ISP PE-routers, and enter Address-Family-VPNv4 mode.
(config-router-af)#neighbor 172.6.7.116 activate	Enable the exchange of routing information with a peer router.
(config-router-af)#exit	Exit Address-Family-VPNv4 mode.
(config-router)#address-family ipv4 vrf VRF1	Enable the exchange of VRF routing information among ISP PE-routers, and enter Address-Family-VRF mode.
(config-router-af)#neighbor 172.3.4.114 remote-as 300000	Specify the neighbor's (CE1) IP address and ASN value.
(config-router-af)#neighbor 172.4.5.114 sendcommunity both	Enable extended community attribute for the neighbor.
(config-router-af)#redistribute static	Configure static redistribution.
(config-router-af)#end	Exit Address-Family mode

CE2

#configure terminal	Enter Configure mode.
(config)#interface eth1	Specify the interface (eth1) to configure, and enter Interface mode.
(config-if)#ip address 172.3.4.114/24	Configure the IP address on this interface
(config-if)#exit	Exit Interface mode, and return to Configure mode.
(config)#bgp extended-asn-cap	Enable 4-octet ASN capability.
(config)#router bgp 300000	Assign the ASN value (300000) to the router.
(config-router)#neighbor 172.3.4.117 remoteas 200000	Specify the neighbor's IP address (172.3.4.117) and the ASN value of the neighbor (200000).

Validation

show ip bgp, show ip bgp neighbors, show ip bgp vpnv4 all, show ip bgp vrf all, show ip bgp summary vrf all

Nexthop Tracking

Nexthop tracking is used to notify the BGP process asynchronously whenever there is any change in the IGP routes. It reduces the convergence time of BGP routes when IGP routes are changed.

Topology

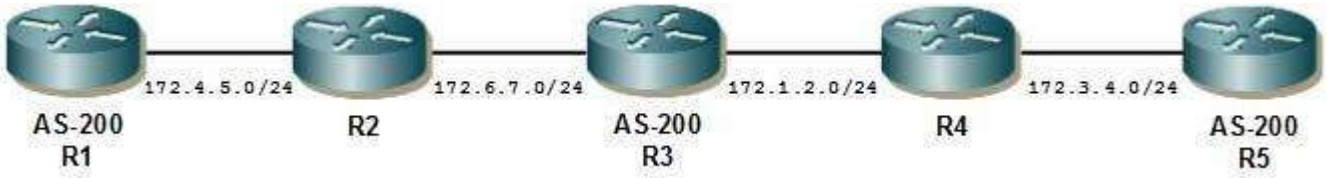


Figure 1-98: BGP Nexthop Tracking

R1

`#configure terminal`	Enter Configure mode.
`(config)#interface lo`	Specify the loopback interface, and enter Interface mode.
`(config-if)#ip address 100.100.100.100/32`	Configure the IP address on this interface.
`(config-if)#exit`	Exit Interface mode, and return to Configure mode.
`(config)#router bgp 200`	Assign the ASN value (`200`) to the router. The ASN range is <1-65535>.
`(config-router)#neighbor 200.200.200.200 remote-as 200`	Specify the neighbor's IP address (`200.200.200.200`) and the ASN value of the neighbor (`200`).
`(config-router)#neighbor 200.200.200.200 update-source lo`	Specify the routing update source.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.
`(config)#router ospf 1`	Configure the OSPF process (`1`).
`#configure terminal`	Enter Configure mode.
`(config)#interface lo`	Specify the loopback interface, and enter Interface mode.
`(config-if)#ip address 100.100.100.100/32`	Configure the IP address on this interface.
`(config-if)#exit`	Exit Interface mode, and return to Configure mode.
`(config-router)#network 172.4.5.0/24 area 0`	Advertise the network in Area `0`.
`(config-router)#redistribute connected`	Redistribute the connected routes.

R2

`#configure terminal`	Enter Configure mode.
`(config)#router ospf 1`	Configure the OSPF process (`1`).
`(config-router)#network 172.4.5.0/24 area 0`	Advertise the network in Area `0`.
`(config-router)#network 172.6.7.0/24 area 0`	Advertise the network in Area `0`.

R3

`#configure terminal`	Enter Configure mode.
`(config)#interface lo`	Specify the loopback interface, and enter Interface mode.
`(config-if)#ip address 200.200.200.200/32`	Configure the IP address on this interface.
`(config-if)#exit`	Exit Interface mode, and return to Configure mode.
`(config)#router bgp 200`	Assign the ASN value (`200`) to the router.

(config-router)#neighbor 100.100.100.100 remote-as 200	Specify the neighbor's IP address (100.100.100.100) and the ASN value of the neighbor (200).
(config-router)#neighbor 100.100.100.100 update-source 200.200.200.200	Specify the routing update source.
(config-router)#neighbor 220.220.220.220 remote-as 200	Specify the neighbor's IP address (220.220.220.220) and the ASN value of the neighbor (200).
(config-router)#neighbor 220.220.220.220 update-source 150.150.150.150	Specify the routing update source.
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#router ospf 1	Configure the OSPF process (1).
(config-router)#network 172.6.7.0/24 area 0	Advertise the network in Area 0.
(config-router)#network 172.1.2.0/24 area 0	Advertise the network in Area 0.
(config-router)#redistribute connected	Redistribute the connected routes.
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#bgp nexthop-trigger enable	Enable Nexthop tracking.

R4

#configure terminal	Enter Configure mode.
(config)#router ospf 1	Configure the OSPF process (1).
(config-router)#network 172.1.2.0/24 area 0	Advertise the network in Area 0.
(config-router)#network 172.3.4.0/24 area 0	Advertise the network in Area 0.

R5

#configure terminal	Enter Configure mode.
(config)#interface lo	Specify the loopback interface, and enter Interface mode.
(config-if)#ip address 220.220.220.220/32	Configure the IP address on this interface.
(config-if)#exit	Exit Interface mode, and return to Configure mode.
(config)#router bgp 200	Assign the ASN value (200) to the router.
(config-router)#neighbor 150.150.150.150 remote-as 200	Specify the neighbor's IP address (200.200.200.200) and the ASN value of the neighbor (200).
(config-router)#neighbor 150.150.150.150 update-source lo	Specify the routing update source.
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#router ospf 1	Configure the OSPF process (1).
(config-router)#network 172.3.4.0/24 area 0	Advertise the network in Area 0.
(config-router)#redistribute connected	Redistribute the connected routes.

Validation

show ip bgp summary, show ip bgp neighbors, show ip bgp, show bgp nexthop-tracking, show ip bgp scan

Nexthop Tracking Delay Timer

The delay interval between routing table walks can be configured for nexthop delay tracking. This time determines how long BGP waits before it starts walking the full BGP routing table after receiving notification from NSM about a next-hop change.

Topology

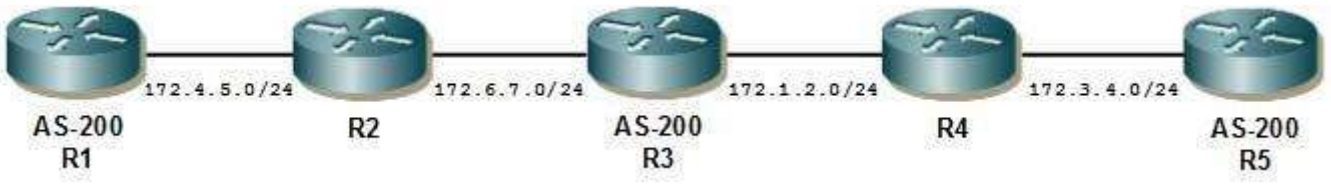


Figure 1-99: Topology for Nexthop Tracking Delay Timer

R1

`#configure terminal`	Enter Configure mode.
`(config)#interface lo`	Specify the loopback interface, and enter Interface mode.
`(config-if)#ip address 100.100.100.100/32`	Configure the IP address on this interface.
`(config-if)#exit`	Exit Interface mode, and return to Configure mode.
`(config)#router bgp 200`	Assign the ASN value (`200`) to the router. The ASN range is <1-65535>.
`(config-router)#neighbor 200.200.200.200 remote-as 200`	Specify the neighbor's IP address (`200.200.200.200`) and the ASN value of the neighbor (`200`).
`(config-router)#neighbor 200.200.200.200 update-source lo`	Specify the routing update source.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.
`(config)#router ospf 1`	Configure the OSPF process (`1`).
`(config-router)#network 172.4.5.0/24 area 0`	Advertise the network in Area `0`.
`(config-router)#redistribute connected`	Redistribute the connected routes.

R2

`#configure terminal`	Enter Configure mode.
`(config)#router ospf 1`	Configure the OSPF process (`1`).
`(config-router)#network 172.4.5.0/24 area 0`	Advertise the network in Area `0`.
`(config-router)#network 172.6.7.0/24 area 0`	Advertise the network in Area `0`.

R3

`#configure terminal`	Enter Configure mode.
`(config)#interface lo`	Specify the loopback interface, and enter Interface mode.
`(config-if)#ip address 200.200.200.200/32`	Configure the IP address on this interface.
`(config-if)#exit`	Exit Interface mode, and return to Configure mode.
`(config)#router bgp 200`	Assign the ASN value (`200`) to the router.
`(config-router)#neighbor 100.100.100.100 remote-as 200`	Specify the neighbor's IP address (`100.100.100.100`) and the ASN value of the neighbor (`200`).

(config-router)#neighbor 100.100.100.100 update-source 200.200.200.200	Specify the routing update source.
(config-router)#neighbor 220.220.220.220 remote-as 200	Specify the neighbor's IP address (220.220.220.220) and the ASN value of the neighbor (200).
(config-router)#neighbor 220.220.220.220 update-source 150.150.150.150	Specify the routing update source.
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#router ospf 1	Configure the OSPF process (1).
(config-router)#network 172.6.7.0/24 area 0	Advertise the network in Area 0.
(config-router)#network 172.1.2.0/24 area 0	Advertise the network in Area 0.
(config-router)#redistribute connected	Redistribute the connected routes.
#configure terminal	Enter Configure mode.
(config)#interface lo	Specify the loopback interface, and enter Interface mode.
(config-if)#ip address 200.200.200.200/32	Configure the IP address on this interface.
(config-if)#exit	Exit Interface mode, and return to Configure mode.
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#bgp nexthop-trigger enable	Enable nexthop tracking.
(config)#bgp nexthop-trigger delay 20	Configure the nexthop trigger-delay time interval.
R4	
#configure terminal	Enter Configure mode.
(config)#router ospf 1	Configure the OSPF process (1).
(config-router)#network 172.1.2.0/24 area 0	Advertise the network in Area 0.
(config-router)#network 172.3.4.0/24 area 0	Advertise the network in Area 0.
R5	
#configure terminal	Enter Configure mode.
(config)#interface lo	Specify the loopback interface, and enter Interface mode.
(config-if)#ip address 220.220.220.220/32	Configure the IP address on this interface.
(config-if)#exit	Exit Interface mode, and return to Configure mode.
(config)#router bgp 200	Assign the ASN value (200) to the router.
(config-router)#neighbor 150.150.150.150 remote-as 200	Specify the neighbor's IP address (150.150.150.150) and the ASN value of the neighbor (200).
(config-router)#neighbor 150.150.150.150 update-source lo	Specify the routing update source.
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#router ospf 1	Configure the OSPF process (1).
(config-router)#network 172.3.4.0/24 area 0	Advertise the network in Area 0.
(config-router)#redistribute connected	Redistribute the connected routes.

Validation

show ip bgp summary, show ip bgp neighbors, show ip bgp, show bgp nexthop-tracking, show ip bgp scan

R1

```
#show ip bgp summary
BGP router identifier 10.12.20.71, local AS number 200
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/
Down   State/PfxRcd
200.200.200.200          4   200   15         16       1      0      0  00:06:37
0
Total number of neighbors 1

Total number of Established sessions 1

#show ip bgp neighbors
BGP neighbor is 200.200.200.200, remote AS 200, local AS 200, internal link
  BGP version 4, remote router ID 200.200.200.200
  BGP state = Established, up for 00:06:40
  Last read 00:06:40, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 15 messages, 0 notifications, 0 in queue
  Sent 16 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is lo
 For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 100.100.100.100, Local port: 37676
Foreign host: 200.200.200.200, Foreign port: 179 Nexthop:
100.100.100.100
Nexthop global: :: Nexthop
local: ::
BGP connection: non shared network

#show bgp nexthop-tracking
Configured NHT: DISABLED
NHT Delay time-interval : 5
BGP VRF: (Default) VRF_ID 0
```

```
BGP Instance: (Default), AS: 200, router-id 10.12.20.71

#show ip bgp scan
BGP VRF: (Default) VRF_ID 0 BGP
scan interval is 60 scan
remain-time: 38 Current BGP
nexthop cache:
```

R3

```
#show ip bgp summary
BGP router identifier 200.200.200.200, local AS number 200
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS    MsgRcv    MsgSen TblVer    InQ   OutQ    Up/
Down   State/PfxRcd
100.100.100.100          4   200    17          19       1       0       0 00:07:41
0
220.220.220.220           4  200    95         101       1       0       0
00:07:12               0

Total number of neighbors 2

Total number of Established sessions 2

#show ip bgp neighbors
BGP neighbor is 100.100.100.100, remote AS 200, local AS 200, internal link
  BGP version 4, remote router ID 10.12.20.71
  BGP state = Established, up for 00:07:46
  Last read 00:07:46, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 17 messages, 0 notifications, 0 in queue
  Sent 19 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
  seconds Update source is 200.200.200.200
 For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 200.200.200.200, Local port: 179
Foreign host: 100.100.100.100, Foreign port: 37676 Nexthop:
200.200.200.200
```

```
Nexthop global: :: Nexthop local:
::
BGP connection: non shared network

BGP neighbor is 220.220.220.220, remote AS 200, local AS 200, internal link
  BGP version 4, remote router ID 220.220.220.220
  BGP state = Established, up for 00:07:17
  Last read 00:07:17, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 94 messages, 1 notifications, 0 in queue
  Sent 97 messages, 4 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
  seconds Update source is 150.150.150.150
 For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 6; dropped 5
Local host: 150.150.150.150, Local port: 39831
Foreign host: 220.220.220.220, Foreign port: 179
    Nexthop: 150.150.150.150
    Nexthop global: :: Nexthop
    local: ::
    BGP connection: non shared network
    Last Reset: 00:07:22, due to BGP Notification received
    Notification Error Message: (Cease/Other Configuration Change.)

    #show bgp nexthop-tracking
    Configured NHT: ENABLED
    NHT Delay time-interval : 5
    BGP VRF: (Default) VRF_ID 0
    BGP Instance: (Default), AS: 200, router-id 200.200.200.200
    NHT is Enabled
    Recvd Msg count from RIB: 0
    NHT delay-timer remaining seconds: 0
    BGP nexthop(s):
    Total number of IPV4 nexthops : 0
    Total number of IPV6 nexthops : 0

    #show ip bgp scan
    BGP VRF: (Default) VRF_ID 0 BGP
    scan interval is 60 scan
    remain-time: 11 Current BGP
    nexthop cache:
```

R5

```
#show ip bgp summary
BGP router identifier 220.220.220.220, local AS number 200
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS    MsgRcv    MsgSen TblVer   InQ   OutQ   Up/
Down   State/PfxRcd
150.150.150.150          4   200    99        101       1      0      0
00:08:26                0

Total number of neighbors 1

Total number of Established sessions 1

#show ip bgp neighbors
BGP neighbor is 150.150.150.150, remote AS 200, local AS 200, internal link
  BGP version 4, remote router ID 200.200.200.200
  BGP state = Established, up for 00:08:29
  Last read 00:08:29, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 96 messages, 3 notifications, 0 in queue
  Sent 99 messages, 2 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Update source is lo
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 6; dropped 5
Local host: 220.220.220.220, Local port: 179
Foreign host: 150.150.150.150, Foreign port: 39831 Nexthop:
220.220.220.220
Nexthop global: :: Nexthop
local: ::
BGP connection: non shared network
Last Reset: 00:08:34, due to BGP Notification sent
Notification Error Message: (Cease/Other Configuration Change.)

#show bgp nexthop-tracking
Configured NHT: DISABLED
NHT Delay time-interval : 5
BGP VRF: (Default) VRF_ID 0
BGP Instance: (Default), AS: 200, router-id 220.220.220.220
```

```
#show ip bgp scan
BGP VRF: (Default) VRF_ID 0
BGP scan interval is 60 scan
remain-time: 22 Current BGP
nexthop cache:
```

BGP Graceful Restart

During a BGP restart, all BGP peers detect that a session had gone down and come back up. SWMRE invalidates the associated portion of the IP forwarding cache, does a BGP route re-computation, and generates BGP routing updates. The forwarding tables become corrupted and unstable.

Graceful restart helps minimize these negative effects on routing caused by a BGP restart by allowing the restarting BGP router to temporarily retain routing information and continue forwarding packets while BGP restarts. In this way, even while a router rebuilds routing and forwarding tables, the router continues to operate across the TCP connection.

Graceful restart allows a restarting router, and its neighbors, to continue forwarding packets, without disrupting network performance. Because neighboring routers assist in the restart, the restarting router can quickly resume full operation.

The graceful restart capability extends to the case when a configuration change forces a peer reset.

Graceful reset is a refinement of graceful restart to help ensure smooth restarts when a configuration change forces BGP peer reset.

In addition, graceful restart is available for BGP with MPLS, when BGP is used to distribute MPLS-VPN labels. Without the graceful restart capability, when BGP distributes MPLS-VPN labels, a BGP route withdrawal accompanies the associated label withdrawal. This causes a routing flap and a BGP route re-computation, generating BGP routing updates, and unnecessary disruption in the forwarding tables. Also, when BGP goes down, label-switched routers (LSRs) clear FEC label bindings (for VPN routes) learned from the restarting LSR. As a result, MPLS forwarding is impacted across the restart.

The graceful restart and graceful reset capabilities provide a way to save MPLS forwarding states in NSM. These capabilities also synchronize with the VRF table when BGP goes down in the control plane. This feature is supported for the VPNv4 address family.

Topology

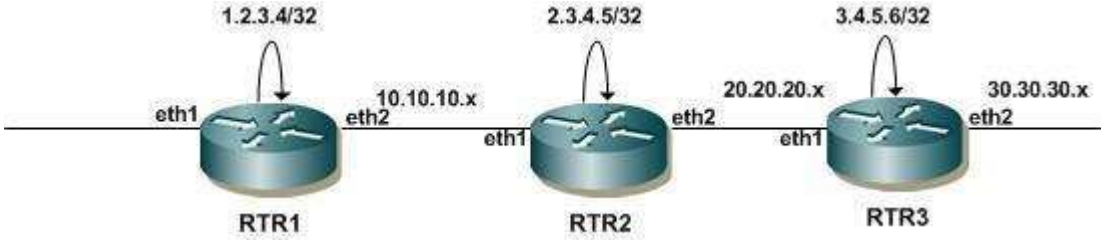


Figure 2: Device topology for BGP in VR/VRF

RTR1

`#configure terminal`	Enter Configuration mode
`(config)#interface lo`	Enter interface mode for loopback
`(config-if)#ip address 1.2.3.4/32`	Configure ip address on loopback
`(config-if)#exit`	Exit interface mode

(config)#interface eth2	Enter interface mode for eth2
(config-if)#ip address 10.10.10.1/24	Configure ip address on eth2
(config-if)#exit	Exit interface mode for eth2
(config)# router bgp 100	Enter router bgp mode
(config-router)# bgp router-id 1.2.3.4	Configure bgp router-id same as loopback ip address
(config-router)# bgp graceful-restart	Configure Graceful Restart for BGP
(config-router)#redistribute connected	Redistributing connected Routes inside BGP
(config-router)# neighbor 10.10.10.2 remote-as 400	Configure Neighbor for AS-400
(config-router)# neighbor 10.10.10.2 capability graceful-restart	Configure GR capability inside router bgp
(config-router)#end	Exit router bgp mode

RTR2

#configure terminal	Enter Configuration mode
(config)#interface lo	Enter interface mode for loopback
(config-if)#ip address 2.3.4.5/32	Configure ip address on loopback
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode for eth1
(config-if)#ip address 10.10.10.2/24	Configure ip address on eth1
(config-if)#exit	Exit interface mode for eth1
(config)#interface eth2	Enter interface mode for eth2
(config-if)#ip address 20.20.20.1/24	Configure ip address on eth2
(config-if)#exit	Exit interface mode for eth2
(config)#router bgp 400	Enter router bgp mode
(config-router)# bgp router-id 2.3.4.5	Configure bgp router-id same as loopback ip address
(config-router)# bgp graceful-restart	Configure Graceful Restart for BGP
(config-router)#redistribute connected	Redistributing connected Routes inside BGP
(config-router)# neighbor 10.10.10.1 remote-as 100	Configure Neighbor for AS-100
(config-router)# neighbor 10.10.10.1 capability graceful-restart	Configure GR capability inside router bgp
(config-router)# neighbor 20.20.20.2 remote-as 300	Configure Neighbor for AS-300
(config-router)# neighbor 20.20.20.2 capability graceful-restart	Configure GR capability inside router bgp
(config-router)#end	Exit router ospf mode

RTR3

#configure terminal	Enter Configuration mode

(config)#interface lo	Enter interface mode for loopback
(config-if)#ip address 3.4.5.6/32	Configure ip address on loopback
(config-if)#exit	Exit interface mode
(config)#interface eth1	Enter interface mode for eth2
(config-if)#ip address 20.20.20.2/24	Configure ip address on eth2
(config-if)#exit	Exit interface mode for eth2
(config)# router bgp 300	Enter router bgp mode
(config-router)# bgp router-id 3.4.5.6	Configure bgp router-id same as loopback ip address
(config-router)# bgp graceful-restart	Configure Graceful Restart for BGP
(config-router)#redistribute connected	Redistributing connected Routes inside BGP
(config-router)# neighbor 20.20.20.1 remote-as 400	Configure Neighbor for AS-400
(config-router)# neighbor 20.20.20.1 capability graceful-restart	Configure GR capability inside router bgp
(config-router)#end	Exit router bgp mode

Validation

RTR1

```
#sh ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2        E1 -
OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area       > -
selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
C    *> 1.2.3.4/32 is directly connected, lo
B    *> 2.3.4.5/32 [20/0] via 10.10.10.2, ge12, 00:00:15
C    *> 10.10.10.0/24 is directly connected, ge12
B    *> 20.20.20.0/24 [20/0] via 10.10.10.2, ge12, 00:00:15
C    *> 127.0.0.0/8 is directly connected, lo
```

RTR2

```
#sh ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2        E1 -
OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area       > -
selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
B    *> 1.2.3.4/32 [20/0] via 10.10.10.1, ge22, 00:02:46
```

```
C    *> 2.3.4.5/32 is directly connected, lo
B    *> 3.4.5.6/32 [20/0] via 20.20.20.2, ge14, 00:01:01
C    *> 10.10.10.0/24 is directly connected, ge22
C    *> 20.20.20.0/24 is directly connected, ge14
C*> 127.0.0.0/8 is directly connected, lo
```

RTR2

```
#sh ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2        E1 -
OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area       > -
selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
B    *> 1.2.3.4/32 [20/0] via 20.20.20.1, ge14, 00:01:15
B    *> 2.3.4.5/32 [20/0] via 20.20.20.1, ge14, 00:01:15
C    *> 3.4.5.6/32 is directly connected, lo
B    *> 10.10.10.0/24 [20/0] via 20.20.20.1, ge14, 00:01:15
C    *> 20.20.20.0/24 is directly connected, ge14
C    *> 127.0.0.0/8 is directly connected,

lo Gateway of last resort is not set
```

Validation After BGP Graceful Restart

RTR2

```
#write
Building configuration... [OK]

#restart bgp graceful
% Warning: You may loose BGP configuration, if not
saved Proceed for graceful restart? (y/n): y
#sh ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2    E1
- OSPF external type 1, E2 - OSPF external type 2
       i  -  IS-IS,  L1  -  IS-IS  level-1,  L2  -  IS-IS  level-2,  ia  -  IS-IS  inter  area
> - selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
B    *>p1.2.3.4/32 [20/0] via 10.10.10.1, ge22, 00:04:25
C    *> 2.3.4.5/32 is directly connected, lo
B    *>p3.4.5.6/32 [20/0] via 20.20.20.2, ge14, 00:02:40
C    *> 10.10.10.0/24 is directly connected, ge22
C    *> 20.20.20.0/24 is directly connected, ge14
C*> 127.0.0.0/8 is directly connected, lo
```

```
Gateway of last resort is not set

#sh nsm forwarding-timer
Protocol-Name GR-State Time Remaining (sec)   Disconnected-time
     BGP        ACTIVE            58           2001/06/07 19:50:38

#sh rib forwarding-timer
Protocol-Name GR-State Time Remaining (sec)   Disconnected-time
     BGP        ACTIVE            57           2001/06/07 19:50:38
```

RTR1

```
#sh ip bgp
BGP table version is 8, local router ID is 1.2.3.4
Status  codes:  s  suppressed,  d damped, h  history,  * valid,  > best, i  - internal,
l - Labeled, S Stale
Origin codes: i - IGP, e - EGP,? - incomplete

     Network            Next Hop            Metric    LocPrf         Weight   Path
*>   1.2.3.4/32         0.0.0.0             0          100           32768    ?
S>   2.3.4.5/32         10.10.10.2          0          100           0       400  ?
S>   3.4.5.6/32         10.10.10.2          0          100           0       400  300  ?
*>   10.10.10.0/24      0.0.0.0             0          100           32768    ?
S                       10.10.10.2          0          100           0       400  ?
S>   20.20.20.0/24      10.10.10.2          0          100           0       400  ?
Announced  routes  count  =  2  Accepted
routes count = 3

Total number of prefixes 5
```

RTR3

```
#sh ip bgp
BGP table version is 14, local router ID is 3.4.5.6
Status  codes:  s  suppressed,  d damped, h  history,  * valid,  > best, i  - internal,
l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network            Next Hop            Metric    LocPrf         Weight   Path
S>   1.2.3.4/32         20.20.20.1          0          100           0       400  100  ?
S>   2.3.4.5/32          20.20.20.1           0          100             0       400 ? *>
3.4.5.6/32          0.0.0.0             0          100           32768    ?
S>   10.10.10.0/24       20.20.20.1           0          100             0       400 ? *>
20.20.20.0/24       0.0.0.0             0          100           32768    ?
S                       20.20.20.1          0          100           0       400  ?

Announced routes  count  =  2  Accepted
routes count = 3

Total number of prefixes 5
```

BGP Distance

Administrative distance in BGP can be configured for a specific address family.

Topology

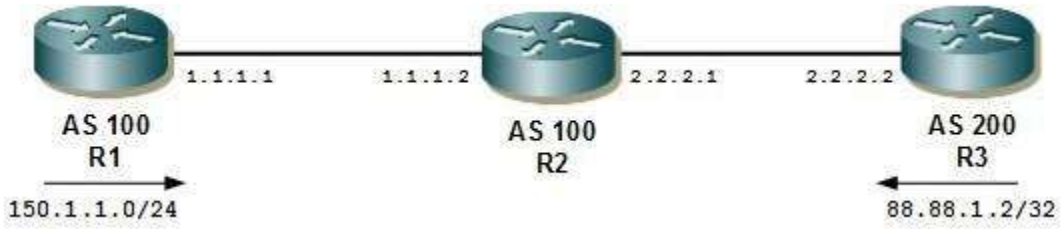


Figure 1-1: Administrative Distance for IPv4 BGP

R1

`#configure terminal`	Enter Configure mode.
`(config)#interface lo`	Enter loopback interface mode.
`(config-if)#ip address 150.1.1.1/24`	Specify IP address for the interface.
`(config-if)#exit`	Exit loopback interface mode.
`(config)#router bgp 100`	Assign the ASN value (`100`) to the router.
`(config-router)#network 150.1.1.0/24`	Specify the network to be advertised by the BGP routing process.
`(config-router)#neighbor 1.1.1.2 remote-as 100`	Specify the neighbor's IP address and ASN value.

R2

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 100`	Assign the ASN value (`100`) to the router.
`(config-router)#neighbor 2.2.2.2 remote-as 200`	Specify the neighbor's IP address and ASN value.
`(config-router)#neighbor 1.1.1.1 remote-as 100`	Specify the neighbor's IP address and the ASN value of another neighbor.
`(config-router)#distance bgp 12 13 120`	Configure the administrative distance for external, internal, and local routes received.
`(config-router)#aggregate-address 150.1.0.0/16 summary-only`	Configure a non-AS-set aggregate route on R2. The local distance is applied to this route.

R3

`#configure terminal`	Enter Configure mode.
`(config)#interface lo`	Enter loopback interface mode.
`(config-if)#ip address 88.88.1.2/32`	Specify IP address for the interface.
`(config-if)#exit`	Exit loopback interface mode.
`(config)#router bgp 200`	Assign the ASN value (`200`) to the router.
`(config-router)#network 88.88.1.2/32`	Specify the network to be advertised by the BGP routing process.

`(config-router)#neighbor 2.2.2.1 remote-as 100`	Specify the neighbor's IP address and ASN value.

Validation

show ip bgp summary, show ip bgp neighbors, show ip route database bgp, show ip route database, show ip route, show ip bgp

```
#show ip bgp summary
BGP router identifier 192.168.56.102, local AS number 100
BGP table version is 7
2 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS    MsgRcv    MsgSen TblVer   InQ   OutQ   Up/
Down   State/PfxRcd
1.1.1.1                   4   100     8          9       7      0      0
00:02:39                1
2.2.2.2                   4   200     4          4       7      0      0
00:00:38                1

Total number of neighbors 2

Total number of Established sessions 2
#show ip bgp neighbors
BGP neighbor is 1.1.1.1, remote AS 100, local AS 100, internal link
  BGP version 4, remote router ID 150.1.1.1
  BGP state = Established, up for 00:02:54
  Last read 00:02:54, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 8 messages, 0 notifications, 0 in queue
  Sent 9 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0 Minimum
 time between advertisement runs is 5 seconds
For address family: IPv4 IPv4
 BGP table version 7, neighbor version 7
 Index 2, Offset 0, Mask 0x4
 Community attribute sent to this neighbor (both)
 1 accepted prefixes
 0 announced prefixes

Connections established 1; dropped 0
Local host: 1.1.1.2, Local port: 49238
Foreign host: 1.1.1.1, Foreign port: 179
Nexthop: 1.1.1.2
Nexthop global: fe80::a00:27ff:fea6:6e3
Nexthop local: ::
BGP connection: non shared network
```

```
BGP neighbor is 2.2.2.2, remote AS 200, local AS 100, external
  link BGP version 4, remote router ID 88.88.1.2
  BGP state = Established, up for 00:00:53
  Last read 00:00:53, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 4 messages, 0 notifications, 0 in queue
  Sent 4 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 IPv4
  BGP table version 7, neighbor version 7
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 2.2.2.1, Local port: 179
Foreign host: 2.2.2.2, Foreign port: 50072
Nexthop: 2.2.2.1
Nexthop global: fe80::a00:27ff:fe77:264e
Nexthop local: ::
BGP connection: non shared network

#show ip route database bgp
IP Route Table for VRF "default"
B    *> 88.88.1.2/32 [12/0] via 2.2.2.2, eth2, 00:01:19
  B    *> 150.1.0.0/16 [120/0] is a summary, Null, 00:02:49B    *>
       150.1.1.0/24 [200/0] via 1.1.1.1, eth1, 00:02:49

Gateway of last resort is not set
#show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF
external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info
    IP Route Table for VRF "default"
  C    *> 1.1.1.0/24 is directly connected, eth1
    C*> 2.2.2.0/24 is directly connected, eth2
    B*> 88.88.1.2/32 [12/0] via 2.2.2.2, eth2, 00:01:32
    C*> 127.0.0.0/8 is directly connected, lo
    B*> 150.1.0.0/16 [120/0] is a summary, Null, 00:03:02
    B*> 150.1.1.0/24 [200/0] via 1.1.1.1, eth1, 00:03:02
    C*> 192.168.56.0/24 is directly connected, eth0

    Gateway of last resort is not set
```

```
#show ip ip
ipv6 #show ip
route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C       1.1.1.0/24 is directly connected, eth1
C2.2.2.0/24 is directly connected, eth2
B88.88.1.2/32 [12/0] via 2.2.2.2, eth2, 00:01:47
C127.0.0.0/8 is directly connected, lo
B150.1.0.0/16 [120/0] is a summary, Null, 00:03:17
B150.1.1.0/24 [200/0] via 1.1.1.1, eth1, 00:03:17
C192.168.56.0/24 is directly connected, eth0

Gateway of last resort is not set
#show ip bgp
BGP table version is 8, local router ID is 192.168.56.102
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf       Weight Path
*>   88.88.1.2/32     2.2.2.2               0        100          0       200 i *>
150.1.0.0         0.0.0.0                 0          100            32768     i s>i
150.1.1.0/24     1.1.1.1              0        100          0        i

Total number of prefixes 3
```

BGP Weight per Peer

A different weight can be assigned per address family of a peer. For example, a system can be configured to prefer VPN4 routes from peer A and IPv4 routes from peer B.

If the neighbor weight command is given under a specific address-family mode, the peer weight is set for that specific address family. If the address family is not specifically set, the weight is updated for the default address-family.

Topology

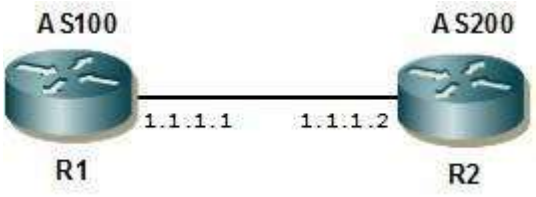


Figure 1-2: BGP Weight Per Peer

R1

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 100`	Assign the ASN value (`100`) to the router.
`(config-router)#neighbor 1.1.1.2 remote-as 200`	Specify the neighbor's IP address and ASN value.

R2

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 200`	Assign the ASN value (`200`) to the router.
`(config-router)#neighbor 1.1.1.1 remote-as 100`	Specify the neighbor's IP address and ASN value.
`(config-router)#neighbor 1.1.1.1 weight 500`	Add a weight of `500` to all the routes coming from the neighbor, `1.1.1.1` (only IPv4 routes).

Validation

R1

```
    #show ip bgp summary
    BGP router identifier 192.168.56.101, local AS number 100
    BGP table version is 1
    0 BGP AS-PATH entries
    0 BGP community entries
    Neighbor V AS MsgRcv MsgSen TblVer InQ OutQ Up/Dow
    n State/PfxRcd
    1.1.1.2 4 200 6 7 1 0 0 00:02:00
0
    Total number of neighbors 1
    Total number of Established sessions 1

    #show ip bgp neighbors
    BGP neighbor is 1.1.1.2, remote AS 200, local AS 100, external link
    BGP version 4, remote router ID 192.168.56.102
    BGP state = Established, up for 00:02:10
    Last read 00:02:10, hold time is 90, keepalive interval is 30 seconds
    Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Received 6 messages, 0 notifications, 0 in queue
    Sent 7 messages, 0 notifications, 0 in queue
    Route refresh request: received 0, sent 0
    Minimum time between advertisement runs is 30 seconds
    For address family: IPv4 IPv4
    BGP table version 1, neighbor version 1
    Index 1, Offset 0, Mask 0x2
    Community attribute sent to this neighbor (both)
    0 accepted prefixes
    0 announced prefixes
    Connections established 1; dropped 0
```

```
Local host: 1.1.1.1, Local port: 179
Foreign host: 1.1.1.2, Foreign port: 34155
Nexthop: 1.1.1.1
Nexthop global: fe80::a00:27ff:fecf:3354
Nexthop local: ::
BGP connection: non shared network

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 -
OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
- candidate default
IP Route Table for VRF "default"
C 1.1.1.0/24 is directly connected, eth1
C 127.0.0.0/8 is directly connected, lo
C 192.168.56.0/24 is directly connected, eth0
Gateway of last resort is not set
```

R2

```
#show ip bgp summary
BGP router identifier 192.168.56.102, local AS number 200
BGP table version is 1
0 BGP AS-PATH entries
0 BGP community entries
Neighbor V AS MsgRcv MsgSen TblVer InQ OutQ Up/Dow
n State/PfxRcd
1.1.1.1 4 100 3 3 1 0 0 00:00:34
0
Total number of neighbors 1
Total number of Established sessions 1

#show ip ip ipv6

#show ip bgp neighbors
BGP neighbor is 1.1.1.1, remote AS 100, local AS 200, external link
BGP version 4, remote router ID 192.168.56.101
BGP state = Established, up for 00:00:59
Last read 00:00:59, hold time is 90, keepalive interval is 30 seconds
Neighbor capabilities:
Route refresh: advertised and received (old and new)
Address family IPv4 Unicast: advertised and received
Received 3 messages, 0 notifications, 0 in queue
Sent 3 messages, 0 notifications, 0 in queue
Route refresh request: received 0, sent 0
Minimum time between advertisement runs is 30 seconds
For address family: IPv4 IPv4
BGP table version 1, neighbor version 1
Index 1, Offset 0, Mask 0x2
```

```
Community attribute sent to this neighbor (both)
Weight500
0 accepted prefixes
0 announced prefixes
Connections established 1; dropped 0
Local host: 1.1.1.2, Local port: 34155
Foreign host: 1.1.1.1, Foreign port: 179
Nexthop: 1.1.1.2
Nexthop global: fe80::a00:27ff:feca:b09a
Nexthop local: ::
BGP connection: non shared network

#show ip bgp neighbors
BGP neighbor is 1.1.1.1, remote AS 100, local AS 200, external link
BGP version 4, remote router ID 192.168.56.101
BGP state = Established, up for 00:01:21
Last read 00:01:21, hold time is 90, keepalive interval is 30 seconds
Neighbor capabilities:
Route refresh: advertised and received (old and new)
Address family IPv4 Unicast: advertised and received
Received 4 messages, 0 notifications, 0 in queue
Sent 4 messages, 0 notifications, 0 in queue
Route refresh request: received 0, sent 0
Minimum time between advertisement runs is 30 seconds
For address family: IPv4 IPv4
BGP table version 1, neighbor version 1
Index 1, Offset 0, Mask 0x2
Community attribute sent to this neighbor (both)
Weight500
0 accepted prefixes
0 announced prefixes
Connections established 1; dropped 0
Local host: 1.1.1.2, Local port: 34155
Foreign host: 1.1.1.1, Foreign port: 179
Nexthop: 1.1.1.2
Nexthop global: fe80::a00:27ff:feca:b09a
Nexthop local: ::
BGP connection: non shared network

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF
external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
- candidate default
IP Route Table for VRF "default"
C 1.1.1.0/24 is directly connected, eth1
C 127.0.0.0/8 is directly connected, lo
C 192.168.56.0/24 is directly connected, eth0
```

```
Gateway of last resort is not set
```

OSPF as PE-CE Protocol for VPNs

In an MPLS VPN environment, customer networks are connected to an MPLS VPN-enabled provider backbone. As shown in Figure 1-3, Customer A areas, Areas 0 and 1, are connected to an MPLS VPN–enabled provider network. Area 0 and Area 1 have routers CE1 and CE2 running OSPF. MP-iBGP is used between PE1 and PE2 to propagate routes between Site 1 (Area 0) and Site 2 (Area 1). Traditional OSPF-BGP redistribution is performed at PE routers, PE1 and PE2. In this case, routes distributed by CE1 into the MP-iBGP cloud are sent to CE2 as external routes, even though both CE1 and CE2 belong to the same customer.

This behavior can be changed with the additional domain ID configuration. Each VRF should be configured a domain ID on the PE routers. If a PE router gets a route through the MP-iBGP cloud and has to send to any customer site, it checks the domain ID value against the list of stored domain ID values. If the incoming domain ID matches any of the stored IDs, that route is inserted into the customer site with the same type, as it was inserted into the MP-BGP cloud; otherwise, it is inserted as external route.

Topology

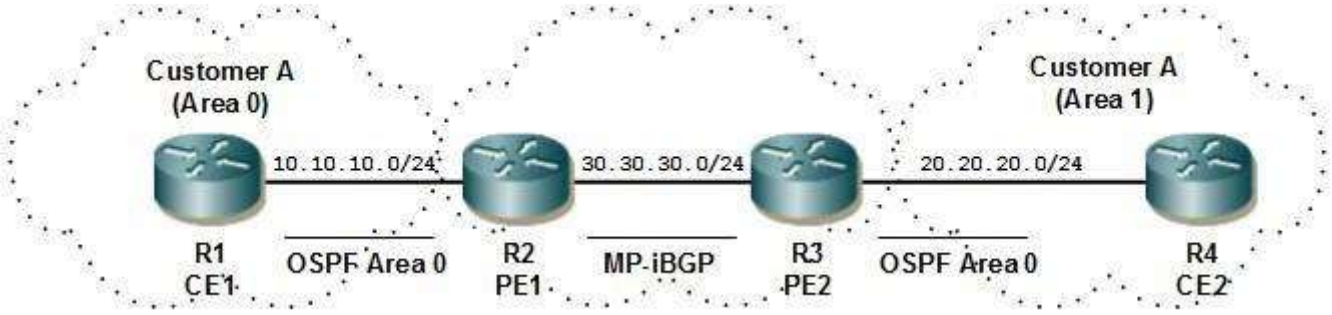


Figure 1-3: OSPF as PE-CE Protocol

CE1

`#configure terminal`	Enter Configure mode.
`(config)#interface lo`	Enter loopback interface mode.
`(config-if)#ip address 60.1.1.1/24`	Specify IP address for the interface.
`(config-if)#exit`	Exit loopback interface mode.
`(config)#router ospf 1`	Configure the routing process and specify the Process ID (`1`).
`(config-router)#network 10.10.10.0/24 area 0`	Advertise the network in OSPF.
`(config-router)#network 60.1.1.0/24 area 0`	Advertise the loopback IP address in area 0 of router OSPF 1.

PE1

`#configure terminal`	Enter Configure mode.
`(config)#ip vrf ABC`	Specify the name of the VRF (`ABC`) to be created.
`(config-vrf)#rd 10:100`	Assign a route distinguisher (RD) for the VRF, which is a unique value on the router. The RD value can be in ASN:NN or A.B.C.D:NN format.

(config-vrf)#route-target both 10:100	Specify the 2-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.
(config-vrf)#exit	Exit VRF mode, and return to Configure mode.
(config)#interface eth1	Specify the interface (eth1) to configure.
(config-if)#ip vrf forwarding ABC	Associate interface eth1 to vrf ABC.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router ospf 1 ABC	Configure OSPF for VRF.
(config-router)#network 10.10.10.0/24 area 0	Advertise the network for OSPF adjacency with CE1.
(config-router)#domain-id 1.1.1.1	Configure the primary domain ID.
(config-router)#domain-id 2.2.2.2 secondary	Configure a secondary domain ID.
(config-router)#domain-id 3.3.3.3 secondary	Configure a secondary domain ID.
(config-router)#exit	Exit Router mode and return to Configure mode.
(config)#router bgp 100	Assign the ASN value (100) to the BGP router.
(config-router)#neighbor 30.30.30.2 remote-as 100	Configure neighbor 30.30.30.2 for iBGP.
(config-router)#address-family vpnv4 unicast	Enter Address-Family-VPNv4 mode.
(config-router-af)#neighbor 30.30.30.2 activate	Activate neighbor 30.30.30.2.
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.
(config-router)#address-family ipv4 vrf ABC	Enter Address-Family-VRF mode.
(config-router)#redistribute ospf	Specify redistributing routes from OSPF into BGP.
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.
PE2	
#configure terminal	Enter Configure mode.
(config)#ip vrf ABC	Specify the name of the VRF (ABC) to be created.
(config-vrf)#rd 10:100	Assign a route distinguisher (RD) for the VRF, which is a unique value on the router. The RD value can be in ASN:NN or A.B.C.D:NN format.
(config-vrf)#route-target both 10:100	Specify the 2-Octet AS specific or IPv4 specific Transitive Route-Target extended community attribute.
(config-vrf)#exit	Exit VRF mode, and return to Configure mode.
(config)#interface eth1	Specify the interface (eth1) to configure.
(config-if)#ip vrf forwarding ABC	Associate interface eth1 to vrf ABC.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router ospf 1 ABC	Configure OSPF for VRF.
(config-router)#network 20.20.20.0/24 area 0	Advertise the network for OSPF adjacency with CE1.
(config-router)#domain-id 1.1.1.1	Configure the primary domain ID.
(config-router)#domain-id 2.2.2.2 secondary	Configure a secondary domain ID.
(config-router)#domain-id 3.3.3.3 secondary	Configure a secondary domain ID.

(config-router)#exit	Exit Router mode and return to Configure mode.
(config)#router bgp 100	Assign the ASN value (100) to the BGP router.
(config-router)#neighbor 30.30.30.1 remote-as 100	Configure neighbor 30.30.30.1 for iBGP.
(config-router)#address-family vpnv4 unicast	Enter Address-Family-VPNv4 mode.
(config-router-af)#neighbor 30.30.30.1 activate	Activate neighbor 30.30.30.1.
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.
(config-router)#address-family ipv4 vrf ABC	Enter Address-Family-VRF mode.
(config-router)#redistribute ospf	Specify redistributing routes from OSPF into BGP.
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.
CE2	
#configure terminal	Enter Configure mode.
(config)#router ospf 1	Configure the routing process, and specify the Process ID (1).
(config-router)#network 20.20.20.0/24 area 0	Advertise the network in OSPF.

Validation

```
#show ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, l
- labeled
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight Path
Route Distinguisher: 10:100 (Default for VRF
IPPU) *> l 60.1.1.1/32 10.10.10.1 12 100 32768 ?
Announced routes count = 1 Accepted routes count
= 0
```

BGP Multipath for IPv4

BGP supports multipath for IPv4 prefixes. BGP Multipath allows load-balancing traffic among multiple BGP routes. It supports both iBGP and eBGP routes. In case of eBGP, the routes should arrive from same AS number.

Topology

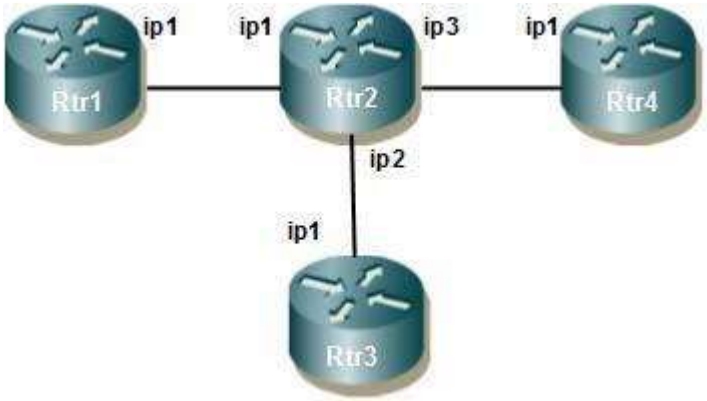


Figure 1-4: Multipath iBGP for IPv4

Rtr1

`#configure terminal`	Enter the Configure mode.
`(config)#router bgp 100`	Assign the ASN value (100) to the BGP router.
`(config-router)#bgp router-id 2.2.2.2`	Configure a fixed Router ID (2.2.2.2).
`(config-router)#redistribute static`	Redistribute the static routes.
`(config-router)#neighbor 30.30.30.9 remoteas 100`	Configure neighbor 30.30.30.9 for iBGP.
`(config-router)#exit`	Exit the BGP Router mode and return to the Configure mode.
`(config)#ip route 88.88.0.0/16 Null`	Configure static route.

Rtr3

`#configure terminal`	Enter the Configure mode.
`(config)#router bgp 100`	Assign the ASN value (100) to the BGP router.
`(config-router)#bgp router-id 4.4.4.4`	Configure a fixed Router ID (4.4.4.4).
`(config-router)#redistribute static`	Redistribute the static routes.
`(config-router)#neighbor 40.40.40.9 remoteas 100`	Configure neighbor 40.40.40.9 for iBGP.
`(config-router)#exit`	Exit the BGP Router mode and return to the Configure mode.
`(config)#ip route 88.88.0.0/16 Null`	Configure static route.

Rtr4

`#configure terminal`	Enter the Configure mode.
`(config)#router bgp 100`	Assign the ASN value (100) to the BGP router.
`(config-router)#bgp router-id 6.6.6.6`	Configure a fixed Router ID (6.6.6.6).
`(config-router)#redistribute static`	Redistribute the static routes.
`(config-router)#neighbor 50.50.50.9 remoteas 100`	Configure neighbor 50.50.50.9 for iBGP.
`(config)#exit`	Exit the BGP Router mode and return to the Configure mode.
`(config)#ip route 88.88.0.0/16 Null`	Configure static route.

Rtr2

#configure terminal	Enter the Configure mode.
(config)#router bgp 100	Assign the ASN value (100) to the BGP router.
(config-router)#max-paths ibgp 2	Configure iBGP max-paths (2).
(config)#bgp router-id 9.9.9.9	Configure a fixed Router ID (9.9.9.9).
(config-router)#neighbor 30.30.30.2 remoteas 100	Configure neighbor 30.30.30.2 for iBGP.
(config-router)#neighbor 40.40.40.4 remoteas 100	Configure neighbor 40.40.40.4 for iBGP.
(config-router)#neighbor 50.50.50.6 remoteas 100	Configure neighbor 50.50.50.6 for iBGP.
(config-router)#exit	Exit the Router mode and return to Configure mode.

Validation

```
#show ip bgp 88.88.0.0
BGP routing table entry for 88.88.0.0/16
Paths: (3 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  Local
    30.30.30.2 from 30.30.30.2 (2.2.2.2)
      Origin incomplete, metric 0, localpref 100, valid,
internal, multipathcandidate, installed, best
      Last update: Wed Mar  2 15:17:38 2016

  Local
    50.50.50.6 from 50.50.50.6 (6.6.6.6)
      Origin incomplete, metric 0, localpref 100, valid,
internal, multipathcandidate
      Last update: Wed Mar  2 15:23:58 2016

  Local
    40.40.40.4 from 40.40.40.4 (4.4.4.4)
      Origin incomplete, metric 0, localpref 100, valid,
internal, multipathcandidate, installed
      Last update: Wed Mar  2 15:21:45 2016

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C       2.2.2.2/32 is directly connected, lo
C       10.12.20.0/24 is directly connected, eth0
```

```
C       30.30.30.0/24 is directly connected, eth1
C40.40.40.0/24 is directly connected, eth2
C50.50.50.0/24 is directly connected, eth3
B88.88.0.0/16 [200/0] via 40.40.40.4, eth2, 00:05:21
                      [200/0] via 30.30.30.2, eth1, 00:05:21
C       127.0.0.0/8 is directly connected, lo

Gateway of last resort is not set

#show running-config router bgp
! router bgp 100 bgp router-id 9.9.9.9
max-paths ibgp 2
 neighbor 30.30.30.2 remote-as 100 neighbor 40.40.40.4 remote-
as 100 neighbor 50.50.50.6 remote-as 100
!
#
```

Multipath eBGP

Topology

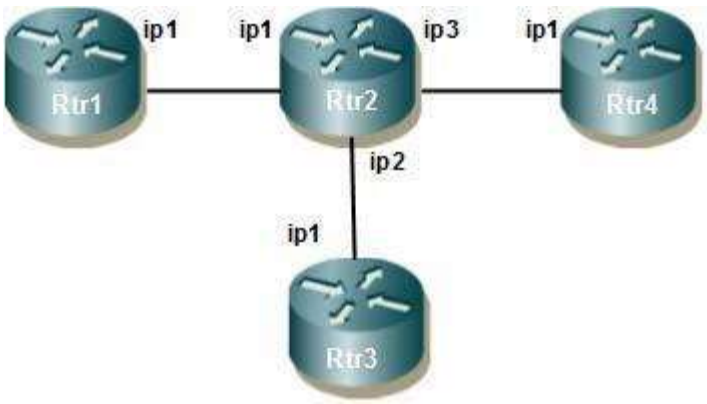


Figure 1-5: Multipath eBGP for IPv4

Rtr1

`#configure terminal`	Enter the Configure mode.
`(config)#router bgp 200`	Assign the ASN value (200) to the BGP router.
`(config-router)#bgp router-id 2.2.2.2`	Configure a fixed Router ID (2.2.2.2).
`(config-router)#redistribute static`	Redistribute the static routes.
`(config-router)#neighbor 30.30.30.9 remoteas 100`	Configure neighbor 30.30.30.9 for eBGP.
`(config-router)#exit`	Exit the BGP Router mode and return to the Configure mode.
`(config)#ip route 88.88.0.0/16 Null`	Configure static route.

Rtr3

`#configure terminal`	Enter the Configure mode.

(config)#router bgp 200	Assign the ASN value (200) to the BGP router.
(config-router)#bgp router-id 4.4.4.4	Configure a fixed Router ID (4.4.4.4).
(config-router)#redistribute static	Redistribute the static routes.
(config-router)#neighbor 40.40.40.9 remoteas 100	Configure neighbor 40.40.40.9 for eBGP.
(config-router)#exit	Exit the BGP Router mode and return to the Configure mode.
(config)#ip route 88.88.0.0/16 Null	Configure static route.

Rtr4

#configure terminal	Enter the Configure mode.
(config)#router bgp 200	Assign the ASN value (200) to the BGP router.
(config-router)#bgp router-id 6.6.6.6	Configure a fixed Router ID (6.6.6.6).
(config-router)#redistribute static	Redistribute the static routes.
(config-router)#neighbor 50.50.50.9 remoteas 100	Configure neighbor 50.50.50.9 for eBGP.
(config)#exit	Exit the BGP Router mode and return to the Configure mode.
(config)#ip route 88.88.0.0/16 Null	Configure static route.

Rtr2

#configure terminal	Enter the Configure mode.
(config)#router bgp 100	Assign the ASN value (100) to the BGP router.
(config-router)#max-paths ebgp 2	Configure eBGP max-paths (2).
(config)#bgp router-id 9.9.9.9	Configure a fixed Router ID (9.9.9.9).
(config-router)#neighbor 30.30.30.2 remoteas 200	Configure neighbor 30.30.30.2 for eBGP.
(config-router)#neighbor 40.40.40.4 remoteas 200	Configure neighbor 40.40.40.4 for eBGP.
(config-router)#neighbor 50.50.50.6 remoteas 200	Configure neighbor 50.50.50.6 for eBGP.
(config-router)#exit	Exit the Router mode and return to Configure mode.

Validation

#**show ip bgp 88.88.0.0**

```
BGP routing table entry for 88.88.0.0/16
Paths: (3 available, best #3, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
  30.30.30.2 50.50.50.6
  200
    30.30.30.2 from 30.30.30.2 (2.2.2.2)
      Origin incomplete metric 0, localpref 100, valid, external, multipath-candidate,
installed
      Last update: Sat Jan  3 02:06:25 1970
```

```
  200
    50.50.50.6 from 50.50.50.6 (6.6.6.6)
      Origin incomplete metric 0, localpref 100, valid, external, multipath-
      candidate Last update: Sat Jan 3 02:05:39 1970

  200
    40.40.40.4 from 40.40.40.4 (4.4.4.4)
      Origin incomplete metric 0, localpref 100, valid, external, multipath-candidate,
installed, best
      Last update: Sat Jan  3 02:05:11 1970

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1  -  OSPF  NSSA  external  type  1,  N2  -  OSPF  NSSA  external  type  2
E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1  - IS-IS  level-1, L2  - IS-IS level-2, ia  - IS-IS inter area
* - candidate default

C       30.30.30.0/24 is directly connected, ge3
C40.40.40.0/24 is directly connected, ge5
C50.50.50.0/24 is directly connected, ge7
B88.88.0.0/16 [20/0] via 30.30.30.2, ge3, 00:00:11
                     [20/0] via 40.40.40.4, ge5, 00:00:11
C       90.90.90.90/32 is directly connected, lo
C127.0.0.0/8 is directly connected, lo #

#show running-config router bgp !
router bgp 100  bgp
router-id 9.9.9.9  max-
paths ebgp 2
 neighbor 30.30.30.2 remote-as 200
neighbor 40.40.40.4 remote-as 200
neighbor 50.50.50.6 remote-as 200 !
```

BGP AS-PATH Multipath-relax

BGP will not load balance across multiple paths by default. We can configure it to do so with the `max-paths ebgp <no-of-multipaths>` command. The criterion of this command is that all attributes must match (Weight, Local preference, AS Path, etc). This is acceptable if we are multi-homed to a single AS, but what if we are multi-homed to different AS.

BGP AS PATH multipath relax effectively allows for ECMP to be done across different neighboring ASN's.

Topology

Below topology explains about BGP AS PATH multipath relax functionality.

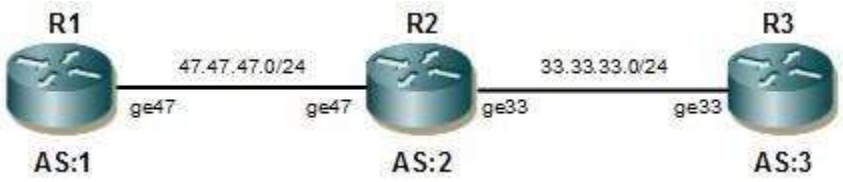


Figure 1-6: BGP AS-PATH Multipath-relax Topology

R1

#configure terminal	Enter the Configure mode.
(config)#interface lo	Enter Interface loopback
(config-if)#ip address 100.1.1.1/24	Configure IP address for interface
(config-if)#exit	Exit Interface mode and enter the Configure mode
(config)#interface ge47	Enter Interface loopback
(config-if)#ip address 47.47.47.1/24	Configure IP address for interface
(config-if)#exit	Exit from interface mode and enter the Configure mode
(config)#router bgp 1	Assign the ASN value (1) to the BGP router
(config-router)#neighbor 47.47.47.2 remoteas 2	Configure eBGP neighbor.
(config-router)#network 100.1.1.0/24	Advertise the loopback network into BGP.
(config-router)#end	Exit from BGP router config mode

R2

#configure terminal	Enter the Configure mode.
(config)#interface ge33	Enter Interface mode
(config-if)#ip address 33.33.33.2/24	Configure IP address for interface
(config-if)#exit	Exit from interface mode and enter the Configure mode
(config)#interface ge47	Enter Interface mode
(config-if)#ip address 47.47.47.2/24	Configure IP address for interface.
(config-if)#exit	Exit from interface mode and enter the Configure mode
(config)#router bgp 2	Assign the ASN value (2) to the BGP router.
(config-router)#neighbor 33.33.33.3 remoteas 3	Configure eBGP neighbor.
(config-router)#neighbor 47.47.47.1 remoteas 1	Configure eBGP neighbor.
(config-router)#max-paths ebgp 8	Configure eBGP Multipath.
(config-router)#bgp bestpath as-path multipath-relax	Configure BGP AS PATH Multipath relax.
(config-router)#end	Exit from BGP router config mode.

R3

#configure terminal	Enter the Configure mode.

(config)#interface lo	Enter Interface loopback.
(config-if)#ip address 100.1.1.1/24	Configure IP address for interface.
(config-if)#exit	Exit from interface mode and enter the Configure mode.
(config)#interface ge33	Enter Interface loopback.
(config-if)#ip address 33.33.33.3/24	Configure IP address for interface.
(config-if)#exit	Exit from interface mode and enter the Configure mode.
(config)#router bgp 3	Assign the ASN value (3) to the BGP router.
(config-router)#neighbor 33.33.33.2 remoteas 2	Configure eBGP neighbor.
(config-router)#network 100.1.1.0/24	Advertise the loopback network into BGP.
(config-router)#end	Exit from BGP router config mode.

Validation

show running-config bgp, show ip bgp summary, show ip bgp, show ip bgp <prefix>

```
R2#show running-config bgp
! router bgp 2
 bgp bestpath as-path multipath-relax max-paths
ebgp 8
 neighbor 33.33.33.3 remote-as 3  neighbor
47.47.47.1 remote-as 1
!
R2#show ip bgp 100.1.1.0
BGP routing table entry for 100.1.1.0/24
Paths: (2 available, best #1, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
  47.47.47.1
  3
    33.33.33.3 from 33.33.33.3 (33.33.33.3)
      Origin IGP, metric 0, localpref 100, valid, external,
multipathcandidate, installed, best
      Last update: Tue Feb 23 03:13:14 2016
  1
    47.47.47.1 from 47.47.47.1 (62.57.1.1)
      Origin IGP, metric 0, localpref 100, valid, external,
multipathcandidate, installed
      Last update: Tue Feb 23 03:13:15 2016
```

BGP Graceful Shutdown

This section contains BGP graceful shutdown configuration examples.

BGP graceful shutdown reduces and avoid packets loss during maintenance shutdown by keeping the path undisturbed even after shutdown by lowering local preference so that routers of an AS can use this until they become aware of new path. If there is no alternate path available in the AS, the same path is used until forwarding failure occurs.

BGP graceful shutdown is supported for both BGP-IPv4 and BGP-IPv6 configurations.

BGP Graceful Shutdown on an Interface

Figure 1-7 shows the minimum configuration required to enable graceful shutdown on an interface. R1, R2, and R3 are three routers in three different ASs. R4 is another router in another AS forming an alternate path – R1 R4 R3 to the primary path.

Note: BGP graceful shutdown is only supported for eBGP configurations. It is not supported for iBGP configurations.

Topology

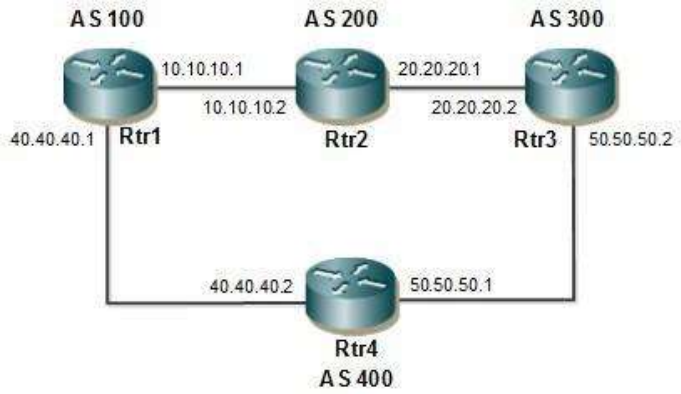


Figure 1-7: BGP Graceful Shutdown Topology 1

Rtr1

`#configure terminal`	Enter the Configure mode.
`(config)#router bgp 100`	Assign the ASN value (100) to BGP router. The AS number should be a unique positive integer identifying the Autonomous System.
`(config-router)#neighbor 10.10.10.2 remoteas 200`	Establish eBGP neighborship with R2.
`(config-router)#neighbor 40.40.40.2 remoteas 400`	Establish eBGP neighborship with R4.

Rtr2

`#configure terminal`	Enter the Configure mode.
`(config)#interface lo`	Enter loopback interface mode.
`(config-if)#ip address 6.6.6.1/24`	Specify IP address.
`(config-if)#exit`	Exit loopback interface mode.
`(config)#router bgp 200`	Assign the ASN value (200) to BGP router. The AS number should be a unique positive integer identifying the Autonomous System.
`(config-router)#neighbor 10.10.10.1 remote-as 100`	Establish eBGP neighborship with R1.
`(config-router)#neighbor 20.20.20.2 remote-as 300`	Establish eBGP neighborship with R3.
`(config-router)#bgp g-shut-capable`	Enable the graceful shutdown capability on the DUT.

(config-router)#neighbor 10.10.10.1 g-shut	Enable graceful shutdown functionality on the connected interface to R1.
(config-router)#neighbor 10.10.10.1 g-shut-timer 70	Configure the value of the graceful shutdown timer. After the timer expires, the BGP session initiated for graceful shutdown is shut down. The supported range for the graceful shutdown timer value is from 10 to 65535, in seconds. The default value is 60 seconds.
(config-router)#network 6.6.6.0/24	Specify the network to be advertised by the BGP routing process from DUT.
Rtr3	
#configure terminal	Enter the Configure mode.
(config)#router bgp 300	Assign the ASN value (300) to BGP router. The AS number should be a unique positive integer identifying the Autonomous System.
(config-router)#neighbor 20.20.20.1 remote-as 200	Establish eBGP neighborship with R2
(config-router)#neighbor 50.50.50.1 remote-as 400	Establish eBGP neighborship with R4.
Rtr4	
#configure terminal	Enter the Configure mode.
(config)#router bgp 400	Assign the ASN value (400) to the BGP router. The AS number should be a unique positive integer identifying the Autonomous System.
(config-router)#neighbor 40.40.40.1 remote-as 100	Establish eBGP neighborship with R1.
(config-router)#neighbor 50.50.50.2 remote-as 300	Establish eBGP neighborship with R3.

Validation

Checking for BGP Graceful Shutdown Community Tag on R2:

```
R2#show ip bgp 6.6.6.0
BGP routing table entry for 6.6.6.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  Local
    0.0.0.0 from 0.0.0.0 (20.20.20.1)
      Origin IGP, localpref 100, weight 32768, valid, sourced, local, best
Community: 0:65535 <<<<<<< community tagged (The community value 65535 is used
for the graceful shutdown)
Last update: Wed Apr 18 15:37:18 2012
Checking for BGP Graceful Shutdown Community Tag on DUT
```

BGP Graceful Shutdown on a Router

Figure 1-8 shows the minimum configuration required to enable graceful shutdown at the router level. R1, R2, and R3 are three routers in three different ASs. R4 is another router in another AS forming an alternate path – R1 R4 R3 to the primary path.

Note: BGP graceful shutdown at the router level is used to bring down all the BGP sessions on the DUT. If there is still an alternate path for the data traffic, it takes that path.

Topology

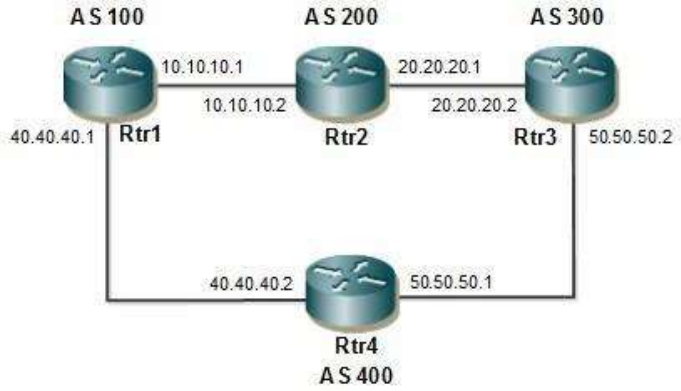


Figure 1-8: BGP Graceful Shutdown Topology 2

Rtr1

`#configure terminal`	Enter the Configure mode.
`(config)#router bgp 100`	Assign the ASN value (100) to the BGP router. The AS number should be a unique positive integer identifying the Autonomous System.
`(config-router)#neighbor 10.10.10.2 remote-as 200`	Establish eBGP neighborship with R2.
`(config-router)#neighbor 40.40.40.2 remote-as 400`	Establish eBGP neighborship with R4.

Rtr2

`#configure terminal`	Enter the Configure mode.
`(config)#interface lo`	Enter loopback interface mode.
`(config-if)#ip address 70.70.70.1/24`	Specify IP address.
`(config-if)#exit`	Exit loopback interface mode.
`(config)#router bgp 200`	Assign the ASN value (200) to the BGP router. The AS number should be a unique positive integer identifying the Autonomous System.
`(config-router)#neighbor 10.10.10.1 remote-as 100`	Establish eBGP neighborship with R1.
`(config-router)#neighbor 20.20.20.2 remote-as 300`	Establish eBGP neighborship with R3.
`(config-router)#bgp g-shut-capable`	Enabling the graceful shutdown capability on the DUT.
`(config-router)#bgp g-shut`	Enable BGP graceful shutdown functionality at the router level.

(config-router)#bgp g-shut-local-preference 100	Configure the local preference value of the routes to be used during graceful shutdown. This local reference is different from the BGP local preference value and is set in order to make the alternative path a preferred one in the case of graceful shutdown. The supported range of the local preference value is from 0 to 4294967295.
(config-router)#network 70.70.70.0/24	Specify the network to be advertised by the BGP routing process from DUT.

Rtr3

#configure terminal	Enter the Configure mode.
(config)#router bgp 300	Assign the ASN value (300) to the BGP router. The AS number should be a unique positive integer identifying the Autonomous System.
(config-router)#neighbor 20.20.20.1 remote-as 200	Establish eBGP neighborship with R2.
(config-router)#neighbor 50.50.50.1 remote-as 400	Establish eBGP neighborship with R4.

Rtr4

#configure terminal	Enter the Configure mode.
(config)#router bgp 400	Assign the ASN value (400) to the BGP router. The AS number should be a unique positive integer identifying the Autonomous System.
(config-router)#neighbor 40.40.40.1 remote-as 100	Establish eBGP neighborship with R1.
(config-router)#neighbor 50.50.50.2 remote-as 300	Establish eBGP neighborship with R3.

Validation

```
    R2#show ip bgp 70.70.70.0
    BGP routing table entry for 70.70.70.0/24
    Paths: (1 available, best #1, table Default-IP-Routing-Table)
      Advertised to non peer-group peers:
      20.20.20.2
      Local
        0.0.0.0 from 0.0.0.0 (20.20.20.1)
          Origin IGP, localpref 100, weight 32768, valid, sourced, local, bestBGP
    routing table entry for 70.70.70.0/24
    Paths: (1 available, best #1, table Default-IP-Routing-Table)
    Community: 0:65535 <<<<<<< community tagged (The community value 65535 is
    used for the graceful shutdown)
Last update: Wed Apr 20 11:21:17 2012
```

BGP FIB Install (Selective Route Download)

The BGP—Selective Route Download feature allows a network administrator to selectively download some or none of the BGP routes into the Routing Information Base (RIB). The primary application for this feature is to suppress the unnecessary downloading of certain BGP routes to the RIB or Forwarding Information Base (FIB) on a dedicated route reflector, which propagates BGP updates without carrying transit traffic. The feature thereby helps to maximize resources available and to improve routing scalability and convergence on the dedicated route reflector.

With RFC 4456, the concept of route reflection was defined; this would allow configuring designated one or more BGP routers in iBGP network as route reflectors. BGP relaxes the re-advertising restriction on these route reflectors, allowing them to accept and propagate IBGP routes to their clients.

The role of a dedicated route reflector (RR) is to propagate BGP updates without participating in the actual forwarding of transit traffic. That means the RR does not need to have all BGP routes downloaded into its RIB or FIB. It is beneficial for the RR to preserve its resources by not processing and storing those routes.

By default, BGP routes are downloaded to the RIB. To save resources on a dedicated route reflector, such downloading can be reduced or prevented by configuring a table map. A table map is so named because it controls what is put into the BGP routing table.

By reducing the route installation in the dedicated route reflectors, we can maximize availability of resources and improve routing scalability and convergence.

A new command 'table map' is being introduced to achieve this. A table map controls what is put into the BGP routing table. When configured it would reduce or prevent downloading routes to RIB.

Table map command references 'route map' rules available in BGP to control the routes going into the BGP routing table.

Table-map command can be used in two ways:

- When a simple table-map command is given (without filter option), the route map referenced in the table-map command shall be used to set certain properties (such as the traffic index) of the routes for installation into the RIB. The route is always downloaded, regardless of whether it is permitted or denied by the route map.
- When the option 'filter' is given in the table map command, the route map referenced is used to control whether a BGP route is to be downloaded to the IP RIB (hence the filter). A BGP route is not downloaded to the RIB if it is denied by the route map.

Topology

Below topology explains about BGP FIB Install functionality

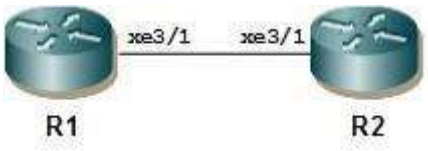


Figure 1-9: BFP FIB Install Topology

R1

`#configure terminal`	Enter the Configure mode.
`(config)#interface xe3/1`	Enter Interface mode.
`(config-if)#ip address 20.1.1.1/24`	Configure IP address for interface
`(config-if)#exit`	Exit Interface mode and enter Configure mode
`(config)# router bgp 100`	Assign the ASN value (100) to the BGP router.
`(config-router)#neighbor 20.1.1.2 remote-as 100`	Configure neighbor in IBGP
`(config-router)#redistribute static`	Redistribute static routes to advertise to its neighbor
`(config-router)#exit`	Exit Router mode and enter Configure mode
`(config)#ip route 1.1.1.0/24 xe3/1`	Configure static route.
`(config)#ip route 2.2.2.0/24 xe3/1`	Configure static route.

(config)#ip route 3.3.3.0/24 xe3/1	Configure static route.
(config)#ip route 4.4.4.0/24 xe3/1	Configure static route.
(config)#ip route 5.5.5.0/24 xe3/1	Configure static route.
(config)#ip route 6.6.6.0/24 xe3/1	Configure static route.

R2

#configure terminal	Enter the Configure mode.
(config)#interface xe3/1	Configure IP address for interface
(config-if)#ip address 20.1.1.2/24	Configure IP address for interface
(config-if)#exit	Exit from interface mode and enter into Configure mode
(config)#router bgp 100	Assign the ASN value (100) to the BGP router.
(config-router)#redistribute static	Redistribute the static routes.
(config-router)#neighbor 20.1.1.1 remote-as 100	Configure neighbor iBGP.
(config-router)#exit	Exit the BGP Router mode and return to the Configure mode.
(config)#access-list 1 permit 2.2.2.0 0.0.0.255	Configure access-list by allowing only one route to install in FIB table.
(config)# route-map test permit 1	Configure route-map to match access-list
(config-route-map)# match ip address 1	Match the above configured access-list 1
(config-route-map)#exit	Exit from route-map Configure mode and enter into Configure mode
(config)#router bgp 100	Enter into BGP router mode
(config-router)# table-map test filter	Apply table-map with route-map created and with filter option
(config-router)#end	Exit from router and Configure mode

Validation

Table-map with filter option

Verify BGP neighborship is up between R1 and R2. Before applying table-map in R2, all routes will be installed in FIB table, as in below output.

R1

```
#show ip bgp summary
BGP router identifier 20.1.1.1, local AS number 100
BGP table version is 3
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS    MsgRcv    MsgSen TblVer   InQ   OutQ    Up/ Dow
n   State/PfxRcd
20.1.1.2                 4   100    5          6       3      0      0  00:01:31
               0
Total number of neighbors 1
```

```
Total number of Established sessions 1
#show ip bgp
BGP table version is 3, local router ID is 20.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i
- internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network          Next Hop            Metric   LocPrf       Weight Path *>
1.1.1.0/24        0.0.0.0             0        100          32768    ?
*>    2.2.2.0/24       0.0.0.0             0        100           32768    ?
*>    3.3.3.0/24       0.0.0.0             0        100           32768    ?
*>    4.4.4.0/24       0.0.0.0             0        100           32768    ?
*>    5.5.5.0/24       0.0.0.0             0        100           32768    ?
*>    6.6.6.0/24       0.0.0.0             0        100           32768    ?

Total number of prefixes 6
#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
S       1.1.1.0/24 [1/0] is directly connected, xe3/1
S2.2.2.0/24 [1/0] is directly connected, xe3/1
S3.3.3.0/24 [1/0] is directly connected, xe3/1
S4.4.4.0/24 [1/0] is directly connected, xe3/1
S5.5.5.0/24 [1/0] is directly connected, xe3/1
S6.6.6.0/24 [1/0] is directly connected, xe3/1
C20.1.1.0/24 is directly connected, xe3/1
C127.0.0.0/8 is directly connected, lo
```

Gateway of last resort is not set

R2

```
#show ip bgp
BGP table version is 3, local router ID is 20.1.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i
- internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network          Next Hop            Metric     LocPrf       Weight Path *>i
1.1.1.0/24        20.1.1.1             0        100          0        ?
*>i   2.2.2.0/24       20.1.1.1             0        100          0        ?
*>i   3.3.3.0/24       20.1.1.1             0        100          0        ?
*>i   4.4.4.0/24       20.1.1.1             0        100          0        ?
*>i   5.5.5.0/24       20.1.1.1             0        100          0        ?
```

```
*>i  6.6.6.0/24       20.1.1.1             0        100          0        ?
Total number of prefixes 6
#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
B       1.1.1.0/24 [200/0] via 20.1.1.1, xe3/1, 00:01:09
B       2.2.2.0/24 [200/0] via 20.1.1.1, xe3/1, 00:01:09
B       3.3.3.0/24 [200/0] via 20.1.1.1, xe3/1, 00:01:09
B       4.4.4.0/24 [200/0] via 20.1.1.1, xe3/1, 00:01:09
B       5.5.5.0/24 [200/0] via 20.1.1.1, xe3/1, 00:01:09
B       6.6.6.0/24 [200/0] via 20.1.1.1, xe3/1, 00:01:09
C       20.1.1.0/24 is directly connected, xe3/1
C       127.0.0.0/8 is directly connected, lo
```

Gateway of last resort is not set

Now verify after applying table-map with filter option, only one route will be installed in FIB table according to route-map and access-list configured, BGP table remains same, table-map effect will be seen only for FIB table After applying table-map, clear BGP with “clear ip bgp table-map”

R2

```
#show ip bgp
BGP table version is 5, local router ID is 20.1.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i
- internal, l - labeled
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network          Next Hop            Metric     LocPrf      Weight Path *>i
1.1.1.0/24        20.1.1.1             0        100          0        ?
*>i   2.2.2.0/24       20.1.1.1             0        100          0        ?
*>i   3.3.3.0/24       20.1.1.1             0        100          0        ?
*>i   4.4.4.0/24       20.1.1.1             0        100          0        ?
*>i   5.5.5.0/24       20.1.1.1             0        100          0        ?
*>i   6.6.6.0/24       20.1.1.1             0        100          0        ?

Total number of prefixes 6
#show ip bgp summary
BGP router identifier 20.1.1.2, local AS number 100
BGP table version is 5
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/ Dow
n   State/PfxRcd
```

```
20.1.1.1                4   100   10          9       5      0      0
00:03:51
               6

Total number of neighbors 1

Total number of Established sessions 1
#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
B       2.2.2.0/24 [200/0] via 20.1.1.1, xe3/1, 00:00:12
C       20.1.1.0/24 is directly connected, xe3/1
C       127.0.0.0/8 is directly connected, lo
```

Gateway of last resort is not set

Table-map without filter option

Remove filter option while applying table-map as below in R2

#configure terminal	Enter the Configure mode.
(config)#router bgp 100	Enter into BGP router mode
(config-router)# table-map test	Apply table-map with route-map created and with filter option
(config-router)#end	Exit from router and Configure mode

```
Do “clear ip bgp table-map” and verify routes in FIB table
Now all routes will be installed in FIB table #show ip
route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
B       1.1.1.0/24 [200/0] via 20.1.1.1, xe3/1, 00:00:05
B       2.2.2.0/24 [200/0] via 20.1.1.1, xe3/1, 00:00:05
B       3.3.3.0/24 [200/0] via 20.1.1.1, xe3/1, 00:00:05
B       4.4.4.0/24 [200/0] via 20.1.1.1, xe3/1, 00:00:05
B       5.5.5.0/24 [200/0] via 20.1.1.1, xe3/1, 00:00:05
B       6.6.6.0/24 [200/0] via 20.1.1.1, xe3/1, 00:00:05
C       20.1.1.0/24 is directly connected, xe3/1
C       127.0.0.0/8 is directly connected, lo
```

Gateway of last resort is not set

Note: Same can be tried with IPV6 VRF –v4 and VRF-v6 address-families and this feature is not supported for VPNV4 address-family

Route Target Constraint

BGP/MPLS IP VPNs use PE routers to Route Target (RT) extended communities and control the distribution of routes into the VRFs. Within a given iBGP mesh, PE routers hold routes marked with RouteTargets pertaining to VRFs that have local CE attachments.

BGP RT Constrained Route Distribution is a feature that can be used by service providers in Multiprotocol Label Switching (MPLS) Layer 3 VPNs to reduce the number of unnecessary routing updates that route reflectors (RRs) send to Provider Edge (PE) routers. The reduction in “routing updates” saves resources by allowing RRs, Autonomous System Boundary Routers (ASBRs), and PEs to carry fewer routes. Route targets are used to constrain routing updates.

With (MPLS)VPNs, the (iBGP) peers or Route Reflectors send all VPN4 and/or VPN6 prefixes to the PE routers. The PE routers drop the VPN4/6 prefixes for which there is no importing VPN route forwarding (VRF).

Topology

The topology below shows Route-target filtering in an L3VPN—with Route Target Constraint (RTC), the RR sends only wanted VPN4/6 prefixes to the PE; wanted” means that the PEs have the VRFs importing the specific prefixes.

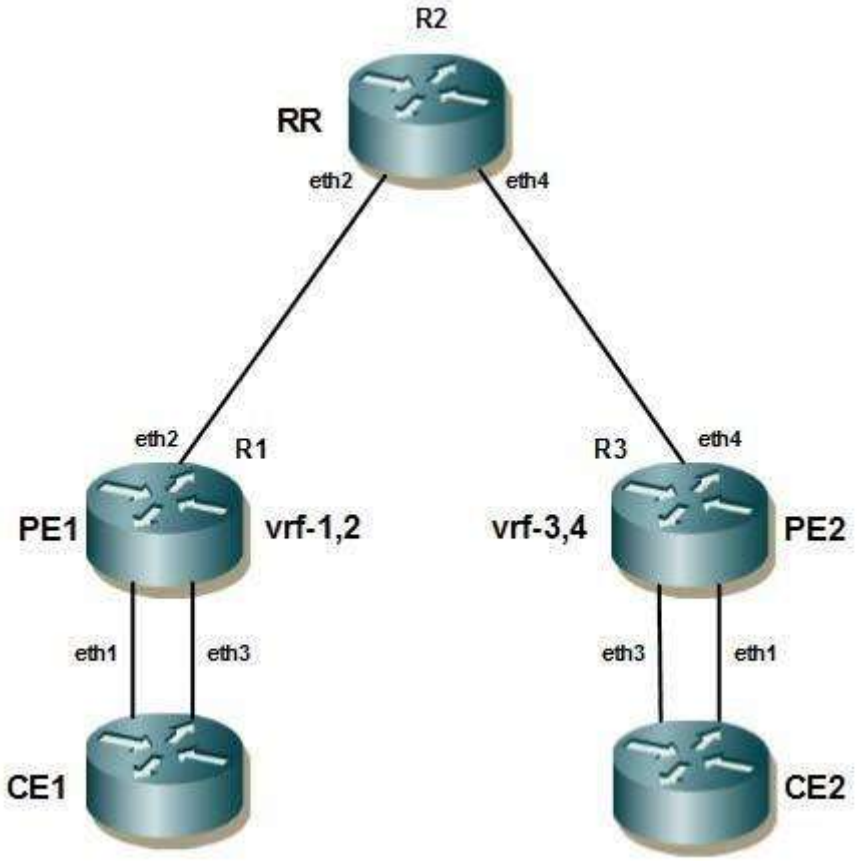


Figure 1-10: Route-target Filter Topology

CE1

`#configure terminal`	Enter Configure mode.

(config)#interface eth1	Enter interface mode
(config-if)#ip address 80.1.1.1/24	Configure IP address for interface
(config-if)#exit	Exit from interface mode and enter into Configure mode
(config)#interface eth3	Enter interface mode
(config-if)#ip address 90.1.1.1/24	Configure IP address for interface
(config-if)#exit	Exit from interface mode and enter into Configure mode
(config)# router bgp 200	Assign the ASN value (100) to the BGP router
(config-router)#neighbor 80.1.1.2 remote-as 100 (config-router)#neighbor 90.1.1.2 remote-as 100	Configure neighbor (RR) in IBGP
(config-router)#redistribute static	Redistribute static routes into BGP
(config-router)#exit	Exit from router mode and enter configure mode
(config)#ip route vrf 1 1.1.1.0/24 eth1	Configure static route with VRF 1 instance
(config)#ip route vrf 2 3.3.3.0/24 eth3	Configure static route with VRF 2 instance
(config)#ip route vrf 2 4.4.4.0/24 eth3	Configure static route with VRF 2 instance
CE2	
#configure terminal	Enter Configure mode.
(config)#interface eth1	Enter interface mode
(config-if)#ip address 101.1.1.1/24	Configure IP address for interface
(config-if)#exit	Exit from interface mode and enter into Configure mode
(config)#interface eth3	Enter interface mode
(config-if)#ip address 100.1.1.1/24	Configure IP address for interface
(config-if)#exit	Exit from interface mode and enter into Configure mode
(config)# router bgp 200	Assign the ASN value (100) to the BGP router
(config-router)#neighbor 100.1.1.2 remote-as 100 (config-router)#neighbor 101.1.1.2 remote-as 100	Configure neighbor (RR) in IBGP
(config-router)#end	Exit from router and configure mode
PE1	
#configure terminal	Enter Configure mode.
(config)#ip vrf 1	Create a VRF instance 1
(config-vrf)#rd 1:100	Configure unique RD value for VRF to identify VRF instance
(config-vrf)#route-target export 1:200	Configure route-target (rt) value for exporting routes into other VRFs (for other PE's)
(config-vrf)#exit	Exit VRF mode and enter Configure mode
(config)#ip vrf 2	Create a VRF instance 2

(config-vrf)#rd 1:300	Configure unique RD value for VRF to identify VRF instance
(config-vrf)#route-target both 1:400	Configure route-target (rt) value for exporting routes into other VRFs (for other PE's)
(config-vrf)#exit	Exit VRF mode and enter Configure mode
(config)#router ldp	Enable LDP.
(config-router)#exit	Exit router LDP mode
(config)#interface lo	Enter loopback interface mode
(config-if)#ip address 11.11.11.11/32	Configure IP address for loopback interface
(config-if)# enable-ldp ipv4	Enable LDP on loopback interface
(config-if)#exit	Exit interface mode and enter configure mode
(config)#interface eth1	Enter interface mode
(config-if)#ip vrf forwarding 1	Bind interface to VRF 1
(config-if)#ip address 80.1.1.2/24	Configure IP address for VRF binded interface
(config-if)#exit	Exit interface mode and enter configure mode
(config)#interface eth2	Enter interface mode
(config-if)#ip address 40.1.1.1/24	Configure an IP address for interface
(config-if)#label-switching	Enable label-switching on interface
(config-if)# enable-ldp ipv4	Enable LDP on connected interface between PE1 and RR
(config-if)#exit	Exit interface mode and enter configure mode
(config)#interface eth3	Enter interface mode
(config-if)#ip vrf forwarding 2	Bind interface to VRF 1
(config-if)#ip address 90.1.1.2/24	Configure IP address for VRF binded interface
(config-if)#exit	Exit interface mode and enter configure mode
(config)#router ospf	Enable OSPF process between PE1 and RR
(config-router)#network 11.11.11.11/32 area 0.0.0.0 (config-router)#network 40.1.1.0/24 area 0.0.0.0	Advertise loopback network in OSPF area 0
(config-router)#exit	Exit router OSPF mode
(config)# router bgp 100	Assign the ASN value (100) to the BGP router
(config-router)#neighbor 22.22.22.22 remoteas 100	Configure neighbor (RR) in IBGP
(config-router)#neighbor 22.22.22.22 updatesource lo	Enable neighbor with loopback interface.
(config-router)#address-family vpnv4 unicast	Enter Address-Family-VPNv4 mode.
(config-router-af)#neighbor 22.22.22.22 activate	Activate RR neighbor
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.

(config-router)#address-family rtfilter unicast	Enable RT filter address-family mode
(config-router-af)#neighbor 22.22.22.22 activate	Activate neighbor
(config-router-af)#exit-address-family	Exit RTfilter Address Family mode and return to Router mode.
(config-router)#address-family ipv4 vrf 1	Enter Address-Family-VRF mode.
(config-router-af)#neighbor 80.1.1.1 remoteas 200	Configure CE neighbor in VRF mode
(config-router-af)#neighbor 80.1.1.1 activate	Activate neighbor in VRF
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.
(config-router)#address-family ipv4 vrf 2	Enter Address-Family-VRF mode.
(config-router-af)#neighbor 90.1.1.1 remoteas 200	Configure CE neighbor in VRF mode
(config-router-af)#neighbor 90.1.1.1 activate	Activate neighbor in VRF
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.
(config-router)#end	Exit from router mode and configure mode

RR

(config)#router ldp	Enable LDP
(config-router)#exit	Exit router LDP mode
(config)#interface lo	Enter loopback interface
(config-if)#ip address 22.22.22.22/32 secondary (config-if)#ip address 44.44.44.44/32 secondary	Configure IP address for loopback interface
(config-if)# enable-ldp ipv4	Enable LDP on loopback interface
(config-if)#exit	Exit interface mode and enter configure mode
(config)#interface eth2	Enter interface mode
(config-if)#ip address 40.1.1.2/24	Configure IP address for interface connecting to PE2
(config-if)#label-switching	Enable label-switching on interface
(config-if)# enable-ldp ipv4	Enable LDP on connected interface between PE1 and RR
(config-if)#exit	Exit interface mode and enter configure mode
(config)#interface eth4	Enter into interface mode
(config-if)#ip address 50.1.1.1/24	Configure an IP address for interface connecting to PE1
(config-if)#label-switching	Enable label-switching on interface
(config-if)# enable-ldp ipv4	Enable LDP on connected interface between PE1 and RR
(config-if)#exit	Exit interface mode and enter configure mode
(config)#router ospf	Enable OSPF process between PE1 and RR
(config-router)#network 22.22.22.22/32 area 0.0.0.0	Advertise loopback network in OSPF area 0

(config-router)#network 40.1.1.0/24 area 0 config-router)#network 44.44.44.44/32 area 0.0.0.0 config-router)#network 50.1.1.0/24 area 0.0.0.0	Advertise PE1 to RR connected network in OSPF
(config-router)#exit	Exit from router OSPF mode
(config)# router bgp 100	Assign the ASN value (100) to the BGP router
(config-router)#neighbor 11.11.11.11 remoteas 100	Configure neighbor (PE1) in IBGP
(config-router)#neighbor 11.11.11.11 updatesource 22.22.22.22	Enable neighbor with loopback interface
(config-router)#neighbor 33.33.33.33 remoteas 100	Configure neighbor (PE2) in IBGP
(config-router)#neighbor 33.33.33.33 updatesource 44.44.44.44	Enable neighbor with loopback interface
(config-router)#address-family vpnv4 unicast	Enter Address-Family-VPNv4 mode.
(config-router-af)#neighbor 11.11.11.11 activate	Activate PE1 neighbor
(config-router-af)#neighbor 33.33.33.33 activate	Activate PE2 neighbor
(config-router-af)#neighbor 11.11.11.11 route-reflector client	Configure PE1 as Route Reflector client
(config-router-af)#neighbor 33.33.33.33 route-reflector client	Configure PE2 as Route Reflector client
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.
(config-router)#address-family rtfilter unicast	Enable RT filter address-family mode
(config-router-af)#neighbor 11.11.11.11 activate	Activate PE1 neighbor in RTfilter family
(config-router-af)#neighbor 33.33.33.33 activate	Activate PE2 neighbor in RTfilter family
(config-router-af)#neighbor 33.33.33.33 route-reflector client	Configure PE2 as Route Reflector client
(config-router-af)#neighbor 11.11.11.11 route-reflector client	Configure PE1 as Route Reflector client
(config-router-af)#exit-address-family	Exit RTfilter Address-Family mode
(config-router)#end	Exit from Address-Family, Router and Configure mode.

PE2

#configure terminal	Enter Configure mode.
(config)#ip vrf 3	Create a VRF instance 3
(config-vrf)#rd 1:600	Configure unique RD value for VRF to identify VRF instance
(config-vrf)#route-target export 1:200	Configure route-target (rt) value for exporting routes into other VRFs (for other PE's)

(config-vrf)#exit	Exit VRF mode and enter Configure mode
(config)#ip vrf 4	Create a VRF instance 4
(config-vrf)#rd 1:900	Configure unique RD value for VRF to identify VRF instance
(config-vrf)#route-target both 1:400	Configure route-target (rt) value for exporting routes into other VRFs (for other PE's)

(config-vrf)#exit	Exit VRF mode and enter Configure mode
(config)#router ldp	Enable LDP.
(config-router)#exit	Exit router LDP mode
(config)#interface lo	Enter loopback interface mode
(config-if)#ip address 33.33.33.33/32	Configure IP address for loopback interface
(config-if)# enable-ldp ipv4	Enable LDP on loopback interface
(config-if)#exit	Exit interface mode and enter configure mode
(config)#interface eth1	Enter interface mode
(config-if)#ip vrf forwarding 3	Bind interface to VRF 3
(config-if)#ip address 101.1.1.2/24	Configure IP address for VRF binded interface
(config-if)#exit	Exit interface mode and enter configure mode
(config)#interface eth3	Enter interface mode
(config-if)#ip vrf forwarding 4	Bind interface to VRF 3
(config-if)#ip address 100.1.1.2/24	Configure IP address for VRF binded interface
(config-if)#exit	Exit interface mode and enter configure mode
(config)#interface eth4	Enter interface mode
(config-if)#ip address 50.1.1.2/24	Configure an IP address for interface
(config-if)#label-switching	Enable label-switching on interface
(config-if)# enable-ldp ipv4	Enable LDP on connected interface between PE2 and RR
(config-if)#exit	Exit interface mode and enter configure mode
(config)#router ospf	Enable OSPF process between PE2 and RR
(config-router)#network 33.33.33.33/32 area 0.0.0.0	Advertise loopback network in OSPF area 0
(config-router)#network 50.1.1.0/24 area 0	Advertise PE2 to RR connected network in OSPF
(config-router)#exit	Exit router OSPF mode
(config)# router bgp 100	Assign the ASN value (100) to the BGP router
(config-router)#neighbor 44.44.44.44 remoteas 100	Configure neighbor (RR) in IBGP
(config-router)#neighbor 44.44.44.44 updatesource 33.33.33.33	Enable neighbor with loopback interface.
(config-router)#address-family vpnv4 unicast	Enter Address-Family-VPNv4 mode.

(config-router-af)#neighbor 44.44.44.44 activate	Activate RR neighbor
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.
(config-router)#address-family rtfilter unicast	Enable RT filter address-family mode
(config-router-af)#neighbor 44.44.44.44 activate	Activate neighbor
(config-router-af)#exit-address-family	Exit RTfilter Address Family mode and return to Router mode.
(config-router)#address-family ipv4 vrf 3	Enter Address-Family-VRF mode.
(config-router-af)#neighbor 101.1.1.1 remoteas 200	Configure CE neighbor in VRF mode
(config-router-af)#neighbor 101.1.1.1 activate	Activate neighbor in VRF
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.
(config-router)#address-family ipv4 vrf 4	Enter Address-Family-VRF mode.
(config-router-af)#neighbor 100.1.1.1 remoteas 200	Configure CE neighbor in VRF mode
(config-router-af)#neighbor 100.1.1.1 activate	Activate neighbor in VRF
(config-router-af)#exit-address-family	Exit Address Family mode and return to Router mode.
(config-router)#end	Exit router and configure mode

Validation

Through RTfilter address-family RT values will be exchanged between RR and PE's. Neighbors are activated under this address-family and configured clients as well in this. RR will learn routes from PE's and send to other PE's if it has any peer requesting for that particular routes based on their RT import values

Below outputs shows the routes sent and learned in PE's and installed in VRF's and display's RT filter values exchanged between them.

CE1

```
CE1#sh ip bgp
BGP table version is 10, local router ID is 90.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled                S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network          Next Hop            Metric   LocPrf       Weight Path *>
1.1.1.0/24        0.0.0.0             0        100          32768    ?
*>    3.3.3.0/24       0.0.0.0              0       100          32768     ?
*>    4.4.4.0/24       0.0.0.0              0       100          32768     ?

Total number of prefixes 3
```

PE1

```
PE1#sh ip bgp vpnv4 all
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled S Stale Origin codes: i
- IGP, e - EGP, ? - incomplete

     Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 1:100 (Default for VRF 1)
*>    1.1.1.0/24       80.1.1.1              0        100          0      200 ?
*>    3.3.3.0/24       80.1.1.1              0        100          0      200 ?
*>    4.4.4.0/24       80.1.1.1              0        100          0      200 ?
 Announced routes count = 3
 Accepted routes count = 0
Route Distinguisher: 1:300 (Default for VRF 2)
*>    1.1.1.0/24       90.1.1.1              0        100          0      200 ?
*>    3.3.3.0/24       90.1.1.1              0        100          0      200 ?
*>    4.4.4.0/24       90.1.1.1              0        100          0      200 ?
 Announced routes count = 3
 Accepted routes count = 0

PE1#sh ip bgp rtfilter all
RTFilter's Received
******************** peer-ip
22.22.22.22 100:2:1:400
RTFilter's Sent
******************** peer-ip
22.22.22.22 100:2:1:400
```

RR

```
RR#sh ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled S Stale Origin codes: i
- IGP, e - EGP, ? - incomplete

     Network          Next Hop            Metric    LocPrf      Weight Path
Route Distinguisher: 1:300
*>i   1.1.1.0/24       11.11.11.11           0        100          0      200 ?
*>i   3.3.3.0/24       11.11.11.11           0        100          0      200 ?
*>i   4.4.4.0/24       11.11.11.11           0        100          0      200 ?
 Announced routes count = 0
 Accepted routes count = 3

RR#sh ip bgp rtfilter all
RTFilter's Received
********************
peer-ip 11.11.11.11
100:2:1:400 peer-ip
33.33.33.33
100:2:1:400
RTFilter's Sent
********************
peer-ip 11.11.11.11
```

```
100:2:1:400 peer-ip
33.33.33.33
100:2:1:400
```

PE2

```
PE2#sh ip bgp vpnv4 all
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, l - labeled S Stale Origin codes: i
- IGP, e - EGP, ? - incomplete

     Network          Next Hop            Metric     LocPrf     Weight Path
Route Distinguisher: 1:300
*>i   1.1.1.0/24       11.11.11.11           0        100          0      200 ?
*>i   3.3.3.0/24       11.11.11.11           0        100          0      200 ?
*>i   4.4.4.0/24       11.11.11.11           0        100          0      200 ?
  Announced routes count = 0
 Accepted routes count = 3
Route Distinguisher: 1:900 (Default for VRF 4)
*>i   1.1.1.0/24       11.11.11.11           0        100          0      200 ?
*>i   3.3.3.0/24       11.11.11.11           0        100          0      200 ?
*>i   4.4.4.0/24       11.11.11.11           0        100          0      200 ?
 Announced routes count = 0
 Accepted routes count = 3

PE2#sh ip bgp rtfilter all
RTFilter's Received
******************** peer-ip
44.44.44.44 100:2:1:400
RTFilter's Sent
******************** peer-ip
44.44.44.44
100:2:1:400
```

CHAPTER 2 BGP4+

This chapter contains basic BGP4+ configuration examples.

For details about the commands used in these examples, see the *Border Gateway Protocol Command Reference*.

Enable iBGP Peering Using a Global Address

This example shows the minimum configuration required to enable BGP on an interface. R1 and R2 are two routers belonging to the same Autonomous System (AS), AS200, connecting to network 3ffe:10::/48. First, specify the IPv6 global address, then define the routing process and AS number to which the routers belong. Configure a fixed Router ID, then, define BGP neighbors to start exchanging routing updates.

Topology

Figure 2-11: iBGP Peering

Configuration

R1

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Specify the interface `(eth1)` to configure.
`(config-if)#ipv6 address 3ffe:10::10/48`	Specify the IPv6 global address.
`(config-if)#exit`	Enter Configure mode.
`(config)#router bgp 200`	Define the routing process. The number `200` specifies the AS number of `R1`.
`(config-router)#bgp router-id 10.10.10.10`	Configure a fixed Router ID (`10.10.10.10`) for the BGP4+ routing process.
`(config-router)#neighbor 3ffe:10::11 remoteas 200`	Define BGP neighbor `R2`, and establish a TCP session by specifying the global IPv6 address (`3ffe:10::11`) and the AS number `(200)` of neighbor R2.
`(config-router)#address-family ipv6`	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.
`(config-router-af)#neighbor 3ffe:10::11 activate`	Activate the neighbor `R2(3ffe:10::11)`, and enable exchange of IPv6 address prefix types with this neighbor.

R2

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Specify the interface `(eth1)` to configure.
`(config-if)#ipv6 address 3ffe:10::11/48`	Specify the IPv6 global address.
`(config-if)#exit`	Enter Configure mode.
`(config)#router bgp 200`	Define the routing process. The number `200` specifies the AS number of `R2`.
`(config-router)#bgp router-id 10.10.10.11`	Configure a fixed Router ID (`10.10.10.11`) for the BGP4+ routing process.
`(config-router)#neighbor 3ffe:10::10 remoteas 200`	Define the BGP neighbor (R1), and establish a TCP session by specifying the global IPv6 address (`3ffe:10::10`) and the AS number `(200)` of neighbor `R1`.
`(config-router)#address-family ipv6`	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.
`(config-router-af)#neighbor 3ffe:10::10 activate`	Activate the neighbor `R1(3ffe:10::10)`, and enable exchange of IPv6 address prefix types with this neighbor.

Validation

show bgp ipv6 summary, show bgp ipv6 neighbors

Enable iBGP Peering Using Link-local Address

This example shows the minimum configuration required to enable iBGP on an interface. R1 and R2 are two routers belonging to the same AS, AS200, connecting to network fe80::/10. First, define the routing process and AS number to which the routers belong. Configure a fixed Router ID for the BGP4+ routing process, then, define BGP neighbors to start exchanging routing updates.

Topology

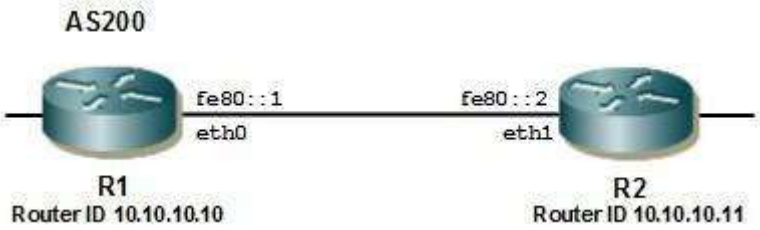


Figure 2-12: iBGP Peering Link-Local Address

Configuration

R1

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 200`	Define the routing process. The number `200` specifies the AS number of `R1`.

(config-router)#bgp router-id 10.10.10.10	Configure a fixed Router ID (10.10.10.10) for the BGP4+ routing process.
(config-router)#neighbor fe80::2 remote-as 200	Define BGP neighbor (R2), and establish a TCP session by specifying the link-local address (fe80::2) and the AS number (200) of neighbor R2.
(config-router)#neighbor fe80::2 interface eth0	To specify a link-local neighbor, configure the interface name of the neighbor fe80::2.
(config-router)#address-family ipv6	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.
(config-router-af)#neighbor fe80::2 activate	Activate the neighbor R2(fe80::2), and enable exchange of IPv6 address prefix types with this neighbor.
R2	
(config)#router bgp 200	Define the routing process. The number 200 specifies the AS number of R2.
(config-router)#bgp router-id 10.10.10.11	Configure a fixed Router ID (10.10.10.11) for the BGP4+ routing process.
(config-router)#neighbor fe80::1 remote-as 200	Define the BGP neighbor (R1), and establish a TCP session by specifying the link-local address R1(fe80::1) and the AS number (200) of neighbor R1.
(config-router)#neighbor fe80::1 interface eth1	To specify a link-local neighbor, configure the interface name of the neighbor fe80::1.
(config-router)#address-family ipv6	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.
(config-router-af)#neighbor fe80::1 activate	Activate the neighbor R1(fe80:1), and enable exchange of IPv6 address prefix types with this neighbor.

Validation

show bgp ipv6 summary, show bgp ipv6, show bgp ipv6 neighbors

Enable eBGP Peering Between Different Autonomous Systems

This example shows the minimum configuration required to enable eBGP on an interface, when the routers belong to different ASs. R1 and R2 are two routers in different ASs, AS200 and AS300 connecting to network 3ffe:10::/64.

Topology

Figure 2-13: BGP Peering - Different AS

Configuration

R1

#configure terminal	Enter Configure mode.
(config)#router bgp 200	Define the routing process. The number 200 specifies the AS number of R1.
(config-router)#bgp router-id 10.10.10.10	Configure a fixed Router ID (10.10.10.10) for the BGP4+ routing process.
(config-router)#neighbor 3ffe:10::11 remoteas 300	Define the BGP neighbor (R2), and establish a TCP session by specifying the IPv6 address (3ffe:10::11) and the AS number (300) of neighbor R2.
(config-router)#address-family ipv6	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.
(config-router-af)#neighbor 3ffe:10::11 activate	Activate the neighbor R2(3ffe:10::11), and enable exchange of IPv6 address prefix types with this neighbor.

R2

(config)#router bgp 300	Define the routing process. The number 300 specifies the AS number of R2.
(config-router)#bgp router-id 10.10.10.11	Configure a fixed Router ID (10.10.10.11) for the BGP4+ routing process.
(config-router)#neighbor 3ffe:10::10 remote-as 200	Define the BGP neighbor (R1), and establish a TCP session by specifying the IPv6 address (3ffe:10::10) and the AS number (200) of neighbor R1.
(config-router)#address-family ipv6	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.
(config-router-af)#neighbor 3ffe:10::10 activate	Activate the neighbor R1(3ffe:10::10) and enable exchange of IPv6 address prefix types with this neighbor.

Validation

show bgp ipv6 summary, show bgp ipv6 neighbors

Route-Map

Use route-maps to filter incoming updates from a BGP peer. In this example, a prefix list named myPrefixList on R1 is configured to deny entry of any routes with the IP address 3ffe:12::/32. To test the filter, R2 is configured to generate network prefixes 3ffe:11::/48 and 3ffe:12::/48. To verify, use the show bgp ipv6 command on R1; it displays R1 receiving only the 3ffe:11::/48 network prefix.

Topology

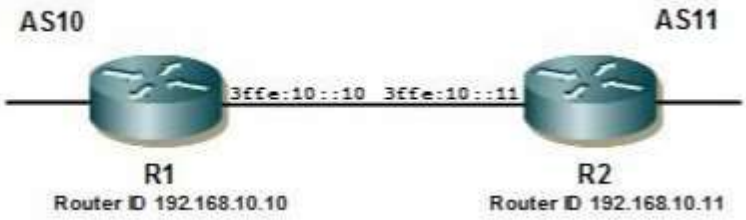


Figure 2-14: Route-Map

Configuration

R1

`#configure terminal`	Enter Configure mode.
`(config)#ipv6 prefix-list myPrefixList seq 5 deny 3ffe:12::/32 ge 48 le 64`	Create an entry in the prefix-list. `myPrefixList` is the name of the map that is created. `5` and `10` specify the sequence number or position of this specific route map. `deny` specifies the packets are to be rejected. `permit` specifies the packets are to be allowed. `48` and `64` are the minimum and maximum prefix lengths, respectively, to be matched.
`(config)#ipv6 prefix-list myPrefixList seq 10 permit any`	Create another entry in the `myPrefixList` map. `10` specifies the sequence number or position of this specific route map. `permit any` specifies accept all packets of any length.
`(config)#route-map myPrefixList permit 1`	Enter Route-map mode.
`(config-route-map)#match ipv6 address prefix-list myPrefixList`	Set the match criteria. In this case, if the route-map name matches `myPrefixList`, the packets from the first sequence will be denied.
`(config-route-map)#exit`	Exit Route-map mode, and return to Configure mode.
`(config)#router bgp 10`	Define the routing process. The number `10` specifies the AS number of `R1`.
`(config-router)#bgp router-id 192.168.10.10`	Configure a fixed Router ID (`192.168.10.10`) for the BGP4+ routing process.
`(config-router)#neighbor 3ffe:10:11 remoteas 11`	Define the BGP neighbor (R2), and establish a TCP session by specifying the IPv6 address (`3ffe:10::11`) and the AS number (`11`) of neighbor `R2`.
`(config-router)#address-family ipv6`	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.
`#configure terminal`	Enter Configure mode.
`(config)#ipv6 prefix-list myPrefixList seq 5 deny 3ffe:12::/32 ge 48 le 64`	Create an entry in the prefix-list. `myPrefixList` is the name of the map that is created. `5` and `10` specify the sequence number or position of this specific route map. `deny` specifies the packets are to be rejected. `permit` specifies the packets are to be allowed. `48` and `64` are the minimum and maximum prefix lengths, respectively, to be matched.

(config)#ipv6 prefix-list myPrefixList seq 10 permit any	Create another entry in the myPrefixList map. 10 specifies the sequence number or position of this specific route map. permit any specifies accept all packets of any length.
(config)#route-map myPrefixList permit 1	Enter Route-map mode.
(config-route-map)#match ipv6 address prefix-list myPrefixList	Set the match criteria. In this case, if the route-map name matches myPrefixList, the packets from the first sequence will be denied.
(config-route-map)#exit	Exit Route-map mode, and return to Configure mode.
(config-router-af)#neighbor 3ffe:10::11 activate	Activate the neighbor R2(3ffe:10::11), and enable exchange of IPv6 address prefix types with this neighbor.
(config-router-af)#neighbor 3ffe:10::11 route-map myPrefixList in	Apply the route-map myPrefixList to all incoming routes.
(config-router-af)#exit-address-family	Exit Address Family mode, and return to Router mode.
(config-router)#exit	Exit Router mode, and return to Configure mode.
R2	
(config)#router bgp 11	Define the routing process. The number 11 specifies the AS number of R2.
(config-router)#bgp router-id 192.168.10.11	Configure a fixed Router ID (192.168.10.11) for the BGP4+ routing process.
(config-router)#neighbor 3ffe:10::10 remoteas 10	Define the BGP neighbor (R1), and establish a TCP session by specifying the IPv6 address (3ffe:10::10) and the AS number (10) of neighbor R1.
(config-router)#address-family ipv6	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.
(config-router-af)#network 3ffe:11::/48	Announce the IPv6 network prefix (3ffe:11::/48).
(config-router-af)#network 3ffe:12::/48	Announce the IPv6 network prefix (3ffe:12::/48).
(config-router-af)#neighbor 3ffe:10::10 activate	Activate the neighbor R1(3ffe:10::10), and enable exchange of IPv6 address prefix types with this neighbor.
(config-router-af)#exit-address-family	Exit Address Family mode, and return to Router mode.

Validation

show bgp ipv6 summary, show bgp ipv6 neighbors, show bgp ipv6, show bgp ipv6 prefix-list

Route Reflector

Use Route Reflectors to reduce the iBGP mesh inside an AS. In this example, R2, R5, and R4 would have to maintain a full mesh among themselves, but by making R5 the Route Reflector, R2 (Client1) has an iBGP session with RR only, and not with R4 (Client 2). The routes learned from R2 are advertised to the other clients, and to iBGP peers outside the cluster; the iBGP routes learned from iBGP peers outside the cluster are advertised to the R2. This reduces the iBGP peer connections in AS1.

Topology

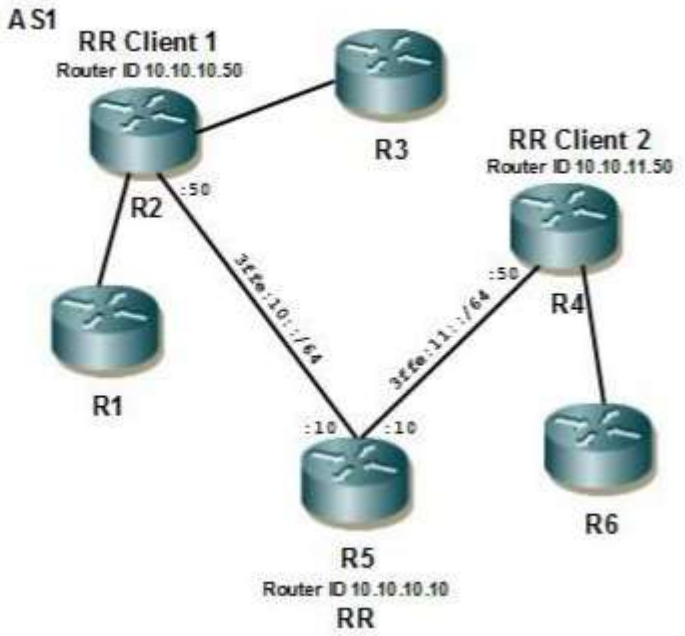


Figure 2-15: BGP4+ Route Reflector

Configuration

RR (R5)

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 1`	Define the routing process. The number `1` specifies the AS number of `R5` (RR).
`(config-router)#bgp router-id 10.10.10.10`	Configure a fixed Router ID (`10.10.10.10`) for the BGP4+ routing process.
`(config-router)#neighbor 3ffe:10::50 remote-as 1`	Define the BGP neighbor (R2), and establish a TCP session by specifying the IPv6 address (`3ffe:10::50`) and the AS number `(1)` of neighbor R2.
`(config-router)#neighbor 3ffe:11::50 remote-as 1`	Define the BGP neighbor (R4), and establish a TCP session by specifying the IPv6 address (`3ffe:11::50`) and the AS number `(1)` of neighbor R4.
`(config-router)#address-family ipv6`	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.
`(config-router-af)#neighbor 3ffe:10::50 activate`	Activate the neighbor `R2(3ffe:10::50)`, and enable exchange of IPv6 address prefix types with this neighbor.
`(config-router-af)#neighbor 3ffe:10::50 routereflector-client`	Configure `R5` as the Route-Reflector (RR) and neighbor `R2` as its client.
`(config-router-af)#neighbor 3ffe:11::50 activate`	Activate the neighbor `R4(3ffe:11::50)`, and enable exchange of IPv6 address prefix types with this neighbor.

`(config-router-af)#neighbor 3ffe:11::50 routereflector-client`	Configure `R5` as the Route-Reflector (RR) and neighbor `R4` as its client.

RR Client 1 (R2)

`(config)#router bgp 1`	Define the routing process. The number `1` specifies the AS number of `R2` (RR Client 1).
`(config-router)#bgp router-id 10.10.10.50`	Configure a fixed Router ID (`10.10.10.50`) for the BGP4+ routing process.
`(config-router)#neighbor 3ffe:10::10 remote-as 1`	Define the BGP neighbor (R5), and establish a TCP session by specifying the IPv6 address (`3ffe:10::10`) and the AS number `(1)` of neighbor `R5`.
`(config-router)#address-family ipv6`	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.
`(config-router-af)#neighbor 3ffe:10::10 activate`	Activate the neighbor `(3ffe:10::10)`, and enable exchange of IPv6 address prefix types with this neighbor.

RR Client 2 (R4)

`(config)#router bgp 1`	Define the routing process. The number `1` specifies the AS number of `R4` (RR Client 2).
`(config-router)#bgp router-id 10.10.11.50`	Configure a fixed Router ID (`10.10.11.50`) for the BGP4+ routing process.
`(config-router)#neighbor 3ffe:11::10 remote-as 1`	Define the BGP neighbor (`R5`), and establish a TCP session by specifying the IPv6 address (`3ffe:11::10`) and the AS number `(1)` of the neighbor.
`(config-router)#address-family ipv6`	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.
`(config-router-af)#neighbor 3ffe:11::10 activate`	Activate the neighbor `(3ffe:11::10)`, and enable exchange of IPv6 address prefix types with this neighbor.

Validation

show bgp ipv6 summary, show bgp ipv6 neighbors

Confederations

In this example, AS1 contains three Confederated Autonomous Systems--AS 1000, AS 1001 and AS 1002. To any outside AS, the overall Confederation is a single AS, AS1. Confederation eBGP is run between R2 and R5, and between R5 and R7. R2 is configured so that its local AS is 1000. Its peer connection to R5 is set up like any other eBGP session. The `bgp confederation identifier` command informs the router that it is a member of a Confederation and passes the Confederation ID. The `bgp confederation peers` command lists the member AS to which R2 is connected. The same command tells the BGP process that the eBGP connection is a Confederation eBGP, rather than a normal eBGP.

Topology

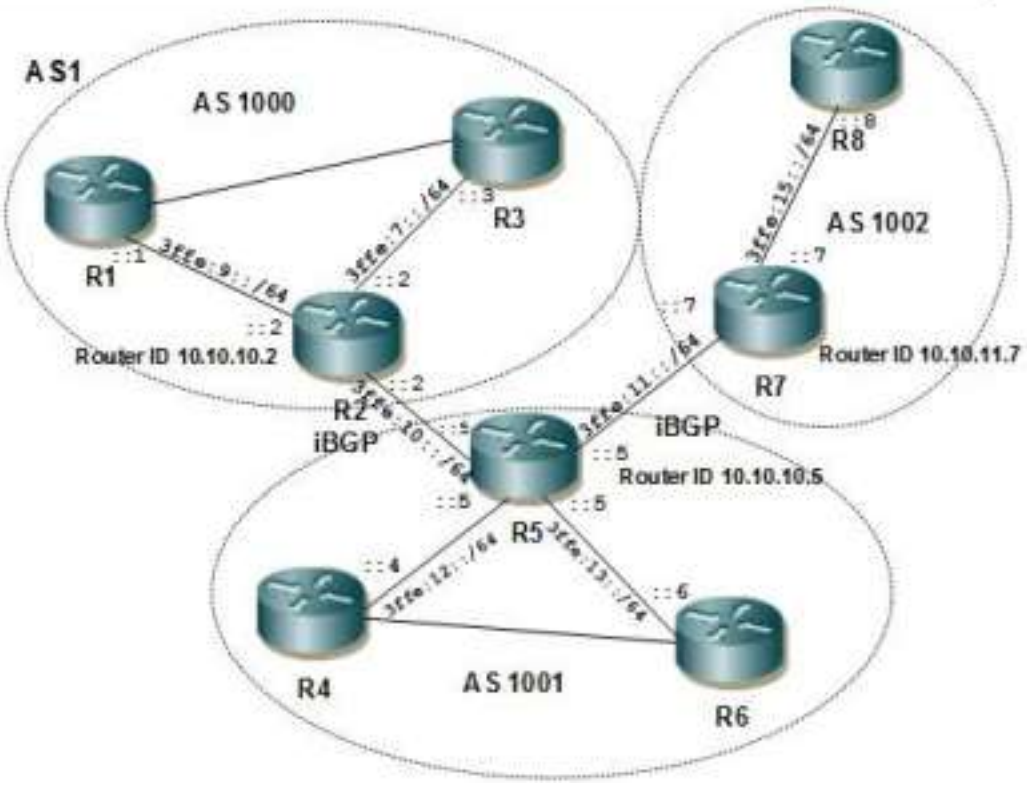


Figure 2-16: BGP4+ Confederations

Configuration

R2

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 1000`	Define the routing process. The number `1000` specifies the AS number of `R2`.
`(config-router)#bgp router-id 10.10.10.2`	Configure a fixed Router ID (`10.10.10.2`) for the BGP4+ routing process.
`(config-router)#bgp confederation identifier 1`	Specify the BGP Confederation Identifier (1). To others, the group will appear as a single AS, and the identifier as its AS number.
`(config-router)#bgp confederation peers 1001 1002`	Specify ASs `1001` and `1002` as confederation peers, making them members of the Confederation.
`(config-router)#neighbor 3ffe:10::5 remoteas 1001`	Define the BGP neighbor (R5), and establish a TCP session by specifying the IPv6 address (`3ffe:10::5`) and the AS number (`1001`) of neighbor `R5`.
`(config-router)#neighbor 3ffe:9::1 remote-as 1000`	Define the BGP neighbor (`R1`), and establish a TCP session by specifying the IPv6 address (`3ffe:9::1`) and the AS number (`1000`) of neighbor `R1`.

(config-router)#neighbor 3ffe:7::3 remote-as 1000	Define the BGP neighbor (R3), and establish a TCP session by specifying the IPv6 address (3ffe:7::3) and the AS number (1000) of neighbor R3.
(config-router)#address-family ipv6	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.
(config-router-af)#neighbor 3ffe:10::5 activate	Activate neighbor R5(3ffe:10::5), and enable exchange of IPv6 address prefix types with this neighbor.
(config-router-af)#neighbor 3ffe:9::1 activate	Activate neighbor R1(3ffe:9::1), and enable exchange of IPv6 address prefix types with this neighbor.
(config-router-af)#neighbor 3ffe:7::3 activate	Activate neighbor R3(3ffe:7::3), and enable exchange of IPv6 address prefix types with this neighbor.

R5

(config)#router bgp 1001	Define the routing process. The number 1001 specifies the AS number of R5.
(config-router)#bgp router-id 10.10.10.5	Configure a fixed Router ID (10.10.10.5) for the BGP4+ routing process.
(config-router)#bgp confederation identifier 1	Specify the BGP Confederation Identifier (1). To others, the group will appear as a single AS, and the identifier as its AS number.
(config-router)#bgp confederation peers 1000 1002	Specify ASs 1001 and 1002 as confederation peers, making them members of the Confederation.
(config-router)#neighbor 3ffe:10::2 remoteas 1000	Define the BGP neighbor (R2), and establish a TCP session by specifying the IPv6 address (3ffe:10::2) and the AS number (1000) of neighbor R2.
(config-router)#neighbor 3ffe:11::7 remoteas 1002	Define the BGP neighbor (R7), and establish a TCP session by specifying the IPv6 address (3ffe:11::7) and the AS number (1002) of neighbor R7.
(config-router)#neighbor 3ffe:12::4 remoteas 1001	Define the BGP neighbor (R4), and establish a TCP session by specifying the IPv6 address (3ffe:12::4) and the AS number (1001) of neighbor R4.
(config-router)#neighbor 3ffe:13::6 remoteas 1001	Define the BGP neighbor (R6), and establish a TCP session by specifying the IPv6 address (3ffe:13::6) and the AS number (1001) of neighbor R6.
(config-router)#address-family ipv6	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.

(config-router-af)#neighbor 3ffe:10::2 activate	Activate the neighbor R2(3ffe:10::2), and enable exchange of IPv6 address prefix types with this neighbor.
(config-router-af)#neighbor 3ffe:11::7 activate	Activate the neighbor R7(3ffe:11::7), and enable exchange of IPv6 address prefix types with this neighbor.
(config-router-af)#neighbor 3ffe:12::4 activate	Activate the neighbor R4(3ffe:12::4), and enable exchange of IPv6 address prefix types with this neighbor.
(config-router-af)#neighbor 3ffe:13::6 activate	Activate the neighbor R6(3ffe:13::6), and enable exchange of IPv6 address prefix types with this neighbor.

R7

(config)#router bgp 1002	Define the routing process. The number 1002 specifies the AS number of R7.
(config-router)#bgp router-id 10.10.11.7	Configure a fixed Router ID (10.10.11.7) for the BGP4+ routing process.
(config-router)#bgp confederation identifier 1	Specify BGP Confederation Identifier (1). To others, the group will appear as a single AS, and the identifier as its AS number.
(config-router)#bgp confederation peers 1000 1001	Specify ASs 1000 and 1001 as confederation peers, making them members of the Confederation.
(config-router)#neighbor 3ffe:11::5 remoteas 1001	Define the BGP neighbor (R5), and establish a TCP session by specifying the IPv6 address (3ffe:11::5) and the AS number (1001) of neighbor R5.
(config-router)#neighbor 3ffe:15::8 remoteas 1002	Define the BGP neighbor (R8), and establish a TCP session by specifying the IPv6 address (3ffe:15::8) and the AS number (1002) of neighbor R8.
(config-router)#address-family ipv6	Enter Address Family mode for configuring routing sessions that use IPv6 address prefixes.
(config-router-af)#neighbor 3ffe:11::5 activate	Activate the neighbor R5(3ffe:11::5), and enable exchange of IPv6 address prefix types with this neighbor.
(config-router-af)#neighbor 3ffe:15::8 activate	Activate the neighbor R8(3ffe:15::8), and enable exchange of IPv6 address prefix types with this neighbor.

Validation

show bgp ipv6 summary, show bgp ipv6 neighbors

BGP4+ Graceful Restart

Using BGP+ graceful restart, the data-forwarding plane of a router can continue to process and forward packets, even if the control plane (which is responsible for determining best paths) fails.

Topology

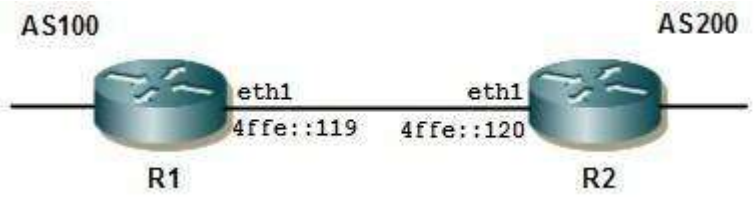


Figure 2-17: BGP4+ Graceful Restart

Configuration

R1

#configure terminal	Enter Configure mode.
(config)#router bgp 100	Assign the ASN value (100) to the router.
(config-router)#bgp graceful-restart	Enable BGP graceful restart support.
(config-router)#neighbor 4ffe::120 remote-as 200	Specify the neighbor's IP address (4ffe::120) and the ASN value of the neighbor (200).
(config-router)#address-family ipv6 unicast	Exchange the IPv6 capabilities, and switch the mode to the IPv6 address family.
(config-router-af)#neighbor 4ffe::120 activate	Specify the neighbor's IPv6 address (4ffe::120), and activate the neighbor.
(config-router-af)#neighbor 4ffe::120 capability graceful-restart	Specify the neighbor's IPv6 address (4ffe::120) for which the graceful restart capability is supported.

R2

#configure terminal	Enter Configure mode.
(config)#router bgp 200	Assign the ASN value (200) to the router.
(config-router)#bgp graceful-restart	Enable BGP graceful restart support.
(config-router)#bgp graceful-restart restarttime 120	Configure the maximum time (120) required for neighbor(s) to restart.
(config-router)#bgp graceful-restart stalepath-time 120	Configure the maximum time (120) to retain stale paths from the restarting neighbor(s).
(config-router)#neighbor 4ffe::119 remote-as 100	Specify the neighbor's IP address (4ffe::119) and the ASN value of the neighbor (100).
(config-router)#address-family ipv6 unicast	Exchange the IPv6 capabilities, and switch the mode to the IPv6 address family.
(config-router-af)#neighbor 4ffe::119 activate	Specify the neighbor's IPv6 address (4ffe::119), and activate the neighbor.
(config-router-af)#neighbor 4ffe::119 capability graceful-restart	Specify the neighbor's IPv6 address (4ffe::119) for which the graceful restart capability is supported.

Validation

show bgp ipv6 summary, show ip bgp neighbors, show bgp ipv6, show ipv6 route database bgp, show ipv6 route database, show ipv6 route

Configure BGP4+ Distance

Administrative distance in BGP+ can be configured for a specific address family.

This example shows configuring the BGP administrative distance for the IPv6 address family.

Topology

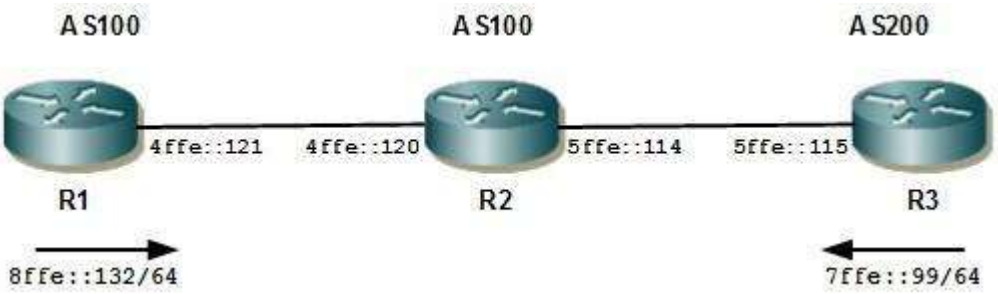


Figure 2-18: BGP4+ Distance

Configuration

R1

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 100`	Assign the ASN value (`100`) to the router.
`(config-router)#network 8ffe::132/64`	Specify the network to be advertised by the BGP routing process.
`(config-router)#neighbor 4ffe::120 remote-as 100`	Specify the neighbor's IP address and ASN value.
`(config-router)#address-family ipv6 unicast`	Enter IPv6 Address-Family mode.
`(config-router-af)#neighbor 4ffe::120 activate`	Activate the IPv6 neighbor.

R2

`#configure terminal`	Enter Configure mode.
`(config)#router bgp 100`	Assign the ASN value (`100`) to the router.
`(config-router)#neighbor 4ffe::121 remote-as` value. `100`	Specify the neighbor's IP address and ASN
`(config-router)#neighbor 5ffe::115 remote-as 200`	Specify the neighbor's IP address and the ASN value of another neighbor.
`(config-router)#address-family ipv6 unicast`	Enter IPv6 Address-Family mode.
`(config-router-af)#aggregate-address 2ffe::102/64 summary-only`	Configure an IPv6 non-AS-set aggregate route on R2. The local distance will be applied to this route.
`(config-router-af)#neighbor 4ffe::121 activate`	Activate the IPv6 neighbor.

(config-router-af)#neighbor 5ffe::115 activate	Activate the IPv6 neighbor.
(config-router-af)#distance 12 13 11	Configure the administrative distance for external, internal, and local routes received in IPv6 Address-Family mode.

R3

#configure terminal	Enter Configure mode.
(config)#router bgp 100	Assign the ASN value (100) to the router.
(config-router)#network 7ffe::99/64	Specify the network to be advertised by the BGP routing process.
(config-router)#neighbor 5ffe::114 remote-as value. 100	Specify the neighbor's IP address and ASN
(config-router)#address-family ipv6 unicast	Enter IPv6 Address-Family mode.
(config-router-af)#neighbor 5ffe::114 activate	Activate the IPv6 neighbor.

Validation

show bgp ipv6 summary, show ip bgp neighbors, show ipv6 route database bgp, show ipv6 route database, show ipv6 route, show bgp ipv6

BGP4+ Graceful Reset

The graceful restart mechanism for BGP+ session reset (the BGP+ daemon is not restarted) is used so that any changes in network configuration do not affect packet forwarding. The `bgp graceful-restart graceful-reset` CLI invokes graceful restart when a configuration change forces a peer reset. Graceful restart is invoked only when these CLI configuration changes force a peer reset.

Topology

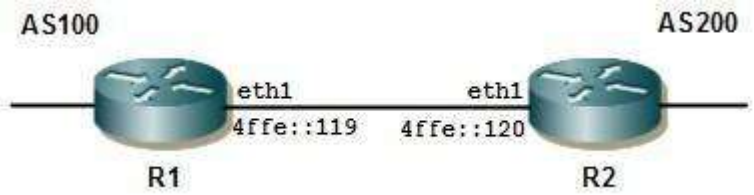


Figure 2-19: BGP4+ Graceful Reset

Configuration

R1

#configure terminal	Enter Configure mode.
(config)#router bgp 100	Assign the ASN value (100) to the router.
(config-router)#bgp graceful-restart	Enable BGP graceful restart support.

(config-router)#bgp graceful-restart graceful-reset	Configure to invoke graceful restart when a configuration change forces a peer reset.
(config-router)#neighbor 4ffe::120 remote-as 200	Specify the neighbor's IP address (4ffe::120) and the ASN value of the neighbor (200).
(config-router)#address-family ipv6 unicast	Exchange the IPv6 capabilities, and switch the mode to the IPv6 address family.
(config-router-af)#neighbor 4ffe::120 activate	Specify the neighbor's IPv6 address (4ffe::120), and activate the neighbor.
(config-router-af)#neighbor 4ffe::120 capability graceful-restart	Specify the neighbor's IPv6 address (4ffe::120) for which the graceful restart capability is supported.

R2

#configure terminal	Enter Configure mode.
(config)#router bgp 200	Assign the ASN value (200) to the router.
(config-router)#bgp graceful-restart	Enable BGP graceful restart support.
(config-router)#bgp graceful-restart graceful-reset	Configure to invoke graceful restart when a configuration change forces a peer reset.
(config-router)#neighbor 4ffe::119 remote-as 100	Specify the neighbor's IP address (4ffe::119) and the ASN value of the neighbor (100).
(config-router)#address-family ipv6 unicast	Exchange the IPv6 capabilities, and switch the mode to the IPv6 address family.
(config-router-af)#neighbor 4ffe::119 activate	Specify the neighbor's IPv6 address (4ffe::119), and activate the neighbor.
(config-router-af)#neighbor 4ffe::119 capability graceful-restart	Specify the neighbor's IPv6 address (4ffe::119) for which the graceful restart capability is supported.

Validation

show bgp ipv6 summary, show ip bgp neighbors, show bgp ipv6, show ipv6 route database bgp, show ipv6 route database, show ipv6 route

CHAPTER 3 OSPFv2

This chapter contains basic OSPFv2 (Open Shortest Path First) configuration examples.

For details about the commands used in these examples, see the *Open Shortest Path First Command Reference*.

Enable OSPF on an Interface

The diagram shows the minimum configuration required to enable OSPF on an interface. R1 and R2 are two routers in Area 0 connecting to network 10.10.10.0/24.

Note: Configure one interface so that it belongs to only one area. It is possible, however, to configure different interfaces on a router to belong to different areas.

Topology

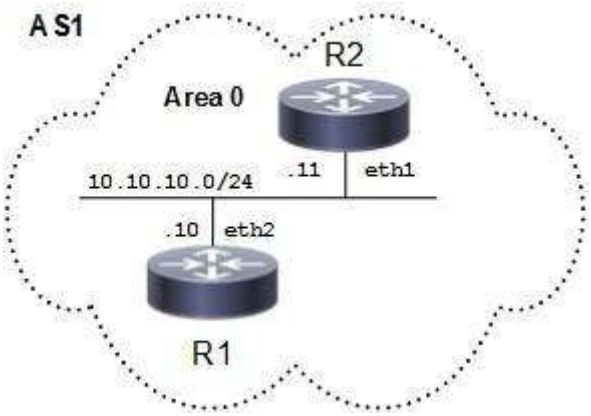


Figure 3-20: Basic OSPF Topology

R1

`#configure terminal`	Enter configure mode
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0`	Define the interface (`10.10.10.0/24`) on which OSPF runs, and associate the area ID (`0`) with the interface (area ID `0` specifies the backbone area).

R2

`#configure terminal`	Enter configure mode
`(config)#router ospf 200`	Configure the routing process, and specify the Process ID `(200)`. The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0`	Define the interface `(10.10.10.0/24)` on which OSPF runs, and associate the area ID `(0)` with the interface.

Validation

R1

```
#show ip ospf
 Routing Process "ospf 100" with ID 10.12.26.88
 Process uptime is 1 minute
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
 Supports only single TOS(TOS0) routes Supports opaque LSA

 Supports Graceful Restart
 SPF schedule delay initial 0 secs 500 msecs
 SPF schedule delay min 0 secs 500 msecs
 SPF schedule delay max 50 secs 0 msecs
 Refresh timer 10 secs
 Number of incomming current DD exchange neighbors 0/64
 Number of outgoing current DD exchange neighbors 0/64
 Initial LSA throttle delay 0 secs 0 msecs
 Minimum hold time for LSA throttle 5 secs 0 msecs
 Maximum wait time for LSA throttle 5 secs 0 msecs
 Minimum LSA arrival 1 secs 0 msecs
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000 Number of
non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 4
 Number of LSA received 4
 Number of areas attached to this router: 1
    Area 0.0.0.0 (BACKBONE)
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 1
        Area has no authentication
        SPF algorithm last executed 00:00:08.102
        ago SPF algorithm executed 3 times Number
        of LSA 7. Checksum 0x0312b5
 Dste Staus: Disabled

#show ip ospf interface eth2 is up,
line protocol is up
  Internet Address 10.10.10.10/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.88, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1, TE Metric 1 Designated
  Router (ID) 10.12.26.88, Interface Address 10.10.10.10 Backup Designated
  Router (ID) 10.12.26.89, Interface Address 10.10.10.11 Timer intervals
  configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:11
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
```

```
  Hello received 13 sent 19, DD received 3 sent 4
  LS-Req received 1 sent 1, LS-Upd received 3 sent 5
  LS-Ack received 3 sent 3, Discarded 0
  No authentication
#show ip ospf neighbor

Total number of full neighbors: 1 OSPF
process 100 VRF(default):
Neighbor ID     Pri   State            Dead Time   Address         Interface
Instance ID
10.12.26.89       1   Full/Backup      00:00:39    10.10.10.11     eth2
0


#show ip ospf route

OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  10.10.10.0/24 [1] is directly connected, eth2, Area 0.0.0.0
```

R2

```
#show  ip ospf
 Routing Process "ospf 200" with ID 10.12.26.89
 Process uptime is 1 minute
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
 Supports only single TOS(TOS0) routes Supports opaque LSA

 Supports Graceful Restart
 SPF schedule delay initial 0 secs 500 msecs
 SPF schedule delay min 0 secs 500 msecs
 SPF schedule delay max 50 secs 0 msecs
 Refresh timer 10 secs
 Number of incomming current DD exchange neighbors 0/64
 Number of outgoing current DD exchange neighbors 0/64
 Initial LSA throttle delay 0 secs 0 msecs
 Minimum hold time for LSA throttle 5 secs 0 msecs
 Maximum wait time for LSA throttle 5 secs 0 msecs
 Minimum LSA arrival 1 secs 0 msecs
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000 Number
of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 3
 Number of LSA received 5
 Number of areas attached to this router: 1
    Area 0.0.0.0 (BACKBONE)
        Number of interfaces in this area is 1(1)
```

```
        Number of fully adjacent neighbors in this area is 1
        Area has no authentication
        SPF algorithm last executed 00:00:45.638 ago
        SPF algorithm executed 4 times
        Number of LSA 7. Checksum 0x0312b5
 Dste Staus: Disabled

#show ip ospf interface eth1 is
up, line protocol is up
  Internet Address 10.10.10.11/24, Area 0.0.0.0, MTU 1500
  Process ID 200, VRF (default), Router ID 10.12.26.89, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.88, Interface Address 10.10.10.10
  Backup Designated Router (ID) 10.12.26.89, Interface Address 10.10.10.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 30 sent 31, DD received 4 sent 3
  LS-Req received 1 sent 1, LS-Upd received 5 sent 3
  LS-Ack received 2 sent 3, Discarded 0
  No authentication


#show ip ospf neighbor

Total number of full neighbors: 1 OSPF
process 200 VRF(default):
Neighbor ID     Pri   State            Dead Time   Address         Interface
Instance ID
10.12.26.88       1   Full/DR          00:00:33    10.10.10.10     eth1
0

#show ip ospf route

OSPF process 200:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  10.10.10.0/24 [1] is directly connected, eth1, Area 0.0.0.0
```

Set Priority

This example shows how to set the priority for an interface. Set a high priority for a router to make it the Designated Router (DR). Router R3 is configured to have a priority of 10, which is higher than the default priority (1) of R1 and R2; making it the DR.

Topology

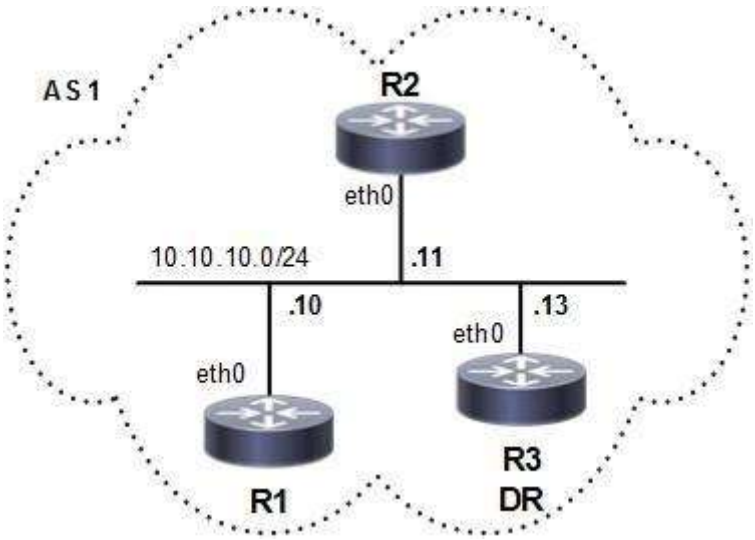


Figure 3-21: Set OSPF Priority

R3

`#configure terminal`	Enter configure mode
`(config)#``interface eth0`	Specify the interface (`eth0`) to configure.
`(config-if)#``ip ospf priority 10`	Specify the router priority to a higher priority (10) to make R3 the Designated Router (DR).
`(config-if)#``exit`	Exit interface mode.
`(config)#``router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#``network 10.10.10.0/24 area 0`	Define the interface (`10.10.10.0/24`) on which OSPF runs, and associate the area ID (`0`) with the interface.

R1

`#configure terminal`	Enter configure mode
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0`	Define the interface (`10.10.10.0/24`) on which OSPF runs, and associate the area ID (`0`) with the interface (area ID `0` specifies the backbone area).

R2

`#configure terminal`	Enter configure mode
`(config)#router ospf 200`	Configure the routing process, and specify the Process ID (`200`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0`	Define the interface (`10.10.10.0/24`) on which OSPF runs, and associate the area ID (`0`) with the interface.

Validation

R1

```
#sh ip ospf neighbor

Total number of full neighbors: 2 OSPF
process 100 VRF(default):
Neighbor ID      Pri   State            Dead Time   Address         Interface
Instance ID
10.12.26.89        1   Full/DROther     00:00:39    10.10.10.11     eth2
0
10.12.26.90       10   Full/DR          00:00:32    10.10.10.13     eth2
0

#sh ip ospf interface
eth2 is up, line protocol is up
  Internet Address 10.10.10.10/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.88, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.90, Interface Address 10.10.10.13
  Backup Designated Router (ID) 10.12.26.88, Interface Address 10.10.10.10
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:10
  Neighbor Count is 2, Adjacent neighbor count is 2
  Suppress hello for 0 neighbor(s)
  Hello received 30 sent 19, DD received 6 sent 8
  LS-Req received 2 sent 2, LS-Upd received 16 sent 6
  LS-Ack received 8 sent 7, Discarded 0
  No authentication

#sh running-config
!
no service password-encryption
!
hostname rtr1
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
!
ip pim register-rp-reachability
! interface lo
mtu 65536
 ip address 127.0.0.1/8 ipv6
address ::1/128
!
interface eth0  ip address 10.12.26.88/24
```

```
!
interface eth1
!
interface eth2  ip address 10.10.10.10/24
!
interface eth3
!
interface eth4
!
interface eth5
!
interface eth6
!
interface eth7
! router ospf 100 network 10.10.10.0/24 area 0.0.0.0 cspf disable-better-
protection
! line con 0  login line vty 0 39  login
! end
```

R2

```
#sh running-config
!
no service password-encryption
!
hostname R2
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
!
ip pim register-rp-reachability
!
interface lo  mtu 65536  ip address 127.0.0.1/8  ipv6 address ::1/128
!
interface eth0  ip address 10.12.26.89/24
!
interface eth1
!
interface eth2
 ip address 10.10.10.11/24
!
interface eth3
!
interface eth4
!
interface eth5
!
```

```
interface eth6
! router ospf 200
 network 10.10.10.0/24 area 0.0.0.0  cspf
disable-better-protection
! line con 0
login line vty
0 39 login
! end

#sh ip ospf neighbor

Total number of full neighbors: 2 OSPF
process 200 VRF(default):
Neighbor ID      Pri   State            Dead Time   Address         Interface
Instance ID
10.12.26.88        1   Full/Backup      00:00:30    10.10.10.10     eth2
0
10.12.26.90       10   Full/DR          00:00:31    10.10.10.13     eth2
0
R2#

R2#sh ip ospf interface eth2 is
up, line protocol is up
  Internet Address 10.10.10.11/24, Area 0.0.0.0, MTU 1500
  Process ID 200, VRF (default), Router ID 10.12.26.89, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State DROther, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.90, Interface Address 10.10.10.13
  Backup Designated Router (ID) 10.12.26.88, Interface Address 10.10.10.10
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  Neighbor Count is 2, Adjacent neighbor count is 2
  Suppress hello for 0 neighbor(s)
  Hello received 71 sent 36, DD received 7 sent 7
  LS-Req received 2 sent 2, LS-Upd received 9 sent 4
  LS-Ack received 3 sent 4, Discarded 1
No authentication
```

R3

```
#sh running-config
!
no service password-encryption
!
hostname R3 !
logging monitor 7
!
ip vrf management
! ip domain-lookup
```

```
spanning-tree mode provider-rstp data-
center-bridging enable ethernet cfm
enable
! interface lo mtu 65536 ip
address 127.0.0.1/8 ipv6
address ::1/128
! interface eth0 ip address
10.12.26.90/24
!
interface eth1
! interface eth2  ip address
10.10.10.13/24  ip ospf priority
10
!
interface eth3
!
interface eth4
!
interface eth5
!
interface eth6
! router ospf 100
 network 10.10.10.0/24 area 0.0.0.0  cspf
disable-better-protection
! line con 0 login
line vty 0 39 login

! end

#sh ip ospf neighbor

Total number of full neighbors: 2 OSPF
process 100 VRF(default):
Neighbor ID      Pri   State            Dead Time   Address         Interface
Instance ID
10.12.26.88        1   Full/Backup      00:00:33    10.10.10.10     eth2
0
10.12.26.89        1   Full/DROther     00:00:30    10.10.10.11     eth2
0


#sh ip ospf interface
eth2 is up, line protocol is up
  Internet Address 10.10.10.13/24, Area 0.0.0.0, MTU 1500
      Process ID 100, VRF (default), Router ID 10.12.26.90, Network Type
    BROADCAST, Cost: 1
      Transmit Delay is 1 sec,  State DR, Priority 10, TE Metric 1
      Designated Router (ID) 10.12.26.90, Interface Address 10.10.10.13
      Backup Designated Router (ID) 10.12.26.88, Interface Address 10.10.10.10
      Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

```
      Hello due in 00:00:05
    Neighbor Count is 2, Adjacent neighbor count is 2
    Suppress hello for 0 neighbor(s)
    Hello received 99 sent 60, DD received 8 sent 6
   LS-Req received 2 sent 2, LS-Upd received 9 sent 12
   LS-Ack received 9 sent 6, Discarded 1 No
authentication
```

Area Border Router

This example shows configuration for an Area Border Router. R2 is an Area Border Router (ABR). On R2, Interface eth0 is in Area 0, and Interface eth1 is in Area 1.

Topology

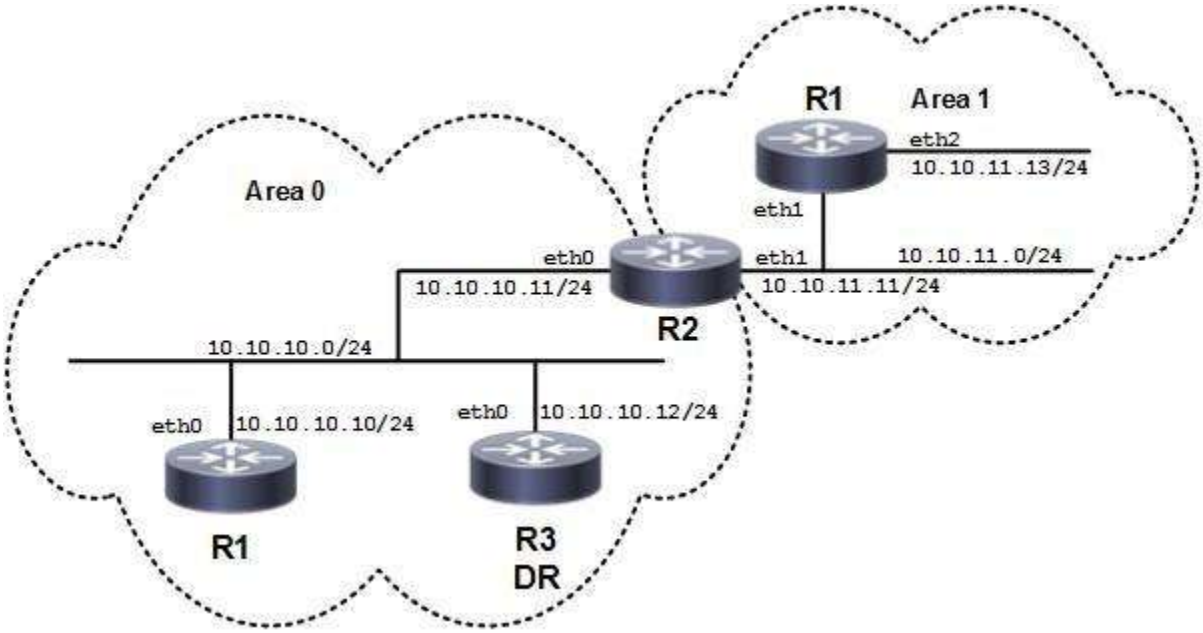


Figure 3-22: OSPF ABR Topology

Configuration

R2

`#configure terminal`	Enter configure mode
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer.
`(config-router)#network 10.10.10.0/24 area 0`	Define one interface (`10.10.10.0/24`) on which OSPF runs, and associate the area ID (`0`) with the interface.
`(config-router)#network 10.10.11.0/24 area 1`	Define the other interface `(10.10.11.0/24)` on which OSPF runs, and associate the area ID `(1)` with the interface.

Validation

R2

```
    #sh running-config
    !
    no service password-encryption
    !
    hostname R2
    !
    logging monitor 7
    !
    ip vrf management
    !
    ip domain-lookup
    !
    ip pim register-rp-reachability
    !
    interface lo  mtu 65536  ip address 127.0.0.1/8  ipv6 address ::1/128
    !
    interface eth0  ip address 10.12.26.89/24
    !
    interface eth1  ip address 10.10.11.11/24
    !
    interface eth2  ip address 10.10.10.11/24
    !
    interface eth3
    !
    interface eth4
    !
    interface eth5
    !
    interface eth6
! router ospf 100
 network 10.10.10.0/24 area 0.0.0.0  network
10.10.11.0/24 area 0.0.0.1 cspf disable-better-
protection
! line con 0 login line
vty 0 39 login
! end

#sh ip ospf
 Routing Process "ospf 100" with ID 10.12.26.89
 Process uptime is 4 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
 Supports only single TOS(TOS0) routes Supports opaque LSA

 Supports Graceful Restart
 This router is an ABR, ABR Type is Alternative Cisco (RFC3509)
```

```
 SPF schedule delay initial 0 secs 500 msecs
 SPF schedule delay min 0 secs 500 msecs
 SPF schedule delay max 50 secs 0 msecs
 Refresh timer 10 secs
 Number of incomming current DD exchange neighbors 0/64
 Number of outgoing current DD exchange neighbors 0/64
 Initial LSA throttle delay 0 secs 0 msecs
 Minimum hold time for LSA throttle 5 secs 0 msecs
 Maximum wait time for LSA throttle 5 secs 0 msecs
 Minimum LSA arrival 1 secs 0 msecs
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000 Number of non-
default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 9
 Number of LSA received 18
 Number of areas attached to this router: 2
    Area 0.0.0.0 (BACKBONE)
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is
        2 Area has no authentication
        SPF algorithm last executed 00:01:54.085
        ago SPF algorithm executed 7 times Number
        of LSA 11. Checksum 0x0428ac
    Area 0.0.0.1
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 1
        Number of fully adjacent virtual neighbors through this area is
        0 Area has no authentication
        SPF algorithm last executed 00:00:41.737 ago
SPF algorithm executed 3 times
        Number of LSA 8. Checksum 0x043ce4
 Dste Staus: Disabled

#show ip ospf interface
eth2 is up, line protocol is up
  Internet Address 10.10.10.11/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.89, Network Type BROADCAST, Cost:
1
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.89, Interface Address 10.10.10.11
  Backup Designated Router (ID) 10.12.26.88, Interface Address 10.10.10.10
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:11
  Neighbor Count is 2, Adjacent neighbor count is 2
  Suppress hello for 0 neighbor(s)
  Hello received 66 sent 38, DD received 11 sent 7 LS-
  Req received 2 sent 2, LS-Upd received 15 sent 14
```

```
  LS-Ack received 14 sent 10, Discarded 0   No
authentication
eth1 is up, line protocol is up
  Internet Address 10.10.11.11/24, Area 0.0.0.1, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.89, Network Type BROADCAST, Cost:
1
  Transmit Delay is 1 sec, State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.92, Interface Address 10.10.11.13
  Backup Designated Router (ID) 10.12.26.89, Interface Address 10.10.11.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
   Hello received 22 sent 24, DD received 3 sent 9
   LS-Req received 1 sent 1, LS-Upd received 4 sent 5
   LS-Ack received 4 sent 3, Discarded 0
   No authentication

#show ip ospf neighbor

Total number of full neighbors: 3 OSPF
process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
10.12.26.88       1   Full/Backup     00:00:34    10.10.10.10     eth2
0
10.12.26.90       1   Full/DROther    00:00:32    10.10.10.12     eth2
0
10.12.26.92       1   Full/DR         00:00:33    10.10.11.13     eth1
0

#show ip ospf database

            OSPF Router with ID (10.12.26.89) (Process ID 100 VRF default)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age     Seq#       CkSum  Link count
10.12.26.88     10.12.26.88     365     0x80000005 0x10bc 1
10.12.26.89     10.12.26.89     312     0x80000006 0x0fb8 1
10.12.26.90     10.12.26.90     363     0x80000003 0x10b8 1

Net Link States (Area 0.0.0.0)

Link ID         ADV Router      Age     Seq#       CkSum
    10.10.10.11     10.12.26.89      364     0x80000002 0xe7fd

                    Summary Link States (Area 0.0.0.0)

    Link ID         ADV Router      Age     Seq#       CkSum      Route
    10.10.11.0      10.12.26.89     312     0x80000001 0x95fd 10.10.11.0/24
```

```
                Area-Local Opaque-LSA (Area 0.0.0.0)

    Link ID         ADV Router      Age      Seq#       CkSum  Opaque ID
    1.0.0.1         10.12.26.88      363     0x80000003 0xa972 1
    1.0.0.1         10.12.26.89      362     0x80000003 0xad6c 1
    1.0.0.1         10.12.26.90      363     0x80000001 0xb564 1
    1.0.0.10        10.12.26.88      363     0x80000003 0x0a32 10
    1.0.0.10        10.12.26.89      362     0x80000002 0x2417 10
    1.0.0.10        10.12.26.90      363     0x80000001 0x3efb 10

                Router Link States (Area 0.0.0.1)

    Link ID         ADV Router       Age     Seq#       CkSum  Link count
    10.12.26.89     10.12.26.89      245     0x80000004 0x3d88 1
    10.12.26.92     10.12.26.92      241     0x80000004 0x2698 1

                Net Link States (Area 0.0.0.1)
    Link ID         ADV Router       Age     Seq#       CkSum
    10.10.11.13     10.12.26.92      246     0x80000001 0x6ffb

                Summary Link States (Area 0.0.0.1)

    Link ID         ADV Router       Age     Seq#       CkSum     Route
    10.10.10.0      10.12.26.89      312     0x80000001 0xa0f3 10.10.10.0/24

                Area-Local Opaque-LSA (Area 0.0.0.1)

    Link ID         ADV Router      Age      Seq#       CkSum  Opaque ID
    1.0.0.1         10.12.26.89      243     0x80000001 0xb16a 1
    1.0.0.1         10.12.26.92      244     0x80000001 0xbd58 1
    1.0.0.8         10.12.26.89      234     0x80000002 0x96a2 8
1.0.0.8         10.12.26.92      244     0x80000001 0xc272  8
```

Redistribute Routes into OSPF

In this example, the configuration causes BGP routes to be imported into the OSPF routing table, and advertised as Type 5 External LSAs into Area 0.

Topology

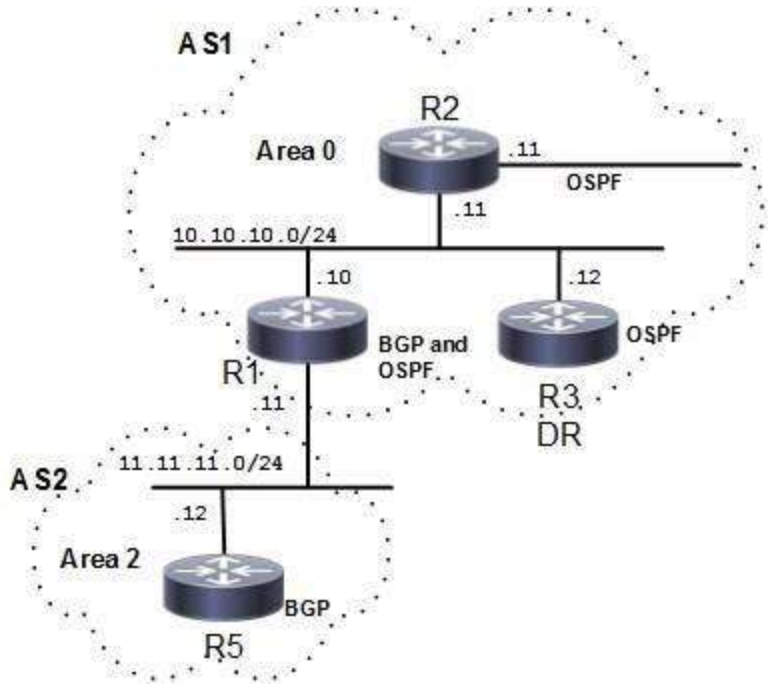


Figure 3-23: Redistribute Routes

R1

`#configure terminal`	Enter configure mode.
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0`	Define one interface (`10.10.10.0/24`) on which OSPF runs, and associate the area ID (`0`) with the interface (area ID `0` specifies the backbone area).
`(config-router)#redistribute bgp`	Specify redistributing routes from other routing protocol (BGP) into OSPF.

Validation

```
#show ip ospf route

OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  10.10.9.0/24 [1] is directly connected, eth2, Area 0.0.0.0
C 10.10.10.0/24 [1] is directly connected, eth3, Area 0.0.0.0
O 10.10.11.0/24 [101] via 10.10.10.11, eth3, Area 0.0.0.0
C 10.10.12.0/24 [1] is directly connected, eth1, Area 0.0.0.0
O 10.10.13.0/24 [102] via 10.10.10.11, eth3, Area 0.0.0.0
O  10.10.14.0/24 [102] via 10.10.10.11, eth3, Area 0.0.0.0
```

Cost

A route can be made the preferred route by changing its cost. In this example, cost has been configured to make R2 the next hop for R1.

The default cost for each interface is 1. Interface eth2 on R2 has a cost of 100, and Interface eth2 on R3 has a cost of 150. The total cost to reach 10.10.14.0/24 (R4) through R2 and R3 is computed as follows:

R2: 1+100 = 101

R3: 1+150 = 151

Therefore, R1 chooses R2 as its next hop to destination 10.10.14.0/24 because it has the lower cost.

Topology

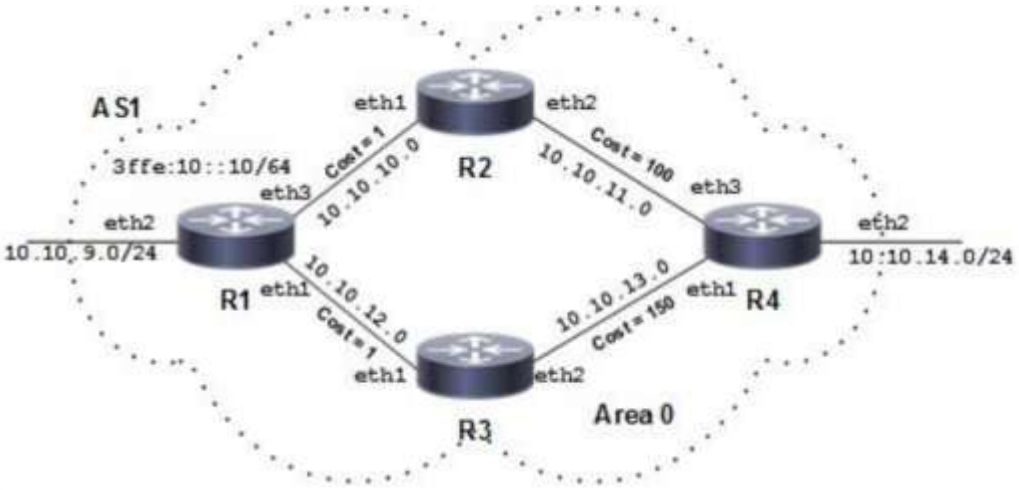


Figure 3-24: Configure Cost Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.

`(config-router)#network 10.10.9.0/24 area 0`
`(config-router)#network 10.10.10.0/24 area 0`
`(config-router)#network 10.10.12.0/24 area 0`
	Define interfaces on which OSPF runs, and associate the area ID `(0)` with the interface (area ID `0` specifies the backbone area).

R2

`(config)#interface eth2`	Specify the interface (`eth2`) to configure.
`(config-if)#ip ospf cost 100`	Set the OSPF cost of this link to `100`.
`(config-if)#exit`	Exit interface mode.

`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0` `(config-router)#network 10.10.11.0/24 area 0`	Define interfaces on which OSPF runs, and associate the area ID `(0)` with the interface.

R3

`(config)#interface eth2`	Specify the interface (`eth2`) to configure.
`(config-if)#ip ospf cost 150`	Set the OSPF cost of this link to `100`.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.12.0/24 area 0` `(config-router)#network 10.10.13.0/24 area 0`	Define interfaces on which OSPF runs, and associate the area ID `(0)` with the interface.

R4

`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.

`(config-router)#network 10.10.11.0/24 area 0`
`(config-router)#network 10.10.13.0/24 area 0`
`(config-router)#network 10.10.14.0/24 area 0`
	Define interfaces on which OSPF runs, and associate the area ID `(0)` with the interface.

Validation

R1

```
#show ip ospf route

OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  10.10.9.0/24 [1] is directly connected, eth2, Area 0.0.0.0
C 10.10.10.0/24 [1] is directly connected, eth3, Area 0.0.0.0
O 10.10.11.0/24 [101] via 10.10.10.11, eth3, Area 0.0.0.0
C 10.10.12.0/24 [1] is directly connected, eth1, Area 0.0.0.0
O 10.10.13.0/24 [102] via 10.10.10.11, eth3, Area 0.0.0.0
O 10.10.14.0/24 [102] via 10.10.10.11, eth3, Area 0.0.0.0
#sh ip ospf interface
eth3 is up, line protocol is up
  Internet Address 10.10.10.10/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.88, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.88, Interface Address 10.10.10.10
```

```
  Backup Designated Router (ID) 10.12.26.89, Interface Address 10.10.10.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
   Neighbor Count is 1, Adjacent neighbor count is 1
   Suppress hello for 0 neighbor(s)
   Hello received 43 sent 69, DD received 3 sent 4
  LS-Req received 1 sent 1, LS-Upd received 16 sent 18
  LS-Ack received 10 sent 11, Discarded 0   No
authentication
eth2 is up, line protocol is up
  Internet Address 10.10.9.10/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.88, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.88, Interface Address
  10.10.9.10 No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
    5 Hello due in 00:00:02
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
  Hello received 0 sent 68, DD received 0 sent 0
  LS-Req received 0 sent 0, LS-Upd received 0 sent
  0 LS-Ack received 0 sent 0, Discarded 0 No
authentication
eth1 is up, line protocol is up
  Internet Address 10.10.12.10/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.88, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.88, Interface Address 10.10.12.10
  Backup Designated Router (ID) 10.12.26.90, Interface Address 10.10.12.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
Hello received 29 sent 66, DD received 3 sent 4
  LS-Req received 1 sent 1, LS-Upd received 10 sent 12
  LS-Ack received 10 sent 9, Discarded 0
  No authentication
```

R2

```
#sh ip ospf route

OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

O  10.10.9.0/24 [2] via 10.10.10.10, eth1, Area 0.0.0.0
C  10.10.10.0/24 [1] is directly connected, eth1, Area 0.0.0.0
```

```
C  10.10.11.0/24 [100] is directly connected, eth2, Area 0.0.0.0
O 10.10.12.0/24 [2] via 10.10.10.10, eth1, Area 0.0.0.0
O 10.10.13.0/24 [101] via 10.10.11.11, eth2, Area 0.0.0.0
O 10.10.14.0/24 [101] via 10.10.11.11, eth2, Area 0.0.0.0

#sh ip ospf interface
eth2 is up, line protocol is up
  Internet Address 10.10.11.10/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.89, Network Type
BROADCAST, Cost: 100
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 100
  Designated Router (ID) 10.12.26.89, Interface Address 10.10.11.10
  Backup Designated Router (ID) 10.12.26.92, Interface Address 10.10.11.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 56 sent 77, DD received 3 sent 4
  LS-Req received 1 sent 1, LS-Upd received 11 sent
  7 LS-Ack received 4 sent 8, Discarded 0 No
authentication
eth1 is up, line protocol is up
  Internet Address 10.10.10.11/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.89, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.88, Interface Address 10.10.10.10
  Backup Designated Router (ID) 10.12.26.89, Interface Address 10.10.10.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 74 sent 75, DD received 4 sent 3 LS-
  Req received 1 sent 1, LS-Upd received 18 sent 16
  LS-Ack received 10 sent 12, Discarded 0 No
authentication
```

R3

```
#sh ip ospf route

OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

O  10.10.9.0/24 [2] via 10.10.12.10, eth1, Area 0.0.0.0 O
10.10.10.0/24 [2] via 10.10.12.10, eth1, Area 0.0.0.0 O
10.10.11.0/24 [102] via 10.10.12.10, eth1, Area 0.0.0.0
C  10.10.12.0/24 [1] is directly connected, eth1, Area 0.0.0.0
```

```
O  10.10.13.0/24 [103] via 10.10.12.10, eth1, Area 0.0.0.0
O 10.10.14.0/24 [103] via 10.10.12.10, eth1, Area 0.0.0.0

#sh ip ospf interface
eth2 is up, line protocol is up
  Internet Address 10.10.13.10/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.90, Network Type
BROADCAST, Cost: 150
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 150
  Designated Router (ID) 10.12.26.90, Interface Address 10.10.13.10
  Backup Designated Router (ID) 10.12.26.92, Interface Address 10.10.13.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 85 sent 94, DD received 3 sent 4
  LS-Req received 0 sent 0, LS-Upd received 3 sent 4
  LS-Ack received 3 sent 3, Discarded 0   No
authentication
eth1 is up, line protocol is up
  Internet Address 10.10.12.11/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.90, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.88, Interface Address 10.10.12.10 Backup
  Designated Router (ID) 10.12.26.90, Interface Address 10.10.12.11 Timer
  intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 92 sent 92, DD received 4 sent 3
  LS-Req received 1 sent 1, LS-Upd received 12 sent 10
  LS-Ack received 8 sent 10, Discarded 0
  No authentication
```

R4

```
#sh ip ospf route

OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

O  10.10.9.0/24 [3] via 10.10.11.10, eth3, Area 0.0.0.0
via 10.10.13.10, eth1, Area 0.0.0.0 O 10.10.10.0/24 [2] via
10.10.11.10, eth3, Area 0.0.0.0
C  10.10.11.0/24 [1] is directly connected, eth3, Area 0.0.0.0
O 10.10.12.0/24 [2] via 10.10.13.10, eth1, Area 0.0.0.0
C  10.10.13.0/24 [1] is directly connected, eth1, Area 0.0.0.0
```

```
C  10.10.14.0/24 [1] is directly connected, eth2, Area 0.0.0.0

#sh ip ospf interface
eth3 is up, line protocol is up
  Internet Address 10.10.11.11/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.92, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.89, Interface Address 10.10.11.10
  Backup Designated Router (ID) 10.12.26.92, Interface Address 10.10.11.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
     Hello due in 00:00:04
   Neighbor Count is 1, Adjacent neighbor count is 1
   Suppress hello for 0 neighbor(s)
   Hello received 95 sent 96, DD received 4 sent 3
  LS-Req received 1 sent 1, LS-Upd received 7 sent 11
  LS-Ack received 7 sent 5, Discarded 0   No
authentication
eth2 is up, line protocol is up
  Internet Address 10.10.14.10/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.92, Network Type BROADCAST,
Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.92, Interface Address 10.10.14.10
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
     Hello due in 00:00:10
   Neighbor Count is 0, Adjacent neighbor count is 0
   Suppress hello for 0 neighbor(s)
   Hello received 0 sent 95, DD received 0 sent 0
  LS-Req received 0 sent 0, LS-Upd received 0 sent
  0 LS-Ack received 0 sent 0, Discarded 0 No
authentication
eth1 is up, line protocol is up
  Internet Address 10.10.13.11/24, Area 0.0.0.0, MTU 1500
  Process ID 100, VRF (default), Router ID 10.12.26.92, Network Type
BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.90, Interface Address 10.10.13.10
  Backup Designated Router (ID) 10.12.26.92, Interface Address 10.10.13.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
 Hello received 92 sent 93, DD received 4 sent 3
  LS-Req received 0 sent 0, LS-Upd received 4 sent
  3 LS-Ack received 3 sent 3, Discarded 0 No
authentication
```

Virtual Links

Virtual links are used to connect a temporarily-disjointed non-backbone area to the backbone area, or to repair a noncontiguous backbone area. In this example, the ABR R3 has temporarily lost connection to Area 0, in turn, disconnecting Area 2 from the backbone area. The virtual link between ABR R1 and ABR R2 connects Area 2 to Area 0. Area 1 is used as a transit area.

Topology

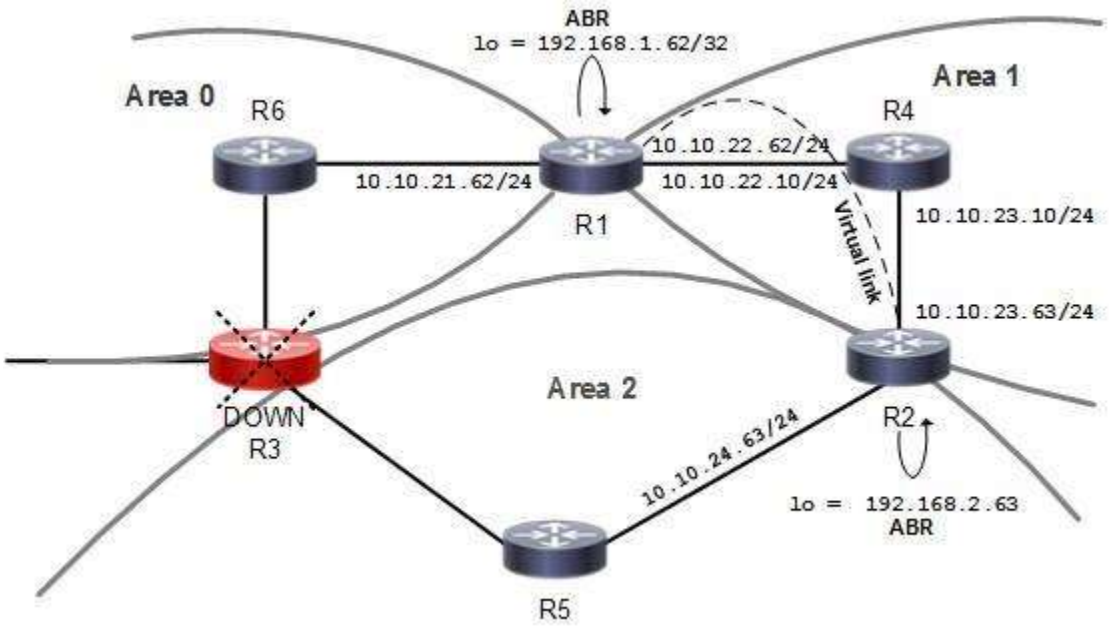


Figure 3-25: Virtual Links Topology

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify loopback as the interface you want to configure.
`(config-if)#ip address 192.168.1.62/32`	Configure the IP address on this interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#ospf router-id 192.168.1.62`	Configure the OSPF Router ID (`192.168.1.62`) for this router.
`(config-router)#network 10.10.21.0/24 area 0` `(config-router)#network 10.10.22.0/24 area 1`	Define interfaces on which OSPF runs, and associate the area IDs `(0 and 1)` with the interface.
`(config-router)#area 1 virtual-link 192.168.2.63`	Configure a virtual link between this router R1 and R2 (Router ID `192.168.2.63`) through transit area 1.

R2

`(config)#interface lo`	Specify loopback as the interface you want to configure.
`(config-if)#ip address 192.168.2.63/32`	Configure the IP address on this interface.

`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#ospf router-id 192.168.2.63`	Configure the OSPF Router ID (`192.168.1.63`) for this router.

`(config-router)#network 10.10.23.0/24 area 1`
`(config-router)#network 10.10.24.0/24 area 2`
`(config-router)#network 192.168.2.63/32 area 2`
	Define interfaces on which OSPF runs, and associate the area IDs `(1` and `2)` with the interface.

`(config-router)#area 1 virtual-link 192.168.1.62`	Configure a virtual link between this router R2 and R1 (Router ID `192.168.2.62`) through transit area `1`.

Validation

show ip ospf virtual-links, show ip ospf neighbor, show ip ospf, show ip ospf route

OSPF Authentication

There are three types of OSPF authentications--Null (Type 0), Simple Text (Type 1), and MD5 (Type 2). With Null authentication, routing exchanges over the network are not authenticated. In Simple Text authentication, the authentication type is the same for all routers that communicate using OSPF in a network. For MD5 authentication, configure a key and a key ID on each router. The router generates a message digest on the basis of the key, key ID, and OSPF packet, and adds it to the OSPF packet.

The authentication type can be configured on a per-interface basis or a per-area basis. Additionally, Interface and Area authentication can be used together. Area authentication is used for an area, and interface authentication is used for a specific interface in the area. If the Interface authentication type is different from the Area authentication type, the Interface authentication type overrides the Area authentication type. If the Authentication type is not specified for an interface, the Authentication type for the area is used. The authentication command descriptions contain details of each type of authentication.

In the example below, R1 and R2 are configured for both the interface and area authentications. The authentication type of interface eth1 on R1 and interface eth0 on R2 is MD5 mode, and is defined by the area authentication command; however, the authentication type of interface eth2 on R1 and interface eth1 on R2 is plain text mode, and is defined by the `ip ospf authentication` command. This interface command overrides the `area authentication` command.

Topology

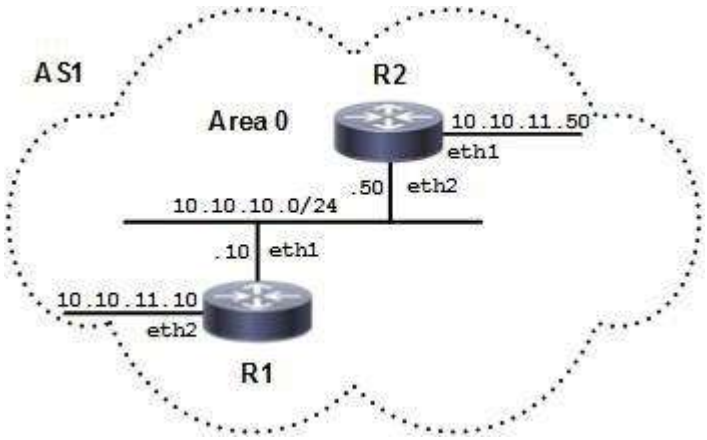


Figure 3-26: OSPF Authentication Topology

R1

`#configure terminal`	Enter configure mode.
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0` `(config-router)#network 10.10.11.0/24 area 0`	Define interfaces on which OSPF runs, and associate the area ID `(0)` with the interface (area ID 0 specifies the backbone area).
`(config-router)#area 0 authentication message-digest`	Enable MD5 authentication on area 0.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to configure.
`(config-if)#ip ospf message-digest-key 1 md5 test`	Register the MD5 key test for OSPF authentication. The key ID is 1.
`(config-if)#exit`	Exit Interface mode, and return to Configure mode
`(config)#interface eth2`	Specify the interface (`eth2`) to configure.
`(config-if)#ip ospf authentication`	Enable the OSPF packet to use text authentication on the current interface (`eth2`).
`(config-if)#ip ospf authentication-key test`	Specify an OSPF authentication password (`test`) for the neighboring routers.

R2

`#configure terminal`	Enter configure mode.
`(config)#router ospf 100`	Configure the routing process, and specify the Process ID (`100`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0` `(config-router)#network 10.10.11.0/24 area 0`	Define interfaces on which OSPF runs, and associate the area ID `(0)` with the interface (area ID 0 specifies the backbone area).
`(config-router)#area 0 authentication message-digest`	Enable MD5 authentication on area 0.

(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#interface eth2	Specify the interface (eth0) to configure.
(config-if)#ip ospf message-digest-key 1 md5 test	Register MD5 key test for OSPF authentication. The key ID is 1.
(config-if)#exit	Exit interface mode.
(config)#interface eth1	Specify the interface (eth2) to configure.
(config-if)#ip ospf authentication	Enable the OSPF packet to use text authentication on the current interface (eth1).
(config-if)#ip ospf authentication-key test	Specify an OSPF authentication password test for the neighboring routers.

Validation

R1

```
    R1#sh running-config
    !
    no service password-encryption
    !
    hostname R1
    !
    logging monitor 7
    !
    ip vrf management
    !
    ip domain-lookup
    !
    ip pim register-rp-reachability
    ! interface lo mtu 65536 ip address 127.0.0.1/8
    ipv6 address ::1/128
    ! interface eth0  ip address 10.12.26.88/24
    ! interface eth1  ip address 10.10.10.10/24
     ip ospf message-digest-key 1 md5 0x293da85becc67703
    ! interface eth2 ip address 10.10.11.10/24 ip ospf
    authentication
     ip ospf authentication-key 0x293da85becc67703
!
    interface eth3
!
    interface eth4
!
    interface eth5
!
    interface eth6
!
    interface eth7
    ! router ospf 100
```

```
 area 0.0.0.0 authentication message-digest network 10.10.9.0/24 area
0.0.0.0 network 10.10.10.0/24 area 0.0.0.0 network 10.10.11.0/24 area
0.0.0.0 network 10.10.12.0/24 area 0.0.0.0 cspf disable-better-
protection
! line con 0  login line vty 0 39  login
! end


R1#sh ip ospf neighbor

Total number of full neighbors: 1 OSPF
process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
10.12.26.89       1   Full/DR         00:00:38    10.10.10.50     eth1
0
```

R2

```
R2#sh running-config
!
no service password-encryption
!
hostname R2
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
!
ip pim register-rp-reachability
! interface lo
mtu 65536
 ip address 127.0.0.1/8 ipv6
address ::1/128
! interface eth0 ip address
10.12.26.89/24
! interface eth1 ip address
10.10.11.50/24 ip ospf
authentication
 ip ospf authentication-key 0x293da85becc67703
! interface eth2  ip address
10.10.10.50/24
 ip ospf message-digest-key 1 md5 0x293da85becc67703  ip
ospf cost 100
!
interface eth3
!
interface eth4
!
```

```
interface eth5
!
interface eth6
! router ospf 100
 area 0.0.0.0 authentication message-
digest network 10.10.10.0/24 area 0.0.0.0
network 10.10.11.0/24 area 0.0.0.0 cspf
disable-better-protection
! line con 0
login line vty
0 39 login
! end



R2#sh ip ospf neighbor

Total number of full neighbors: 1 OSPF
process 100 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
10.12.26.88       1   Full/Backup     00:00:33    10.10.10.10     eth2
0
```

Multiple OSPF Instances

By using multiple OSPF instances, OSPF routes can be segregated, based on their instance number. Routes of one instance are stored differently from routes of another instance running in the same router.

To configure multiple OSPF instances, perform the following procedures referring to the topology diagram below:

1. Enable OSPF on an interface.
2. Enable multiple instances.
3. Configure redistribution among multiple instances.

   Note: Optionally, redistribution can be configured with the metric, type or route-map options.

Topology

Figure 3-27: Multiple OSPF Instances

Enable Multiple OSPF Instances on a Router

In this example, routers R1, R2, and R3 are in Area 0, and all run OSPF.

R1

`(config)#interface eth1`	Enter the Interface mode for `eth1`.
`(config-if)#ip address 2.2.2.2/24`	Specify the IP address of the interface.
`(config-if)#no shutdown`	Activate the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 10`	Configure an OSPF instance with an instance ID of `10`.
`(config-router)#router-id 5.5.5.5`	Configure the router ID to use on this instance.
`(config-router)#network 2.2.2.0/24 area 0`	Advertise the network with the area ID.

R2

`(config)#interface eth1`	Enter the Interface mode for `eth1`.
`(config-if)#ip address 2.2.2.3/24`	Specify the IP address of the interface.
`(config-if)#no shutdown`	Activate the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 10`	Configure an OSPF instance with an instance ID of `10`.
`(config-router)#router-id 6.6.6.6`	Configure the router ID to use on this instance.
`(config-router)#network 2.2.2.0/24 area 0`	Advertise the network with the area ID.
`(config-router)#exit`	Exit router mode.
`(config)#interface eth2`	Enter the Interface mode for `eth2`.
`(config-if)#ip address 4.4.4.4/24`	Configure the IP address.
`(config-if)#no shutdown`	Activate the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 15`	Configure an OSPF instance with an instance ID of `15`.
`(config-router)#router-id 8.8.8.8`	Configure the router ID to use on this instance.
`(config-router)#network 4.4.4.0/24 area 0`	Advertise the network with the area ID.

R3

`(config)#``interface eth1`	Enter the Interface mode for `eth1`.
`(config-if)#``ip address 4.4.4.5/24`	Configure the IP address.
`(config-if)#``no shutdown`	Activate the interface.
`(config-if)#``exit`	Exit interface mode.
`(config)#``router ospf 15`	Configure an OSPF instance with an instance ID of `15`.
`(config-router)#``router-id 7.7.7.7`	Configure the router ID to use on this instance.
`(config-router)#``network 4.4.4.0/24 area 0`	Advertise the network with the area ID.

Validation

R1

```
R1#sh running-config
```

```
!
no service password-encryption
!
hostname R1
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
!
ip pim register-rp-reachability
!
interface lo  mtu 65536  ip address 127.0.0.1/8  ipv6 address ::1/128
!
interface eth0  ip address 10.12.26.88/24
!
interface eth1  ip address 2.2.2.2/24
!
interface eth2  ip address 10.10.11.10/24
!
interface eth3
!
interface eth4
!
interface eth5
!
interface eth6
!
interface eth7
!
router ospf 10 ospf router-id 5.5.5.5 network 2.2.2.0/24 area 0.0.0.0 cspf
disable-better-protection
! line con 0  login line vty 0 39  login
! end
```

```
R1#sh ip ospf neighbor
Total number of full neighbors: 1 OSPF
process 10 VRF(default):
Neighbor ID     Pri   State            Dead Time   Address         Interface
Instance ID
6.6.6.6           1   Full/Backup      00:00:39    2.2.2.3         eth1
0
```

```
R1#sh ip ospf route
```

```
OSPF process 10:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
C  2.2.2.0/24 [1] is directly connected, eth1, Area 0.0.0.0
```

R2

```
R2#sh running-config
!
no service password-encryption
!
hostname R2
!
logging monitor 7
!
ip vrf management
!
ip domain-lookup
!
ip pim register-rp-reachability
! interface lo
mtu 65536
 ip address 127.0.0.1/8 ipv6
address ::1/128
! interface eth0 ip address
10.12.26.89/24
! interface eth1  ip
address 2.2.2.3/24
! interface eth2 ip
address 4.4.4.4/24
!
interface eth3
!
interface eth4
!
interface eth5
!
interface eth6
! router ospf 10  ospf router-id
6.6.6.6  network 2.2.2.0/24 area
0.0.0.0 cspf disable-
better-protection
! router ospf 15  ospf router-id
8.8.8.8  network 4.4.4.0/24 area
0.0.0.0  no capability cspf
! line con 0
login line vty
0 39  login
! end

R2#sh ip ospf neighbor

Total number of full neighbors: 1 OSPF
process 10 VRF(default):
```

```
Neighbor ID      Pri   State            Dead Time   Address         Interface
Instance ID
5.5.5.5            1   Full/DR          00:00:33    2.2.2.2         eth1
0

Total number of full neighbors: 1 OSPF
process 15 VRF(default):
Neighbor ID      Pri   State            Dead Time   Address         Interface
Instance ID
7.7.7.7            1   Full/Backup      00:00:31    4.4.4.5         eth2
0

R2#sh ip ospf route

OSPF process 10:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2 C

2.2.2.0/24 [1] is directly connected, eth1, Area 0.0.0.0

OSPF process 15:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  4.4.4.0/24 [1] is directly connected, eth2, Area 0.0.0.0
```

R3

```
R3#sh running-config
!
no service password-encryption
!
hostname R3
!
logging monitor 7
!
ip vrf management
! ip domain-lookup
!
ip pim register-rp-reachability
! interface lo
mtu 65536
 ip address 127.0.0.1/8  ipv6
address ::1/128
! interface eth0 ip address
10.12.26.90/24
! interface eth1 ip
address 4.4.4.5/24
! interface eth2 ip address
10.10.13.10/24
```

```
!
interface eth3
!
interface eth4
!
interface eth5
!
interface eth6
! router ospf 15  ospf router-id
7.7.7.7  network 4.4.4.0/24 area
0.0.0.0 cspf disable-better-
protection
! line con 0
login line vty
0 39  login
! end

R3#sh ip ospf neighbor

Total number of full neighbors: 1 OSPF
process 15 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface
Instance ID
8.8.8.8           1   Full/DR         00:00:30    4.4.4.4         eth1
0
```

Redistribute among Multiple Instances

In this example, routes of one instance are redistributed to another instance to enable ping from R1 to R3 or vice versa; and R2 redistributes routes from one instance to another.

R2

`(config)#router ospf 15`	Configure an OSPF instance with instance ID `15`.
`(config-router)#router-id 8.8.8.8`	Configure the router ID.
`(config-router)#redistribute ospf 10`	Redistribute instance `10` routes.
`(config-router)#redistribute connected`	Redistribute connected routes to instance `15`.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.
`(config)#router ospf 10`	Configure an OSPF instance with instance ID `10`.
`(config-router)#router-id 6.6.6.6`	Configure the router ID.
`(config-router)#redistribute ospf 15`	Redistribute instance `15` routes.
`(config-router)#redistribute connected`	Redistribute connected routes to instance `10`.

Redistribution with the Metric Option

In this example, on R3, R1 and R2 have each other's routes with a metric of 100.

R2

(config)#router ospf 15	Configure an OSPF instance with instance ID 15.
(config-router)#router-id 8.8.8.8	Configure the router ID.
(config-router)#redistribute ospf 10 metric 100	Redistribute instance 10 routes with metric 100.
(config-router)#redistribute connected	Redistribute connected routes to instance 15.
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#router ospf 10	Configure an OSPF instance with instance ID 10.
(config-router)#router-id 6.6.6.6	Configure the router ID.
(config-router)#redistribute ospf 15 metric 100	Redistribute instance 15 routes with metric 100.
(config-router)#redistribute connected	Redistribute connected routes to instance 10.

Redistribution with the Type Option

In this example, on R3, R1 has R3 routes as type 2, and R2 has R1 routes as type 1.

R2

(config)#router ospf 15	Configure an OSPF instance with instance ID 15.
(config-router)#router-id 8.8.8.8	Configure the router ID.
(config-router)#redistribute ospf 10 metrictype 1	Redistribute instance 10 routes with metric-type 1.
(config-router)#redistribute connected	Redistribute connected routes to instance 15.
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#router ospf 10	Configure an OSPF instance with instance ID 10.
(config-router)#router-id 6.6.6.6	Configure the router ID.
(config-router)#redistribute ospf 15 metrictype 2	Redistribute instance 15 routes with type 2.
(config-router)#redistribute connected	Redistribute connected routes to instance 10.

Redistribution with the Route-Map Option

R2

(config)#route-map 1 permit 10	Enter route-map mode, specifying route-map ID.
(config-route-map)#set metric 100	Set metric value.
(config-route-map)#set metric-type type-2	Set metric-type.
(config-route-map)#exit	Exit route-map mode.
(config)#route-map 2 permit 10	Enter route-map mode, specifying route-map ID.
(config-route-map)#set metric 200	Set metric value.
(config-route-map)#set metric-type type-1	Set metric-type.
(config-route-map)#exit	Exit route-map mode.

(config)#router ospf 15	Configure an OSPF instance with instance ID 15.
(config-router)#router-id 8.8.8.8	Configure the router ID.
(config-router)#redistribute ospf 10 routemap 1	Redistribute instance 10 routes with route map 1.
(config-router)#redistribute connected	Redistribute connected routes to instance 15.
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#router ospf 10	Configure an OSPF instance with instance ID 10.
(config-router)#router-id 6.6.6.6	Configure the router ID.
(config-router)#redistribute ospf 15 routemap 2	Redistribute instance 15 routes with route map 2.
(config-router)#redistribute connected	Redistribute connected routes to instance 10.

Validation

show ip ospf neighbor, show ip route, show ip ospf route, show route-map

Multiple OSPF Instances on Same Subnet

Multiple OSPF instances can be configured on the same subnet. The OSPF instance ID supports separate OSPFv2 protocol instances. With this feature, an adjacency is formed only if the received packet's instance ID is the same as the instance ID configured for that interface.

Topology

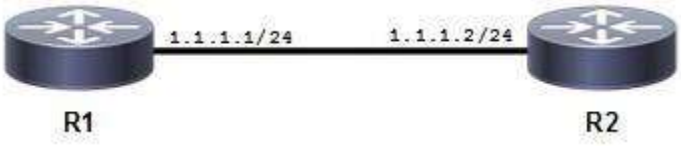


Figure 3-28: Multiple Instances on the Same Subnet

Configuration

R1

#configure terminal	Enter configure mode.
(config)#enable ext-ospf-multi-inst	Enable multiple-instance capability.
(config)#router ospf 1	Configure an OSPF instance with an instance ID of 1.
(config-router)#network 1.1.1.0/24 area 0 instance-id 1	Advertise the network in Area 0 with an instance ID of 1.
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#router ospf 2	Configure an OSPF instance with an instance ID of 2.
(config-router)#network 1.1.1.0/24 area 0 instance-id 2	Advertise the network in Area 0 with an instance ID of 2.

(config-router)#exit	Exit Router mode, and return to Configure mode.

R2

#configure terminal	Enter configure mode.
(config)#enable ext-ospf-multi-inst	Enable multiple-instance capability.
(config)#router ospf 1	Configure an OSPF instance with an instance ID of 1.
(config-router)#network 1.1.1.0/24 area 0 instance-id 1	Advertise the network in Area 0 with an instance ID of 1.
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#router ospf 2	Configure an OSPF instance with an instance ID of 2.
(config-router)#network 1.1.1.0/24 area 0 instance-id 2	Advertise the network in Area 0 with an instance ID of 2.
(config-router)#exit	Exit Router mode, and return to Configure mode.

Validation

R1

```
R1#show ip ospf interface eth1 is
up, line protocol is up
  Internet Address 1.1.1.1/24, Area 0.0.0.0, MTU 1500
  Process ID 1, VRF (default), Router ID 10.12.26.88, Network Type BROADCAST,
Cost: 1
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.88, Interface Address 1.1.1.1
  Backup Designated Router (ID) 10.12.26.89, Interface Address 1.1.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:10
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 7 sent 16, DD received 3 sent 4
  LS-Req received 1 sent 1, LS-Upd received 3 sent 5
  LS-Ack received 3 sent 3, Discarded 0
  No authentication
  Internet Address 1.1.1.1/24, Area 0.0.0.0, MTU 1500
  Process ID 2, VRF (default), Router ID 10.12.26.88, Network Type BROADCAST,
Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1, TE Metric 1 Designated
  Router (ID) 10.12.26.88, Interface Address 1.1.1.1 Backup Designated
  Router (ID) 10.12.26.89, Interface Address 1.1.1.2 Timer intervals
  configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 4 sent 12, DD received 3 sent 4
  LS-Req received 1 sent 1, LS-Upd received 3 sent 5
  LS-Ack received 3 sent 3, Discarded 0
  No authentication
```

```
R1#show ip ospf neighbor

Total number of full neighbors: 1 OSPF
process 1 VRF(default):
Neighbor ID      Pri   State            Dead Time   Address         Interface
Instance ID
10.12.26.89        1   Full/Backup      00:00:35    1.1.1.2         eth1
1

Total number of full neighbors: 1 OSPF
process 2 VRF(default):
Neighbor ID      Pri   State            Dead Time   Address         Interface
Instance ID
10.12.26.89        1   Full/Backup      00:00:33    1.1.1.2         eth1
2
```

R2

```
R2#sh ip ospf interface eth1 is
up, line protocol is up
  Internet Address 1.1.1.2/24, Area 0.0.0.0, MTU 1500
  Process ID 1, VRF (default), Router ID 10.12.26.89, Network Type BROADCAST,
Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.88, Interface Address 1.1.1.1
  Backup Designated Router (ID) 10.12.26.89, Interface Address 1.1.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 17 sent 17, DD received 4 sent 3
  LS-Req received 1 sent 1, LS-Upd received 5 sent 3
  LS-Ack received 2 sent 3, Discarded 0
  No authentication
  Internet Address 1.1.1.2/24, Area 0.0.0.0, MTU 1500
  Process ID 2, VRF (default), Router ID 10.12.26.89, Network Type BROADCAST,
Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.12.26.88, Interface Address 1.1.1.1
  Backup Designated Router (ID) 10.12.26.89, Interface Address 1.1.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Neighbor Count is 1, Adjacent neighbor count is 1
  Suppress hello for 0 neighbor(s)
  Hello received 13 sent 14, DD received 4 sent 3
  LS-Req received 1 sent 1, LS-Upd received 5 sent 3
  LS-Ack received 2 sent 3, Discarded 0
  No authentication

R2#sh ip ospf neighbor
```

```
Total number of full neighbors: 1 OSPF
process 1 VRF(default):
Neighbor ID      Pri   State            Dead Time   Address         Interface
Instance ID
10.12.26.88        1   Full/DR          00:00:32    1.1.1.1         eth1
1

Total number of full neighbors: 1 OSPF
process 2 VRF(default):
Neighbor ID      Pri   State            Dead Time   Address         Interface
Instance ID
10.12.26.88        1   Full/DR          00:00:37    1.1.1.1         eth1
2
```

Multi-Area Adjacency Configuration

Multiple OSPF areas for a same subnet can be configured between two routers. In the diagram below, OSPF is enabled between R2 and R3 under area 0 and area 1, though there is only one link available between these two routers. Multi-area adjacency allows establishing adjacency on multiple areas between the Area Border Routers (ABRs). The specified interface of the ABR is associated with multiple areas.

Each multi-area-adjacency internally implements point-to-point functionality, once the adjacency reaches the FULL state. This point-to-point link provides a topological path for that area. Like a virtual link, there is no restriction for multi-area adjacency that the packets always go through the backbone.

Topology

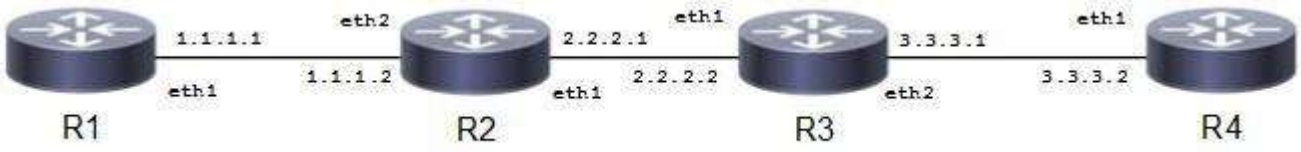


Figure 3-29: One Subnet with Multiple OSPF Areas

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router ospf 1`	Configure an OSPF instance with an instance ID of `1`.
`(config-router)#network 1.1.1.0/24 area 1`	Configure OSPF between R1 and R2 under area `1`.
`(config-router)#exit`	Exit Router mode, and return to Configure mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#router ospf 1`	Configure an OSPF instance with an instance ID of `1`.
`(config-router)#network 1.1.1.0/24 area 1`	Configure OSPF between R1 and R2 under area `1`.

(config-router)#network 2.2.2.0/24 area 0	Configure OSPF between R2 and R3 under area 0.
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ip address 2.2.2.1/24	Configure IP address on the interface.
(config-if)#ip ospf 1 multi-area 0.0.0.1 neighbor 2.2.2.2	Configure multi area adjacency.
(config-if)#exit	Exit interface mode, and return to Configure mode.

R3

#configure terminal	Enter configure mode.
(config)#router ospf 1	Configure an OSPF instance with an instance ID of 1.
(config-router)#network 2.2.2.0/24 area 0	Configure OSPF between R2 and R3 under area 0.
(config-router)#network 3.3.3.0/24 area 1	Configure OSPF between R3 and R4 under area 1.
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ip address 2.2.2.2/24	Configure IP address on the interface.
(config-if)#ip ospf 1 multi-area 0.0.0.1 neighbor 2.2.2.1	Configure multi area adjacency.
(config-if)#exit	Exit interface mode, and return to Configure mode.

R4

#configure terminal	Enter configure mode.
(config)#router ospf 1	Configure an OSPF instance with an instance ID of 1.
(config-router)#network 3.3.3.0/24 area 1	Configure OSPF between R3 and R4 under area 1.
(config-router)#exit	Exit Router mode, and return to Configure mode.

Validation

show ip ospf multi-area-adjacencies, show ip ospf neighbor, show ip ospf route, show ip route

R2

```
R2#show ip ospf multi-area-adjacencies
  Multi-area-adjacency link on interface eth1 to neighbor 2.2.2.2
  Internet Address 2.2.2.1/24, Area 0.0.0.1, MTU 1500
  Process ID 1, Router ID 10.12.26.89, Network Type POINTTOPOINT, Cost:
  1 Transmit Delay is 1 sec, State Point-To-Point, TE Metric 1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
    5 Hello due in 00:00:00
  Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 16 sent 53, DD received 3 sent 4
  LS-Req received 1 sent 1, LS-Upd received 10 sent 5
  LS-Ack received 3 sent 9, Discarded 0

R2#show ip ospf neighbor
```

```
Total number of full neighbors: 3 OSPF
process 1 VRF(default):
Neighbor ID      Pri   State            Dead Time   Address         Interface
Instance ID
10.12.26.88        1   Full/DR          00:00:35    1.1.1.1         eth2
0
10.12.26.90        1   Full/Backup      00:00:33    2.2.2.2         eth1
0
10.12.26.90        1   Full/ -          00:00:35    2.2.2.2         eth1

R2#show ip ospf route

OSPF process 1:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  1.1.1.0/24 [1] is directly connected, eth2, Area 0.0.0.1
C 2.2.2.0/24 [1] is directly connected, eth1, Area 0.0.0.0
O 3.3.3.0/24 [2] via 2.2.2.2, eth1, Area 0.0.0.1


R2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C       1.1.1.0/24 is directly connected, eth2
C2.2.2.0/24 is directly connected, eth1
O3.3.3.0/24 [110/2] via 2.2.2.2, eth1, 00:05:44
C10.12.26.0/24 is directly connected, eth0
C127.0.0.0/8 is directly connected, lo

Gateway of last resort is not set
```

R3

```
R3#show ip ospf multi-area-adjacencies
  Multi-area-adjacency link on interface eth1 to neighbor 2.2.2.1
  Internet Address 2.2.2.2/24, Area 0.0.0.1, MTU 1500
  Process ID 1, Router ID 10.12.26.90, Network Type POINTTOPOINT, Cost:
  1 Transmit Delay is 1 sec, State Point-To-Point, TE Metric 1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 41 sent 41, DD received 4 sent 3
  LS-Req received 1 sent 1, LS-Upd received 5 sent 10
  LS-Ack received 8 sent 3, Discarded 0
```

```
R3#sh ip ospf neighbor

Total number of full neighbors: 3 OSPF
process 1 VRF(default):
Neighbor ID      Pri   State            Dead Time   Address         Interface
Instance ID
10.12.26.89        1   Full/DR          00:00:39    2.2.2.1         eth1
0
10.12.26.92        1   Full/Backup      00:00:36    3.3.3.2         eth2
0
10.12.26.89        1   Full/ -          00:00:30    2.2.2.1         eth1
R3#sh ip ospf route

OSPF process 1:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

O  1.1.1.0/24 [2] via 2.2.2.1, eth1, Area 0.0.0.1
C  2.2.2.0/24 [1] is directly connected, eth1, Area 0.0.0.0
C 3.3.3.0/24 [1] is directly connected, eth2, Area 0.0.0.1

R3#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
O       1.1.1.0/24 [110/2] via 2.2.2.1, eth1, 00:07:31
C2.2.2.0/24 is directly connected, eth1
C3.3.3.0/24 is directly connected, eth2
C10.12.26.0/24 is directly connected, eth0
C127.0.0.0/8 is directly connected, lo

Gateway of last resort is not set
```

LSA Throttling

This section contains basic OSPF LSA throttling configuration examples.

The OSPF Link-State Advertisement (LSA) throttling feature provides a mechanism to dynamically slow down link-state advertisement (LSA) updates in OSPF during times of network instability. It also allows faster OSPF convergence by providing LSA rate limiting in milliseconds, when network is stable.

How OSPF LSA Throttling Works

The `timers throttle lsa all` command controls the generation (sending) of LSAs. The first LSA is always generated immediately upon an OSPF topology change, and the next LSA generated is controlled by the minimum start interval. The subsequent LSAs generated for the same LSA are rate-limited until the maximum interval is reached.

The “same LSA” is defined as an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID.

The `timers lsa arrival` command controls the minimum interval for accepting the same LSA. If an instance of the same LSA arrives sooner than the interval that is set, the LSA is dropped. It is recommended that the arrival interval be less than or equal to the hold-time interval of the `timers throttle lsa all` command.

Topology

The diagram shows the minimum configuration required to enable OSPF LSA Throttling Timers feature. R1 and R2 are two routers in Area 0 connecting to network 10.10.10.0/24.

Note: Configure one interface so that it belongs to only one area. It is possible, however, to configure different interfaces on a router to belong to different areas.

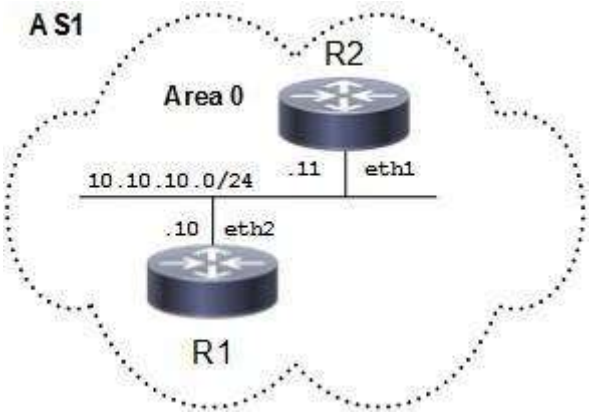


Figure 3-30: Basic OSPF Topology

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the interface loopback to configure.
`(config-if)#ip address 1.1.1.1/32`	Configure the ip address (1.1.1.1) to interface loopback.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 1`	Configure the routing process, and specify the Process ID (`1`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0`	Define the interface (`10.10.10.0/24`) on which OSPF runs, and associate the area ID (`0`) with the interface (area ID `0` specifies the backbone area).
`(config-router)#network 1.1.1.1/32 area 0`	Define the interface (`1.1.1.1/32`) on which OSPF runs, and associate the area ID (`0`) with the interface (area ID `0` specifies the backbone area).

(config-router)#timers throttle lsa all 10000 20000 45000	Configure LSA Throttling timers (Starting interval: <0-600000>, Min Hold Interval: <1-600000> and Max Wait Interval:< 1-600000>) in milliseconds. The Default value for corresponding timers are: Starting interval: 0, Min Hold Interval: 5 sec and Max Wait Interval: 5 sec.
(config-router)#end	Exit router mode

R2

#configure terminal	Enter configure mode.
(config)#router ospf 1	Configure the routing process, and specify the Process ID (1). The Process ID should be a unique positive integer identifying the routing process.
(config-router)#network 10.10.10.0/24 area 0	Define the interface (10.10.10.0/24) on which OSPF runs, and associate the area ID (0) with the interface.

Validation

R1

Check the output of show ip ospf and verify the initial throttle delay, minimum hold time for LSA throttle and maximum wait time for LSA throttle.

```
#show ip ospf 1
 Routing Process "ospf 1" with ID 4.1.1.1
 Process uptime is 1 minute
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
 Supports only single TOS(TOS0) routes Supports opaque LSA

 Supports Graceful Restart
 This router is an ASBR (injecting external routing information)
 SPF schedule delay min 0 secs 500 msecs
 SPF schedule delay max 50 secs 0 msecs
 Refresh timer 10 secs
 Number of incomming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Initial LSA throttle delay 10 secs 0 msecs
 Minimum hold time for LSA throttle 20 secs 0 msecs
 Maximum wait time for LSA throttle 45 secs 0 msecs
 Minimum LSA arrival 1 secs 0 msecs
 Number of external LSA 5. Checksum 0x010632
 Number of opaque AS LSA 0. Checksum 0x000000 Number of
non-default external LSA 5
 External LSA database is unlimited.
 Number of LSA originated 6
 Number of LSA received 0
 Number of areas attached to this router: 1
    Area 0 (BACKBONE)
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 0
```

```
        Area has no authentication
        SPF algorithm last executed 00:00:47.558
        ago SPF algorithm executed 2 times Number
        of LSA 1. Checksum 0x0041e0
```

Check the output of show ip ospf neighbor and verify that OSPF adjacency is up.

```
#sh ip ospf neighbor

OSPF process 1:
Neighbor ID     Pri   State           Dead Time   Address         Interface Inst
ance ID
10.12.49.102      1   Full/DR         00:00:38    10.10.10.10     eth2       0
```

Enable ospf database-timer rate-limit debugging to verify the LSA refresh being sent according to configured LSA throttling timers. #debug ospf database-timer rate-limit

```
#show debugging ospf
OSPF debugging status:
  OSPF rate limit timer events debugging is on
```

Perform shut/no shut based on LSA throttling timers and check if the LSA refresh are sent accordingly.

```
(config)#interface lo
(config-if)#shutdown
<pvr> : 2012/06/07 03:16:52 OSPF[ 2050]: Starting Rate Limit Timer for
LSA[0.0.0.0:Type1:4.1.1.1:(self)]: with 10000 msec delay

(config-if)#
<pvr> : 2012/06/07 03:17:02 OSPF[ 2050]: Rate Limit Timer for
LSA[0.0.0.0:Type1:4.1.1.1:(self)]: expired
<pvr> : 2012/06/07 03:17:02 OSPF[ 2050]: For Next Instance of
LSA[0.0.0.0:Type1:4.1.1.1:(self)]: generation wait 20000 msec

(config-if)#no shutdown
<pvr> : 2012/06/07 03:17:05 OSPF[ 2050]: Starting Rate Limit Timer for
LSA[0.0.0.0:Type1:4.1.1.1:(self)]: with 17107 msec delay

(config-if)#
<pvr> : 2012/06/07 03:17:22 OSPF[ 2050]: Rate Limit Timer for
LSA[0.0.0.0:Type1:4.1.1.1:(self)]: expired
<pvr> : 2012/06/07 03:17:22 OSPF[ 2050]: For Next Instance of
LSA[0.0.0.0:Type1:4.1.1.1:(self)]: generation wait 40000 msec

(config-if)#shutdown
<pvr> : 2012/06/07 03:17:25 OSPF[ 2050]: Starting Rate Limit Timer for
LSA[0.0.0.0:Type1:4.1.1.1:(self)]: with 36873 msec delay

(config-if)#no shutdown
<pvr> : 2012/06/07 03:18:03 OSPF[ 2050]: Rate Limit Timer for
LSA[0.0.0.0:Type1:4.1.1.1:(self)]: expired
<pvr> : 2012/06/07 03:18:03 OSPF[ 2050]: For Next Instance of
LSA[0.0.0.0:Type1:4.1.1.1:(self)]: generation wait 45000 msec
<pvr> : 2012/06/07 03:18:04 OSPF[ 2050]: Starting Rate Limit Timer for
LSA[0.0.0.0:Type1:4.1.1.1:(self)]: with 43332 msec delay
```

```
(config-if)#
<pvr> : 2012/06/07 03:18:48 OSPF[ 2050]: Rate Limit Timer for
LSA[0.0.0.0:Type1:4.1.1.1:(self)]: expired
<pvr> : 2012/06/07 03:18:48 OSPF[ 2050]: For Next Instance of
LSA[0.0.0.0:Type1:4.1.1.1:(self)]: generation wait 45000 msec R2
```

Check the output of “show ip ospf neighbor” and verify that OSPF adjacency is up.

```
#show ip ospf neighbor

OSPF process 1:
Neighbor ID      Pri   State           Dead Time   Address         Interface
Inst ance ID
4.1.1.1            1   Full/Backup     00:00:36    10.10.10.11     eth1       0
```

Check the output of `show ip ospf database` and verify that LSA (router LSA in this example) is updated according to the configured LSA throttling timers configured on its neighbor.

```
#sh ip ospf database

            OSPF Router with ID (10.12.49.102) (Process ID 1)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#      CkSum  Link count
4.1.1.1         4.1.1.1           76 0x80000002 0x8ee5 2 10.12.49.102
10.12.49.102       77 0x80000002 0x6d39 1

#sh ip ospf database

            OSPF Router with ID (10.12.49.102) (Process ID 1)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
4.1.1.1         4.1.1.1           85 0x80000002 0x8ee5 2 10.12.49.102
10.12.49.102       83 0x80000002 0x6d39 1

#sh ip ospf database

            OSPF Router with ID (10.12.49.102) (Process ID 1)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
4.1.1.1         4.1.1.1            1 0x80000003 0x945d 1 10.12.49.102
10.12.49.102       84 0x80000002 0x6d39 1

#sh ip ospf database

            OSPF Router with ID (10.12.49.102) (Process ID 1)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
```

```
4.1.1.1          4.1.1.1          20 0x80000003 0x945d 2 10.12.49.102
10.12.49.102      104 0x80000002 0x6d39 1

#sh ip ospf database

            OSPF Router with ID (10.12.49.102) (Process ID 1)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
4.1.1.1         4.1.1.1           1 0x80000004 0x8ae7 2 10.12.49.102
10.12.49.102      105 0x80000002 0x6d39 1

#sh ip ospf database

            OSPF Router with ID (10.12.49.102) (Process ID 1)
                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
4.1.1.1         4.1.1.1          40 0x80000004 0x8ae7 2 10.12.49.102
10.12.49.102      144 0x80000002 0x6d39 1

#sh ip ospf database

            OSPF Router with ID (10.12.49.102) (Process ID 1)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
4.1.1.1         4.1.1.1           1 0x80000005 0x905f 1 10.12.49.102
10.12.49.102      145 0x80000002 0x6d39 1

#sh ip ospf database

            OSPF Router with ID (10.12.49.102) (Process ID 1)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
4.1.1.1         4.1.1.1          45 0x80000005 0x905f 1 10.12.49.102
10.12.49.102      190 0x80000002 0x6d39 1
```

Configure OSPF LSA Arrival Timers

The diagram shows the minimum configuration required to enable OSPF Minimum LSA Arrival Timers feature. R1 and R2 are two routers in Area 0 connecting to network 10.10.10.0/24.

Note: Configure one interface so that it belongs to only one area. It is possible, however, to configure different interfaces on a router to belong to different areas.

Topology

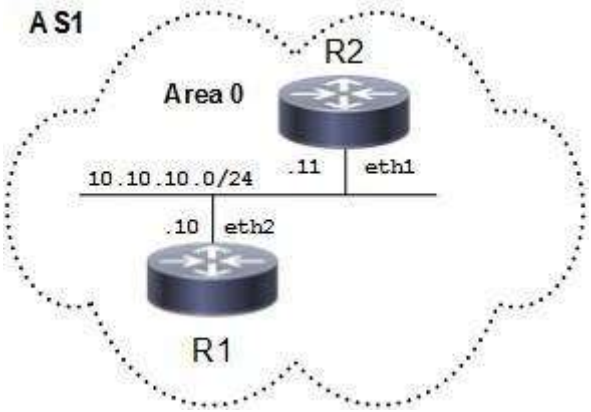


Figure 3-31: Basic OSPF Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Specify the interface loopback to configure.
`(config-if)#ip address 1.1.1.1/32`	Configure the ip address (1.1.1.1) to interface loopback.
`(config-if)#exit`	Exit interface mode.
`(config)#router ospf 1`	Configure the routing process, and specify the Process ID (`1`). The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0`	Define the interface (`10.10.10.0/24`) on which OSPF runs, and associate the area ID (`0`) with the interface (area ID `0` specifies the backbone area).
`(config-router)#network 1.1.1.1/32 area 0`	Define the interface (`1.1.1.1/32`) on which OSPF runs, and associate the area ID (`0`) with the interface (area ID `0` specifies the backbone area).
`(config-router)#end`	Exit router mode

R2

`#configure terminal`	Enter configure mode.
`(config)#router ospf 1`	Configure the routing process, and specify the Process ID `(1)`. The Process ID should be a unique positive integer identifying the routing process.
`(config-router)#network 10.10.10.0/24 area 0`	Define the interface `(10.10.10.0/24)` on which OSPF runs, and associate the area ID `(0)` with the interface.
`(config-router)#timers lsa arrival 100000`	Configure Minimum LSA Arrival timers (Minimum LSA arrival Interval:< 0-600000>) in milliseconds. The Default value for Minimum LSA Arrival timer is: 1 sec.

Validation

R1

Check the output of `show ip ospf` and verify that the minimum LSA arrival timer by default is set to 1 sec.

```
#show ip ospf
 Routing Process "ospf 1" with ID 4.1.1.1
 Process uptime is 2 hours 26 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
 Supports only single TOS(TOS0) routes Supports opaque LSA

 Supports Graceful Restart
 SPF schedule delay min 0 secs 500 msecs
 SPF schedule delay max 50 secs 0 msecs
 Refresh timer 10 secs
 Number of incomming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Initial LSA throttle delay 0 secs 0 msecs
 Minimum hold time for LSA throttle 5 secs 0 msecs
 Maximum wait time for LSA throttle 5 secs 0 msecs
 Minimum LSA arrival 1 secs 0 msecs
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000 Number
of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 3
 Number of LSA received 24
 Number of areas attached to this router: 1
    Area 0 (BACKBONE)
        Number of interfaces in this area is 5(5)
        Number of fully adjacent neighbors in this area is 1
        Area has no authentication
        SPF algorithm last executed 02:23:11.479
        ago SPF algorithm executed 8 times Number
        of LSA 7. Checksum 0x04136d
```

Check the output of `show ip ospf neighbor` and verify that OSPF adjacency is up.

```
#show ip ospf neighbor

OSPF process 1:
Neighbor ID      Pri   State           Dead Time   Address         Interface
Inst ance ID
10.12.49.102       1   Full/DR         00:00:39    10.10.10.10     eth2       0
```

R2

Check the output of `show ip ospf` and verify that the minimum LSA arrival timer is set to 100 sec.

```
#show ip ospf
 Routing Process "ospf 1" with ID 10.12.49.102
```

```
 Process uptime is 2 hours 28 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
 Supports only single TOS(TOS0) routes Supports opaque LSA

 Supports Graceful Restart
 SPF schedule delay min 0 secs 500 msecs
 SPF schedule delay max 50 secs 0 msecs
 Refresh timer 10 secs
 Number of incomming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Initial LSA throttle delay 0 secs 0 msecs
 Minimum hold time for LSA throttle 5 secs 0 msecs
 Maximum wait time for LSA throttle 5 secs 0 msecs
 Minimum LSA arrival 100 secs 0 msecs Number
 of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000 Number
of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 6
 Number of LSA received 29
 Number of areas attached to this router: 1
    Area 0 (BACKBONE)
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 1
        Area has no authentication
        SPF algorithm last executed 02:25:31.431
        ago SPF algorithm executed 11 times Number
        of LSA 7. Checksum 0x04116e
```

Check the output of show ip ospf neighbor and verify that OSPF adjacency is up.

```
#show ip ospf neighbor

OSPF process 1:
Neighbor ID      Pri   State           Dead Time   Address         Interface
Instance ID
4.1.1.1            1   Full/Backup     00:00:37    10.10.10.11     eth1       0
```

Check the output of “show ip ospf database” and verify that LSA is accepted only after a time difference of 100 sec between two consecutive LSAs.

```
#sh ip ospf database

            OSPF Router with ID (10.12.49.102) (Process ID 1)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
4.1.1.1         4.1.1.1          120  0x8000000b 0x8465 1
10.12.49.102    10.12.49.102     621 0x80000003  0x6b3a 1

#sh ip ospf database
```

```
            OSPF Router with ID (10.12.49.102) (Process ID 1)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router       Age Seq#       CkSum  Link count
4.1.1.1         4.1.1.1           121 0x8000000c 0x7aef 5
10.12.49.102    10.12.49.102      621 0x80000003 0x6b3a 1  #
```

CHAPTER 4 OSPFv3

This chapter contains basic OSPFv3 configuration examples.

For details about the commands used in these examples, see the *Open Shortest Path First Command Reference*.

Enable OSPFv3 on an Interface

This example shows the minimum configuration required for enabling OSPFv3 on an interface. R1 and R2 are two routers in Area 0 connecting to the network 3ffe:10::/64. After enabling OSPFv3 on an interface, create a routing instance, and specify the Router ID.

Note: You must explicitly specify a Router ID for the OSPFv3 process to be activated.

Topology

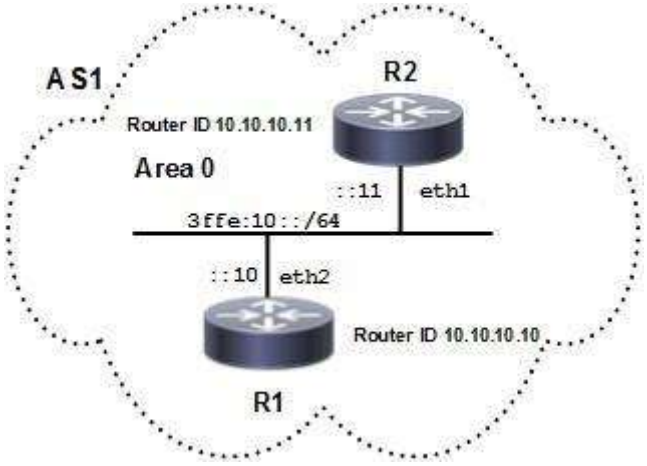


Figure 4-32: Basic OSPFv3 Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 10.10.10.10`	Specify a Router ID for the OSPFv3 routing process.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#interface eth2`	Specify the interface (`eth2`) to configure, and enter Interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID `0`.

R2

`#configure terminal`	Enter configure mode.

(config)#router ipv6 ospf	Create an OSPFv3 routing instance.
(config-router)#router-id 10.10.10.11	Specify a Router ID (10.10.10.11) for the OSPFv3 routing process.
(config-router)#exit	Exit OSPF router mode.
(config)#interface eth1	Specify the interface (eth1) to configure, and enter Interface mode.
(config-if)#ipv6 router ospf area 0	Enable OSPFv3 routing on an interface, and assign the Area ID (0).

Validation

R1

```
#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID      Pri   State           Dead Time   Interface  Instance ID
10.10.10.11        1   Full/Backup     00:00:35    eth2       0

#show ipv6 ospf database

            OSPFv3 Router with ID (10.10.10.10) (Process *null*)

                Link-LSA (Interface eth2)

Link State ID   ADV Router       Age      Seq#       CkSum  Prefix
0.0.0.4         10.10.10.10       164      0x80000001 0xf3c6       1
0.0.0.3         10.10.10.11       106      0x80000001 0xd973       1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age      Seq#       CkSum    Link
0.0.0.0         10.10.10.10        94      0x80000003 0xb2f0       1
0.0.0.0         10.10.10.11        95      0x80000003 0x9e05       1

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age      Seq#       CkSum
0.0.0.4         10.10.10.10        94      0x80000001 0xf990

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age      Seq#       CkSum  Prefix  Reference
0.0.0.2         10.10.10.10        93      0x80000001 0xc35d       1  NetworkLSA

                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age      Seq#       CkSum
0.0.0.4         10.10.10.10        94      0x80000002 0x3504
0.0.0.3         10.10.10.11        95      0x80000002 0x6bcc
#show ipv6 ospfv3 topology

OSPFv3 Process (*null*)
```

```
OSPFv3 paths to Area (0.0.0.0) routers
Router ID         Bits  Metric     Next-Hop             Interface
10.10.10.10             --
10.10.10.11             1          10.10.10.11          eth2
```

R2

```
#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID      Pri   State           Dead Time   Interface  Instance ID
10.10.10.10        1   Full/DR         00:00:31    eth1       0

R2#show ipv6 ospf database

            OSPFv3 Router with ID (10.10.10.11) (Process *null*)

                Link-LSA (Interface eth1)

Link State ID   ADV Router       Age      Seq#       CkSum  Prefix
0.0.0.4         10.10.10.10       341      0x80000001  0xf3c6      1
0.0.0.3         10.10.10.11       281      0x80000001  0xd973      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age      Seq#       CkSum    Link
0.0.0.0         10.10.10.10       271      0x80000003  0xb2f0      1
0.0.0.0         10.10.10.11       270      0x80000003  0x9e05      1

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age      Seq#       CkSum
0.0.0.4         10.10.10.10       271      0x80000001  0xf990

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age      Seq#       CkSum  Prefix  Reference
0.0.0.2         10.10.10.10       270      0x80000001  0xc35d      1  NetworkLSA

                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age      Seq#       CkSum
0.0.0.4         10.10.10.10       271      0x80000002  0x3504
0.0.0.3         10.10.10.11       270      0x80000002  0x6bcc


R2#show ipv6 ospfv3 topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID         Bits  Metric     Next-Hop             Interface
10.10.10.10             1          10.10.10.10          eth1 10.10.10.11
--
```

Set Priority

This example shows how to set priority for an interface. Set a high priority for a router to make it the Designated Router (DR). Router R3 is configured with a priority of 10; this is higher than the default priority (default priority is 1) set for R1 and R2. This makes R3 the DR.

Topology

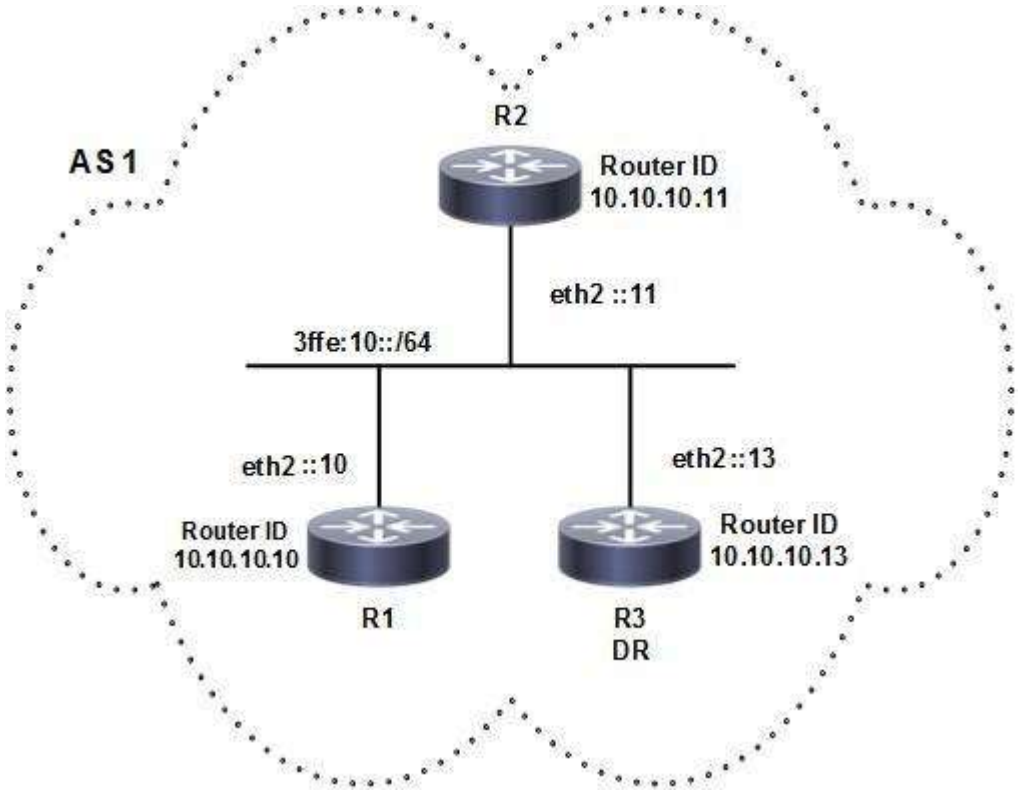


Figure 4-33: OSPFv3 Set Priority

R3

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 10.10.10.13`	Specify a Router ID (`10.10.10.13`) for the OSPFv3 routing process.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#interface eth2`	Specify the interface (`eth2`) to configure, and enter Interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID `(0)`.
`(config-if)#ipv6 ospf priority 10`	Specify the router priority to a higher priority (10) to make R3 the Designated Router (DR).

R1

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.

(config-router)#router-id 10.10.10.10	Specify a Router ID (10.10.10.10) for the OSPFv3 routing process.
(config-router)#exit	Exit OSPF router mode.
(config)#interface eth2	Specify the interface (eth2) to configure, and enter Interface mode.
(config-if)#ipv6 router ospf area 0	Enable OSPFv3 routing on an interface, and assign the Area ID (0).

R2

(config)#router ipv6 ospf	Create an OSPFv3 routing instance.
(config-router)#router-id 10.10.10.11	Specify a Router ID (10.10.10.11) for the OSPFv3 routing process.
(config-router)#exit	Exit OSPF router mode.
(config)#interface eth2	Specify the interface (eth2) to configure, and enter Interface mode.
(config-if)#ipv6 router ospf area 0	Enable OSPFv3 routing on an interface, and assign the Area ID (0).

Validation

R1
```
rtr1#show ipv6 ospf neighbor
    OSPFv3 Process (*null*)
    Neighbor ID      Pri   State           Dead Time   Interface Instance ID
    10.10.10.11        1   Full/DROther    00:00:37    eth2        0
    10.10.10.13       10   Full/DR         00:00:37    eth2        0

    rtr1#show ipv6 ospf database
                OSPFv3 Router with ID (10.10.10.10) (Process *null*)

                    Link-LSA (Interface eth2)

    Link State ID   ADV Router       Age      Seq#       CkSum Prefix
    0.0.0.4         10.10.10.10       398      0x80000001  0xf3c6      1
    0.0.0.4         10.10.10.11        71      0x80000001  0x4768      1
    0.0.0.4         10.10.10.13       611      0x80000002  0x695b      1

    Router-LSA (Area 0.0.0.0)

    Link State ID   ADV Router       Age      Seq#       CkSum     Link
    0.0.0.0         10.10.10.10        49      0x80000004  0xf2ac      1
    0.0.0.0         10.10.10.11        50      0x80000004  0xecb1      1
    0.0.0.0         10.10.10.13        61      0x80000004  0xe0bb      1

                    Network-LSA (Area 0.0.0.0)
    Link State ID   ADV Router       Age      Seq#       CkSum
    0.0.0.4         10.10.10.13        61      0x80000002  0xa6b0

                    Intra-Area-Prefix-LSA (Area 0.0.0.0)
```

```
Link State ID   ADV Router      Age       Seq#       CkSum   Prefix  Reference
0.0.0.2         10.10.10.13       60       0x80000002 0xd940       1  NetworkLSA

                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.4         10.10.10.10       49       0x80000003 0x75bf
0.0.0.4         10.10.10.11       50       0x80000004 0x9f92
0.0.0.4         10.10.10.13       61       0x80000003 0xf935


rtr1#show ipv6 ospfv3 topology
OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits Metric     Next-Hop             Interface
10.10.10.10            --
10.10.10.11            1          10.10.10.11          eth2
10.10.10.13            1          10.10.10.13          eth2
```

R2

```
R2#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID      Pri   State           Dead Time   Interface Instance ID
10.10.10.10        1   Full/Backup     00:00:31    eth2        0
10.10.10.13       10   Full/DR         00:00:39    eth2        0

R2#show ipv6 ospf database
            OSPFv3 Router with ID (10.10.10.11) (Process *null*)

                Link-LSA (Interface eth2)

Link State ID   ADV Router       Age      Seq#       CkSum   Prefix
0.0.0.4         10.10.10.10       525      0x80000001 0xf3c6       1
0.0.0.4         10.10.10.11       194      0x80000001 0x4768       1
0.0.0.4         10.10.10.13       736      0x80000002 0x695b       1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age      Seq#       CkSum     Link
0.0.0.0         10.10.10.10       175      0x80000004 0xf2ac       1
0.0.0.0         10.10.10.11       174      0x80000004 0xecb1       1
0.0.0.0         10.10.10.13       186      0x80000004 0xe0bb       1

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age      Seq#       CkSum
0.0.0.4         10.10.10.13       186      0x80000002 0xa6b0
                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age      Seq#       CkSum   Prefix  Reference
```

```
0.0.0.2         10.10.10.13      185       0x80000002  0xd940       1 NetworkLSA

                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.4         10.10.10.10      175       0x80000003  0x75bf
0.0.0.4         10.10.10.11      174       0x80000004  0x9f92
0.0.0.4         10.10.10.13      186       0x80000003  0xf935

R2#show ipv6 ospfv3 topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits Metric     Next-Hop             Interface
10.10.10.10            1          10.10.10.10          eth2
10.10.10.11            --
10.10.10.13            1          10.10.10.13          eth2
```

R3

```
R3#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID      Pri   State           Dead Time   Interface  Instance ID
10.10.10.10        1   Full/Backup     00:00:38    eth2       0
10.10.10.11        1   Full/DROther    00:00:29    eth2       0

R3#show ipv6 ospf database
            OSPFv3 Router with ID (10.10.10.13) (Process *null*)

                Link-LSA (Interface eth2)

Link State ID   ADV Router       Age      Seq#       CkSum   Prefix
0.0.0.4         10.10.10.10       658      0x80000001  0xf3c6       1
0.0.0.4         10.10.10.11       329      0x80000001  0x4768       1
0.0.0.4         10.10.10.13       869      0x80000002  0x695b       1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age      Seq#       CkSum     Link
0.0.0.0         10.10.10.10       309      0x80000004  0xf2ac       1
0.0.0.0         10.10.10.11       309      0x80000004  0xecb1       1
0.0.0.0         10.10.10.13       319      0x80000004  0xe0bb       1

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age      Seq#       CkSum
0.0.0.4         10.10.10.13       319      0x80000002  0xa6b0

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age      Seq#       CkSum   Prefix  Reference
0.0.0.2         10.10.10.13       318      0x80000002  0xd940       1  NetworkLSA
```

```
                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age         Seq#       CkSum
0.0.0.4         10.10.10.10      309        0x80000003  0x75bf
0.0.0.4         10.10.10.11      309        0x80000004  0x9f92
0.0.0.4         10.10.10.13      319        0x80000003  0xf935

R3#show ipv6 ospfv3 topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits Metric     Next-Hop             Interface
10.10.10.10            1          10.10.10.10          eth2
10.10.10.11            1          10.10.10.11          eth2
10.10.10.13            --
```

Area Border Router

This example shows configuration for an Area Border Router. R2 is an Area Border Router (ABR). On R2, interface eth0 is in Area 0, and interface eth1 is in Area 1.

Topology

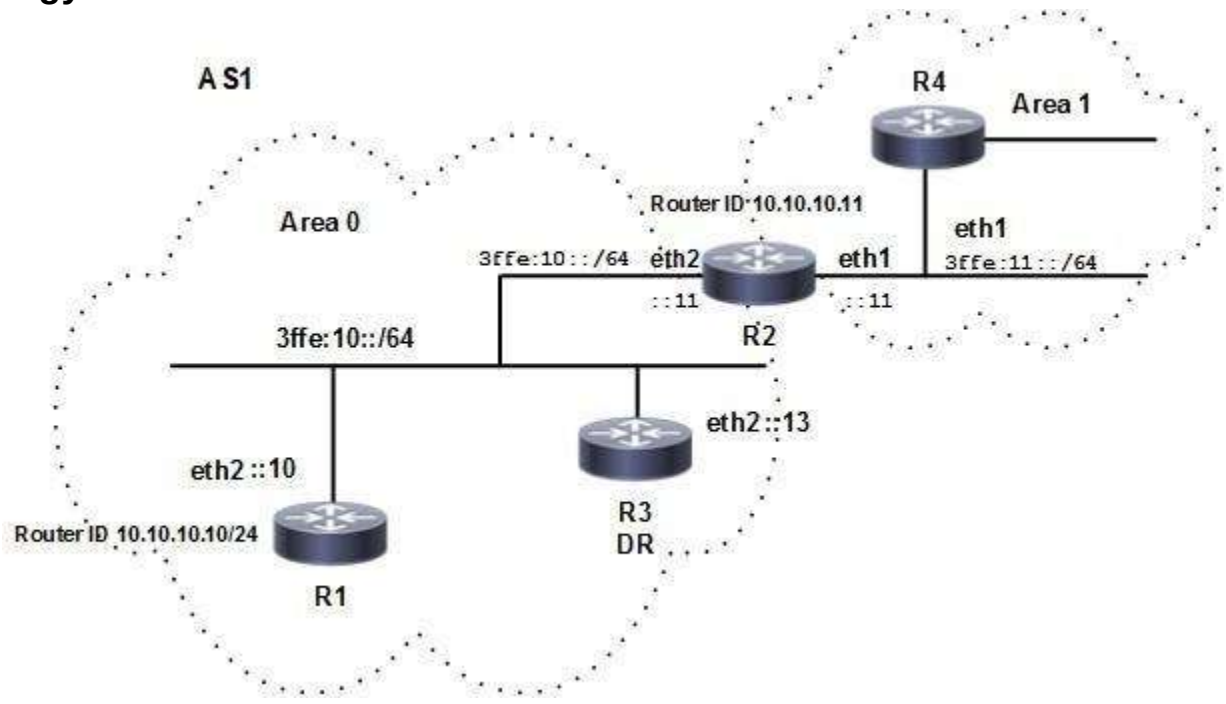


Figure 4-34: OSPFv3 Area Border Router

Configuration

R2

`#configure terminal`	Enter configure mode.

(config)#router ipv6 ospf	Create an OSPFv3 routing instance.
(config-router)#router-id 10.10.10.11	Specify a Router ID (10.10.10.11) for the OSPFv3 routing process.
(config-router)#exit	Exit OSPF router mode.
(config)#interface eth2	Specify the interface (eth2) to configure, and enter Interface mode.
(config-if)#ipv6 router ospf area 0	Enable OSPFv3 routing on an interface, and assign the Area ID (0).
(config-if)#exit	Exit interface mode.
(config)#interface eth1	Specify the interface (eth1) to configure, and enter Interface mode.
(config-if)#ipv6 router ospf area 1	Enable OSPFv3 routing on the other interface, and assign the other Area ID (1).

Validation

R2

```
R2#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID      Pri   State           Dead Time   Interface  Instance ID
10.10.10.10        1   Full/Backup     00:00:40    eth2       0
10.10.10.13        1   Full/DR         00:00:35    eth2       0


R2#show ipv6 ospf database

            OSPFv3 Router with ID (192.168.0.2) (Process *null*)

                Link-LSA (Interface eth1)

Link State ID   ADV Router       Age      Seq#       CkSum  Prefix 0.0.0.3
192.168.0.2      663       0x80000001 0x17f2       1

                Link-LSA (Interface eth2)

Link State ID   ADV Router       Age      Seq#       CkSum  Prefix
0.0.0.4         10.10.10.10      1494      0x80000003 0xefc8       1
0.0.0.4         10.10.10.13       362      0x80000005 0x4882       1
0.0.0.4         192.168.0.2       663      0x80000001 0x620b       1

Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age      Seq#       CkSum    Link
0.0.0.0         10.10.10.10       648      0x80000007 0xecaf       1
0.0.0.0          10.10.10.13      653      0x80000007 0xdabe       1
0.0.0.0          192.168.0.2      643      0x80000005 0x0951       1

               Network-LSA (Area 0.0.0.0)
```

```
Link State ID   ADV Router       Age      Seq#       CkSum
0.0.0.4         10.10.10.13       653      0x80000006 0xef21

                Inter-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age      Seq#       CkSum
0.0.0.1         192.168.0.2       658      0x80000002 0xf543

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age      Seq#       CkSum   Prefix  Reference
0.0.0.2         10.10.10.13       652      0x80000005 0xd343       1  NetworkLSA

                Intra-Area-Te-LSA (Area 0.0.0.0)
Link State ID   ADV Router       Age      Seq#       CkSum
0.0.0.4         10.10.10.10       648      0x80000006 0x6fc2
0.0.0.4         10.10.10.13       653      0x80000006 0xf338
0.0.0.4         192.168.0.2       646      0x80000002 0xbe33

                Router-LSA (Area 0.0.0.1)

Link State ID   ADV Router       Age      Seq#       CkSum    Link 0.0.0.0
192.168.0.2      623       0x80000002 0xdcc6       0

                Inter-Area-Prefix-LSA (Area 0.0.0.1)

Link State ID   ADV Router       Age      Seq#       CkSum
0.0.0.1         192.168.0.2       658      0x80000002 0xe752

                Intra-Area-Prefix-LSA (Area 0.0.0.1)

Link State ID   ADV Router       Age      Seq#       CkSum   Prefix  Reference
0.0.0.1         192.168.0.2       622      0x80000002 0x316c       1  RouterLSA

                Intra-Area-Te-LSA (Area 0.0.0.1)

Link State ID   ADV Router       Age      Seq#       CkSum
0.0.0.3         192.168.0.2       651      0x80000001 0xe439



R2#show ipv6 ospfv3 topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits  Metric     Next-Hop             Interface
10.10.10.10            1          10.10.10.10          eth2
10.10.10.13            1          10.10.10.13          eth2 192.168.0.2
B  --
    OSPFv3 paths to Area (0.0.0.1) routers
    Router ID        Bits  Metric     Next-Hop             Interface
    192.168.0.2         B  --
```

```
R2#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP Timers:
Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 00:54:11
C      3ffe:10::/64 via ::, eth2, 00:40:02
C3ffe:11::/64 via ::, eth1, 00:39:13
Cfe80::/64 via ::, eth2, 00:40:01
Kff00::/8 [0/256] via ::, eth1, 00:52:31


R2#show ipv6 ospf route
OSPFv3 Process (*null*)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe:10::/64                                      1
directly connected, eth2, Area 0.0.0.0
C  3ffe:11::/64                                      1
directly connected, eth1, Area 0.0.0.1
```

Redistribute Routes into OSPFv3

In this example, the BGP routes are imported into the OSPF routing table, and advertised as Type 5 External LSAs into Area 0.

Topology

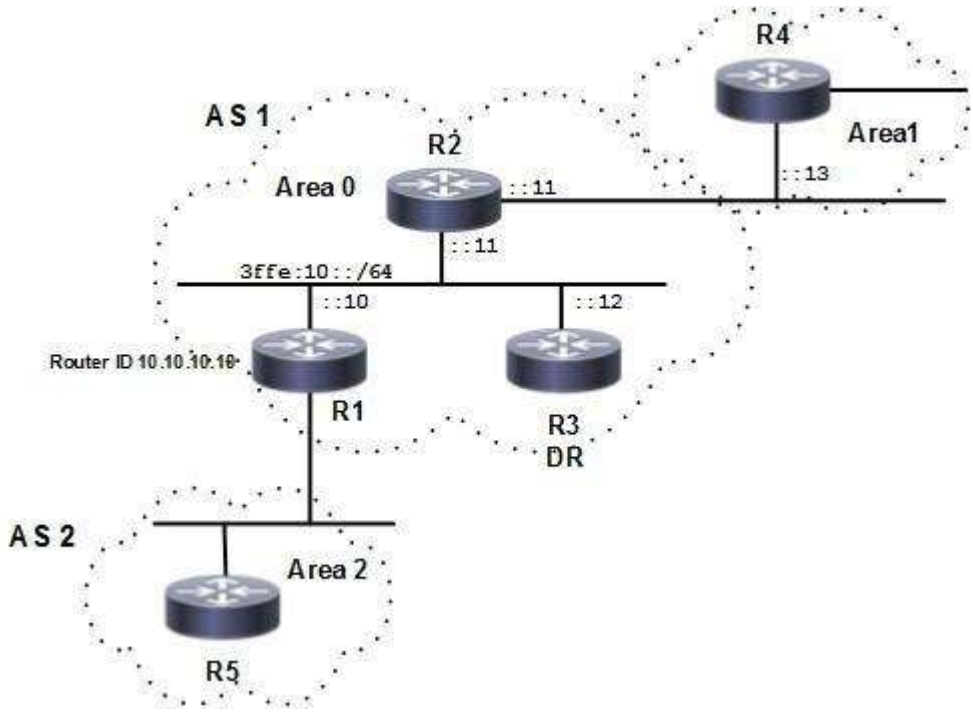


Figure 4-35: OSPFv3 Redistribute Routes

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 10.10.10.10`	Specify a Router ID `(10.10.10.10)` for the OSPFv3 routing process.
`(config-router)#redistribute bgp`	Specify redistributing routes from the other routing protocol (BGP) into OSPFv3.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#interface eth0`	Specify the interface (`eth0`) to configure, and enter Interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID `(0)`.

Validation

show ipv6 ospf neighbor, show ipv6 ospf database, show ipv6 ospfv3 topology, show ipv6 ospf route, show ipv6 route

Cost

Make a route the preferred route by changing its cost. In this example, cost has been configured to make R2 the next hop for R1.

The default cost for each interface is 10. Interface eth2 on R2 has a cost of 100, and Interface eth2 on R3 has a cost of 150. The total cost to reach 10.10.14.0/24 (R4) through R2 and R3 is computed as follows:

R2: 10+100 = 110

R3: 10+150 = 160

For this reason, R1 chooses R2 as its next hop to destination 10.10.14.0/24, because it has the lower cost.

Topology

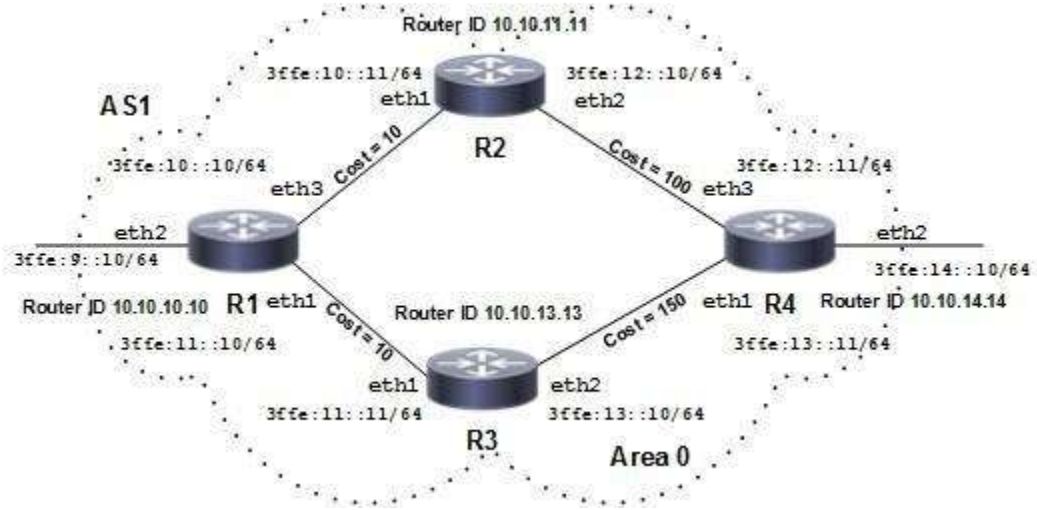


Figure 4-36: Configure Cost OSPFv3

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 10.10.10.10`	Specify a Router ID (`10.10.10.10`) for the OSPFv3 routing process.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#interface eth3`	Specify the interface (`eth3`) to configure, and enter Interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID `(0)`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to configure, and enter Interface mode.
`#configure terminal`	Enter configure mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on an interface, and assign the Area ID `(0)`.
`(config-if)#exit`	Exit interface mode.

(config)#interface eth2	Specify the interface (eth2) to configure, and enter Interface mode.
(config-if)#ipv6 router ospf area 0	Enable OSPFv3 routing on an interface, and assign the Area ID (0).

R2

(config)#router ipv6 ospf	Create an OSPFv3 routing instance.
(config-router)#router-id 10.10.11.11	Specify a Router ID (10.10.11.11) for the OSPFv3 routing process.
(config-router)#exit	Exit OSPF router mode.
(config)#interface eth1	Specify the interface (eth1) to configure, and enter Interface mode.
(config-if)#ipv6 router ospf area 0	Enable OSPFv3 routing on an interface, and assign the Area ID (0).
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Specify the interface (eth2) to configure, and enter Interface mode.
(config-if)#ipv6 router ospf area 0	Enable OSPFv3 routing on an interface, and assign the Area ID (0).
(config-if)#ipv6 ospf cost 100	Set the cost of the link-state metric (on eth2) to 100.

R3

(config)#router ipv6 ospf	Create an OSPFv3 routing instance.
(config-router)#router-id 10.10.13.13	Specify a Router ID (10.10.13.13) for the OSPFv3 routing process.
(config-router)#exit	Exit OSPF router mode.
(config)#interface eth1	Specify the interface (eth1) to configure, and enter Interface mode.
(config-if)#ipv6 router ospf area 0	Enable OSPFv3 routing on an interface, and assign the Area ID (0).
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Specify the interface (eth2) to configure, and enter Interface mode.
(config-if)#ipv6 router ospf area 0	Enable OSPFv3 routing on an interface, and assign the Area ID (0).
(config-if)#ipv6 ospf cost 150	Set the cost of link-state metric to 150.

R4

(config)#router ipv6 ospf	Create an OSPFv3 routing instance.
(config-router)#router-id 10.10.14.14	Specify a Router ID (10.10.14.14) for the OSPFv3 routing process.
(config-router)#exit	Exit OSPF router mode.
(config)#interface eth3	Specify the interface (eth3) to configure, and enter Interface mode.

(config-if)#ipv6 router ospf area 0	Enable OSPFv3 routing on an interface, and assign the Area ID (0).
(config-if)#exit	Exit interface mode.
(config)#interface eth1	Specify the interface (eth1) to configure, and enter Interface mode.
(config-if)#ipv6 router ospf area 0	Enable OSPFv3 routing on an interface, and assign the Area ID (0).

Validation

R1

```
R1#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID      Pri   State           Dead Time    Interface  Instance ID
10.10.13.13        1   Full/Backup     00:00:37     eth1       0
10.10.11.11        1   Full/Backup     00:00:34     eth3       0


R1#show ipv6 ospfv3 topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID         Bits  Metric     Next-Hop             Interface
10.10.10.10             --
10.10.11.11             1          10.10.11.11           eth3
10.10.13.13             1          10.10.13.13           eth1
10.10.14.14             101        10.10.11.11           eth3



rtr1#show ipv6 ospf database

            OSPFv3 Router with ID (10.10.10.10) (Process *null*)

                Link-LSA (Interface eth1)

Link State ID   ADV Router       Age      Seq#       CkSum  Prefix
0.0.0.3         10.10.10.10       868      0x80000003 0x4839      1
0.0.0.3         10.10.13.13       747      0x80000003 0x5544      1

                Link-LSA (Interface eth3)

Link State ID   ADV Router       Age      Seq#       CkSum  Prefix
0.0.0.5         10.10.10.10       898      0x80000003 0xf33e      1
0.0.0.3         10.10.11.11       817      0x80000003 0xce7b      1

               Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age      Seq#       CkSum     Link
0.0.0.0         10.10.10.10        58      0x80000008 0xabaf      2
```

```
0.0.0.0         10.10.11.11      1767       0x80000008 0x26cd       2
0.0.0.0         10.10.13.13      1753       0x80000008 0x9724       2
0.0.0.0         10.10.14.14      1753       0x80000007 0x96b5       2

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age       Seq#       CkSum
0.0.0.3         10.10.10.10        58       0x80000003 0x4341
0.0.0.5         10.10.10.10       163       0x80000003 0xf88d
0.0.0.4         10.10.11.11      1767       0x80000002 0x5c22
0.0.0.4         10.10.13.13      1753       0x80000002 0x680e

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age       Seq#       CkSum  Prefix   Reference
0.0.0.1         10.10.10.10       813       0x80000003 0xd34b       1  Network-
LSA
0.0.0.2         10.10.10.10       743       0x80000003 0xcb53       1  Network-
LSA
0.0.0.2         10.10.11.11       652       0x80000003 0xf91f       1  Network-
LSA
0.0.0.3         10.10.13.13       684       0x80000003 0x22ec       1  NetworkLSA
                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age       Seq#       CkSum
0.0.0.3         10.10.10.10       868       0x80000004 0x4fe8
0.0.0.5         10.10.10.10       898       0x80000004 0x39fb
0.0.0.3         10.10.11.11       817       0x80000004 0x72c1
0.0.0.4         10.10.11.11       802       0x80000005 0xe1ea
0.0.0.3         10.10.13.13       747       0x80000004 0x5ad6
0.0.0.4         10.10.13.13       727       0x80000005 0x8f02
0.0.0.3         10.10.14.14       688       0x80000004 0x2df8
0.0.0.5         10.10.14.14       653       0x80000004 0x9c8c


rtr1#show ipv6 ospf route
OSPFv3 Process (*null*)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                      Metric
     Next-hop
C  3ffe:10::/64                                       1     directly
connected, eth3, Area 0.0.0.0
C  3ffe:11::/64                                       1     directly
connected, eth1, Area 0.0.0.0
O  3ffe:12::/64                                     101     via
fe80::a00:27ff:fef9:2432, eth3, Area 0.0.0.0
    O  3ffe:13::/64                                   102     via
    fe80::a00:27ff:fef9:2432, eth3, Area 0.0.0.0
```

```
rtr1#show ipv6 route IPv6
Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP Timers:
Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 01:22:59
C      3ffe:10::/64 via ::, eth3, 00:51:14
C3ffe:11::/64 via ::, eth1, 00:50:44
O3ffe:12::/64 [110/101] via fe80::a00:27ff:fef9:2432, eth3, 00:49:33
O3ffe:13::/64 [110/102] via fe80::a00:27ff:fef9:2432, eth3, 00:48:21
Cfe80::/64 via ::, eth1, 01:13:13
Kff00::/8 [0/256] via ::, eth0, 01:22:47
```

R2

```
R2#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID      Pri   State           Dead Time    Interface Instance ID
10.10.10.10        1   Full/DR         00:00:32     eth1      0
10.10.14.14        1   Full/Backup     00:00:33     eth2      0


R2#show ipv6 ospfv3 topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID         Bits  Metric     Next-Hop             Interface
10.10.10.10             1          10.10.10.10           eth1
10.10.11.11             --
10.10.13.13             2          10.10.10.10           eth1
10.10.14.14             100        10.10.14.14           eth2



R2#show ipv6 ospf database

            OSPFv3 Router with ID (10.10.11.11) (Process *null*)

                Link-LSA (Interface eth1)

Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
0.0.0.5         10.10.10.10     1373       0x80000003 0xf33e      1
0.0.0.3         10.10.11.11     1290       0x80000003 0xce7b      1

                Link-LSA (Interface eth2)
Link State ID   ADV Router      Age       Seq#       CkSum  Prefix
```

```
0.0.0.4         10.10.11.11      1275       0x80000003 0x802a       1
0.0.0.5         10.10.14.14      1126       0x80000003 0x4f29       1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age       Seq#       CkSum    Link
0.0.0.0         10.10.10.10       533       0x80000008 0xabaf       2
0.0.0.0         10.10.11.11       440       0x80000009 0x24ce       2
0.0.0.0         10.10.13.13       427       0x80000009 0x9525       2
0.0.0.0         10.10.14.14       426       0x80000008 0x94b6       2

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age       Seq#       CkSum
0.0.0.3         10.10.10.10       533       0x80000003 0x4341
0.0.0.5         10.10.10.10       638       0x80000003 0xf88d
0.0.0.4         10.10.11.11       440       0x80000003 0x5a23
0.0.0.4         10.10.13.13       427       0x80000003 0x660f

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age       Seq#       CkSum  Prefix   Reference
0.0.0.1         10.10.10.10      1288       0x80000003 0xd34b       1  Network-
LSA
0.0.0.2         10.10.10.10      1218       0x80000003 0xcb53       1  Network-
LSA
0.0.0.2         10.10.11.11      1125       0x80000003 0xf91f       1  Network-
LSA
0.0.0.3         10.10.13.13      1158       0x80000003 0x22ec       1 NetworkLSA
                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age       Seq#       CkSum
0.0.0.3         10.10.10.10      1343       0x80000004 0x4fe8
0.0.0.5         10.10.10.10      1373       0x80000004 0x39fb
0.0.0.3         10.10.11.11      1290       0x80000004 0x72c1
0.0.0.4         10.10.11.11      1275       0x80000005 0xe1ea
0.0.0.3         10.10.13.13      1223       0x80000004 0x5ad6
0.0.0.4         10.10.13.13      1203       0x80000005 0x8f02
0.0.0.3         10.10.14.14      1161       0x80000004 0x2df8
0.0.0.5         10.10.14.14      1126       0x80000004 0x9c8c



R2#show ipv6 ospf route
OSPFv3 Process (*null*)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
```

```
C  3ffe:10::/64                                          1     directly
connected, eth1, Area 0.0.0.0
    O  3ffe:11::/64                                        2
    via fe80::a00:27ff:fe6e:21d8, eth1, Area 0.0.0.0 C
    3ffe:12::/64                                       100
    directly connected, eth2, Area 0.0.0.0
    O  3ffe:13::/64                                      101     via
    fe80::a00:27ff:fe01:c94d, eth2, Area 0.0.0.0
```

```
R2#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP Timers:
Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 01:26:25
C      3ffe:10::/64 via ::, eth1, 00:54:14
O      3ffe:11::/64 [110/2] via fe80::a00:27ff:fe6e:21d8, eth1, 00:55:03
C3ffe:12::/64 via ::, eth2, 00:53:58
O3ffe:13::/64 [110/101] via fe80::a00:27ff:fe01:c94d, eth2, 00:52:43
Cfe80::/64 via ::, eth2, 01:20:38
Kff00::/8 [0/256] via ::, eth2, 01:20:39
```

R3

```
R3#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID      Pri   State           Dead Time    Interface Instance ID
10.10.10.10        1   Full/DR         00:00:33     eth1      0
10.10.14.14        1   Full/Backup     00:00:38     eth2      0
```

```
R3#show ipv6 ospfv3 topology

OSPFv3 Process (*null*)
OSPFv3 paths to Area (0.0.0.0) routers
Router ID         Bits  Metric     Next-Hop             Interface
10.10.10.10             1          10.10.10.10           eth1
10.10.11.11             2          10.10.10.10           eth1
10.10.13.13             --
10.10.14.14             102        10.10.10.10           eth1
```

```
R3#show ipv6 ospfv3 topology
```

```
    OSPFv3 Process (*null*)
    OSPFv3 paths to Area (0.0.0.0) routers
    Router ID        Bits  Metric     Next-Hop             Interface
    10.10.10.10             1          10.10.10.10          eth1
    10.10.11.11             2          10.10.10.10          eth1
10.10.13.13            --
10.10.14.14            102         10.10.10.10          eth1

R3#
R3#show ipv6 ospf database

            OSPFv3 Router with ID (10.10.13.13) (Process *null*)

                Link-LSA (Interface eth1)

Link State ID   ADV Router       Age      Seq#       CkSum   Prefix
0.0.0.3         10.10.10.10      1591      0x80000003 0x4839       1
0.0.0.3         10.10.13.13      1468      0x80000003 0x5544       1

                Link-LSA (Interface eth2)

Link State ID   ADV Router       Age      Seq#       CkSum   Prefix
0.0.0.4         10.10.13.13      1448      0x80000003 0x9d29       1
0.0.0.3         10.10.14.14      1409      0x80000003 0x50cf       1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age      Seq#       CkSum     Link
0.0.0.0         10.10.10.10       780      0x80000008 0xabaf       2
0.0.0.0         10.10.11.11       689      0x80000009 0x24ce       2
0.0.0.0         10.10.13.13       673      0x80000009 0x9525       2
0.0.0.0         10.10.14.14       673      0x80000008 0x94b6       2

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age      Seq#       CkSum
0.0.0.3         10.10.10.10       780      0x80000003 0x4341
0.0.0.5         10.10.10.10       885      0x80000003 0xf88d
0.0.0.4         10.10.11.11       689      0x80000003 0x5a23
0.0.0.4         10.10.13.13       673      0x80000003 0x660f

                Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age      Seq#       CkSum   Prefix  Reference
0.0.0.1         10.10.10.10      1536      0x80000003 0xd34b       1  Network-
LSA
0.0.0.2         10.10.10.10      1466      0x80000003 0xcb53       1  Network-
LSA
0.0.0.2         10.10.11.11      1374      0x80000003 0xf91f       1  Network-
LSA
0.0.0.3         10.10.13.13      1403      0x80000003 0x22ec       1  NetworkLSA
               Intra-Area-Te-LSA (Area 0.0.0.0)
```

```
Link State ID   ADV Router      Age       Seq#       CkSum
0.0.0.3         10.10.10.10     1591       0x80000004 0x4fe8
0.0.0.5         10.10.10.10     1621       0x80000004 0x39fb
0.0.0.3         10.10.11.11     1539       0x80000004 0x72c1
0.0.0.4         10.10.11.11     1524       0x80000005 0xe1ea
0.0.0.3         10.10.13.13     1468       0x80000004 0x5ad6
0.0.0.4         10.10.13.13     1448       0x80000005 0x8f02
0.0.0.3         10.10.14.14     1409       0x80000004 0x2df8
    0.0.0.5         10.10.14.14     1374       0x80000004 0x9c8c
```

```
R3#show ipv6 ospf route
OSPFv3 Process (*null*)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                        Metric
     Next-hop
O  3ffe:10::/64                                          2
via fe80::a00:27ff:fe7d:2a72, eth1, Area 0.0.0.0 C
3ffe:11::/64                                           1
directly connected, eth1, Area 0.0.0.0
O  3ffe:12::/64                                         102
via fe80::a00:27ff:fe7d:2a72, eth1, Area 0.0.0.0 O
3ffe:13::/64                                         103     via
fe80::a00:27ff:fe7d:2a72, eth1, Area 0.0.0.0
```

```
R3#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP Timers:
Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 01:28:16
O      3ffe:10::/64 [110/2] via fe80::a00:27ff:fe7d:2a72, eth1, 00:58:14
C3ffe:11::/64 via ::, eth1, 00:55:44
O3ffe:12::/64 [110/102] via fe80::a00:27ff:fe7d:2a72, eth1, 00:56:36
C3ffe:13::/64 via ::, eth2, 00:55:26
Cfe80::/64 via ::, eth1, 01:20:39
Kff00::/8 [0/256] via ::, eth2, 01:21:40
```

R4

```
R4#show ipv6 ospf neighbor
```

```
    OSPFv3 Process (*null*)
    Neighbor ID      Pri   State           Dead Time   Interface  Instance ID
    10.10.13.13        1   Full/DR         00:00:30    eth1       0
    10.10.11.11        1   Full/DR         00:00:30    eth3       0



    R4#show ipv6 ospfv3 topology

    OSPFv3 Process (*null*)
    OSPFv3 paths to Area (0.0.0.0) routers
    Router ID        Bits   Metric     Next-Hop             Interface
    10.10.10.10              2          10.10.11.11          eth3
                                       10.10.13.13          eth1
10.10.11.11            1             10.10.11.11          eth3
10.10.13.13            1             10.10.13.13          eth1
10.10.14.14            --


R4#show ipv6 ospf database

            OSPFv3 Router with ID (10.10.14.14) (Process *null*)

                Link-LSA (Interface eth1)

Link State ID   ADV Router       Age      Seq#       CkSum   Prefix
0.0.0.4         10.10.13.13      1634      0x80000003 0x9d29      1
0.0.0.3         10.10.14.14      1592      0x80000003 0x50cf      1

Link-LSA (Interface eth3)

Link State ID   ADV Router       Age      Seq#       CkSum   Prefix
0.0.0.4         10.10.11.11      1708      0x80000003 0x802a      1
0.0.0.5         10.10.14.14      1557      0x80000003 0x4f29      1

                Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age      Seq#       CkSum     Link
0.0.0.0         10.10.10.10       966      0x80000008 0xabaf      2
0.0.0.0         10.10.11.11       873      0x80000009 0x24ce      2
0.0.0.0         10.10.13.13       859      0x80000009 0x9525      2
0.0.0.0         10.10.14.14       857      0x80000008 0x94b6      2

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age      Seq#       CkSum
0.0.0.3         10.10.10.10       966      0x80000003 0x4341
0.0.0.5         10.10.10.10      1071      0x80000003 0xf88d
0.0.0.4         10.10.11.11       873      0x80000003 0x5a23
0.0.0.4         10.10.13.13       859      0x80000003 0x660f

                Intra-Area-Prefix-LSA (Area 0.0.0.0)
```

```
Link State ID   ADV Router       Age      Seq#       CkSum  Prefix   Reference
0.0.0.1         10.10.10.10      1721      0x80000003 0xd34b       1  Network-
LSA
0.0.0.2         10.10.10.10      1651      0x80000003 0xcb53       1  Network-
LSA
0.0.0.2         10.10.11.11      1558      0x80000003 0xf91f       1  Network-
LSA
0.0.0.3         10.10.13.13      1589      0x80000003 0x22ec       1  NetworkLSA

  Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age      Seq#       CkSum
0.0.0.3         10.10.10.10      1776      0x80000004 0x4fe8
0.0.0.5         10.10.10.10         6      0x80000005 0x37fc
0.0.0.3         10.10.11.11      1723      0x80000004 0x72c1
0.0.0.4         10.10.11.11      1708      0x80000005 0xe1ea
     0.0.0.3         10.10.13.13     1654      0x80000004 0x5ad6
     0.0.0.4         10.10.13.13     1634      0x80000005 0x8f02
     0.0.0.3         10.10.14.14     1592      0x80000004 0x2df8
     0.0.0.5         10.10.14.14     1557      0x80000004 0x9c8c
```

```
R4#show ipv6 ospf route
OSPFv3 Process (*null*)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                        Metric
     Next-hop
O  3ffe:10::/64                                          2
via fe80::a00:27ff:fe0d:fbe3, eth3, Area 0.0.0.0 O
3ffe:11::/64                                           2
via fe80::a00:27ff:fecf:8873, eth1, Area 0.0.0.0 C
3ffe:12::/64                                          1
directly connected, eth3, Area 0.0.0.0
C  3ffe:13::/64                                          1
directly connected, eth1, Area 0.0.0.0
```

```
R4#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP Timers:
Uptime

IP Route Table for VRF "default"
```

```
C      ::1/128 via ::, lo, 01:32:01
O      3ffe:10::/64 [110/2] via fe80::a00:27ff:fe0d:fbe3, eth3, 01:02:49
O3ffe:11::/64 [110/2] via fe80::a00:27ff:fecf:8873, eth1, 01:02:19
C3ffe:12::/64 via ::, eth3, 00:58:46
C3ffe:13::/64 via ::, eth1, 00:59:18
Cfe80::/64 via ::, eth1, 01:27:01
Kff00::/8 [0/256] via ::, eth3, 01:27:31
```

Virtual Links

Virtual links are used to connect a temporarily-disjointed non-backbone area to the backbone area, or to repair a noncontiguous backbone area. In this example, the ABR R3 has temporarily lost connection to Area 0, in turn disconnecting Area 2 from the backbone area. The virtual link between ABR R1 and ABR R2 connects Area 2 to Area 0. Area 1 is used as a transit area.

Topology

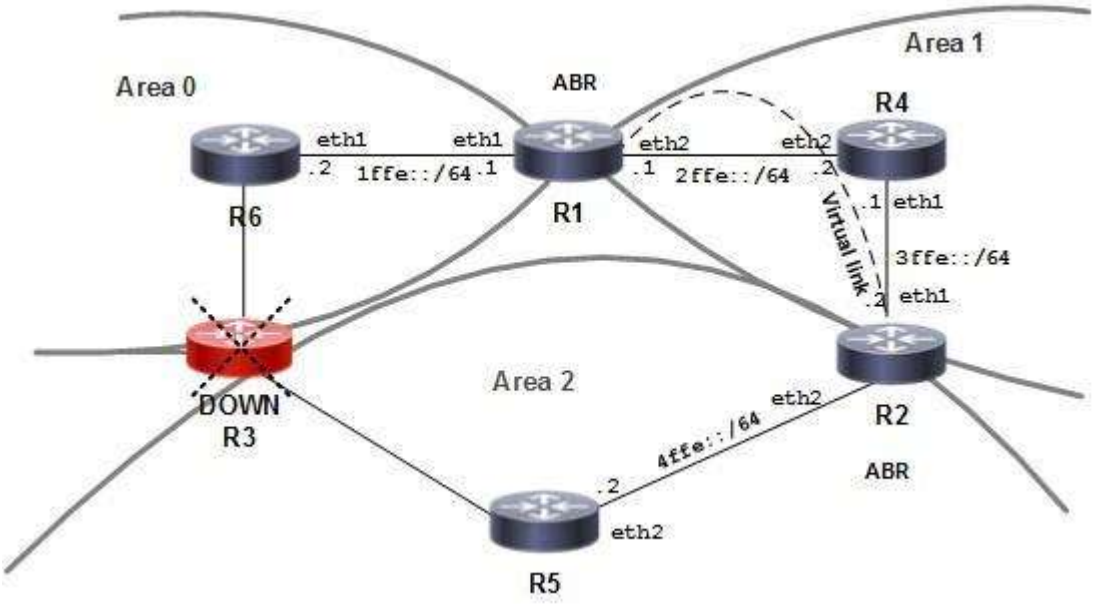


Figure 4-37: OSPFv3 Virtual Links

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to configure, and enter Interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on this interface, and assign the Area ID `(0)`.
`(config-if)#exit`	Exit interface mode.

(config)#interface eth2	Specify the interface (eth2) to configure, and enter Interface mode.
(config-if)#ipv6 router ospf area 1	Enable OSPFv3 routing on this interface, and assign the Area ID (1).
(config-if)#exit	Exit interface mode.
(config)#router ipv6 ospf	Create an OSPFv3 routing instance.
(config-router)#router-id 1.1.1.1	Specify a Router ID (1.1.1.1) for the OSPFv3 routing process.
(config-router)#area 1 virtual-link 2.2.2.2	Configure a virtual link between this router R1 and R2 (Router ID 2.2.2.2) through transit area 1.

R2

#configure terminal	Enter configure mode.
(config)#interface eth1	Specify the interface (eth1) to configure, and enter Interface mode.
(config-if)#ipv6 router ospf area 1	Enable OSPFv3 routing on this interface, and assign the Area ID (1).
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Specify the interface (eth2) to configure, and enter Interface mode.
(config-if)#ipv6 router ospf area 2	Enable OSPFv3 routing on this interface, and assign the Area ID (2).
(config-if)#exit	Exit interface mode.
(config)#router ipv6 ospf	Create an OSPFv3 routing instance.
(config-router)#router-id 2.2.2.2	Specify a Router ID (2.2.2.2) for the OSPFv3 routing process.
(config-router)#area 1 virtual-link 1.1.1.1	Configure a virtual link between this router R1 and R2 (Router ID 1.1.1.1) through transit area 1.

R4

#configure terminal	Enter configure mode.
(config)#interface eth1	Specify the interface (eth1) to configure, and enter Interface mode.
(config-if)#ipv6 router ospf area 1	Enable OSPFv3 routing on this interface, and assign the Area ID (1).
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Specify the interface (eth2) to configure, and enter Interface mode.
(config-if)#ipv6 router ospf area 1	Enable OSPFv3 routing on this interface, and assign the Area ID (1).
(config-if)#exit	Exit interface mode.
(config)#router ipv6 ospf	Create an OSPFv3 routing instance.
(config-router)#router-id 4.4.4.4	Specify a Router ID (4.4.4.4) for the OSPFv3 routing process.

R5

`#configure terminal`	Enter configure mode.
`(config)#interface eth2`	Specify the interface (`eth2`) to configure, and enter Interface mode.
`(config-if)#ipv6 router ospf area 2`	Enable OSPFv3 routing on this interface, and assign the Area ID `(2)`.
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 5.5.5.5`	Specify a Router ID (`5.5.5.5`) for the OSPFv3 routing process.

R6

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to configure, and enter Interface mode.
`(config-if)#ipv6 router ospf area 0`	Enable OSPFv3 routing on this interface, and assign the Area ID `(0)`.
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf`	Create an OSPFv3 routing instance.
`(config-router)#router-id 6.6.6.6`	Specify a Router ID (`6.6.6.6`) for the OSPFv3 routing process.

Validation

show ipv6 ospf virtual-links, show ipv6 ospf neighbor, show ipv6 ospf, show ipv6 ospf route

Multiple Instances

By using multiple OSPFv3 instances, OSPFv3 routes can be segregated, based on their instance number. Routes of one instance are stored differently from routes of another instance running in the same router.

To configure multiple OSPFv3 instances, refer to the topology diagram and follow the procedures below.

1. Enable OSPFv3 on an interface.
2. Enable multiple instances.
3. Configure redistribution among multiple instances.

   Note: Optionally, redistribution can be configured with the metric, type, or route-map options.

Topology

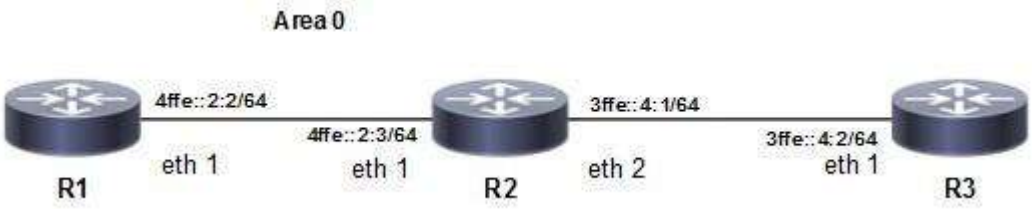


Figure 4-38: Multiple OSPFv3 Instances

Enable OSPFv3 on an Interface

This example shows how to enable OSPFv3 on an interface. R1 and R2 are two routers in Area 0 connecting to network 4ffe::2:/64.

R1

`(config)#router ipv6 ospf 10`	Configure an OSPFv3 instance with an instance ID of `10`.
`(config-router)#router-id 151.151.151.151`	Configure the router ID to use on this instance.
`(config-router)#exit`	Exit Router mode, and return to Interface mode.
`(config)#interface eth1`	Specify the interface on which OSPFv3 is to be enabled.
`(config-if)#ipv6 address 4ffe::2:2/64`	Configure the IPv6 address.
`(config-if)#ipv6 router ospf area 0 tag 10`	Configure the area number and instance value: match the instance ID with the instance ID created previously.
`(config-if)#no shutdown`	Activate the interface.

R2

`(config)#router ipv6 ospf 10`	Configure an OSPFv3 instance with an instance ID of `10`.
`(config-router)#router-id 152.152.152.152`	Configure the router ID to use on this instance.
`(config-router)#exit`	Exit Router mode, and return to Interface mode.
`(config)#interface eth1`	Specify the interface on which OSPFv3 is to be enabled.
`(config-if)#ipv6 address 4ffe::2:3/64`	Configure the IPv6 address.
`(config-if)#ipv6 router ospf area 0 tag 10`	Configure the area number and instance value: match the instance ID with the instance ID created previously.
`(config-if)#no shutdown`	Activate the interface.

Validation

show ipv6 interface brief, show ipv6 ospf route, show ipv6 ospf neighbor

Enable Multiple OSPFv3 Instances on a Router Based on Tags

In this example, routers R1, R2, and R3 are in Area 0, and all run OSPFv3.

R1

`(config)#router ipv6 ospf 5`	Configure an OSPFv3 instance with an instance ID of `5`.

(config-router)#router-id 5.5.5.5	Configure the router ID to use on this instance.
(config-router)#exit	Exit Router mode, and return to Interface mode.
(config)#interface eth1	Specify the interface on which OSPFv3 is to be enabled.
(config-if)#ipv6 address 4ffe::2:2/64	Configure the IPv6 address.
(config-if)#ipv6 router ospf area 0 tag 5	Configure the area number and instance value: match the instance ID with the instance ID created previously.
(config-if)#no shutdown	Activate the interface.

R2

(config)#router ipv6 ospf 5	Configure an OSPFv3 instance with an instance ID of 5.
(config-router)#router-id 149.149.149.149	Configure the router ID to use on this instance.
(config-router)#exit	Exit Router mode, and return to Interface mode.
(config)#interface eth1	Configure the interface to connect to R1.
(config-if)#ipv6 address 4ffe::2:3/64	Configure the IPv6 address.
(config-if)#ipv6 router ospf area 0 tag 5	Configure the area number and instance value: match the instance ID with the instance ID created previously.
(config-if)#no shutdown	Activate the interface.
(config)#router ipv6 ospf 15	Configure an OSPFv3 instance with an instance ID of 15.
(config-router)#router-id 159.159.159.159	Configure the router ID to use on this instance.
(config-router)#exit	Exit Router mode, and return to Interface mode.
(config)#interface eth2	Configure the interface to connect to R3.
(config-if)#ipv6 address 4ffe::4:1/64	Configure the IPv6 address.
(config-if)#no shutdown	Activate the interface.
(config-if)#ipv6 router ospf area 0 tag 15	Configure the area number and instance value: match the instance ID with the instance ID created previously.

R3

(config)#router ipv6 ospf 15	Configure an OSPFv3 instance with an instance ID of 15.
(config-router)#router-id 152.152.152.152	Configure the router ID to use on this instance.
(config-router)#exit	Exit Router mode, and return to Interface mode.
(config)#interface eth1	Specify the interface on which OSPFv3 is to be enabled.
(config-if)#ipv6 address 3ffe::4:2/64	Configure the IPv6 address.
(config-if)#ipv6 router ospf area 0 tag 15	Configure the area number and instance value: match the instance ID with the instance ID created previously.
(config-if)#no shutdown	Activate the interface.

Validation

R1

```
R1#show ipv6 ospf route
OSPFv3 Process (5)
```

```
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  4ffe:2::/64                                        1      directly
connected, eth1, Area 0.0.0.0

R1#show ipv6 ospf neighbor
OSPFv3 Process (5)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
149.149.149.149   1   Full/Backup     00:00:32    eth1       0
```

R2

```
R2#show ipv6 ospf route
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe:4::/64                                        1     directly
connected, eth2, Area 0.0.0.0
O  3ffe:12::/64                                       1     directly
connected, eth2, Area 0.0.0.0
O  3ffe:13::/64                                       2     via
fe80::a00:27ff:fe01:c94d, eth2, Area 0.0.0.0
OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  4ffe:2::/64                                        1     directly
connected, eth1, Area 0.0.0.0

R2#sh ipv6 ospf neighbor
OSPFv3 Process (15)
Neighbor ID     Pri   State           Dead Time    Interface Instance ID
152.152.152.152   1   Full/DR         00:00:35     eth2      0
OSPFv3 Process (5)
Neighbor ID     Pri   State           Dead Time    Interface Instance ID 5.5.5.5
1   Full/DR          00:00:33    eth1        0
```

R3

```
R3#show ipv6 ospf route
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
```

```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

    Destination                                    Metric
      Next-hop
C   3ffe:4::/64                                      1     directly
connected, eth1, Area 0.0.0.0
O   3ffe:12::/64                                     1     directly
connected, eth1, Area 0.0.0.0
O   3ffe:13::/64                                     2     via
fe80::a00:27ff:fe01:c94d, eth1, Area 0.0.0.0



R3#sh ipv6 ospf neighbor
OSPFv3 Process (15)
Neighbor ID      Pri   State           Dead Time   Interface  Instance ID
 159.159.159.159   1   Full/Backup     00:00:34    eth1       0
```

Redistribute among Multiple Instances

In this example, routes of one instance are redistributed to another instance to enable ping from R1 to R3 or vice versa; and R2 redistributes routes from one instance to another.

R2

(config)#router ipv6 ospf 15	Configure an OSPFv3 instance with instance ID 15.
(config-router)#router-id 159.159.159.159	Configure the router ID.
(config-router)#redistribute ospf 5	Redistribute instance 5 routes.
(config-router)#redistribute connected	Redistribute co routes to instance 15.
(config-router)#exit	Exit OSPF router mode.
(config)#router ipv6 ospf 5	Configure an OSPFv3 instance with instance ID 5.
(config-router)#router-id 149.149.149.149	Configure the router ID.
(config-router)#redistribute ospf 15	Redistribute instance 15 routes.
(config-router)#redistribute connected	Redistribute connected routes to instance 5.

Validation

R1

```
R1#show ipv6 ospf route
OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
```

```
E2 3ffe:4::/64                                        1/20
via fe80::a00:27ff:fef9:2432, eth1
C  4ffe:2::/64                                           1
directly connected, eth1, Area 0.0.0.0


rtr1#show ipv6 ospf neighbor
OSPFv3 Process (5)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
149.149.149.149   1   Full/Backup     00:00:32    eth1       0
```

R2

```
R2#show ipv6 ospf route
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                      Metric
Next-hop
C  3ffe:4::/64                                         1     directly
connected, eth2, Area 0.0.0.0
OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                      Metric
     Next-hop
C  4ffe:2::/64                                         1     directly
connected, eth1, Area 0.0.0.0

R2#show ipv6 ospf neighbor
OSPFv3 Process (15)
Neighbor ID     Pri   State           Dead Time    Interface Instance ID
152.152.152.152   1   Full/DR         00:00:34     eth2      0
OSPFv3 Process (5)
Neighbor ID     Pri   State           Dead Time    Interface Instance ID 5.5.5.5
1   Full/DR          00:00:30   eth1        0
```

R3

```
R3#show ipv6 ospf route
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
```

```
C  3ffe:4::/64                                        1     directly
connected, eth1, Area 0.0.0.0
E2 4ffe:2::/64                                      1/20     via
fe80::a00:27ff:fe0d:fbe3, eth1


R3#show ipv6 ospf neighbor
OSPFv3 Process (15)
Neighbor ID      Pri   State           Dead Time    Interface Instance ID
159.159.159.159    1   Full/Backup     00:00:33     eth1      0
```

Redistribute with Metric Option

In this example, on R3, R1 and R2 have each other's routes with a metric of 100.

R2

`(config)#router ipv6 ospf 15`	Configure an OSPFv3 instance with instance ID `15`.
`(config-router)#router-id 159.159.159.159`	Configure the router ID.
`(config-router)#redistribute ospf 5 metric 100`	Redistribute instance `15` routes with metric `100`.
`(config-router)#redistribute connected`	Redistribute connected routes to instance `15`.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#router ipv6 ospf 5`	Redistribute routes into instance `5`.
`(config-router)#router-id 149.149.149.149`	Configure the router ID.
`(config-router)#redistribute ospf 5 metric 100`	Redistribute instance `15` routes with metric `100`.
`(config-router)#redistribute connected`	Redistribute connected routes to instance `5`.

Validation

R1

```
R1#show ipv6 ospf route
OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                      Metric
     Next-hop
E2 3ffe:4::/64                                      1/20     via
fe80::a00:27ff:fef9:2432, eth1
C  4ffe:2::/64                                        1     directly
connected, eth1, Area 0.0.0.0

R1#show ipv6 ospf neighbor
```

```
OSPFv3 Process (5)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
149.149.149.149   1   Full/Backup     00:00:36    eth1       0
```

R2

```
R2#show ipv6 ospf route
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe:4::/64                                        1     directly
connected, eth2, Area 0.0.0.0
OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  4ffe:2::/64                                        1     directly
connected, eth1, Area 0.0.0.0
R2#show ipv6 ospf neighbor
OSPFv3 Process (15)
Neighbor ID     Pri   State           Dead Time    Interface Instance ID
152.152.152.152   1   Full/DR         00:00:33     eth2      0
OSPFv3 Process (5)
Neighbor ID     Pri   State           Dead Time    Interface Instance ID 5.5.5.5
1   Full/DR          00:00:40   eth1        0
```

R3

```
R3#show ipv6 ospf route
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe:4::/64                                        1     directly
connected, eth1, Area 0.0.0.0
E2 4ffe:2::/64                                      1/20    via
fe80::a00:27ff:fe0d:fbe3, eth1
```

```
R3#show ipv6 ospf neighbor
OSPFv3 Process (15)
Neighbor ID      Pri   State           Dead Time   Interface  Instance ID
159.159.159.159    1   Full/Backup     00:00:37    eth1       0
```

Redistribute with Type Option

In this example, on R3, R1 has R3 routes as type 2, and R2 has R1 routes as type 1.

R2

`(config)#router ipv6 ospf 15`	Configure an OSPFv3 instance with instance ID `15`.
`(config-router)#router-id 159.159.159.159`	Configure the router ID.
`(config-router)#redistribute ospf 5 metrictype 1`	Redistribute instance `15` routes as type `1`.
`(config-router)#redistribute connected`	Redistribute connected routes to instance `15`.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#router ipv6 ospf 5`	Redistribute routes into instance `5`.
`(config-router)#router-id 149.149.149.149`	Configure the router ID.
`(config-router)#redistribute ospf 15 metrictype 2`	Redistribute instance `15` routes with type `2`.
`(config-router)#redistribute connected`	Redistribute instance `15` as type `2`.

Validation

R1

```
R1#show ipv6 ospf route
OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
E2 3ffe:4::/64                                      1/20     via
fe80::a00:27ff:fef9:2432, eth1
C  4ffe:2::/64                                         1     directly
connected, eth1, Area 0.0.0.0


rtr1#show ipv6 ospf neighbor
OSPFv3 Process (5)
Neighbor ID      Pri   State           Dead Time    Interface Instance I
D
149.149.149.149    1   Full/Backup     00:00:32     eth1      0 R2

R2#show ipv6 ospf route
```

```
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C   3ffe:4::/64                                      1     directly
connected, eth2, Area 0.0.0.0
OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C   4ffe:2::/64                                      1     directly
connected, eth1, Area 0.0.0.0

R2#show ipv6 ospf neighbor
OSPFv3 Process (15)
Neighbor ID      Pri   State           Dead Time   Interface  Instance I
D
152.152.152.152    1   Full/DR         00:00:36    eth2       0
OSPFv3 Process (5)
Neighbor ID      Pri   State           Dead Time   Interface  Instance I
D
5.5.5.5            1   Full/DR         00:00:32    eth1       0
```

R3

```
R3#show ipv6 ospf neighbor
OSPFv3 Process (15)
Neighbor ID      Pri   State           Dead Time   Interface  Instance I
D
159.159.159.159    1   Full/Backup     00:00:36    eth1       0
R3#show ipv6 ospf route
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C   3ffe:4::/64                                      1     directly
connected, eth1, Area 0.0.0.0
 E2 4ffe:2::/64                                   1/20     via
fe80::a00:27ff:fe0d:fbe3, eth1


R3#show ipv6 ospf neighbor
```

```
OSPFv3 Process (15)
Neighbor ID      Pri   State           Dead Time   Interface  Instance I
D
159.159.159.159    1   Full/Backup     00:00:36    eth1       0
```

Redistribute with Route-Map Option

R2

`(config)#router ipv6 ospf 15`	Configure an OSPFv3 instance with instance ID `15`.
`(config-router)#router-id 159.159.159.159`	Configure the router ID.
`(config-router)#redistribute ospf 5 route-map 1`	Redistribute instance `5` routes with route map `1`.
`(config-router)#redistribute connected`	Redistribute connected routes to instance `15`.
`(config-router)#exit`	Exit OSPF router mode.
`(config)#router ipv6 ospf 5`	Redistribute routes into instance `5`.
`(config-router)#router-id 149.149.149.149`	Configure the router ID.
`(config-router)#redistribute ospf 15 routemap 1`	Redistribute instance `15` routes with route map `1`.
`(config-router)#redistribute connected`	Redistribute connected routes to instance `15`.

Validation

R1

```
R1#show ipv6 ospf route
OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
E2 3ffe:4::/64                                      1/20      via
fe80::a00:27ff:fef9:2432, eth1
C  4ffe:2::/64                                         1      directly
connected, eth1, Area 0.0.0.0


R1#show ipv6 ospf neighbor
OSPFv3 Process (5)
Neighbor ID     Pri   State           Dead Time   Interface  Instance I
D
149.149.149.149   1   Full/DR         00:00:34    eth1       0
```

R2

```
R2#sh ipv6 ospf route
OSPFv3 Process (15)
```

```
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  3ffe:4::/64                                        1     directly
connected, eth2, Area 0.0.0.0
OSPFv3 Process (5)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  4ffe:2::/64                                        1     directly
connected, eth1, Area 0.0.0.0

R2#sh ipv6  ospf neighbor
OSPFv3 Process (15)
Neighbor ID      Pri   State           Dead Time    Interface Instance ID
152.152.152.152    1   Full/Backup     00:00:32     eth2      0
OSPFv3 Process (5)
Neighbor ID      Pri   State           Dead Time    Interface Instance ID 5.5.5.5
1   Full/Backup      00:00:38    eth1        0
```

R3

```
R3#show ipv6 ospf route
OSPFv3 Process (15)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                   Metric
     Next-hop
C  3ffe:4::/64                                       1
     directly connected, eth1, Area 0.0.0.0
E2 4ffe:2::/64                                     1/20
via fe80::a00:27ff:fe0d:fbe3, eth1

R3#show ipv6 ospf neighbor
OSPFv3 Process (15)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
159.159.159.159   1   Full/DR         00:00:34    eth1       0 R3#
```

Graceful Restart

The possibility of maintaining a router's data forwarding capability while the router's control software restarts is called graceful restart or non-stop forwarding. After the router restarts and reloads, it must change its OSPF processing until it re-establishes full adjacencies with all its former fully adjacent neighbors. The time period between the restart/reload and

re-establishment of adjacencies is called the grace period. Essentially, the OSPF procedure for graceful restart is as follows:

- The router attempting a graceful restart originates link-local Opaque-LSAs, called Grace-LSAs, announcing its intention to perform a graceful restart within a specified amount of time (grace period).
- During the grace period, neighbors continue to announce the restarting router in their LSAs as if it were fully adjacent (OSPF neighbor state Full), but only if the network topology remains static (the contents of the LSAs in the link-state database that have LS types 1-5 and 7 remain unchanged, and periodic refreshes are allowed).

Topology

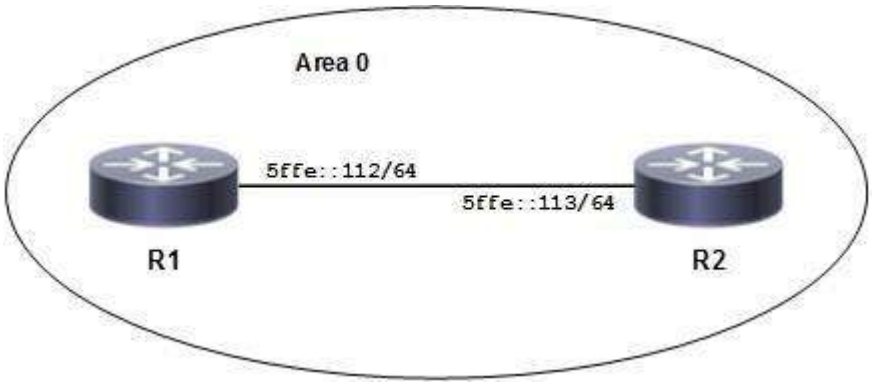


Figure 4-39: OSPFv3 Graceful Restart

Configure R1 for Graceful Restart

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to configure, and enter Interface mode.
`(config-if)#ipv6 address 5ffe::112/64`	Assign the IPv6 address to the interface.
`(config-if)#ipv6 router ospf area 0 tag 1`	Configure the interface for OSPFv3 on area 0.
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf 1`	Create an OSPFv3 routing instance.
`(config-router)#router-id 1.1.1.1`	Specify a Router ID (`1.1.1.1`) for the OSPFv3 routing process.
`(config-router)#capability restart graceful`	Enable graceful restart capability.
`(config-router)#end`	Exit Configure mode and enter Privileged Exec mode.
`#write`	Save the configuration.
`#restart ipv6 ospf graceful grace-period 200`	Restart OSPFv3 with a 200-second grace period, so that the neighbor maintains adjacency and preserves the routes for 200 seconds.

Configure R2 as Restart Helper

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to configure, and enter Interface mode.

(config-if)#ipv6 address 5ffe::113/64	Assign the IPv6 address to the interface.
(config-if)#ipv6 router ospf area 0 tag 1	Configure the interface for OSPFv3 on area 0.
(config-if)#exit	Exit interface mode.
(config)#router ipv6 ospf 1	Create an OSPFv3 routing instance.
(config-router)#router-id 2.2.2.2	Specify a Router ID (2.2.2.2) for the OSPFv3 routing process.
(config-router)#exit	Exit Router mode and enter Configure mode.
(config)#ipv6 ospf restart helper max-graceperiod 300	Configure R2 to act as the helper when the grace period is less than 300.

Remove Helper Configuration from R2

#configure terminal	Enter configure mode.
(config)#router ipv6 ospf 1	Create an OSPFv3 routing instance.
(config-router)#router-id 1.1.1.1	Specify a Router ID (1.1.1.1) for the OSPFv3 routing process.
(config-router)#exit	Exit Router mode and enter Configure mode.
(config)#ipv6 ospf restart helper never	Configure R2 to not work as the helper.

Make R2 Helper when Restart Reason is Reload

#configure terminal	Enter configure mode.
(config)#router ipv6 ospf 1	Create an OSPFv3 routing instance.
(config-router)#router-id 1.1.1.1	Specify a Router ID (1.1.1.1) for the OSPFv3 routing process.
(config-router)#exit	Exit Router mode and enter Configure mode.
(config)#ipv6 ospf restart helper only-reload	Configure R2 to work as the helper only when the restart reason is reload.

Make R2 Helper when Restart Reason is Upgrade

#configure terminal	Enter configure mode.
(config)#router ipv6 ospf 1	Create an OSPFv3 routing instance.
(config-router)#router-id 1.1.1.1	Specify a Router ID (1.1.1.1) for the OSPFv3 routing process.
(config-router)#exit	Exit Router mode and enter Configure mode.
(config)#ipv6 ospf restart helper onlyupgrade	Configure R2 to work as the helper only when the restart reason is upgrade.

Validation

R1 After Configuring Graceful Restart

```
R1#show ipv6 ospf neighbor
OSPFv3 Process (1)
```

```
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
2.2.2.2           1   Full/DR         00:00:39    eth1       0


R1#show ipv6 ospf route
OSPFv3 Process (1)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  5ffe::/64                                         1      directly
connected, eth1, Area 0.0.0.0




rtr1#show ipv6 route IPv6 Routing
Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP
Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 02:02:28
C      5ffe::/64 via ::, eth1, 00:23:16
C      fe80::/64 via ::, eth1, 01:25:04 K      ff00::/8
[0/256] via ::, eth0, 01:25:05



rtr1#show ipv6 ospf database grace

            OSPFv3 Router with ID (1.1.1.1) (Process 1)
```

R1 After Graceful Restart

```
R1#show ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
2.2.2.2           1   Full/DR         00:00:37    eth1       0



rtr1#show ipv6 ospf route
OSPFv3 Process (1)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
```

```
     Next-hop
C  5ffe::/64                                          1      directly
connected, eth1, Area 0.0.0.0


rtr1#show ipv6 route IPv6 Routing
Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 02:02:28
C      5ffe::/64 via ::, eth1, 00:23:16
C      fe80::/64 via ::, eth1, 01:25:04 K      ff00::/8
[0/256] via ::, eth1, 01:25:05



rtr1#show ipv6 ospf database grace

            OSPFv3 Router with ID (1.1.1.1) (Process 1)
```

R2 Before Graceful Restart

```
R2#show ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID      Pri   State           Dead Time   Interface  Instance ID
1.1.1.1            1   Full/Backup     00:00:40    eth1       0


R2#sh ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID      Pri   State           Dead Time   Interface  Instance ID
1.1.1.1            1   Full/Backup     00:00:40    eth1       0
R2#
R2#show ipv6 ospf route
OSPFv3 Process (1)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  5ffe::/64                                          1      directly
connected, eth1, Area 0.0.0.0


R2#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
```

```
       IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF
       external type 2, N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
       external type 2, I - IS-IS, B - BGP Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 01:54:20
C      5ffe::/64 via ::, eth1, 00:12:16
Cfe80::/64 via ::, eth2, 01:17:21
Kff00::/8 [0/256] via ::, eth1, 01:19:12



R2#show ipv6 ospf database grace

            OSPFv3 Router with ID (2.2.2.2) (Process 1)
```

R2 During graceful restart

```
R2#show ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
1.1.1.1           1   Full/Backup     00:02:25*    eth1       0


R2#show ipv6 ospf route
OSPFv3 Process (1)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  5ffe::/64                                         1      directly
connected, eth1, Area 0.0.0.0


R2#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP Timers: Uptime
IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 01:57:26
C      5ffe::/64 via ::, eth1, 00:15:22
Cfe80::/64 via ::, eth2, 01:20:27
Kff00::/8 [0/256] via ::, eth1, 01:22:18


R2#show ipv6 ospf database grace

            OSPFv3 Router with ID (2.2.2.2) (Process 1)

                Grace-LSA (Interface eth1)
```

```
  LS age: 65
  LS Type: Grace LSA
  Link State ID: 0.0.0.3
  Advertising Router: 1.1.1.1
  LS Seq Number: 0x80000001
  Checksum: 0x1660   Length: 36

      Grace Period: 200
      Restart Reason:
           Software Restart
```

R2 After graceful restart

```
R2#show ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
1.1.1.1           1   Full/Backup     00:00:34    eth1       0



R2#show ipv6 ospf route
OSPFv3 Process (1)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination                                    Metric
     Next-hop
C  5ffe::/64                                          1      directly
connected, eth1, Area 0.0.0.0


R2#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 02:07:14
C      5ffe::/64 via ::, eth1, 00:25:10
Cfe80::/64 via ::, eth2, 01:30:15
Kff00::/8 [0/256] via ::, eth2, 01:30:17

R2#show ipv6 ospf database grace

            OSPFv3 Router with ID (2.2.2.2) (Process 1)
```

Not-So-Stubby Area

This section contains OSPFv3 NSSA (Not-So-Stubby Area) configuration examples.

An NSSA allows external routes to be advertised into the OSPF autonomous system while retaining the characteristics of a stub area to the rest of the autonomous system. To do this, the ASBR in an NSSA will originate type 7 LSAs to advertise the external destinations. These NSSA external LSAs are flooded throughout the NSSA but are blocked at the ABR.

The NSSA external LSA has a flag in its header known as the P-bit. The NSSA ASBR has the option of setting or clearing the P-bit. If an NSSA's ABR receives a type 7 LSA with the P-bit set to one, it translates the type 7 LSA into a type 5 LSA and floods it throughout the other areas. If the P-bit is set to zero, no translation takes place and the destination in the type 7 LSA is not advertised outside of the NSSA.

Topology

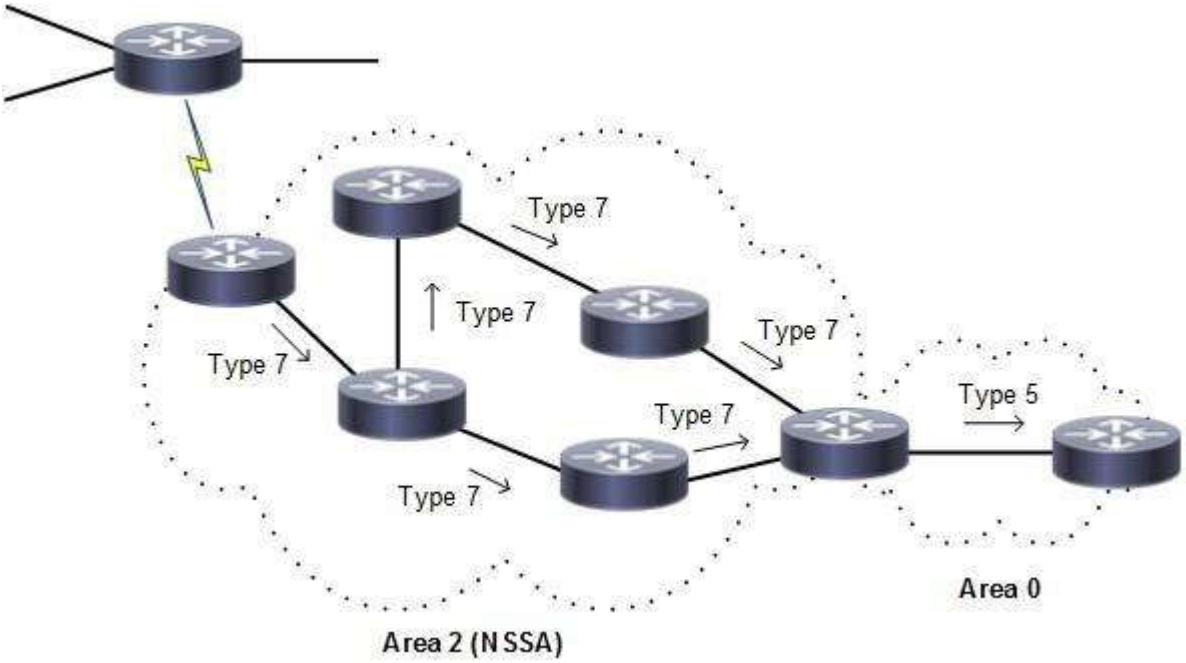


Figure 4-40: Translating Type 7 LSAs into Type 5 LSAs

NSSA with Route Options

This example shows the configuration to enable NSSA and to configure different route options for NSSA. There are three `area nssa` command options for originating default Type-3 LSA and default Type-7 LSA, and for blocking redistribution of Type-7 LSA into an NSSA:

- `no-summary`: The NSSA ABR blocks all type-3 and type-4 LSAs into the NSSA area and sends a single type-3 LSA into the area to advertise a default route
- `default-information-originate`: The NSSA ABR advertises a default route into the NSSA as a type-7 LSA.
- `no-redistribution`: The NSSA ABR bocks type-7 LSA from being redistributed into the NSSA area.

In Figure 4-41, R2 is an NSSA ABR as well as an NSSA ASBR that maps the router interfaces to two different areas and redistributes the connected routes of the loopback interface. Also, this example sets the `no-summary`, `noredistribution`, and `default-information-originate` options on R2 to originate default Type-3 LSAs and default Type-7 LSAs into the NSSA and to block Type-7 LSAs.

Topology

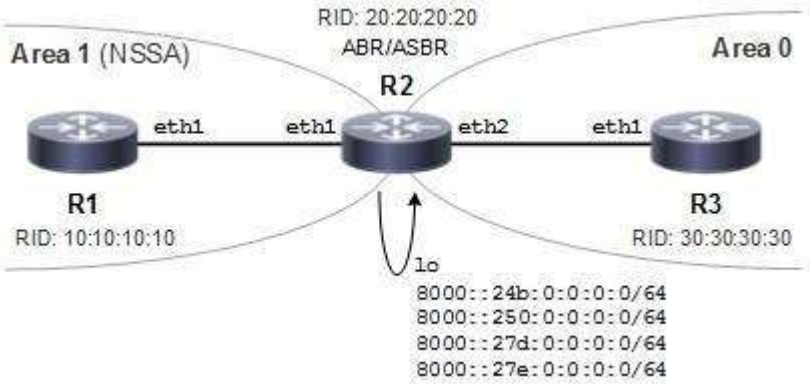


Figure 4-41: NSSA with Route Options

R1

`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ipv6 router ospf tag 100 area 1`	Configure interface in an area assigned with the area ID (1).
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf 100`	Configure the routing process and specify the tag (`100`).
`(config-router)#router-id 10.10.10.10`	Configure the router ID to use on this instance (100)
`(config-router)#area 1 nssa`	Configure area as NSSA
`(config-router)#exit`	Exit interface mode

R2

`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ipv6 router ospf tag 100 area 1`	Configure interface in an area assigned with the area ID (1).
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode for `eth2`
`(config-if)#ipv6 router ospf tag 100 area 0`	Configure interface in backbone
`(config-if)#interface lo`	Enter interface mode for Loopback
`(config-if)#ipv6 address 8000::24b:0:0:0:0/64`	Assign IPv6 address to loopback interface
`(config-if)#ipv6 address 8000::250:0:0:0:0/64`	Assign IPv6 address to loopback interface
`(config-if)#ipv6 address 8000::27d:0:0:0:0/64`	Assign IPv6 address to loopback interface
`(config-if)#ipv6 address 8000::27e:0:0:0:0/64`	Assign IPv6 address to loopback interface
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf 100`	Configure the routing process and specify the tag (`100`).
`(config-router)#router-id 20.20.20.20`	Configure the router ID to use on this instance (100)
`(config-router)#redistribute connected`	Redistribute the configured loopback network into the NSSA

`(config-router)#area 1 nssa no-redistribution default-information-originate no-summary`	Configure the Router to originate default Type-3 LSAs and default Type-7 LSAs, and to block Type-7 LSAs into the NSSA
`(config-router)#exit`	Exit interface mode

R3

`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ipv6 router ospf tag 100 area 0`	Configure interface in an area assigned with the area ID (1).
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf 100`	Configure the routing process and specify the tag (`100`).
`(config-router)#router-id 30.30.30.30`	Configure the router ID to use on this instance (100)
`(config-router)#exit`	Exit interface mode

Validation 1

In the output of `show ipv6 ospf neighbor` below, verify that OSPFv3 adjacency is in state “full” for both R1 and R2 under the process identifier 100.

```
R1#sh ipv6 ospf neighbor
OSPFv3 Process (100)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
20.20.20.20       1   Full/DR         00:00:34    eth2       0

R2#sh ipv6 ospf neighbor
OSPFv3 Process (100)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
10.10.10.10       1   Full/Backup     00:00:38    eth1       0
```

Validation 2

The output below shows originating default Type-3 LSAs into the NSSA with the no-summary option. The advertising router identifier is for R2 (20.20.20.20, the NSSA-ABR). Also, the prefix is ::/0 and the LS-Type is Inter-Area-Prefix-LSA for the default Type-3 LSA route into the NSSA.

```
R1#sh ipv6 ospf database inter-prefix

            OSPFv3 Router with ID (10.10.10.10) (Process 100)

                Inter-Area-Prefix-LSA (Area 0.0.0.1)
  LS age: 1234
  LS Type: Inter-Area-Prefix-LSA
  Link State ID: 0.0.0.6
  Advertising Router: 20.20.20.20
  LS Seq Number: 0x80000001
  Checksum: 0x17D0
  Length: 28
    Metric: 1
    Prefix: ::/0
    Prefix Options: 0
```

Validation 3

The output below shows originating default type-7 LSAs alone after setting the no-redistribution and default-information originate options. The advertising router identifier is for R2 (20.20.20.20, the NSSA-ABR). Also, the prefix is ::/0 and LS-Type is NSSA-external-LSA for the default Type-7 LSA route into the NSSA

```
R1#sh ipv6 ospf database nssa-external

            OSPFv3 Router with ID (10.10.10.10) (Process 100)

                NSSA-external-LSA (Area 0.0.0.1)

  LS age: 1758
  LS Type: NSSA-external-LSA
  Link State ID: 0.0.0.20
  Advertising Router: 20.20.20.20
  LS Seq Number: 0x80000002
  Checksum: 0x6468
  Length: 32
    Metric Type: 2 (Larger than any link state path)
    Metric: 1
    Prefix: ::/0
    Prefix Options: 0 (-|-|-|-)
    External Route Tag: 0
```

NSSA with the Summary Address Option

Figure 4-42 shows the configuration to originate external LSAs (Type-7) and translate them into external LSAs (Type5):

- R1 is an NSSA-ASBR configured with loopback IPv6 addresses that are redistributed into OSPFv3
- R2 is an NSSA-ABR
- R3 is backbone router

R1 originates Type-7 LSAs which are summarized into a single Type-7 into the NSSA by the `summary-address` option and this summarized Type-7 is converted to Type-5 LSA by R2.

Also, the summarized route can be tagged using the `tag` command and the advertisement of summarized routes can be suppressed by the `not-advertise` option.

Topology

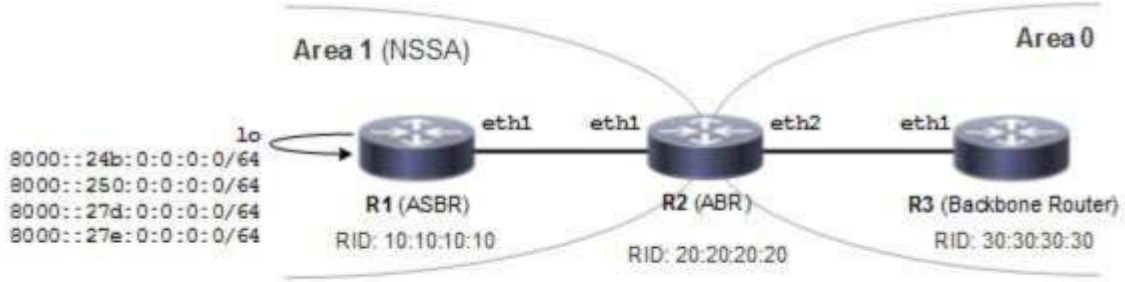


Figure 4-42: Using the summary-address Option

Configuration

R1

(config)#interface eth1	Enter interface mode for eth1.
(config-if)#ipv6 router ospf tag 100 area 1	Configure interface in an area assigned with the area ID (1).
(config-if)#exit	Exit interface mode.
(config-if)#interface lo	Enter interface mode for loopback
(config-if)#ipv6 address 8000::24b:0:0:0:0/64	Assign IPv6 address to loopback interface
(config-if)#ipv6 address 8000::250:0:0:0:0/64	Assign IPv6 address to loopback interface
(config-if)#ipv6 address 8000::27d:0:0:0:0/64	Assign IPv6 address to loopback interface
(config-if)#ipv6 address 8000::27e:0:0:0:0/64	Assign IPv6 address to loopback interface
(config-if)#exit	Exit interface mode.
(config)#router ipv6 ospf 100	Configure the routing process and specify the tag (100).
(config-router)#router-id 10.10.10.10	Configure the router ID to use on this instance (100)
(config-router)#area 1 nssa	Configure the area as NSSA.
(config-router)#redistribute connected	Redistribute the configured loopback network into OSPFv3 NSSA. Note: Connected networks can be redistributed by setting the metric and metric type.
(config-router)#summary-address 8000::/48 tag 10	Summarize the address range and tag the summarized route
(config-router)#exit	Exit interface mode

R2

(config)#interface eth1	Enter interface mode for eth1.
(config-if)#ipv6 router ospf tag 100 area 1	Configure interface in an area assigned with the area ID (1).
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode for eth2
(config-if)#ipv6 router ospf tag 100 area 0	Configure interface in backbone area (0)
(config-if)#exit	Exit interface mode.
(config)#router ipv6 ospf 100	Configure the routing process and specify the tag (100).
(config-router)#router-id 20.20.20.20	Configure the router ID to use on this instance (100)
(config-router)#area 1 nssa	Configure the Router in NSSA
(config-router)#exit	Exit interface mode

R3

(config)#interface eth1	Enter interface mode for eth1.
(config-if)#ipv6 router ospf tag 100 area 0	Configure interface in backbone area (0)

(config-if)#exit	Exit interface mode.
(config)#router ipv6 ospf 100	Configure the routing process and specify the tag (100).
(config-router)#router-id 30.30.30.30	Configure the router ID to use on this instance (100)
(config-router)#exit	Exit interface mode

In the configurations above, you can suppress the external route summarization by NSSA-ASBR by specifying the not-advertise parameter as shown below:

```
(config-router)#summary-address 8000::/48 not-advertise
```

Also, connected networks can be redistributed by setting the metric and metric type as shown below:

```
(config-router)#redistribute connected metric 20 metric-type 1
```

Validation 1

The output below shows the summarized route generated by NSSA-ASBR (R1) with a tag. The output has the LS Type as NSSA-external-LSA with advertising router identifier (10.10.10.10) of the NSSA-ASBR (R1). Also, check the Prefix which is summarized route and external route tag as configured.

```
R1#sh ipv6 ospf database nssa-external

            OSPFv3 Router with ID (10.10.10.10) (Process 100)

NSSA-external-LSA (Area 0.0.0.1)

  LS age: 90
  LS Type: NSSA-external-LSA   Advertising Router:
10.10.10.10
  Link State ID: 0.0.0.11
  LS Seq Number: 0x80000003
  Checksum: 0x69B3
  Length: 40
    Metric Type: 2 (Larger than any link state path)
    Metric: 21
    Prefix: 8000::/48     External Route Tag: 10
    Prefix Options: 8 (P|-|-|-)
```

Validation 2

```
The output below on the NSSA-ABR that is translating Type-7 LSAs to Type-5
LSAs shows summarized address in Type-7 and Type-5 LSA. Check for the
same prefix, external route tag in both Type7 and Type-5 LSA. R2#sh ipv6
ospf database nssa-external

            OSPFv3 Router with ID (20.20.20.20) (Process 100)

                NSSA-external-LSA (Area 0.0.0.1)

  LS age: 241
  LS Type: NSSA-external-LSA
  Link State ID: 0.0.0.11
  Advertising Router: 10.10.10.10
  LS Seq Number: 0x80000003
```

```
  Checksum: 0x69B3
  Length: 40
    Metric Type: 2 (Larger than any link state path)
    Metric: 21
    Prefix: 8000::/48
    Prefix Options: 8 (P|-|-|-)
External Route Tag: 10

R2#sh ipv6 ospf database external

            OSPFv3 Router with ID (20.20.20.20) (Process 100)

                AS-external-LSA

  LS age: 245
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.3
  Advertising Router: 20.20.20.20
  LS Seq Number: 0x80000003
  Checksum: 0x8660
  Length: 40
    Metric Type: 2 (Larger than any link state path)
    Metric: 21
    Prefix: 8000::/48
    Prefix Options: 0 (-|-|-|-)
    External Route Tag: 10
```

Validation 3

The output below on the backbone router shows the summarized address in the translated Type-5 LSA. The prefix and external route tag are the same as the summarized Type-7 LSA originated by R1.

```
R3#sh ipv6 ospf database external

            OSPFv3 Router with ID (30.30.30.30) (Process 100)

                AS-external-LSA

  LS age: 409
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.3
  Advertising Router: 20.20.20.20
  LS Seq Number: 0x80000003
  Checksum: 0x8660
  Length: 40
    Metric Type: 2 (Larger than any link state path)
    Metric: 21
    Prefix: 8000::/48
    Prefix Options: 0 (-|-|-|-)
    External Route Tag: 10
```

NSSA with the Translator Role Option

Type-7 to Type-5 translation is done by an NSSA-ABR. If an NSSA has multiple NSSA-ABRs, only one will perform the translation. The NSSA-ABR translator role options are:

- Candidate (default)
- Always

In the topology in Figure 4-43:

- R1 is NSSA-ASBR
- R2 and R3 are NSSA-ABRs
- R4 is a backbone router

In this example, the NSSA translator role `candidate` is configured on both NSSA-ABRs (R2 and R3). The Type-7 to Type-5 translation is done by the router with the higher router identifier (R3).

Topology

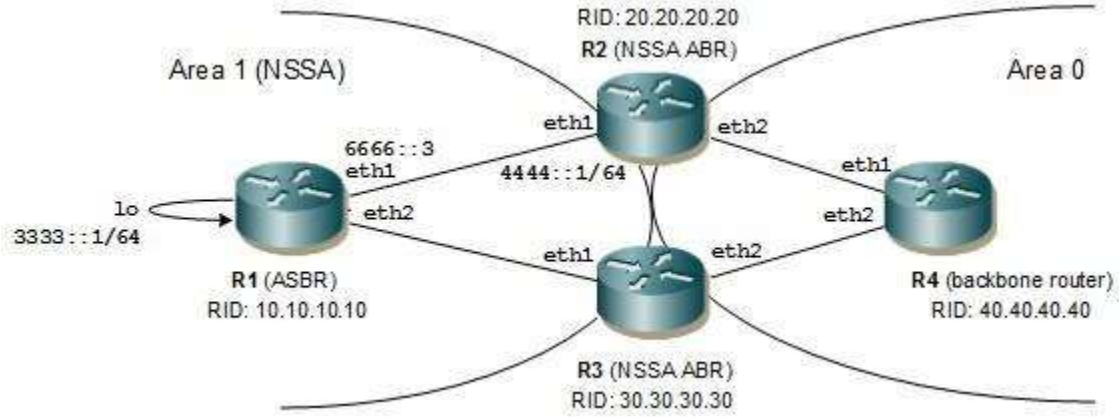


Figure 4-43: Using the translator-role Option

Configuration

When one NSSA-ABR is configured with the translator role as `always` and the other as `candidate`, then translation is done by the router configured as `always`. In this scenario, the translation can be biased by setting the translator role to `always` on the router that has the lower router identifier.

R1

`(config)#interface eth1`	Enter interface mode for `eth1`.
`(config-if)#ipv6 router ospf tag 100 area 1`	Configure interface in an area assigned with the area ID (1).
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode for `eth2`.
`(config-if)#ipv6 router ospf tag 100 area 1`	Configure interface in an area assigned with the area ID (1).
`(config-if)#exit`	Exit interface mode.
`(config-if)#interface lo`	Enter interface mode for Loopback
`(config-if)#ipv6 address 3333::1/64`	Assign IPv6 address to loopback interface

(config-if)#exit	Exit interface mode.
(config)#router ipv6 ospf 100	Configure the routing process and specify the tag (100).
(config-router)#router-id 10.10.10.10	Configure the router ID to use on this instance (100)
(config-router)#area 1 nssa	Configure the area as NSSA.
(config-router)#redistribute static	Redistribute the static route configured into the OSPF NSSA
(config-router)#redistribute connected	Redistribute the connected network into OSPF NSSA
(config-router)#exit	Exit interface mode
(config)#ipv6 route 4444::1/64 6666::3	Configure the static route with the nexthop address as R2's eth1 IPv6 address
(config)#exit	Exit interface mode.

R2

(config)#interface eth1	Enter interface mode for eth1.
(config-if)#ipv6 router ospf tag 100 area 1	Configure interface in an area assigned with the area ID (1).
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode for eth2
(config-if)#ipv6 router ospf tag 100 area 0	Configure interface in backbone area (0)
(config-if)#exit	Exit interface mode.
(config)#router ipv6 ospf 100	Configure the routing process and specify the tag (100).
(config-router)#router-id 20.20.20.20	Configure the router ID to use on this instance (100)
(config-router)#area 1 nssa translator-role candidate	Configure the NSSA-ABR with the translator role candidate.
(config-router)#exit	Exit interface mode

R3

(config)#interface eth1	Enter interface mode for eth1.
(config-if)#ipv6 router ospf tag 100 area 1	Configure interface in an area assigned with the area ID (1).
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode for eth2
(config-if)#ipv6 router ospf tag 100 area 0	Configure interface in backbone area (0)
(config-if)#exit	Exit interface mode.
(config)#router ipv6 ospf 100	Configure the routing process and specify the tag (100).
(config-router)#router-id 30.30.30.30	Configure the router ID to use on this instance (100)
(config-router)#area 1 nssa translator-role candidate	Configure the NSSA-ABR with the translator role candidate.
(config-router)#exit	Exit interface mode

R4

(config)#interface eth1	Enter interface mode for eth1.
(config-if)#ipv6 router ospf tag 100 area 0	Configure interface in backbone area (0)

(config)#interface eth2	Enter interface mode for eth2
(config-if)#ipv6 router ospf tag 100 area 0	Configure interface in backbone area (0)
(config-if)#exit	Exit interface mode.
(config)#router ipv6 ospf 100	Configure the routing process and specify the tag (100).
(config-router)#router-id 40.40.40.40	Configure the router ID to use on this instance (100)
(config-router)#exit	Exit interface mode

The command to configure the NSSA-Translator role as always is:

```
(config-router)#area 1 nssa translator-role always
```

The NSSA-ABR can continue to perform translation after its services are no longer required for the stability interval which is set using the command below on the NSSA-ABR.

```
(config-router)#area 1 nssa stability-interval 7777
```

Validation 1

The translation is done by the NSSA-ABR with the higher router identifier. In the output below, check the router identifier of the NSSA-ABR. Also, check the router which is elected and the router which is disabled.

```
R2#sh ipv6 ospf
 Routing Process "OSPFv3 (100)" with ID
 20.20.20.20 Process uptime is 21 minutes
 SPF schedule delay min 0.500 secs, SPF schedule delay max 50.0
 secs Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
 Number of incoming current DD exchange neighbors
 0/5 Number of outgoing current DD exchange
 neighbors 0/5 Number of external LSA 4. Checksum
 Sum 0x1F816 Number of AS-Scoped Unknown LSA 0
 Number of LSA originated 28
 Number of LSA received 58
 Number of areas in this router is 2
    Area BACKBONE(0)
        Number of interfaces in this area is 1(1)
        SPF algorithm executed 7 times
        Number of LSA 19.  Checksum Sum 0x7454D
        Number of Unknown LSA 0
    Area 0.0.0.1 (NSSA)
        Number of interfaces in this area is 1(1)
        SPF algorithm executed 14 times
        Number of LSA 19.  Checksum Sum 0xA4D18
        Number of Unknown LSA 0
        NSSA Translator State is disabled
R3#sh ipv6 ospf
 Routing Process "OSPFv3 (100)" with ID
 30.30.30.30 Process uptime is 19 minutes
 SPF schedule delay min 0.500 secs, SPF schedule delay max 50.0
 secs Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
 Number of incomming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
```

```
Number of external LSA 4. Checksum Sum 0x1F816
Number of AS-Scoped Unknown LSA 0
Number of LSA originated 31
Number of LSA received 69
Number of areas in this router is 2
   Area BACKBONE(0)
       Number of interfaces in this area is 1(1)
       SPF algorithm executed 15 times
       Number of LSA 19.  Checksum Sum 0x7454D
       Number of Unknown LSA 0
   Area 0.0.0.1 (NSSA)
       Number of interfaces in this area is 1(1)
       SPF algorithm executed 10 times
       Number of LSA 19.  Checksum Sum 0xA4D18
       Number of Unknown LSA 0
       NSSA Translator State is elected
```

Validation 2

The translated Type-5 LSA in R4 in area 0 has the advertising router identifier of R3. In the output below, the LS Type is AS-External-LSA and the advertising router has the higher router identifier.

```
R4#sh ipv6 ospf database external

            OSPFv3 Router with ID (40.40.40.40) (Process 100)

                AS-external-LSA

  LS age: 885
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.7
  Advertising Router: 30.30.30.30
  LS Seq Number: 0x80000001
  Checksum: 0xD3FE
  Length: 40
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 3333::/64
    Prefix Options: 0 (-|-|-|-)
    External Route Tag: 0


  LS age: 18
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.8
  Advertising Router: 30.30.30.30
  LS Seq Number: 0x80000003
  Checksum: 0x7457
  Length: 56
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
```

```
Prefix: 4444::/64
Prefix Options: 0 (-|-|-|-)
Forwarding Address: 6666::3
External Route Tag: 0
```

Link LSA Suppression

If link LSA suppression is enabled and the interface type is not broadcast or NBMA, the router will not originate a linkLSA for the link. This implies that other routers on that link will determine the router's next hop address using a mechanism other than the link LSA.

Topology

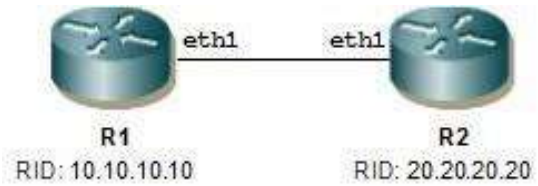


Figure 4-44: LSA Suppression

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf 100-ABC`	Configure the routing process and specify the tag (`100ABC`) which uniquely identifies the routing process.
`(config-router)#router-id 10.10.10.10`	Configure the router ID to use on this instance.
`(config-router)#exit`	Exit OSPF router mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ipv6 router ospf tag 100-ABC area 1`	Configure interface in an area assigned with the area ID (1). The tag uniquely identifies the routing process.
`(config-if)#ipv6 ospf network point-to-point`	Configure the OSPF interface network type as point to point
`(config-if)#ipv6 ospf link-lsa-suppression enable`	Enable the link LSA suppression mechanism
`(config-if)#exit`	Exit interface mode

R2

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf 100-ABC`	Configure the routing process and specify the tag (`100ABC`) which uniquely identifies the routing process.
`(config-router)#router-id 20.20.20.20`	Configure the router ID to use on this instance.
`(config-router)#exit`	Exit OSPF router mode
`(config)#interface eth1`	Enter interface mode

(config-if)#ipv6 router ospf tag 100-ABC area 1	Configure interface in an area assigned with the area ID (1). The tag uniquely identifies the routing process.
(config-if)#ipv6 ospf network point-to-point	Configure the OSPF interface network type as point to point
(config-if)#ipv6 ospf link-lsa-suppression enable	Enable the link LSA Suppression Mechanism
(config-if)#exit	Exit interface mode

Note: This is not applicable for broadcast and NBMA networks.

Validation 1

Verify that adjacency has been established.

```
R1#sh ipv6 ospf neighbor
OSPFv3 Process (100)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
20.20.20.20       1   Full/ -         00:00:37    eth2       0
```

Validation 2

Verify that DUT should not have the Link LSA in the Link state database.

Note: The output below is captured after link lsa suppression enabled which has not Link LSA in the LSDB.

```
DUT#sh ipv6 ospf database

            OSPFv3 Router with ID (10.10.10.10) (Process 100)

Router-LSA (Area 0.0.0.1)

Link State ID   ADV Router       Age Seq#       CkSum     Link
0.0.0.0         10.10.10.10       15 0x80000004 0x3264       1
0.0.0.0         20.20.20.20       15 0x80000002 0xdbba       1

                Intra-Area-Prefix-LSA (Area 0.0.0.1)

Link State ID   ADV Router       Age Seq#       CkSum   Prefix Reference
0.0.0.12        10.10.10.10       14 0x80000004 0xaab4       1 Router-LSA
0.0.0.13        20.20.20.20       15 0x80000002 0x8f7f       1 Router-LSA

                Intra-Area-Te-LSA (Area 0.0.0.1)

Link State ID   ADV Router       Age Seq#       CkSum
0.0.0.4         10.10.10.10       15 0x80000004 0xa326
0.0.0.3         20.20.20.20       15 0x80000002 0xffec R1#sh ipv6
ospf database link

            OSPFv3 Router with ID (10.10.10.10) (Process 100)
```

Address Family IPv4 Unicast Configuration

This chapter contains basic OSPFv3 address family IPv4 unicast configuration examples.

The address family feature lets OSPFv3 IPv6 networks support both IPv6 and IPv4 unicast traffic. It uses multiple instance identifiers to support multiple address families. By default OSPFv3 supports only IPv6 unicast traffic.

The purpose of supporting address families in OSPFv3 is to advertise IPv4 unicast address family routes in OSPFv3 by assigning different instance identifier ranges to different address families. With this feature, users may have two router processes per interface, but only one process per address family. Each instance identifier implies a separate OSPFv3 instance with its own neighbor adjacencies, link state database, and SPF computation. A single IPv4 or IPv6 OSPFv3 process running multiple instances on the same interface is not supported.

Enable Address Family IPv4 Unicast

The diagram below shows the minimum configuration required to enable the OSPFv3 address family feature and to establish the adjacency between R1 and R2 to support the IPv4 address family.

Note: To enable the IPv4 unicast address family in an OSPFv3 router, you need to configure an IPv4 address on the OSPFv3 enabled interface.

Topology

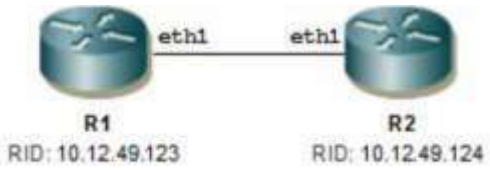


Figure 4-45: IPv4 Address Family on OSPFv3

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf 100-ABC`	Configure the routing process and specify the tag (`100ABC`) which uniquely identifies the routing process.
`(config-router)#router-id 10.12.49.123`	Configure the router ID to use for this process .
`(config-router)#address-family ipv4 unicast`	Enable the ipv4 address family
`(config-router-af)#exit-address-family`	Exit Router AF configuration mode
`(config-router)#exit`	Exit OSPF router mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ipv6 router ospf area 0 tag 100-ABC instance-id 64`	Configure the interface in area 0. The tag uniquely identifies the routing process and the instance identifier is 64-95 for the IPv4 address family
`(config-if)#exit`	Exit interface mode

R2

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf 100-ABC`	Configure the routing process and specify the tag (`100ABC`) which uniquely identifies the routing process.
`(config-router)#router-id 10.12.49.124`	Configure the router ID to use on this tag.

`(config-router)#address-family ipv4 unicast`	Enable the ipv4 address family
`(config-router-af)#exit-address-family`	Exit Router AF configuration mode
`(config-router)#exit`	Exit OSPF router mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ipv6 router ospf area 0 tag 100-ABC instance-id 64`	Configure the interface in area 0. The tag uniquely identifies the routing process and the instance identifier is 64-95 for the IPv4 address family
`(config-if)#end`	Exit interface mode

Note: Use the process identifier to tag the interface, The instance identifier should be same on R1 and R2. In the above example, the process identifiers (`100-ABC`) and the instance identifiers are the same (64).

Validation

Verify that adjacency has been established with the configured instance identifier.

```
R2#sh ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri    State           Dead Time    Interface Instance ID
10.12.49.123      1    Full/DR         00:00:37    eth1            64

R2#sh ipv6 ospf interface eth1 eth1
is up, line protocol is up
  Interface ID 3
  IPv6 Prefixes
    fe80::5054:ff:fe4e:32d1/64 (Link-Local Address)
  OSPFv3 Process (1), Area 0.0.0.0, Instance ID 64
    Router ID 10.12.49.124, Network Type BROADCAST, Cost: 1, TE Metric:
    0 Transmit Delay is 1 sec, State Backup, Priority 1
    Designated Router (ID) 10.12.49.123
      Interface Address fe80::5054:ff:fe7e:3466
    Backup Designated Router (ID) 10.12.49.129
      Interface Address fe80::5054:ff:fe4e:32d1
    Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:04
    Neighbor Count is 1, Adjacent neighbor count is 1
```

Originate Type-7 LSAs and Translate to Type-5

Figure 4-46 shows the configuration to originate Type-7 LSAs and translate them into Type-5 LSAs. R3 is an NSSAASBR that originates Type-7 LSAs into the NSSA which are converted to Type-5 LSAs by R2 which is an NSSA-ABR. R1 is a backbone router.

Topology

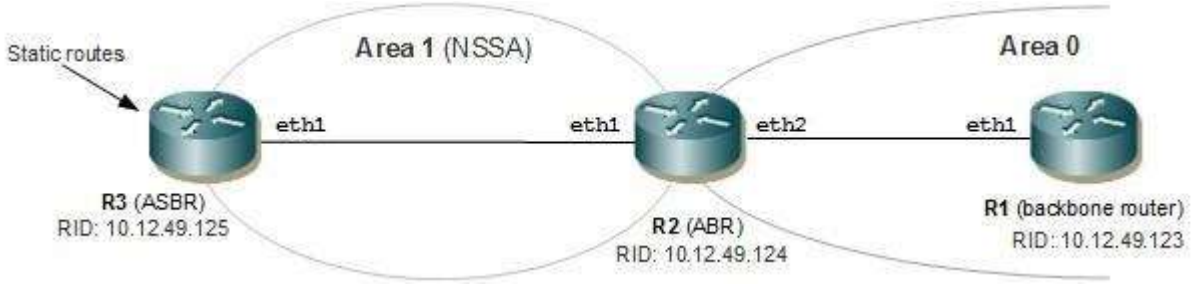


Figure 4-46: Originate Type-7 LSAs and Translate to Type-5 under Address Family IPv4

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf 100-ABC`	Configure the routing process and specify the tag (`100ABC`) which uniquely identifies the routing process
`(config-router)#router-id 10.12.49.123`	Configure the router ID to use on this tag
`(config-router)#address-family ipv4 unicast`	Enable the IPv4 address family
`(config-router-af)#exit-address-family`	Exit Router AF configuration mode
`(config-router)#exit`	Exit OSPF router mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ipv6 router ospf area 0 tag 100-ABC instance-id 64`	Configure the interface in an area assigned with the area ID (0) which uniquely identifies the routing process and the instance identifier which is 64-95 for the IPv4 address family.

R2

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf 100-ABC`	Configure the routing process and specify the tag (`100ABC`) which uniquely identifies the routing process.
`(config-router)#ip route 15.15.15.0/24 null`	Configure the static route with the nexthop address set to null
`(config-router)#router-id 10.12.49.124`	Configure the router ID to use for this process
`(config-router)#area 1 nssa`	Configure the area 1 as NSSA.
`(config-router)#address-family ipv4 unicast`	Enable the ipv4 address family
`(config-router-af)#exit-address-family`	Exit Router AF configuration mode
`(config-router)#exit`	Exit OSPF router mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ipv6 router ospf area 0 tag 100-ABC instance-id 64`	Configure the interface in an area assigned with the area ID (0) which uniquely identifies the routing process and the instance identifier which is 64-95 for the IPv4 address family.

(config-if)#ipv6 router ospf area 1 tag 100-ABC instance-id 65	Configure the interface in an area assigned with the area ID (1) which uniquely identifies the routing process and the instance identifier which is 64-95 for the IPv4 address family.
(config-if)#exit	Exit interface mode

R3

#configure terminal	Enter configure mode.
(config)#router ipv6 ospf 100-ABC	Configure the routing process and specify the tag (100ABC) which uniquely identifies the routing process.
(config-router)#router-id 10.12.49.125	Configure the router ID to use for this process
(config-router)#area 1 nssa	Configure the area 1 as NSSA.
(config-router)#address-family ipv4 unicast	Enable the ipv4 address family
(config-router-af)#redistribute static	Redistribute the static routes configured into the OSPF NSSA
(config-router-af)#exit-address-family	Exit Router AF configuration mode
(config-router)#exit	Exit OSPF router mode
(config)#interface eth1	Enter interface mode
(config-if)#ipv6 router ospf area 1 tag 100-ABC instance-id 65	Configure the interface in an area assigned with the area ID (1) which uniquely identifies the routing process and the instance identifier which is 64-95 for the IPv4 address family.

Validation 1

Verify that adjacency has been established with the configured instance identifier.

```
DUT#sh ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID      Pri   State           Dead Time   Interface   Instance ID
10.12.49.123       1   Full/DR         00:00:31       eth1            95
10.12.49.124       1   Full/Backup     00:00:38    eth2           94
```

Validation 2

Verify that the ABR has External LSA Type 5 in its Database.

Note: Check that R3 has generated a Type 7 LSA.

```
R3#sh ipv6 ospf database external

            OSPFv3 Router with ID (10.12.49.129) (Process 1)

                AS-external-LSA

  LS age: 1517
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.1
  Advertising Router: 10.12.49.124
  LS Seq Number: 0x80000003
  Checksum: 0x597D
```

```
    Length: 36
      Metric Type: 2 (Larger than any link state path)
  Metric: 20
  Prefix: 10.12.49.0/24
  Prefix Options: 0 (-|-|-|-)
  External Route Tag: 0


LS age: 991
LS Type: AS-External-LSA
Link State ID: 0.0.0.11
Advertising Router: 10.12.49.124
LS Seq Number: 0x80000001
Checksum: 0x4C60
Length: 36
  Metric Type: 2 (Larger than any link state path)
  Metric: 21
  Prefix: 33.33.33.0/29
  Prefix Options: 0 (-|-|-|-)
  External Route Tag: 0


LS age: 442
LS Type: AS-External-LSA
Link State ID: 0.0.0.13
Advertising Router: 10.12.49.129
LS Seq Number: 0x80000001
Checksum: 0x376B
Length: 36
  Metric Type: 2 (Larger than any link state path)
  Metric: 20
  Prefix: 33.33.33.1/32
  Prefix Options: 0 (-|-|-|-)
  External Route Tag: 0


LS age: 442
LS Type: AS-External-LSA
Link State ID: 0.0.0.14
Advertising Router: 10.12.49.129
LS Seq Number: 0x80000001
Checksum: 0x3B65
Length: 36
  Metric Type: 2 (Larger than any link state path)
  Metric: 20
  Prefix: 33.33.33.2/32
  Prefix Options: 0 (-|-|-|-)
  External Route Tag: 0


LS age: 442
```

```
LS Type: AS-External-LSA
Link State ID: 0.0.0.15
Advertising Router: 10.12.49.129
LS Seq Number: 0x80000001
Checksum: 0x3F5F
Length: 36
  Metric Type: 2 (Larger than any link state path)
  Metric: 20
      Prefix: 33.33.33.3/32
      Prefix Options: 0 (-|-|-|-)
      External Route Tag: 0


    LS age: 442
    LS Type: AS-External-LSA
    Link State ID: 0.0.0.16
    Advertising Router: 10.12.49.129
    LS Seq Number: 0x80000001
    Checksum: 0x4359
    Length: 36
      Metric Type: 2 (Larger than any link state path)
      Metric: 20
      Prefix: 33.33.33.4/32
      Prefix Options: 0 (-|-|-|-)
      External Route Tag: 0
```

Validation 3

Verify that FIB of backbone router has External Route as “O E2”.

```
R3#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Gateway of last resort is 10.12.49.1 to network 0.0.0.0

K*      0.0.0.0/0 via 10.12.49.1, eth0
C       10.12.49.0/24 is directly connected, eth0
C11.11.11.0/24 is directly connected, eth1
C11.13.11.0/24 is directly connected, eth3
C11.14.11.0/24 is directly connected, eth4
C11.15.11.0/24 is directly connected, eth5
C12.12.12.0/24 is directly connected, eth1
O IA    30.30.30.0/24 [110/2] via 12.12.12.12, eth1
O E2    33.33.33.0/29 [110/21] via 12.12.12.12, eth1
O E2    33.33.33.1/32 [110/20] via 12.12.12.12, eth1
O E2    33.33.33.2/32 [110/20] via 12.12.12.12, eth1
```

```
O E2     33.33.33.3/32 [110/20] via 12.12.12.12, eth1
O E2     33.33.33.4/32 [110/20] via 12.12.12.12, eth1
C        127.0.0.0/8 is directly connected, lo K
169.254.0.0/16 is directly connected, eth0
```

Summarize Intra-Area and External Routes

Figure 4-47 shows the configuration to enable intra-area and external route summarization. The IPv4 address family is enabled on R1. R2 summarizes the internal OSPF routes which R3 redistributes.

Topology

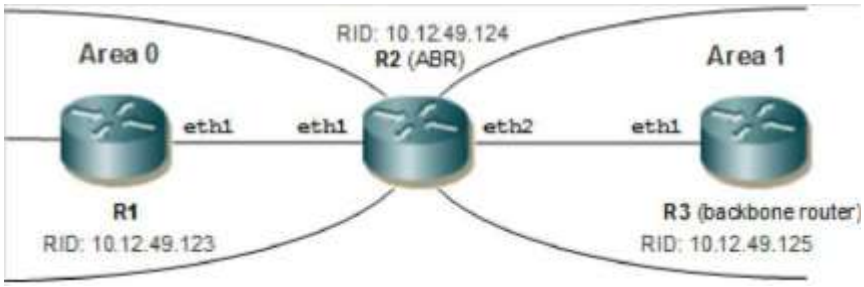


Figure 4-47: Enabling Intra-Area and External Route Summarization

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf 100-ABC`	Configure the routing process and specify the tag (`100ABC`) which uniquely identifies the routing process
`(config-router)#router-id 10.12.49.123`	Configure the router ID to use for this process.
`(config-router)#address-family ipv4 unicast`	Enable the IPv4 address family
`(config-router-af)#exit-address-family`	Exit Router AF configuration mode
`(config-router)#exit`	Exit OSPF router mode
`(config)#interface eth1`	Enter interface mode
`(config-if)#ipv6 router ospf area 0 tag 100-ABC instance-id 64`	Configure the interface in an area assigned with the area ID (0) which uniquely identifies the routing process and the instance identifier which is 64-95 for the IPv4 address family.

R2

`#configure terminal`	Enter configure mode.
`(config)#router ipv6 ospf 100-ABC`	Configure the routing process and specify the tag (`100ABC`) which uniquely identifies the routing process
`(config-router)#router-id 10.12.49.124`	Configure the router ID to use for this process
`(config-router)#address-family ipv4 unicast`	Enable the IPv4 address family

(config-router-af)#exit-address-family	Exit Router AF configuration mode
(config-router)#exit	Exit OSPF router mode
(config)#interface eth1	Enter interface mode
(config-if)#ipv6 router ospf area 0 tag 100-ABC instance-id 64	Configure the interface in an area assigned with the area ID (0) which uniquely identifies the routing process and the instance identifier which is 64-95 for the IPv4 address family.
(config)#interface eth2	Enter interface mode
(config-if)#ipv6 router ospf area 1 tag 100-ABC instance-id 65	Configure the interface in an area assigned with the area ID (1) which uniquely identifies the routing process and the instance identifier which is 64-95 for the IPv4 address family.
(config)#interface lo	Enter interface mode
(config-if)#ipv6 router ospf area 1 tag 101 instance-id 65	Configure the interface in an area assigned with the area ID (1) which uniquely identifies the routing process and the instance identifier which is 64-95 for the IPv4 address family.
(config-router-af)#area 1 range 11.11.11.11/29 advertise	Summarize the internal OSPF routes.
(config-if)#exit	Exit interface mode

R3

#configure terminal	Enter configure mode.
(config)#router ipv6 ospf 100-ABC	Configure the routing process and specify the tag (100ABC) which uniquely identifies the routing process.
(config-router)#router-id 10.12.49.125	Configure the router ID to use for this process.
(config-router)#address-family ipv4 unicast	Enable the IPv4 address family
(config-router-af)#exit-address-family	Exit Router AF configuration mode
(config-router)#exit	Exit OSPF router mode
(config)#interface eth1	Enter interface mode
(config-if)#ipv6 router ospf area 1 tag 100-ABC instance-id 65	Configure the interface in an area assigned with the area ID (1) which uniquely identifies the routing process and the instance identifier which is 64-95 for the IPv4 address family.
(config-router)#address-family ipv4 unicast	Enable the IPv4 address family
(config-router-af)#redistribute connected	Redistribute the connected route to generate external LSAs
(config-router-af)#summary address 51.51.51.51/29	Summarize the external route at the ASBR.

Inter Area Route Aggregation Validation

Validation 1: Verify that adjacency has been established with the configured instance identifier.

```
DUT#sh ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID     Pri   State           Dead Time   Interface Instance ID
10.12.49.123      1   Full/DR         00:00:34    eth1       95
```

```
10.12.49.124      1   Full/DR         00:00:36    eth2       94
```

Validation 2: Verify that a single aggregated OSPF IA route is available in FIB of R1.

```
R1#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Gateway of last resort is 10.12.49.1 to network 0.0.0.0

K*      0.0.0.0/0 via 10.12.49.1, eth0
C       10.12.49.0/24 is directly connected, eth0
C11.11.11.0/24 is directly connected, eth1
C11.13.11.0/24 is directly connected, eth3
C11.14.11.0/24 is directly connected, eth4
C11.15.11.0/24 is directly connected, eth5
C12.12.12.0/24 is directly connected, eth1
O IA    33.33.33.0/29 [110/2] via 12.12.12.12, eth1
C       127.0.0.0/8 is directly connected, lo
K       169.254.0.0/16 is directly connected, eth0
```

Validation 3: Verify that the Inter-Area-Prefix-LSA has one prefix in the R1 Link State Database.

```
R1#sh ipv6 ospf database

            OSPFv3 Router with ID (10.12.49.123) (Process 1)

                Link-LSA (Interface eth1)

Link State ID   ADV Router       Age  Seq#        CkSum  Prefix
0.0.0.3         10.12.49.123       88 0x8000008b  0xe531      2
0.0.0.3         10.12.49.129     1406 0x8000008a 0xfc61      1

Router-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age  Seq#        CkSum   Link
0.0.0.0         10.12.49.123    1409 0x80000006  0x1f6e      1
0.0.0.0         10.12.49.129    1411 0x80000004  0x087e      1

                Network-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age  Seq#        CkSum
0.0.0.3         10.12.49.123    1409 0x80000002  0xe4f0

                Inter-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   ADV Router       Age  Seq#        CkSum
0.0.0.7         10.12.49.129     112 0x80000001  0xc722

                Intra-Area-Prefix-LSA (Area 0.0.0.0)
```

```
Link State ID   ADV Router      Age  Seq#       CkSum   Prefix Reference
0.0.0.2         10.12.49.123    1409 0x80000002 0xfb99       3 Network-LSA

                Intra-Area-Te-LSA (Area 0.0.0.0)

Link State ID   ADV Router      Age  Seq#       CkSum
0.0.0.3         10.12.49.123    1409 0x80000005 0x9cdb
0.0.0.3         10.12.49.129    1411 0x80000003 0x7cf7
```

External Route Summarization Validation:

Note: External route summarization is done at the ASBR.

Validation 1: Verify that single summarized external route in the ABR.

```
R2#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Gateway of last resort is 10.12.49.1 to network 0.0.0.0

K*      0.0.0.0/0 via 10.12.49.1, eth0
C       10.12.49.0/24 is directly connected, eth0
O       11.11.11.0/24 [110/1] is directly connected, eth1
C12.12.12.0/24 is directly connected, eth1
C30.30.30.0/24 is directly connected, eth2
O E233.33.33.0/29 [110/21] via 30.30.30.1, eth2
C127.0.0.0/8 is directly connected, lo
K169.254.0.0/16 is directly connected, eth0
```

Validation 2: Verify that a single Type 5 LSA is in the ABR's Link State Data Base.

```
R2#sh ipv6 ospf database

            OSPFv3 Router with ID (10.12.49.129) (Process 1)

                Link-LSA (Interface eth1)

Link State ID   ADV Router       Age Seq#        CkSum  Prefix
0.0.0.3         10.12.49.123    1161 0x8000008e  0xdf34      2
0.0.0.3         10.12.49.129     675 0x8000008e  0xf465      1

                Link-LSA (Interface eth2)
Link State ID   ADV Router       Age Seq#        CkSum  Prefix
0.0.0.3         10.12.49.124     785 0x80000001  0xc0d5      1
0.0.0.4         10.12.49.129     759 0x80000001  0xc4c9      1

                Router-LSA (Area 0.0.0.0)
Link State ID   ADV Router       Age Seq#        CkSum   Link
0.0.0.0         10.12.49.123     674 0x8000000a  0x1772      1
```

```
0.0.0.0         10.12.49.129      759 0x80000008 0xf98a       1

                Network-LSA (Area 0.0.0.0)
Link State ID   ADV Router       Age Seq#       CkSum
0.0.0.3         10.12.49.123      674 0x80000006 0xdcf4

                Inter-Area-Prefix-LSA (Area 0.0.0.0)
Link State ID   ADV Router       Age Seq#       CkSum
0.0.0.8         10.12.49.129      759 0x80000001 0x2ec8

                Inter-Area-Router-LSA (Area 0.0.0.0)
Link State ID   ADV Router       Age Seq#       CkSum
0.0.0.2         10.12.49.129      699 0x80000001 0x4056

                Intra-Area-Prefix-LSA (Area 0.0.0.0)
Link State ID   ADV Router       Age Seq#       CkSum   Prefix Reference
0.0.0.2         10.12.49.123      674 0x80000006 0xf39d       3 Network-LSA

                Intra-Area-Te-LSA (Area 0.0.0.0)
Link State ID   ADV Router       Age Seq#       CkSum
0.0.0.3         10.12.49.123      674 0x80000009 0x94df
0.0.0.3         10.12.49.129      680 0x80000007 0x74fb

                Router-LSA (Area 0.0.0.1)

Link State ID   ADV Router       Age Seq#       CkSum     Link
0.0.0.0         10.12.49.124      719 0x80000004 0xb9cb       1
0.0.0.0         10.12.49.129      714 0x80000004 0xa6d9       1

                Network-LSA (Area 0.0.0.1)
Link State ID   ADV Router       Age Seq#       CkSum
0.0.0.4         10.12.49.129      719 0x80000001 0xae20

                Inter-Area-Prefix-LSA (Area 0.0.0.1)
Link State ID   ADV Router       Age Seq#       CkSum
0.0.0.38        10.12.49.129      754 0x80000002 0x50c0
0.0.0.39        10.12.49.129      754 0x80000002 0x6aa2

                Intra-Area-Prefix-LSA (Area 0.0.0.1)
Link State ID   ADV Router       Age Seq#       CkSum   Prefix Reference
0.0.0.5         10.12.49.129      713 0x80000001 0x6c12       2 Network-LSA

                Intra-Area-Te-LSA (Area 0.0.0.1)
Link State ID   ADV Router       Age Seq#       CkSum
0.0.0.3         10.12.49.124      715 0x80000004 0x2f42
0.0.0.4         10.12.49.129      719 0x80000003 0x0963

                AS-external-LSA
Link State ID   ADV Router       Age Seq#       CkSum          Tag
0.0.0.11        10.12.49.124       40 0x80000001 0x4c60 E2      0
```

Distribute List

To filter the routes that Open Shortest Path First Version 3 (OSPFv3) installs in the Routing Information Base (RIB), use the `distribute-list in` command in an appropriate configuration mode.

To filter the routes redistributed into Open Shortest Path First Version 3 (OSPFv3) from other routing protocols, use the `distribute-list out` command in an appropriate configuration mode.

Topology

Figure 4-48 shows the configuration to illustrate the distribute-list support for OSPFv3

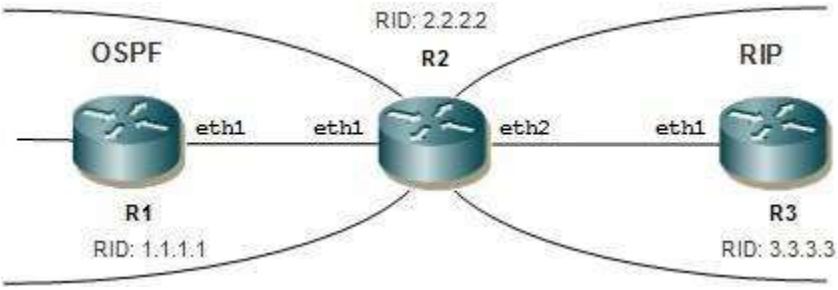


Figure 4-48: Basic Topology for Distribute-list

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 address 2000::1/64`	Configure the IPv6 address of the interface.
`(config-if)#ipv6 router ospf area 0 tag proc1`	Configure the interface in an area assigned with the area ID (0) which uniquely identifies the routing process
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf proc1`	Configure the routing process
`(config-router)#router-id 1.1.1.1`	Configure router-id to uniquely identify the router
`(config-router)#end`	Exit router mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 address 2000::50/64`	Configure the IPv6 address of the interface.
`(config-if)#ipv6 router ospf area 0 tag proc1`	Configure the interface in an area assigned with the area ID (0) which uniquely identifies the routing process
`(config-if)#exit`	Exit interface mode.

(config)#interface eth2	Enter interface mode.
(config-if)#ipv6 address 4000::50/64	Configure the IPv6 address of the interface.
(config-if)#ipv6 router ospf area 0 tag proc1	Configure the interface in an area assigned with the area ID
(config-if)#ipv6 router rip	Configure rip instance under interface
(config-if)#exit	Exit interface mode.
(config)#router ipv6 rip	Configure the rip routing process
(config-router)#neighbor fe80::5054:ff:fe85:19bc eth1	Configure RIP neighbor peer
(config-router)#exit	Exit router mode.
(config)#ipv6 access-list 1 permit 7777::/64	Configure access list to permit 7777::/64 and deny 8888::/64
(config)#router ipv6 ospf proc1	Configure the routing process
(config-router)#router-id 2.2.2.2	Configure router-id to uniquely identify the router
(config-router)#redistribute rip	Redistribute rip routes
(config-router)#distribute-list 1 out rip	Configure distribute list to allow the permitted routes
(config-router)#exit	Exit router mode.
(Config)#ipv6 access-list 1 permit 8888::/64	Configure static route
(config-router)#exit	Exit router mode.

R3

#configure terminal	Enter configure mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ipv6 address 4000::51/64	Configure the IPv6 address of the interface.
(config-if)#ipv6 router rip	Configure rip instance under interface
(config-if)#exit	Exit interface mode.
(config)#router ipv6 rip	Configure the rip routing process
(config-router)#neighbor fe80::5054:ff:fec6:69f eth2	Configure rip neighbor peer
(config-router)#end	Exit router mode.
(config)#ipv6 route 7777::/64 eth2	Configure static route
(config)#ipv6 route 8888::/64 eth3	Configure static route
(config)#router ipv6 rip	Configure the rip routing process

(config-router)#redistribute static	Redistribute configured static routes
(config-router)#end	Exit router mode.

Validation 1

Verify OSPF neighborship is up between R1and R2

R2

```
R2#show ipv6 ospf neighbor
OSPFv3 Process (Proc1)
          Neighbor ID    Pri    State           Dead Time   Interface  Instance ID
 1.1.1.1           1   Full/Backup      00:00:38    eth1        0
```

Validation 2

Check if permitted route 7777::/64 is present in route table and denied route 8888::/64 is not present.

R1

```
R1#show ipv6 ospf route
OSPFv3 Process (Proc1)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1  - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1  - OSPF external type 1, E2 - OSPF external type 2
   Destination      Metric          Next-hop
C  2000::/64          1            directly connected, eth1, Area 0.0.0.0
E2 7777::/64         1/20   via    fe80::5054:ff:fe1e:269d, eth1
```

Validation 3

Check both the routes 7777::/64 and 8888::/64 are present after 8888::/64 is permitted

R1

```
rtr1#show ipv6 ospf route
OSPFv3 Process (Proc1)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

   Destination    Metric     Next-hop
C  2000::/64         1     directly connected, eth1, Area 0.0.0.0
E2 7777::/64       1/20    via fe80::5054:ff:fe1e:269d, eth1
E2 8888::/64       1/20    via fe80::5054:ff:fe1e:269d, eth1
```

Loop Free Alternate

The diagram shows the configuration for the OSPFv3 Loop Free Alternate (LFA) feature.

Topology

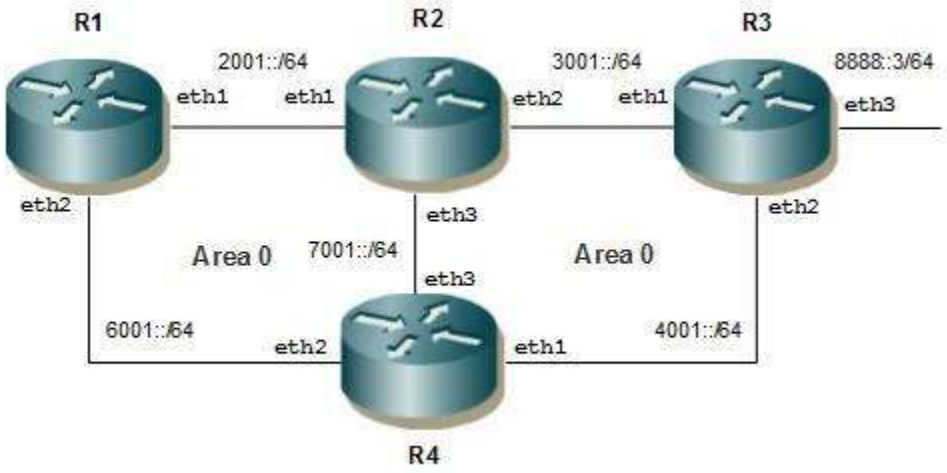


Figure 4-49: Basic OSPFv3 LFA Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 address 2001::1/64`	Configure the IPv6 address of the interface.
`(config-if)#ipv6 router ospf area 0 tag 1`	Enable OSPFv3 on the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 address 6001::1/64`	Configure the IPv6address of the interface.
`(config-if)#ipv6 router ospf area 0 tag 1`	Enable OSPFv3 on the interface.
`(config-if)#ipv6 ospf cost 5`	Configure cost for the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#router ipv6 ospf 1`	Configure the routing process and specify the Process ID (`1`).
`(config)#router-id 1.1.1.1`	Configure the router-id
`(config-router)#fast-reroute keep-allpaths`	Configure LFA-FRR to calculate the available backup path.
`(config-router)#end`	Exit router mode.

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 address 2001::2/64`	Configure the IPv6 address of the interface.

(config-if)#ipv6 router ospf area 0 tag 1	Enable OSPFv3 on the interface.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ipv6 address 3001::2/64	Configure the IPv6 address of the interface.
(config-if)#ipv6 router ospf area 0 tag 1	Enable OSPFv3 on the interface.
(config-if)#exit	Exit interface mode.
(config)#interface eth3	Enter interface mode.
(config-if)#ipv6 address 7001::2/64	Configure the IP v6address of the interface.
(config-if)#ipv6 router ospf area 0 tag 1	Enable OSPFv3 on the interface.
(config-if)#ipv6 ospf cost 2	Configure cost for the interface.
(config)#router ipv6 ospf 1	Configure the routing process, and specify the Process ID (1). The Process ID should be a unique positive integer identifying the routing process.
(config)#router-id 2.2.2.2	Configure the router-id
(config-router)#end	Exit router mode.

R3

#configure terminal	Enter configure mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ipv6 address 3001::3/64	Configure the IPv6 address of the interface.
(config-if)#ipv6 router ospf area 0 tag 1	Enable OSPFv3 on the interface.
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Enter interface mode.
(config-if)#ipv6 address 4001::3/64	Configure the IP v6address of the interface.
(config-if)#ipv6 router ospf area 0 tag 1	Enable OSPFv3 on the interface.
(config-if)#ipv6 ospf cost 2	Configure cost for the interface.
(config)#interface eth3	Enter interface mode.
(config-if)#ipv6 address 8888::3/64	Configure the IP v6address of the interface.
(config-if)#ipv6 router ospf area 0 tag 1	Enable OSPFv3 on the interface.
(config-if)#exit	Exit interface mode.
(config)#router ipv6 ospf 1	Configure the routing process, and specify the Process ID (1). The Process ID should be a unique positive integer identifying the routing process.
(config)#router-id 3.3.3.3	Configure the router-id
(config-router)#end	Exit router mode.

R4

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ipv6 address 5001::4/64`	Configure the IPv6 address of the interface.
`(config-if)#ipv6 router ospf area 0 tag 1`	Enable OSPFv3 on the interface.
`(config-if)#ipv6 ospf cost 2`	Configure cost for the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ipv6 address 6001::4/64`	Configure the IPv6 address of the interface.
`(config-if)#ipv6 router ospf area 0 tag 1`	Enable OSPFv3 on the interface.
`(config-if)#ipv6 ospf cost 5`	Configure cost for the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth3`	Enter interface mode.
`(config-if)#ipv6 address 7001::4/64`	Configure the IPv6 address of the interface.
`(config-if)#ipv6 router ospf area 0 tag 1`	Enable OSPFv3 on the interface.
`(config-if)#ipv6 ospf cost 2`	Configure cost for the interface.
`(config)#router ipv6 ospf 1`	Configure the routing process, and specify the Process ID (`1`). The Process ID should be a unique positive integer identifying the routing process.
`(config)#router-id 4.4.4.4`	Configure the router-id.
`(config-router)#end`	Exit router mode.

Validation

Check OSPFv3 neighborship. `rtr1#show ipv6 ospf neighbor`

```
OSPFv3 Process (1)
Neighbor ID      Pri   State           Dead Time   Interface  Instance ID
2.2.2.2            1   Full/DR         00:00:35    eth1       0
4.4.4.4            1   Full/DR         00:00:35    eth2       0
```

Check the OSPF route installation and LFA-FRR backup path for the primary path.

```
rtr1#show ipv6 route IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP Timers: Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 1d18h11m
C      2001::/64 via ::, eth1, 01:33:09
```

```
O      3001::/64 [110/2] via fe80::5054:ff:feed:dc42, eth1, 00:00:34
O4001::/64 [110/3] via fe80::5054:ff:feed:dc42, eth1, 00:00:34
C5001::/64 via ::, eth3, 1d18h01m
C6001::/64 via ::, eth2, 17:06:18
O7001::/64 [110/3] via fe80::5054:ff:feed:dc42, eth1, 00:00:34
O8888::/64 [110/3] via fe80::5054:ff:feed:dc42, eth1, 00:00:34
Cfe80::/64 via ::, eth2, 17:48:03 rtr1#show ipv6
route fast-reroute
IPv6 Fast-reroute Routing Table
Codes: R - RIP, O - OSPF,
       I - IS-IS, B - BGP
O3001::/64 [110/8] via fe80::5054:ff:fe7b:921e, eth2 inactive, 00:00:59
O4001::/64 [110/7] via fe80::5054:ff:fe7b:921e, eth2 inactive, 00:00:09
O7001::/64 [110/7] via fe80::5054:ff:fe7b:921e, eth2 inactive, 00:00:59
O8888::/64 [110/8] via fe80::5054:ff:fe7b:921e, eth2 inactive, 00:00:09
```

Not mandatory that for all primary path, there exists an LFA backup path only if inequality equation satisfies according to attributes configured on routers, backup path will be calculated.

To prohibit an interface from being used as a repair path, disable fast reroute calculation on the interface.

```
(config)#interface eth2
(config-if)#ipv6 ospf fast-reroute per-prefix candidate disable (config-if)#end
```

Verify that the `eth2` interface is not used for backup path calculation.

```
rtr1#show ipv6 route IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP Timers:
Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 1d18h11m
C      2001::/64 via ::, eth1, 01:33:09
O      3001::/64 [110/2] via fe80::5054:ff:feed:dc42, eth1, 00:00:34
O4001::/64 [110/3] via fe80::5054:ff:feed:dc42, eth1, 00:00:34
C5001::/64 via ::, eth3, 1d18h01m
C6001::/64 via ::, eth2, 17:06:18
O7001::/64 [110/3] via fe80::5054:ff:feed:dc42, eth1, 00:00:34
O8888::/64 [110/3] via fe80::5054:ff:feed:dc42, eth1, 00:00:34
Cfe80::/64 via ::, eth2, 17:48:03 rtr1#show ipv6
route fast-reroute
```

Now there is no LFA backup paths as we have disabled the interface from backup path calculation

Tie-Breaking Configuration:

By default, LFA backup path is calculated based on interface-disjoint. Other supported attributes are:

- Primary Path
- Broadcast-link protecting
- Node-protection

```
(config)#router ipv6 ospf 1
```

```
rtr1(config-router)#fast-reroute tie-break node-protecting index 1
```

Verify `show ipv6 route` and `show ipv6 route fast-reroute` for backup path calculated according to attributes configured above.

```
rtr1#show ipv6 route IPv6
Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP Timers:
Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 1d18h15m
C      2001::/64 via ::, eth1, 01:37:43
O      3001::/64 [110/2] via fe80::5054:ff:feed:dc42, eth1, 00:01:29
O4001::/64 [110/3] via fe80::5054:ff:feed:dc42, eth1, 00:01:29
C5001::/64 via ::, eth3, 1d18h06m
C6001::/64 via ::, eth2, 17:10:52
O7001::/64 [110/3] via fe80::5054:ff:feed:dc42, eth1, 00:01:29
O8888::/64 [110/3] via fe80::5054:ff:feed:dc42, eth1, 00:01:29
Cfe80::/64 via ::, eth2, 17:52:37 rtr1#show ipv6
route fast-reroute
IPv6 Fast-reroute Routing Table
Codes: R - RIP, O - OSPF,
       I - IS-IS, B - BGP
O4001::/64 [110/7] via fe80::5054:ff:fe7b:921e, eth2 inactive, 00:01:28
O7001::/64 [110/7] via fe80::5054:ff:fe7b:921e, eth2 inactive, 00:01:28
O8888::/64 [110/8] via fe80::5054:ff:fe7b:921e, eth2 inactive, 00:01:28
```

CHAPTER 5 IS-IS IPv4

This chapter contains basic IS-IS (Intermediate System to Intermediate System) configuration examples.

Enable IS-IS on an Interface

This example shows the minimum configuration required for enabling IS-IS on an interface. R1 and R2 are two routers in the `ABC` instance connecting to the network 10.10.10.0/24. After enabling IS-IS on an interface, create a routing instance, and specify the Network Entity Title (NET). IS-IS explicitly specifies a NET to begin routing. NET is comprised of the area address and the system ID of the router.

Topology

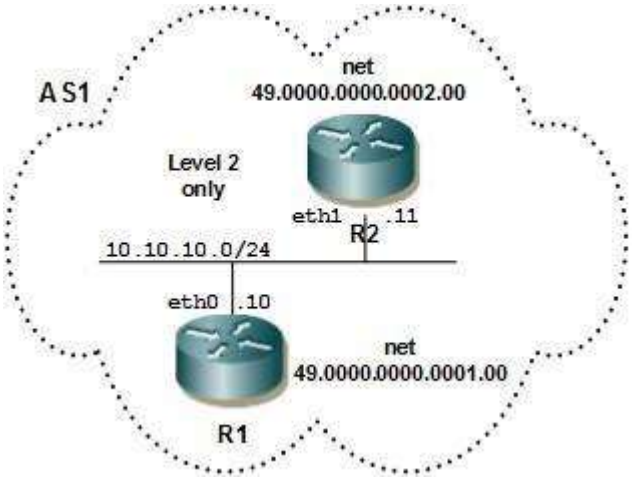


Figure 5-50: Basic IS-IS Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth0`	Specify the interface (`eth0`) to configure, and enter Interface mode.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on an interface for area `49 (ABC)`.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area 49 (`ABC`).
`(config-router)#is-type level-2-only`	Configure instance as `level-2-only` routing.
`(config-router)#net 49.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R2

`#configure terminal`	Enter configure mode.

`(config)#interface eth0`	Specify the interface (`eth0`) to configure, and enter Interface mode.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on an interface for area `49 (ABC)`.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area `49 (ABC)`.
`(config-router)#is-type level-2-only`	Configure instance as `level-2-only` routing.
`(config-router)#net 49.0000.0000.0002.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.

Validation

```
#sh clns  neighbors
Tag 1:  VRF : default
System Id       Interface  SNPA                State  Holdtime  Type Protocol
0001.0000.0002 eth1        0800.2718.1dc2      Up      24        L1   IS-IS
                                               Up      24        L2   IS-IS
#sh ip isis route
Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, D - discard, e - external metric
Tag 1:  VRF : default
    Destination     Metric      Next-Hop            Interface      Tag
L1   1.1.1.0/24      20          2.2.2.1              eth1          0
C    2.2.2.0/24      10          -                    eth1          0
```

Set Priority

This example describes how to set the priority for an interface. Set a high priority for a router to make it the Designated IS (DIS). Router R3 is configured to have a priority of 70, this is higher than the default priority (64) of R1 and R2. This makes R3 the DIS.

Topology

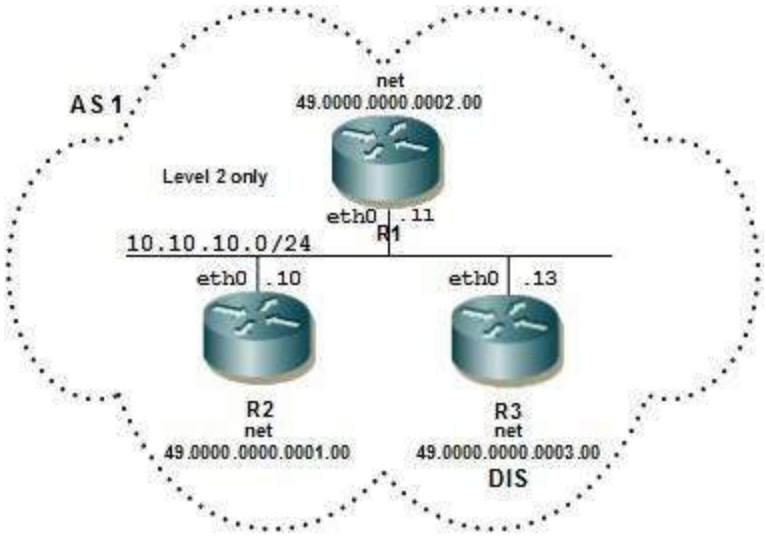


Figure 5-51: Set IS-IS Priority

Configuration

R3

#configure terminal	Enter configure mode.
(config)#interface eth0	Specify the interface (eth0) to configure, and enter Interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#isis priority 70	Specify the router priority to a higher priority (70) to make R3 the designated IS (DIS).
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#net 49.0000.0000.0003.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R1

(config)#interface eth0	Specify the interface (eth0) to configure, and enter Interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#net 49.0000.0000.0001.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R2

(config)#interface eth0	Specify the interface (eth0) to configure, and enter Interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#net 49.0000.0000.0002.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.

Validation

show clns neighbors, show isis database, show isis topology, show isis interface

Redistribute Routes into IS-IS

In this example, the configuration causes BGP routes to be imported into the IS-IS routing table, and advertised into the `ABC` instance.

Topology

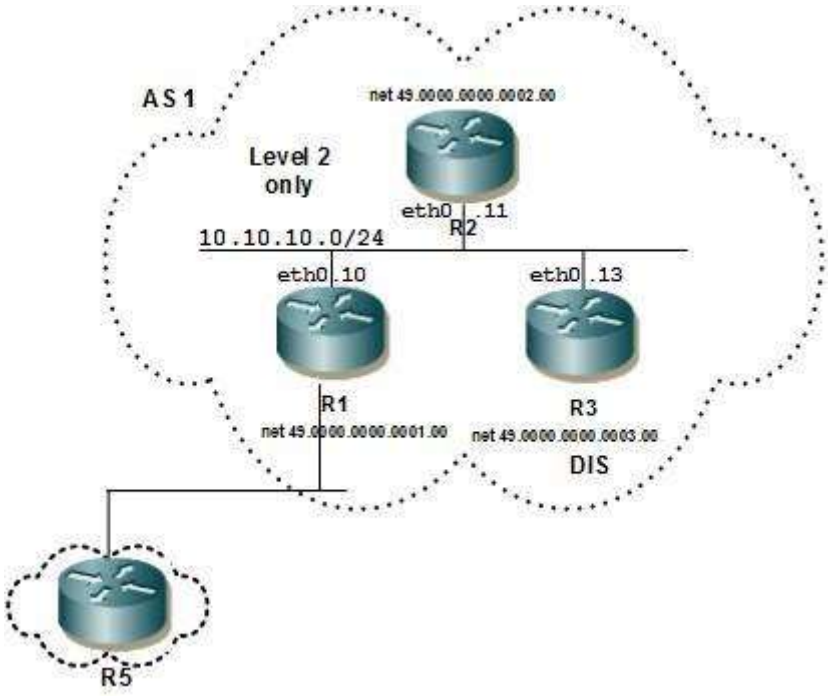


Figure 5-52: Redistribute Routes Into IS-IS

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth0`	Specify the interface (`eth0`) to configure, and enter Interface mode.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on an interface for area `49 (ABC)`.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis ABC`	Create an IS-IS routing instance for area `49` (`ABC`).
`(config-router)#is-type level-2-only`	Set the IS level for this area as `level-2-only`.
`(config-router)#net 49.0000.0000.0001.00`	Set a Network Entity Title for this instance, specifying the area address and the system ID.
`(config-router)#redistribute bgp`	Specify redistributing routes from other routing protocol (BGP) into IS-IS.

Validation

show clns neighbors, show isis database, show isis topology, show ip isis route, show ip route

Metric

You can make a route the preferred route by changing its metric. In this example, the cost has been configured to make R3 the next hop for R1.

The default metric for each interface is 10. Interface eth2 on R2 has a metric of 20, and Interface eth2 on R3 has a metric of 30. The total cost to reach 10.10.14.0/24 (R4) through R2 and R3 is computed as follows:

R2: 10+20 = 30

R3: 10+30 = 40

In this topology, R1 chooses R2 as its next hop for destination 10.10.14.0/24.

Topology

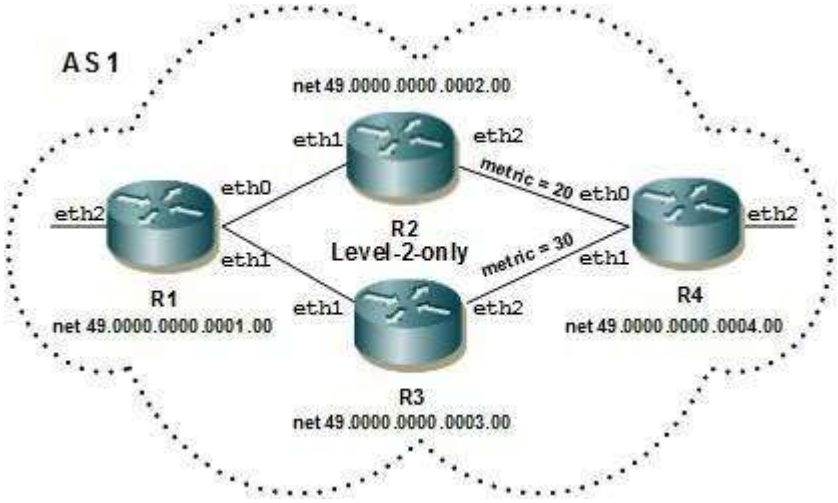


Figure 5-53: Configure IS-IS Metric

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth0`	Specify the interface (`eth0`) to configure, and enter Interface mode.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on an interface for area `49 (ABC).`
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to configure, and enter Interface mode.
`(config-if)#ip router isis ABC`	Enable IS-IS routing on an interface for area `49 (ABC).`
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Specify the interface (`eth2`) to configure, and enter Interface mode.

(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#net 49.0000.0000.0001.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R2

(config)#interface eth1	Specify the interface (eth1) to configure, and enter Interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Specify the interface (eth2) to configure, and enter Interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#isis metric 20	Set the value of IS-IS metric (on eth2) to 20.
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#net 49.0000.0000.0002.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R3

(config)#interface eth1	Specify the interface (eth1) to configure, and enter Interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#exit	Exit interface mode.
(config)#interface eth2	Specify the interface (eth2) to configure, and enter Interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#isis metric 30	Set the value of IS-IS metric (on eth2) to 30.
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#net 49.0000.0000.0003.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R4

(config)#interface eth0	Specify the interface (eth0) to configure, and enter Interface mode.

(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#exit	Exit interface mode.
(config)#interface eth1	Specify the interface (eth1) to configure, and enter Interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area 49 (ABC).
(config-router)#is-type level-2-only	Configure instance as level-2-only routing.
(config-router)#net 49.0000.0000.0004.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.

Validation

show clns neighbors, show isis database, show isis topology, show ip isis route, show ip route, show isis interface

L1-L2 Area Routing with a Single Instance

IS-IS supports a two-level hierarchy for handling and scaling the functionality of large networks. The Level-1 (L1) area is mainly for Leaf networks, and the Level-2 (L2) area is the backbone area connecting Level-1 areas. In this example, R3 and R4 are configured as Level-1 routers, and reside in the Level-1 area. R1 and R2 are configured as Level-1-2 routers, and connect these two Level-1 areas with a backbone Level-2 area. You can configure Level-1-2 routers with single or multiple instances: This configuration shows the single-instance version of the Level-1-2 router.

Topology

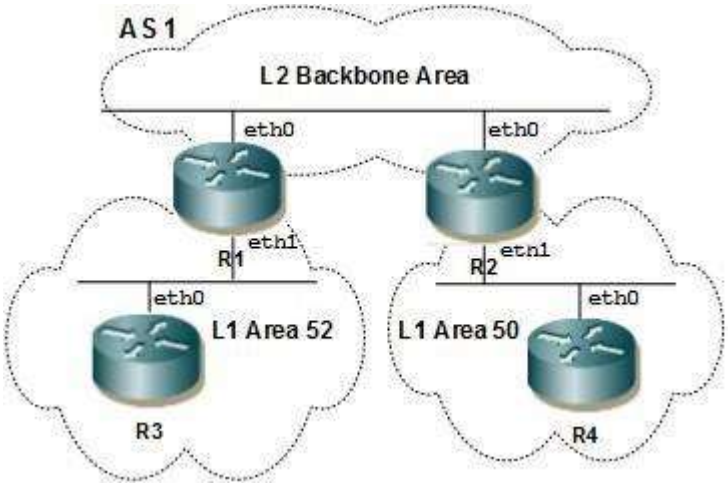


Figure 5-54: Single-Instance L1-L2 Area Routing

Configuration

R1

#configure terminal	Enter configure mode.

(config)#interface eth0	Specify the interface (eth0) to configure, and enter Interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on the interface eth0 for area ABC.
(config-if)#isis circuit-type level-2-only	Set the circuit type for the interface eth0.
(config-if)#exit	Exit interface mode.
#configure terminal	Enter configure mode.
(config)#interface eth1	Specify the interface (eth1) to configure, and enter Interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on the interface eth1 for area ABC.
(config-if)#isis circuit-type level-1	Set the circuit type for interface eth1 to level 1.
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area ABC.
(config-router)#net 52.0000.0000.0001.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R2

(config)#interface eth0	Specify the interface (eth0) to configure, and enter Interface mode.
(config-if)#ip router isis bb	Enable IS-IS routing on the interface eth0 for area bb.
(config-if)#isis circuit-type level-2-only	Set the circuit type for the interface eth0 to level-2 only.
(config-if)#exit	Exit interface mode.
(config)#interface eth1	Specify the interface (eth1) to configure, and enter Interface mode.
(config-if)#ip router isis bb	Enable IS-IS routing on interface eth1 for area bb.
(config-if)#isis circuit-type level-1	Set the circuit type for interface eth1 to level 1.
(config-if)#exit	Exit interface mode.
(config)#router isis bb	Create an IS-IS routing instance for area bb.
(config-router)#net 50.0000.0000.0002.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R3

(config)#interface eth0	Specify the interface (eth0) to configure, and enter Interface mode.
(config-if)#ip router isis xyz	Enable IS-IS routing on the interface eth0 for area xyz.
(config-if)#exit	Exit interface mode.
(config)#router isis xyz	Create an IS-IS routing instance for area xyz.
(config-router)#is-type level-1	Set the IS level for this area (xyz) as level-1.
(config-router)#net 52.0000.0000.0003.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R4

(config)#interface eth0	Specify the interface (eth0) to configure, and enter Interface mode.

(config-if)#ip router isis aa	Enable IS-IS routing on the interface eth0 for area aa.
(config-if)#exit	Exit interface mode.
(config)#router isis aa	Create an IS-IS routing instance for area aa.
(config-router)#is-type level-1	Set the IS level for this area (aa) as level-1.
(config-router)#net 50.0000.0000.0004.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.

Validation

show ip isis route, show ip route, show clns neighbors, show isis database

L1-L2 Area Routing with Multiple Instances

IS-IS supports a two-level hierarchy for handling and scaling the functionality of large networks. The Level-1 (L1) area is mainly for Leaf networks, and the Level-2 (L2) area is the backbone area connecting Level-1 areas. In this example, R3 and R4 are configured as Level-1 routers, and reside in the Level-1 area. R1 and R2 are configured as Level-1-2 routers, and connect these two Level-1 areas with a backbone Level-2 area. You can configure Level-1-2 routers with single or multiple instances: This configuration shows the multiple-instance version of the Level-1-2 router.

Topology

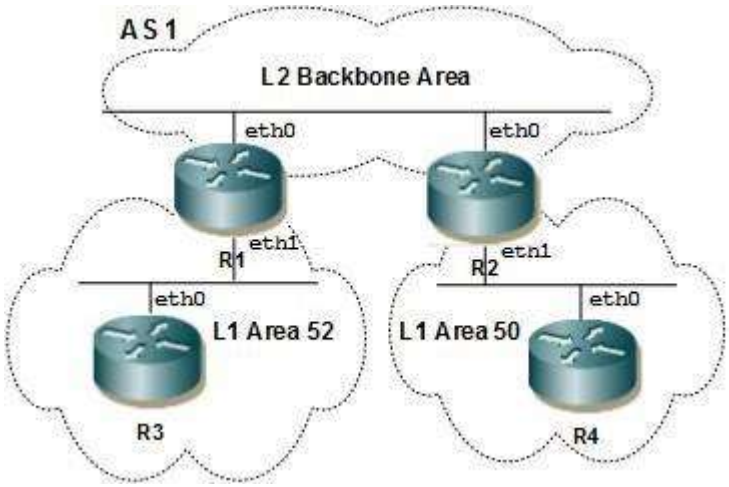


Figure 5-55: Multiple-Instance L1-L2 Area Routing

Configuration

R1

#configure terminal	Enter configure mode.
(config)#interface eth0	Specify the interface (eth0) to configure, and enter Interface mode.
(config-if)#ip router isis aaa	Enable IS-IS routing on interface eth0 for area aaa.

(config-if)#exit	Exit interface mode.
(config)#router isis aaa	Create an IS-IS routing instance for area aaa.
(config-router)#is-type level-2-only	Set the IS level for this area (aaa) as level-2-only.
#configure terminal	Enter configure mode.
(config-router)#net bb.0000.0000.0001.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#interface eth1	Specify the interface (eth1) to configure, and enter Interface mode.
(config-if)#ip router isis ccc	Enable IS-IS routing on interface eth1 for area ccc.
(config-if)#exit	Exit interface mode.
(config)#router isis ccc	Create an IS-IS routing instance for area ccc.
(config-router)#is-type level-1	Set the IS level for this area (ccc) as level-1.
(config-router)#net cc.0000.0000.0002.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
R2	
(config)#interface eth0	Specify the interface (eth0) to configure, and enter Interface mode.
(config-if)#ip router isis bb	Enable IS-IS routing on interface eth0 for area bb.
(config-if)#exit	Exit interface mode.
(config)#router isis bb	Create an IS-IS routing instance for area bb.
(config-router)#is-type level-2-only	Set the IS level for this area (bb) as level-2-only.
(config-router)#net bb.0000.0000.0002.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#exit	Exit Router mode, and return to Configure mode.
(config)#interface eth1	Specify the interface (eth1) to configure, and enter Interface mode.
(config-if)#ip router isis ABC	Enable IS-IS routing on interface eth1 for area ABC.
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance for area ABC.
(config-router)#is-type level-1	Set the IS level for this area (ABC) as level-1.
(config-router)#net cc.0000.0000.0003.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
R3	
(config)#interface eth0	Specify the interface (eth0) to configure, and enter Interface mode.
(config-if)#ip router isis xyz	Enable IS-IS routing on interface eth0 for area xyz.
(config-if)#exit	Exit interface mode.
(config)#router isis xyz	Create an IS-IS routing instance for area xyz.

(config-router)#is-type level-1	Set the IS level for this area (xyz) as level-1.
(config-router)#net 52.0000.0000.0003.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.

R4

(config)#interface eth0	Specify the interface (eth0) to configure, and enter Interface mode.
(config-if)#ip router isis aa	Enable IS-IS routing on interface eth0 for area aa.
(config-if)#exit	Exit interface mode.
(config)#router isis aa	Create an IS-IS routing instance for area aa.
(config-router)#is-type level-1	Set the IS level for this area (aa) as level-1.
(config-router)#net 52.0000.0000.0004.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.

Validation

```
#sh ip isis route
Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, D - discard, e - external metric
Tag aaa: VRF : default
     Destination         Metric      Next-Hop             Interface       Tag
C    10.10.10.0/24       10           --                   eth2            0

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, D - discard, e - external metric

Tag ccc: VRF : default
     Destination         Metric      Next-Hop             Interface       Tag
C    11.11.11.0/24       10           --                   eth1            0

#sh clns  neighbors

Tag aaa: VRF : default
System Id      Interface   SNPA               State  Holdtime  Type Protocol
Tag ccc: VRF : default
System Id      Interface   SNPA               State  Holdtime  Type Protocol
0000.0000.0004 eth1        0800.277b.411d     Up     9         L1   IS-IS

#sh isis database
Tag aaa: VRF : default
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum   LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00* 0x00000003   0x907B        1165              0/0/0

Tag ccc: VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum   LSP Holdtime      ATT/P/OL
0000.0000.0002.00-00* 0x00000002   0x3B97        587               0/0/0
0000.0000.0004.00-00  0x00000002   0x3996        614               0/0/0
```

```
      0000.0000.0004.01-00  0x00000001    0x31A5        586               0/0/0
```

Route Leaking

Route leaking is defined in RFC 2966. For Level-1 (L1) routers, only level-1 routes are populated in the routing table. The L1 router has a default route to the nearest Level-1/Level-2 (L1/L2) router: This could result in sub-optimal routing in certain scenarios. Route leaking causes an L1/L2 router to advertise the level-2 routes in its database to the L1 router, thus allowing the L1 router to acknowledge the prefixes advertised by the Level-2 (L2) router. In this way, the L1 router has the ability to learn the true cost to reach other areas.

In the following example, R1 is the L1 router, R2 is the L1/L2 router doing the route leaking, and R3 is the L2 router. The following configuration is given only for R2, assuming that the adjacency with R1 and R3 are already up, and the route tables with appropriate routes are already populated.

Topology

Figure 5-56: Route Leaking Topology

Configuration

R2

`#configure terminal`	Enter configure mode.
`(config)#router isis 1`	Create an IS-IS routing instance for area `49 (1)`.
`(config-router)#redistribute isis level-2 into level-1`	Redistribute routes learned from level 2 into level 1 (route leaking).
`(config-router)#end`	Exit Router mode.

In the example, route, `i ia 3.3.3.0/24 [115/30] via 15.1.1.32, eth2, 00:00:02`, is the L2 route leaked by the L1/L2 router into the L1 router.

```
Router1#show ip route

Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default


Gateway of last resort is 15.1.1.32 to network 0.0.0.0


i*L1    0.0.0.0/0 [115/10] via 15.1.1.32, eth2, 00:00:59
```

```
i ia    3.3.3.0/24 [115/30] via 15.1.1.32, eth2, 00:00:02
C       10.1.2.0/24 is directly connected, eth0
K10.10.0.0/16 via 10.1.2.1, eth0
K10.10.3.0/24 is directly connected, eth0
C13.1.1.0/24 is directly connected, eth1
C15.1.1.0/24 is directly connected, eth2
C31.31.31.31/32 is directly connected, lo
C127.0.0.0/8 is directly connected, lo
K169.254.0.0/16 is directly connected, eth0
```

Validation

show ip route, show isis database, show ip isis route

Route Summarization

Route summarization makes the routing table smaller, but still allows complete IP connectivity, if everything is configured properly.

The following example consists of a three-router topology, in which R2 is doing the summarization. In this example, R1 is the L1 router, R2 is the L1/L2 router doing the summarization, and R3 is the L2 router. The following configuration is given only for R2, assuming that the adjacencies with R1 and R3 are already up, and the route tables with the appropriate routes are already populated.

Topology

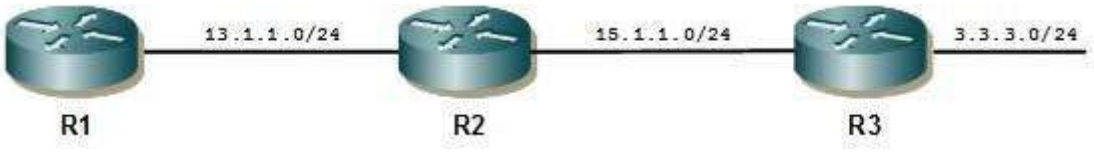


Figure 5-57: Route Summarization Topology

Configuration

R2

`#configure terminal`	Enter configure mode.
`(config)#router isis 1`	Create an IS-IS routing instance for area `49 (1)`.
`(config-router)#summary-address 20.0.0.0/6 level-1 metric 1`	The prefixes, 20.10.3.0/8, 21.10.3.0/8, 22.10.3.0/8, and 23.10.3.0/8 are summarized to 20.0.0.0/6.
`(config-router)#end`	Exit Router mode.

Validation

show ip route

Graceful Restart

ISIS provides graceful restart, in which the adjacency and routes are maintained in the routing table for the grace period. In this way, the data flow is not affected, and there is no packet loss during the restart phase.

In the following example, R1 is the L1/L2 router, and R2 is the L1/L2 restart-helper router. The following configuration is given only for R2, assuming that the adjacency with R1 is already up, and the route tables with the appropriate routes are already populated.

Topology

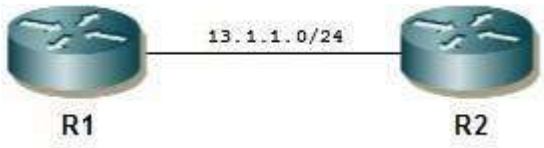


Figure 5-58: IS-IS Graceful Restart

Configuration

R2

`#configure terminal`	Enter configure mode.
`(config)#isis restart helper`	Configure this router as a restart helper.
`(config)#isis restart grace-period 100`	Set the grace period to 100 seconds. The restarting router should come up before 100 seconds, otherwise, the adjacency and routes will be deleted.

Note: The IS-IS daemon in the restarting router must be manually restarted: it does not restart automatically.

Validation

show ip route, show clns neighbors, show ip route database

IS-IS Distance

Administrative distance in IS-IS can be configured for a specified source ID or for all routes.

This example shows configuring the IS-IS administrative distance for the IPv4 address family.

Topology

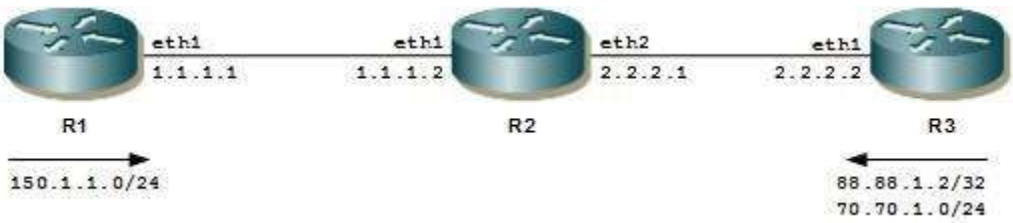


Figure 5-59: IS-IS Distance Topology

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to configure, and enter Interface mode.
`(config-if)#ip address 1.1.1.1/24`	Assign the IP address on this interface (`eth1`).
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface `eth1`.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis 1`	Create an IS-IS routing instance (`1`).
`(config-router)#net 49.0001.0000.0001.00`	Set a Network Entity Title (NET) for this instance, specifying the address and the system ID.
`(config-router)#redistribute static`	Redistribute the static routes.

R2

`#configure terminal`	Enter configure mode.
`(config)#access-list DIST permit 88.88.1.2/32`	Create an access list to permit the `88.88.1.2/32` route from R3.
`(config)#interface eth1`	Specify the interface (`eth1`) to configure, and enter Interface mode.
`(config-if)#ip address 1.1.1.2/24`	Assign the IP address on this interface (`eth1`).
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface `eth1`.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Specify the interface (`eth2`) to configure, and enter Interface mode.
`(config-if)#ip address 2.2.2.1/24`	Assign the IP address on this interface (`eth2`).
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface `eth2`.
`(config-if)#exit`	Exit interface mode.
`(config)#router isis 1`	Create an IS-IS routing instance (`1`).
`(config-router)#net 49.0001.0000.0002.00`	Specify the NET address.
`(config-router)#distance 100`	Configure the administrative distance for all routes received from R1 and R2.

(config-router)#distance 20 0000.0000.0001	Configure the administrative distance for all routes received from R1. This command overwrites the applied distance, 100, and will apply distance 20 for all routes received from R1.
(config-router)#distance 30 0000.0000.0003 DIST	Configure the distance, 30, to the route, 88.88.1.2/32, received from R3. All other routes from R3 (for example, 70.70.1.0/24) will have the distance applied as 100. If the distance, 100, is not configured, all other routes will have a default distance of 115.

R3

#configure terminal	Enter configure mode.
(config)#interface eth1	Specify the interface (eth1) to configure, and enter Interface mode.
(config-if)#ip address 2.2.2.2/24	Assign the IP address on this interface (eth1).
(config-if)#ip router isis 1	Enable IS-IS routing on interface eth1.
(config-if)#exit	Exit interface mode.
(config)#router isis 1	Create an IS-IS routing instance (1).
(config-router)#net 49.0001.0000.0003.00	Specify the NET address.
(config-router)#redistribute static	Redistribute the static routes.

Validation

```
#sh clns  neighbors
Tag 1:  VRF : default
System Id      Interface   SNPA            State   Holdtime Type Protocol
0001.0000.0002 eth1        0800.2718.1dc2   UP      24       L1   IS-IS
                                            UP      24       L2   IS-IS
#sh ip isis route

Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, D - discard, e - external metric

Tag 1:  VRF : default
     Destination    Metric    Next-Hop Interface      Tag
L1    1.1.1.0/24       20      2.2.2.1  eth1           0
C      2.2.2.0/24      10        --     eth1           0
```

Overload Bit

The expanded use of the overload bit in IS-IS is useful to Internet Service Providers (ISPs) who run both BGP and IS-IS to avoid certain black-hole scenarios. The overload bit feature allows configuration of a router to disable the overload bit automatically when BGP has converged.

IS-IS disables the overload bit if BGP is not converged in ten minutes, and the wait-for-bgp option is configured.

When the set overload-bit wait-for-bgp is configured after restart (for example, using the set-overloadbit on-startup wait-for-bgp or set-overload-bit on-startup <5-86400> commands), the IS-IS router advertises the overload bit to all its neighbors, informing them not to route traffic through this router, except for the traffic destined to directly-connected networks of this router.

Whenever an interface is configured as no set-overload-bit (using the `no set-overload-bit` command), the router does not advertise or set the overload bit on startup.

Topology

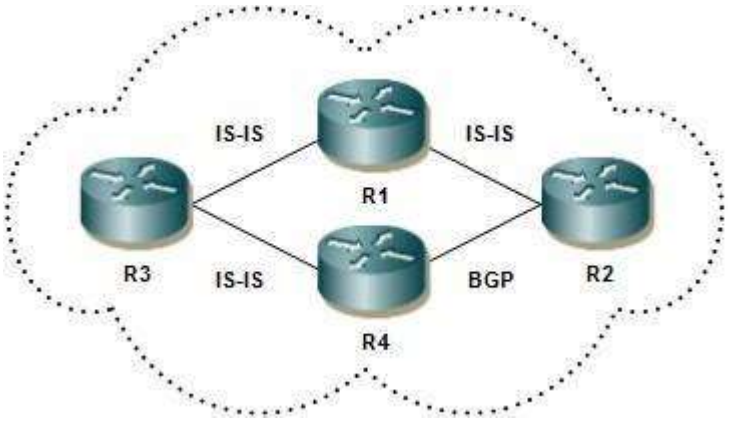


Figure 5-60: Configure Overload Bit

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router isis 1`	Create an IS-IS routing instance (`1`).
`(config-router)#net 49.0001.0000.0000.0001.00`	Define the NET address.
`(config-router)#exit`	Exit router mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to configure and enter Interface mode.
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface `eth1` (connected to R2).
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface eth2`	Specify the interface (`eth2`) to configure and enter Interface mode.
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface `eth2` (connected to R3).
`(config-if)#isis metric 50`	Increase the value of IS-IS metric from R1-R3.

R2

`#configure terminal`	Enter configure mode.
`(config)#router bgp 100`	Create a BGP routing instance (`100`).
`(config-router)#neighbor 1.1.1.2 remote-as 2`	Specify the neighbor's IP address (`1.1.1.2`) and the ASN value of the neighbor (`2`).
`(config-router)#exit`	Exit router mode.

(config)#interface eth1	Specify the interface (eth1) to configure and enter Interface mode.
(config-if)#ip router isis 1	Enable IS-IS routing on interface eth1 (connected to R1).
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface eth2	Specify the interface (eth2) to configure and enter Interface mode.
(config-if)#ip router isis 1	Enable IS-IS routing on interface eth2 (connected to R4).
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router isis 1	Create an IS-IS routing instance (1).
(config-router)#net 49.0001.0000.0000.0002.00	Define the NET address.
(config-router)#set-overload-bit on-startup wait-for-bgp	Configure IS-IS to set the overload bit until BGP is completely converged (maximum 600 seconds) only on restart.
(config-router)#set-overload-bit on-startup wait-for-bgp suppress external	Configure IS-IS to suppress external routes until the configured value (in seconds) only on startup.
(config-router)#set-overload-bit on-startup wait-for-bgp suppress interlevel	Configure IS-IS to suppress inter-level routes until the configured value (in seconds) only on startup.

R3

#configure terminal	Enter configure mode.
(config)#router isis 1	Create an IS-IS routing instance (1).
(config-router)#net 49.0001.0000.0000.0003.00	Define the NET address.
(config-router)#exit	Exit router mode.
(config)#interface eth1	Specify the interface (eth1) to configure and enter Interface mode.
(config-if)#ip router isis 1	Enable IS-IS routing on interface eth1 (connected to R4).
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface eth2	Specify the interface (eth2) to configure and enter Interface mode.
(config-if)#ip router isis 1	Enable IS-IS routing on interface eth2 (connected to R1).

R4

#configure terminal	Enter configure mode.
(config)#router bgp 100	Create a BGP routing instance (100).
(config-router)#neighbor 1.1.1.1 remote-as 1	Specify the neighbor's IP address (1.1.1.1) and the ASN value of the neighbor (1).
#configure terminal	Enter configure mode.
(config-router)#exit	Exit router mode.
(config)#router isis 1	Create an IS-IS routing instance (1).
(config-router)#net 49.0001.0000.0000.0004.00	Define the NET address.
(config-router)#exit	Exit router mode.

`(config)#interface eth1`	Specify the interface (`eth1`) to configure and enter Interface mode.
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface `eth1` (connected to R3).
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface eth2`	Specify the interface (`eth2`) to configure and enter Interface mode.
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface `eth2` (connected to R2).

Validation

Use the following commands to verify adjacency and protocol-related details:

show clns neighbors, show isis database, show ip bgp summary

Passive Interface

In ISP and large enterprise networks, many of the distribution routers have more than 200 interfaces. Before the Default Passive-Interface feature, there were two possibilities for obtaining routing information from tall of these interfaces:

- Configure a routing protocol on the backbone interfaces and redistribute connected interfaces.
- Configure the routing protocol on all interfaces and manually set most of them as passive, which was time consuming.

The solution to this problem was to configure the routing protocol on all interfaces and manually set the `passiveinterface` command on the interfaces where adjacency was not desired. In certain networks, this meant coding 200 or more passive-interface statements. With the Default Passive Interface feature, this problem is solved by allowing all interfaces to be set as passive by default using a single `passive-interface` default command, then configuring individual interfaces in which adjacencies are desired using the `no passive-interface` command.

Usage

1. When a specific interface is configured as passive using the `passive-interface` command:
   - The interface loses its adjacency on that interface, for example, eth1.
   - The interface (eth1) is still advertised by other IS-IS speaking interfaces to their neighbors.
2. When a specific interface is configured as passive using `passive-interface` command followed by removing the configuration using `no passive-interface` command:
   - The interface is IS-IS disabled and must be enabled using the `ip router isis` command (for example, `ip router isis 1`).
   - The interface (for example, eth1) is not advertised by other IS-IS speaking interfaces to their neighbors.
3. When an interface is configured with the `passive interface` command:
   - All interfaces lose their adjacency, except the interface with the higher index number. (For example: If eth1, eth2, eth3, and eth4 are the router interfaces, eth4 has the highest index number.) • All interfaces are advertised by the active IS-IS speaking interface to its neighbors.

4. When an interface is configured with the `no passive interface` command:
   - All interfaces are IS-IS disabled, except the interface that was active, and all interfaces must enable IS-IS on these interfaces using the `ip router isis` command (for example, `ip router isis 1`).
   - All interfaces are not advertised by the active IS-IS speaking interface to its neighbors.

Topology

Figure 5-61 shows a passive-interface configuration example.

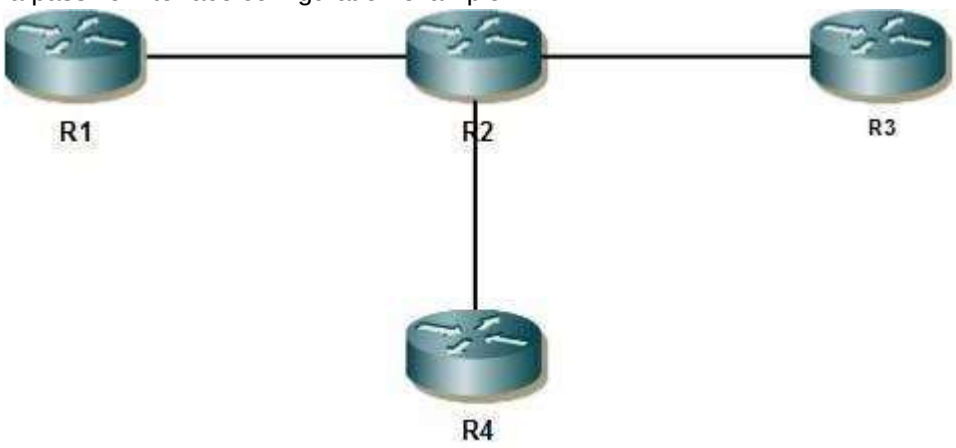


Figure 5-61: IS-IS Passive Interface

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#router isis 1`	Create an IS-IS routing instance `(1)`.
`(config-router)#net 49.0001.0000.0000.0001.00`	Define the NET address.
`(config-router)#exit`	Exit router mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to configure and enter Interface mode.
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface `eth1` (connected to R2).

R2

`#configure terminal`	Enter configure mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to configure and enter Interface mode.
`(config-if)#ip router isis 1`	Enable IS-IS routing on interface `eth1` (connected to R1).
`#configure terminal`	Enter configure mode.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface eth2`	Specify the interface (`eth2`) to configure and enter Interface mode.

(config-if)#ip router isis 1	Enable IS-IS routing on interface eth2 (connected to R3).
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface eth3	Specify the interface (eth3) to configure and enter Interface mode.
(config-if)#ip router isis 1	Enable IS-IS routing on interface eth2 (connected to R4).
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router isis 1	Create an IS-IS routing instance (1).
(config-router)#net 49.0001.0000.0000.0002.00	Define the NET address.
(config-router)#passive-interface eth1	Configure the eth1 interface as passive.
(config-router)#passive-interface	Configure all interfaces as passive, except one (interface with the higher index number).

R3

#configure terminal	Enter configure mode.
(config)#router isis 1	Create an IS-IS routing instance (1).
(config-router)#net 49.0001.0000.0000.0003.00	Define the NET address.
(config-router)#exit	Exit router mode.
(config)#interface eth1	Specify the interface (eth1) to configure and enter Interface mode.
(config-if)#ip router isis 1	Enable IS-IS routing on interface eth1 (connected to R2).

R4

#configure terminal	Enter configure mode.
(config)#router isis 1	Create an IS-IS routing instance (1).
(config-router)#net 49.0001.0000.0000.0004.00	Define the NET address.
(config-router)#exit	Exit router mode.
(config)#interface eth1	Specify the interface (eth1) to configure and enter Interface mode.
(config-if)#ip router isis 1	Enable IS-IS routing on interface eth1 (connected to R2).

Validation

R2

```
#sh isis database detail
Tag 1:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                                 LSP Seq Num     LSP Checksum    LSP
Holdtime       ATT/P/OL
0000.0000.0002.00-00* 0x00000002     0x67BB                  760
0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  Metric:   0          IP 11.11.11.0 255.255.255.0
```

```
  Metric:    0         IP 10.10.10.0 255.255.255.0
  Metric:    0         IP 12.12.12.0 255.255.255.0
  Metric:    0         IP 10.12.4.0 255.255.255.0

IS-IS Level-2 Link State Database:
LSPID                                 LSP Seq Num    LSP Checksum   LSP
Holdtime      ATT/P/OL
0000.0000.0002.00-00* 0x00000003    0x56CB                 790
0/0/0
  Area Address: 49.0001
  NLPID:        0xCC
  Metric:    0         IP 10.10.10.0 255.255.255.0
  Metric:    0         IP 10.12.4.0 255.255.255.0
  Metric:    0         IP 11.11.11.0 255.255.255.0
  Metric:    0         IP 12.12.12.0 255.255.255.0
```

R1:

```
#sh isis database detail
Tag 1:  VRF : default
IS-IS Level-1 Link State Database:
LSPID                                  LSP Seq Num   LSP Checksum   LSP
Holdtime      ATT/P/OL
0001.0000.0001.00-00* 0x00000003      0x4835                 463
0/0/0
  Area Address: 49
  NLPID:        0xCC
  IP Address:   10.10.10.1
  Metric:   10          IP 10.10.10.0 255.255.255.0

IS-IS Level-2 Link State Database:
LSPID                                  LSP Seq Num   LSP Checksum  LSP
Holdtime      ATT/P/OL
0001.0000.0001.00-00* 0x00000003      0x4835                 463
0/0/0
  Area Address: 49
  NLPID:        0xCC
  IP Address:   10.10.10.1
  Metric:   10          IP 10.10.10.0 255.255.255.0
```

CHAPTER 6 IS-IS IPv6

This chapter contains basic IS-IS (IPv6) configuration examples.

For details about the commands used in these examples, see the *Intermediate System to Intermediate System Command Reference*.

Enable IS-IS on an Interface

This example shows the minimum configuration required for enabling IS-IS (IPv6) on an interface. R1 and R2 are two routers in the `Inst1` instance connecting to the network 3ffe:10::/64. After enabling IS-IS on an interface, create a routing instance, and specify the Network Entity Title (NET). IS-IS explicitly specifies a NET to begin routing. NET is comprised of the area address and the system ID of the router.

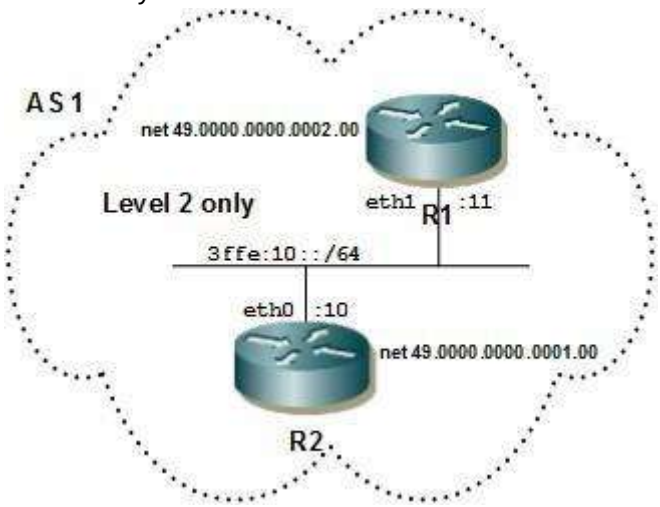


Figure 6-62: Enable IS-ISv6

R1

`# configure terminal`	Enter Configure mode.
`(config)# interface eth0`	Specify the interface (`eth0`) to configure, and enter Interface mode.
`(config-if)# ipv6 router isis Inst1`	Enable IS-IS routing on an interface for area `49` (`Inst1`).
`(config-if)# exit`	Exit Interface mode, and return to Configure mode.
`(config)# router isis Inst1`	Create an IS-IS routing instance for area `49` (`Inst1`).
`(config-router)# is-type level-2-only`	Configure instance `Inst1` as `level-2-only` routing.
`(config-router)# net 49.0000.0000.0001.00`	Establish a Network Entity Title for this instance, specifying the area address and system ID.

R2

`# configure terminal`	Enter Configure mode.

`(config)# interface eth0`	Specify the interface (`eth0`) to configure, and enter Interface mode.
`(config-if)# ipv6 router isis Inst1`	Enable IS-IS routing on an interface for area `49 (Inst1).`
`(config-if)# exit`	Exit Interface mode, and return to Configure mode.
`(config)# router isis Inst1`	Create an IS-IS routing instance for area `49 (Inst1`).
`(config-router)# is-type level-2-only`	Configure instance `Inst1` as `level-2-only` routing.
`(config-router)# net 49.0000.0000.0002.00`	Establish a Network Entity Title for this instance, specifying the area address and the system ID.

Validation

show clns neighbors, show isis database, show ipv6 isis topology

Set Priority

This example shows setting the priority for an interface. Set a high priority for a router to make it the Designated IS (DIS). Router R3 is configured to have a priority of 70; this is higher than the default priority (60) of R1 and R2. This makes R3 the DIS.

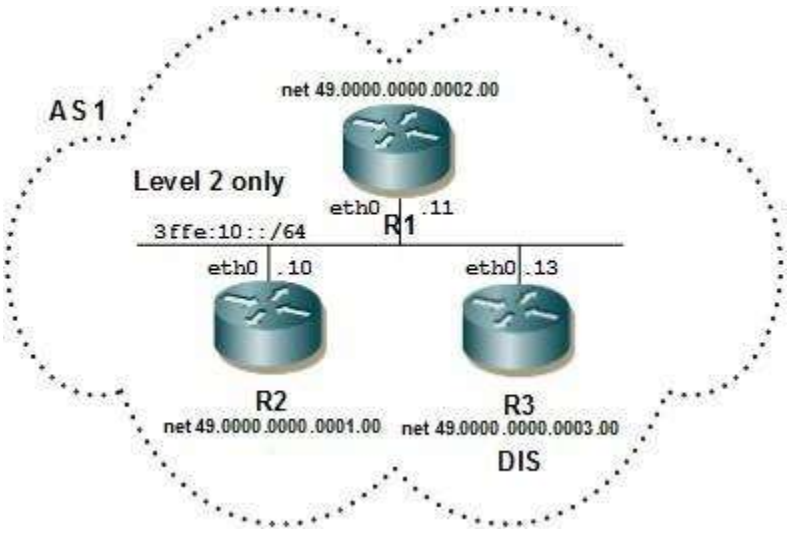


Figure 6-63: Set IS-ISv6 Priority

R3

`# configure terminal`	Enter Configure mode.
`(config)# interface eth0`	Specify the interface (`eth0`) to configure, and enter Interface mode.
`(config-if)# ipv6 router isis Inst1`	Enable IS-IS routing on an interface for area `49 (Inst1).`
`(config-if)# isis priority 70`	Specify the router priority to a higher priority `(70)` to make R3 the designated IS (DIS).
`(config-if)# exit`	Exit Interface mode, and return to Configure mode.

(config)# router isis Inst1	Create an IS-IS routing instance for area 49 (Inst1).
(config-router)# is-type level-2-only	Configure instance Inst1 as level-2-only routing.
(config-router)# net 49.0000.0000.0003.00	Establish a Network Entity Title for this instance, specifying the area address and the system ID.

R1

(config)# interface eth0	Specify the interface (eth0) to configure, and enter Interface mode.
(config-if)# ipv6 router isis Inst1	Enable IS-IS routing on an interface for area 49 (Inst1).
(config-if)# exit	Exit Interface mode, and return to Configure mode.
(config)# router isis Inst1	Create an IS-IS routing instance for area 49 (Inst1).
(config-router)# is-type level-2-only	Configure instance Inst1 as level-2-only routing.
(config-router)# net 49.0000.0000.0000.00	Establish a Network Entity Title for this instance, specifying the area address and the system ID.

R2

(config)# interface eth0	Specify the interface (eth0) to configure, and enter Interface mode.
(config-if)# ipv6 router isis Inst1	Enable IS-IS routing on an interface for area 49 (Inst1).
(config-if)# exit	Exit Interface mode, and return to Configure mode.
(config)# router isis Inst1	Create an IS-IS routing instance for area 49 (Inst1).
(config-router)# is-type level-2-only	Configure instance Inst1 as level-2-only routing.
(config-router)# net 49.0000.0000.0002.00	Establish a Network Entity Title for this instance, specifying the area address and the system ID.

Validation

show clns neighbors, show isis database, show ipv6 isis topology

Redistribute Routes into IS-IS

In this example, the configuration causes BGP routes to be imported into the IS-IS routing table, and advertised into the Inst1 instance.

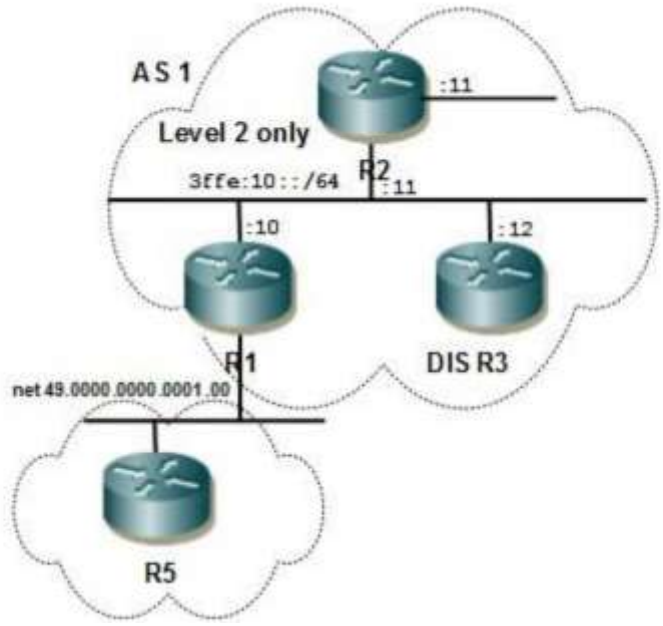


Figure 6-64: Redistribute Routes Into IS-ISv6

R1

`# configure terminal`	Enter Configure mode.
`(config)# interface eth0`	Specify the interface (`eth0`) to configure, and enter Interface mode.
`(config-if)# ipv6 router isis Inst1`	Enable IS-IS routing on an interface for area `49 (Inst1)`.
`(config-if)# exit`	Exit Interface mode, and return to Configure mode.
`(config)# router isis Inst1`	Create an IS-IS routing instance for area `49` (`Inst1`).
`(config-router)# is-type level-2-only`	Establish the IS level for this area (`Inst1`) as `level-2only`.
`(config-router)# net 49.0000.0000.0001.00`	Establish a Network Entity Title for this instance, specifying the area address and system ID.
`(config-router)# address-family ipv6`	Enter Address-Family mode.
`(config-router-af)# redistribute bgp`	Specify redistributing routes from the other routing protocol (BGP) into IS-IS.

Validation

show clns neighbors, show isis database, show ipv6 isis topology, show ipv6 isis route, show ipv6 route

Metric

Make a route the preferred route by changing its metric. In this example, cost has been configured to make R3 the next hop for R1.

The default metric on each interface is 10. Interface eth2 on R2 has a metric of 20, and Interface eth2 on R3 has a metric of 30. The total cost to reach 3ffe:10::/64 (R4) through R2 and R3:

R2: 10+20 = 30

R3: 10+30 = 40

In this topology, R1 chooses R2 as its next hop for destination 10.10.14.0/24.

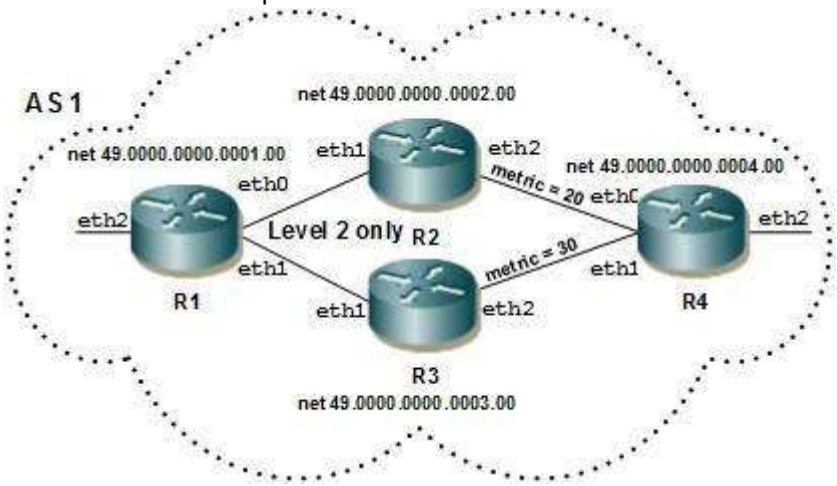


Figure 6-65: IS-ISv6 Metric

R1

`# configure terminal`	Enter Configure mode.
`(config)# interface eth0`	Specify the interface (`eth0`) to configure, and enter Interface mode.
`(config-if)# ipv6 router isis Inst1`	Enable IS-IS routing on an interface for area `49 (Inst1).`
`(config-if)# exit`	Exit Interface mode, and return to Configure mode.
`(config)# interface eth1`	Specify the interface (`eth1`) to configure, and enter Interface mode.
`(config-if)# ipv6 router isis Inst1`	Enable IS-IS routing on an interface for area `49 (Inst1).`
`(config-if)# exit`	Exit Interface mode, and return to Configure mode.
`(config)# interface eth2`	Specify the interface (`eth2`) to configure, and enter Interface mode.
`(config-if)# ipv6 router isis Inst1`	Enable IS-IS routing on an interface for area `49 (Inst1).`
`(config-if)# exit`	Exit Interface mode, and return to Configure mode.
`(config)# router isis Inst1`	Create an IS-IS routing instance for area `49` (`Inst1`).
`(config-router)# is-type level-2-only`	Configure instance `Inst1` as `level-2-only` routing.
`(config-router)# net 49.0000.0000.0001.00`	Establish a Network Entity Title for this instance, specifying the area address and the system ID.

R2

`(config)# interface eth1`	Specify the interface (`eth1`) to configure, and enter Interface mode.
`(config-if)# ipv6 router isis Inst1`	Enable IS-IS routing on an interface for area `49(Inst1)`.
`(config-if)# exit`	Exit Interface mode, and return to Configure mode.
`(config)# interface eth2`	Specify the interface (`eth2`) to configure, and enter Interface mode.
`(config-if)# ipv6 router isis Inst1`	Enable IS-IS routing on an interface for area `49(Inst1)`.
`(config-if)# isis metric 20`	Set the value of IS-IS metric (on `eth2`) to `20`.
`(config-if)# exit`	Exit Interface mode, and return to Configure mode.
`(config)# router isis Inst1`	Create an IS-IS routing instance for area `49` (`Inst1`).
`(config-router)# is-type level-2-only`	Configure instance `Inst1` as `level-2-only` routing.
`(config-router)# net 49.0000.0000.0002.00`	Establish a Network Entity Title for this instance, specifying the area address and the system ID.

R3

`(config)# interface eth1`	Specify the interface (`eth1`) to configure, and enter Interface mode.
`(config-if)# ipv6 router isis Inst1`	Enable IS-IS routing on an interface for area `49 (Inst1)`.
`(config-if)# exit`	Exit Interface mode, and return to Configure mode.
`(config)# interface eth2`	Specify the interface (`eth2`) to configure, and enter Interface mode.
`(config-if)# ipv6 router isis Inst1`	Enable IS-IS routing on an interface for area `49 (Inst1)`.
`(config-if)# isis metric 30`	Set the value of IS-IS metric (on `eth2`) to `30`.
`(config-if)# exit`	Exit Interface mode, and return to Configure mode.
`(config)# router isis Inst1`	Create an IS-IS routing instance for area `49` (`Inst1`).
`(config-router)# is-type level-2-only`	Configure instance `Inst1` as `level-2-only` routing.
`(config-router)# net 49.0000.0000.0003.00`	Establish a Network Entity Title for this instance, specifying the area address and the system ID.

R4

`(config)# interface eth0`	Specify the interface (`eth0`) to configure, and enter Interface mode.
`(config-if)# ipv6 router isis Inst1`	Enable IS-IS routing on an interface for area `49 (Inst1)`.

`(config-if)# exit`	Exit Interface mode, and return to Configure mode.
`(config)# interface eth1`	Specify the interface (`eth1`) to configure, and enter Interface mode.
`(config-if)# ipv6 router isis Inst1`	Enable IS-IS routing on an interface for area `49 (Inst1)`.
`(config-if)# exit`	Exit Interface mode, and return to Configure mode.
`(config)# router isis Inst1`	Create an IS-IS routing instance for area `49 (Inst1)`.
`(config-router)# is-type level-2-only`	Configure instance `Inst1` as `level-2-only` routing.
`(config-router)# net 49.0000.0000.0004.00`	Establish a Network Entity Title for this instance, specifying the area address and the system ID.

Validation

show clns neighbors, show isis database, show ipv6 isis topology, show ipv6 isis route, show ipv6 route

L1-L2 Area Routing with a Single Instance

IS-IS supports a two-level hierarchy for handling and scaling the functionality of large networks. The Level-1 (L1) area is mainly for Leaf networks, and the Level-2 (L2) area is the backbone area connecting Level-1 areas. In this example, R3 and R4 are configured as Level-1 routers, and reside in the Level-1 area. R1 and R2 are configured as Level-1-2 routers, and connect these two Level-1 areas with a backbone Level-2 area. You can configure Level-1-2 routers with single or multiple instances: This configuration shows the single-instance version of the Level-1-2 router.

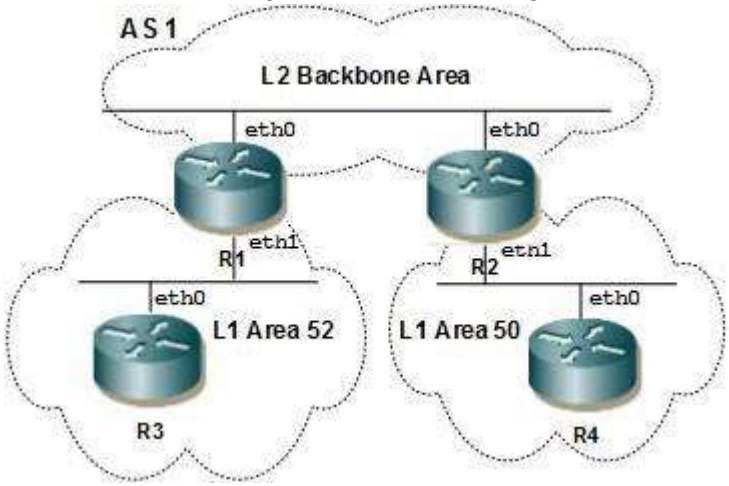


Figure 6-66: Single-Instance L1-L2 Area Routing

R1

`# configure terminal`	Enter Configure mode.
`(config)# interface eth0`	Specify the interface (`eth0`) to configure, and enter Interface mode.

(config-if)# ipv6 router isis abc	Enable IS-IS routing on the interface eth0 for area abc.
(config-if)# isis circuit-type level-2-only	Set the circuit type for the interface eth0.
(config-if)# exit	Exit Interface mode, and return to Configure mode.
(config)# interface eth1	Specify the interface (eth1) to configure, and enter Interface mode.
(config-if)# ipv6 router isis abc	Enable IS-IS routing on the interface eth1 for area abc.
(config-if)# isis circuit-type level-1	Set the circuit type for the interface eth1.
(config-if)# exit	Exit Interface mode, and return to Configure mode.
(config)# router isis abc	Create an IS-IS routing instance for area abc.
(config-router)# net 52.0000.0000.0001.00	Establish a Network Entity Title for this instance, specifying the area address and the system ID.

R2

(config)# interface eth0	Specify the interface (eth0) to configure, and enter Interface mode.
(config-if)# ipv6 router isis bb	Enable IS-IS routing on the interface eth0 for area bb.
(config-if)# isis circuit-type level-2-only	Set the circuit type for the interface eth0.
(config-if)# exit	Exit Interface mode, and return to Configure mode.
(config)# interface eth1	Specify the interface (eth1) to configure, and enter Interface mode.
(config-if)# ipv6 router isis bb	Enable IS-IS routing on the interface eth1 for area bb.
(config-if)# isis circuit-type level-1	Set the circuit type for the interface eth1.
(config-if)# exit	Exit Interface mode, and return to Configure mode.
(config)# router isis bb	Create an IS-IS routing instance for area bb.
(config-router)# net 50.0000.0000.0002.00	Establish a Network Entity Title for this instance, specifying the area address and the system ID.

R3

(config)# interface eth0	Specify the interface (eth0) to configure, and enter Interface mode.
(config-if)# ipv6 router isis xyz	Enable IS-IS routing on the interface eth0 for area xyz.
(config-if)# exit	Exit Interface mode, and return to Configure mode.
(config)# router isis xyz	Create an IS-IS routing instance for area xyz.
(config-router)# is-type level-1	Establish the IS level for this area (xyz) as level-1.
(config-router)# net 52.0000.0000.0003.00	Establish a Network Entity Title for this instance, specifying the area address and the system ID.

R4

`(config)# interface eth0`	Specify the interface (`eth0`) to configure, and enter Interface mode.
`(config-if)# ipv6 router isis aa`	Enable IS-IS routing on the interface `eth0` for area `aa`.
`(config-if)# exit`	Exit Interface mode, and return to Configure mode.
`(config)# router isis aa`	Create an IS-IS routing instance for area `aa`.
`(config-router)# is-type level-1`	Establish the IS level for this area (`aa`) as `level-1`.
`(config-router)# net 50.0000.0000.0004.00`	Establish a Network Entity Title for this instance, specifying the area address and the system ID.

L1-L2 Area Routing with Multiple Instances

IS-IS supports a two-level hierarchy for handling and scaling the functionality of large networks. The Level-1 (L1) area is mainly for Leaf networks, and the Level-2 (L2) area is the backbone area connecting Level-1 areas. In this example, R3 and R4 are configured as Level-1 routers, and reside in the Level-1 area. R1 and R2 are configured as Level-1-2 routers, and connect these two Level-1 areas with a backbone Level-2 area. You can configure Level-1-2 routers with single or multiple instances. This configuration shows the multiple-instance version of the Level-1-2 router.

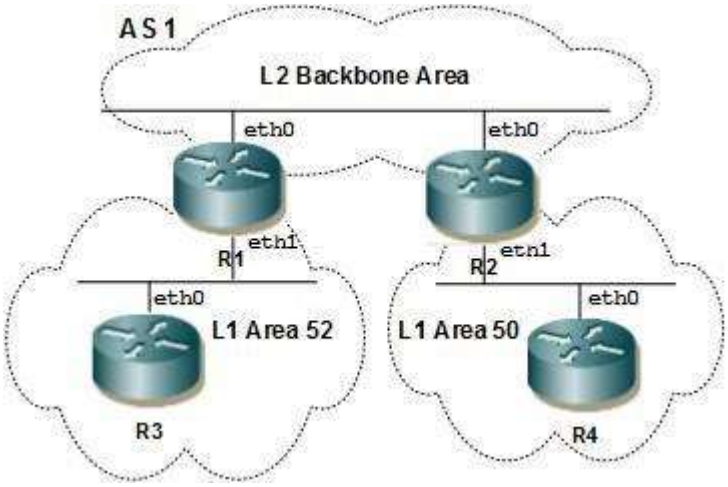


Figure 6-67: Multiple-Instance L1-L2 Area Routing

R1

`# configure terminal`	Enter Configure mode.
`(config)# interface eth0`	Specify the interface (`eth0`) to configure, and enter Interface mode.
`(config-if)# ipv6 router isis aaa`	Enable IS-IS routing on the interface `eth0` for area `aaa`.
`# configure terminal`	Enter Configure mode.
`(config-if)# exit`	Exit Interface mode, and return to Configure mode.
`(config)# router isis aaa`	Create an IS-IS routing instance for area `aaa`.
`(config-router)# is-type level-2-only`	Establish the IS level for this area (`aaa`) as `level-2only`.

(config-router)# net bb.0000.0000.0001.00	Establish a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)# exit	Exit Router mode, and return to Configure mode.
(config)# interface eth1	Specify the interface (eth1) to configure, and enter Interface mode.
(config-if)# ipv6 router isis ccc	Enable IS-IS routing on the interface eth1 for area ccc.
(config-if)# exit	Exit Interface mode, and return to Configure mode.
(config)# router isis ccc	Create an IS-IS routing instance for area ccc.
(config-router)# is-type level-1	Establish the IS level for this area (ccc) as level-1.
(config-router)# net 52.0000.0000.0001.00	Establish a Network Entity Title for this instance, specifying the area address and the system ID.

R2

(config)# interface eth0	Specify the interface (eth0) to configure, and enter Interface mode.
(config-if)# ipv6 router isis bb	Enable IS-IS routing on the interface eth0 for area bb.
(config-if)# exit	Exit Interface mode, and return to Configure mode.
(config)# router isis bb	Create an IS-IS routing instance for area bb.
(config-router)# is-type level-2-only	Establish the IS level for this area (bb) as level-2-only.
(config-router)# net bb.0000.0000.0002.00	Establish a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)# exit	Exit Router mode, and return to Configure mode.
(config)# interface eth1	Specify the interface (eth1) to configure, and enter Interface mode.
(config-if)# ipv6 router isis abc	Enable IS-IS routing on the interface eth1 for area abc.
(config-if)# exit	Exit Interface mode, and return to Configure mode.
(config)# router isis abc	Create an IS-IS routing instance for area abc.
(config-router)# is-type level-1	Establish the IS level for this area (abc) as level-1.
(config-router)# net 52.0000.0000.0002.00	Establish a Network Entity Title for this instance, specifying the area address and the system ID.

R3

(config)# interface eth0	Specify the interface (eth0) to configure, and enter Interface mode.
(config-if)# ipv6 router isis xyz	Enable IS-IS routing on the interface eth0 for area xyz.
(config-if)# exit	Exit Interface mode, and return to Configure mode.
(config)# router isis xyz	Create an IS-IS routing instance for area xyz.
(config-router)# is-type level-1	Establish the IS level for this area (xyz) as level-1.
(config-router)# net 52.0000.0000.0003.00	Establish a Network Entity Title for this instance, specifying the area address and the system ID.

R4

`(config)# interface eth0`	Specify the interface (`eth0`) to configure, and enter Interface mode.
`(config-if)# ipv6 router isis aa`	Enable IS-IS routing on the interface `eth0` for area `aa`.
`(config-if)# exit`	Exit Interface mode, and return to Configure mode.
`(config)# router isis aa`	Create an IS-IS routing instance for area `aa`.
`(config-router)# is-type level-1`	Establish the IS level for this area (`aa`) as `level-1`.
`(config-router)# net 50.0000.0000.0004.00`	Establish a Network Entity Title for this instance, specifying the area address and the system ID.

Validation

show ipv6 isis route, show ipv6 route

Configure IS-IS IPv6 Distance

Administrative distance can be configured for an IS-IS IPv6 address family.

This example shows configuring the IS-IS administrative distance for the IPv6 address family.

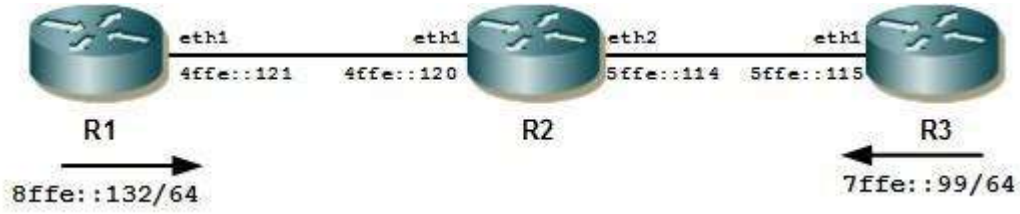


Figure 6-68: IS-ISv6 Distance

R1

`# configure terminal`	Enter Configure mode.
`(config)# interface eth1`	Specify the interface (`eth1`) to configure, and enter Interface mode.
`(config-if)# ipv6 address 4ffe::121/24`	Assign the IPv6 address on this interface (`eth1`).
`(config-if)# ipv6 router isis 1`	Enable IS-ISv6 routing on interface `eth1`.
`(config-if)# exit`	Exit Interface mode, and return to Configure mode.
`(config)# router isis 1`	Create an IS-IS routing instance (`1`).
`(config-router)# net 49.0001.0000.0001.00`	Establish a Network Entity Title (NET) for this instance, specifying the address and the system ID.
`(config-router)# address-family ipv6`	Enter IPv6 Address-Family mode.
`(config-router-af)# redistribute static`	Redistribute the static routes.

R2

`# configure terminal`	Enter Configure mode.
`(config)# interface eth1`	Specify the interface (`eth1`) to configure, and enter Interface mode.
`(config-if)# ipv6 address 4ffe::120/24`	Assign the IPv6 address on this interface (`eth1`).
`(config-if)# ipv6 router isis 1`	Enable IS-ISv6 routing on interface `eth1`.
`(config-if)# exit`	Exit Interface mode, and return to Configure mode.
`(config)# interface eth2`	Specify the interface (`eth2`) to configure, and enter Interface mode.
`(config-if)# ipv6 address 5ffe::114/24`	Assign the IPv6 address on this interface (`eth2`).
`(config-if)# ipv6 router isis 1`	Enable IS-ISv6 routing on interface `eth2`.
`(config-if)# exit`	Exit Interface mode, and return to Configure mode.
`(config)# router isis 1`	Create an IS-IS routing instance (`1`).
`(config-router)# net 49.0001.0000.0002.00`	Specify the NET address.
`(config-router)# address-family ipv6`	Enter IPv6 Address-Family mode.
`(config-router)# distance 60`	Configure the administrative distance in IPv6 Address-Family mode.

R3

`# configure terminal`	Enter Configure mode.
`(config)# interface eth1`	Specify the interface (`eth1`) to configure, and enter Interface mode.
`(config-if)# ipv6 address 5ffe::115/24`	Assign the IPv6 address on this interface (`eth1`).
`(config-if)# ipv6 router isis 1`	Enable IS-ISv6 routing on interface `eth1`.
`(config-if)# exit`	Exit Interface mode, and return to Configure mode.
`(config)# router isis 1`	Create an IS-IS routing instance (`1`).
`(config-router)# net 49.0001.0000.0003.00`	Specify the NET address.
`(config-router)# address-family ipv6`	Enter IPv6 Address-Family mode.
`(config-router)# redistribute static`	Redistribute the static routes.

Validation

show clns neighbors, show ipv6 route, show ipv6 route database, show ipv6 protocols isis, show ipv6 isis route

CHAPTER 7 Forwarding Plane Load Balancing

SWMRE uses Forwarding Plane Load Balancing when the kernel supports Equal Cost Multipath (ECMP). SWMRE installs the maximum number of ECMP routes supported by the kernel. This allows for load balancing to be performed with more than one nexthop to reach a destination. If the router receives and installs multiple paths with the same administrative distance and cost to a destination, load-balancing is possible.

Ideally, multiple nexthops have different interfaces to the destination, but this is not mandatory. The algorithm for distributing traffic across ECMP routes is dependent on the kernel, and typically based on the protocol, source address, destination address, and port.

Enable Load Balancing

The following example illustrates how to enable Equal Cost Multipath (ECMP), and configure a routing protocol (OSPF is used in this example) for load balancing. However, this example will not work if the kernel does not support load balancing. In this topology, R1, R2, and R3 are three Linux routers connected to each other. R1 can reach R3 through two links available to R2.

Topology

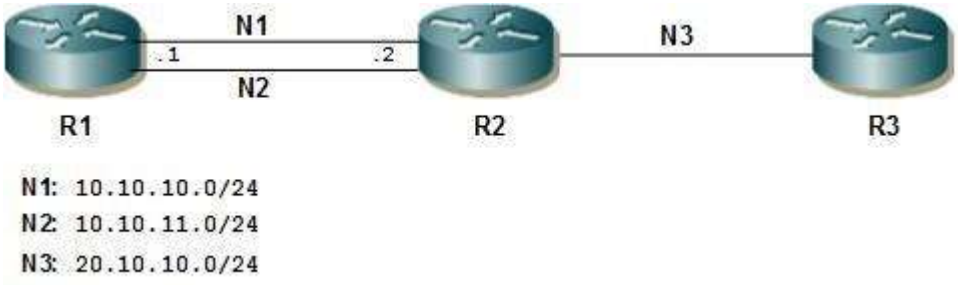


Figure 8-74: Load Balancing Topology

Configuration

R1 - NSM

1. Enable multipath support and set the maximum number of paths to be installed in the Forwarding Information Base (FIB):

```
#configure terminal
(config)#maximum-paths 2
% System Reboot is required for new Maximum-Path value to take effect.
```

Note: User can save and reboot to bring changes into effect.

R1 - OSPF

1. Configure OSPF on all interfaces on R1, R2, and R3.

   R1 learns about R3 through 2 nexthops (both networks N1 and N2).

Forwarding Plane Load Balancing

Validation

R1 - OSPF

Run the `show ip ospf route` command on R1. The OSPF routing table displays that it can reach R3 through both of the nexthops:

```
R1#show ip ospf route
    O  10.10.10.0/24 [10] is directly connected, eth1, Area 0.0.0.0 O
    10.10.11.0/24 [10] is directly connected, eth2, Area 0.0.0.0 O
    20.10.10.0/24 [20] via 10.10.10.2, eth1, Area 0.0.0.0
via 10.10.11.2, eth2, Area 0.0.0.0
```

Run the `show ip route` command on R1. It displays that R1 has installed both nexthops to reach R3 in the NSM routing table:

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default

K       10.10.0.0/24 via 10.70.0.1, eth0
C       10.10.10.0/24 is directly connected, eth1
C10.10.11.0/24 is directly connected, eth2
C10.70.0.0/24 is directly connected, eth0
O20.10.10.0/24 [110/20] via 10.10.10.2, eth1, 00:12:40
                   [110/20] via 10.10.11.2, eth2, 00:12:40
C       127.0.0.0/8 is directly connected, lo
S       192.16.1.0/24 [1/0] is directly connected, eth1
```


CHAPTER 9 VLAN Interfaces

This chapter contains examples for configuring VLAN interfaces.

For details about the commands used in these examples, see the *Layer 2 Command Reference*.

Overview

Several Virtual LAN (VLAN) interfaces can be configured on a single Ethernet interface. Once created, a VLAN interface functions the same as any physical interface.

NSM recognizes VLAN interfaces as physical interfaces. Once VLAN interfaces are created in the kernel, and IP addresses are assigned to them, SWMRE commands can be used to configure and display VLAN interfaces the same as any physical interface. SWMRE routing protocols, such as RIP, OSPF and BGP, can run across networks using VLAN interfaces.

Two systems with physical connectivity (either directly connected or connected through a switch), can communicate with each other via VLAN interfaces that have the same VLAN IDs and belong to the same network.

If the physical interfaces are not directly connected to a switch, the corresponding ports on the switch must be configured as trunks, and should not be associated to any VLANs in the switch. The commands to configure switch ports as trunks depend on the type of the switch, and are beyond the scope of this document.

Topology

Figure 9-75 is used to describe VLAN interface configuration. In this example, there are two routers, R1 and R2, and the eth1 interface of R1 is connected directly to eth2 using an ethernet cable.

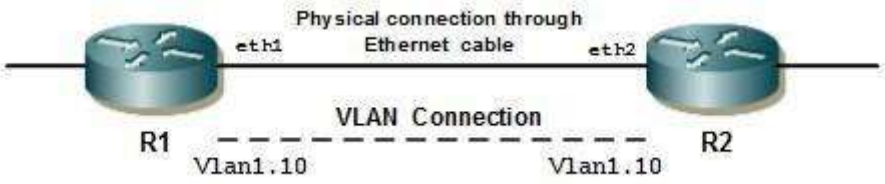


Figure 9-75: VLAN Connections

The `vlan1.10` VLAN interface is created on R1, and `vlan1.10` is created on R2. The VLAN interfaces are configured in the same network: R1 and R2 can reach each other using the VLAN connection.

Note: A VLAN ID of both VLAN interfaces is the same (10). Two systems with different VLAN IDs cannot communicate, even if they are in the same network, since a VLAN ID tags packets sent on a VLAN interface.

Create a VLAN Interface

When a VLAN interface is configured, a Layer 3 interface based on the bridge-group number and VLAN ID is created. This Layer 3 interface is advertised to all the Layer 3 protocols.

`#configure terminal`	Enter Configure mode.
`(config)#bridge 1 protocol mstp`	Create a MSTP bridge.
`(config)#vlan database`	Enter VLAN mode.

VLAN Interfaces

`(config-vlan)#vlan 10 bridge 1`	Enable VLAN 10 on bridge 1.
`(config-vlan)#exit`	Exit VLAN mode.
`(config)#interface eth1`	Enter interface mode
`(config-if)#switchport`	Configure interface as Layer2 interface.
`(config-if)#bridge-group 1`	Associate bridge group 1.

`(config-if)#switchport mode trunk`	Configure interface eth1 as Layer2 trunk mode.
`(config-if)#switchport trunk allowed vlan add 10`	Associate VLAN 10 as trunk port.
`(config-if)#exit`	Exit interface mode.

Add IP Addresses to VLAN Interface

In NSM, you can add or remove IP addresses from VLAN interfaces, like normal interfaces. Using IMISH type:

```
#configure terminal
(config)#interface vlan1.10
(config-if)#ip address 192.168.1.50/24
```

Display VLAN Interfaces

In SWMRE, VLAN interfaces appear as any physical interfaces, in the `show running-config` or the `show ip interface brief` outputs, and can be configured as any other interface.

The following is a sample output of the `show ip interface brief` command on R1.

Note:The IP address of interface `eth1.1` has correctly been changed by NSM:

```
#show ip interface brief
Interface          IP-Address      Status                    Protocol
lo                 127.0.0.1       up                        up gre0
unassigned       administratively down    down eth0
10.70.0.77      up                        up
.... sit0               unassigned      administratively down
down vlan1.10             192.168.1.50    up
up tunl0              unassigned      administratively down
down
```

Below is the NSM routing table, which shows the connected network `192.168.1.0/24` of `eth1.10`. These interfaces will now act as any physical interfaces, and all routing protocols will run across this network.

```
#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       area * - candidate default
Gateway of last resort is 10.70.0.1 to network 0.0.0.0
K*      0.0.0.0/0 via 10.70.0.1, eth0
B       2.2.2.0/24 [200/0] via 192.168.1.145, eth4.2, 01:14:38
....
C       127.0.0.0/8 is directly connected, lo
K       169.254.0.0/16 is directly connected, eth4
```



```
C       192.168.1.0/24 is directly connected, vlan1.10
```

CHAPTER 13 Layer 3 Link Aggregation

This chapter contains a complete sample Link Aggregation Control Protocol (LACP) configuration (L3 LAG).

Link Aggregation is the method of combining individual physical network interfaces or ports to increase the capacity of the link to support and sustain beyond the individual port capability. Features like Spanning Tree, VLAN, FDB, Multicast operate on both physical ports as well as Link Aggregated Logical Ports. It bundles all of the controller's distribution system ports into a single 802.3ad port channel, thereby reducing the number of IP addresses needed to configure the ports on your controller. When LAG is enabled, the system dynamically manages port redundancy and load balances access points transparently to the user.

LACP is based on the 802.3ad IEEE specification. It allows bundling of several physical interfaces to form a single logical channel providing enhanced performance and redundancy. The aggregated interface is viewed as a single link to each switch. The spanning tree views it as one interface and not as two or three interfaces. When there is a failure in one physical interface, the other interfaces stay up and there is no disruption.

The SWMRE LACP implementation supports the aggregation of a maximum of six physical Ethernet links into a single logical channel.

Topology

In this example, 3 links are configured between the two switches R1 and R2. These three links are assigned the same administrative key (1) so that they aggregate to form a single channel 1. They are viewed by STP as one interface.

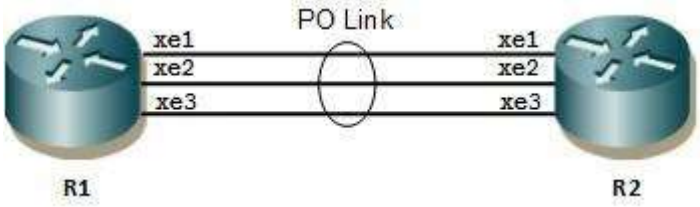


Figure 13-91: L3_LAG Topology

Configuration

R1

`R1#configure terminal`	Enter configure mode.
`R1(config)#lacp system-priority 20000`	Set the system priority of this switch. This priority is used for determining the system that is responsible for resolving conflicts in the choice of aggregation groups. A lower numerical value has a higher priority.
`R1(config)#interface xe1`	Enter interface mode.
`R1(config-if)#no switchport`	Making Interface as L3 Port

R1(config-if)#channel-group 10 mode active	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
R1(config-if)#exit	Exit interface mode.
R1(config)#interface xe2	Enter interface mode.
R1(config-if)#no switchport	Making Interface as L3 Port

Layer 3 Link Aggregation

R1(config-if)#channel-group 10 mode active	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
R1(config-if)#exit	Exit interface mode.
R1(config)#interface xe3	Enter interface mode.
R1(config-if)#no switchport	Making Interface as L3 Port
R1(config-if)#channel-group 10 mode active	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
R1(config-if)#exit	Exit interface mode.
R1(config)#interface po10	Enter interface mode.
R1(config-if)#ip address 1.1.1.1/24	Assigning IP Address to PO Interface
R1(config-if)#exit	Exit interface mode.

R2

R2#configure terminal	Enter configure mode.
R2(config)#lacp system-priority 20000	Set the system priority of this switch. This priority is used for determining the system that is responsible for resolving conflicts in the choice of aggregation groups. A lower numerical value has a higher priority.
R2(config)#interface xe1	Enter interface mode.
R2(config-if)#no switchport	Making Interface as L3 Port
R2(config-if)#channel-group 10 mode active	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
R2(config-if)#exit	Exit interface mode.
R2(config)#interface xe2	Enter interface mode.
R2(config-if)#no switchport	Making Interface as L3 Port
R2(config-if)#channel-group 10 mode active	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
R2(config-if)#exit	Exit interface mode.
R2(config)#interface xe3	Enter interface mode.
R2(config-if)#no switchport	Making Interface as L3 Port

R2(config-if)#channel-group 10 mode active	Add this interface to channel group 10 and enable link aggregation so that it can be selected for aggregation by the local system.
R2(config-if)#exit	Exit interface mode.
R1(config)#interface po10	Enter interface mode.
R1(config-if)#ip address 1.1.1.2/24	Assigning IP Address to PO Interface
R1(config-if)#exit	Exit interface mode.

Layer 3 Link Aggregation

Static Channel-group

R1

R1#configure terminal	Enter configure mode.
R1(config)#interface xe1	Enter interface mode.
R1(config-if)#static-channel-group 12	Add this interface to channel group 12 and enable link aggregation so that it can be selected for aggregation by the local system.
R1(config-if)#exit	Exit interface mode.
R1(config)#interface sa12	Enter interface mode.
R1(config-if)#no switchport	Making Interface as L3 Port
R1(config-if)#ip address 2.2.2.1/24	Assigning IP Address to PO Interface
R1(config-if)#exit	Exit interface mode.

R2

R2#configure terminal	Enter configure mode.
R2(config)#interface xe1	Enter interface mode.
R2(config-if)#static-channel-group 12	Add this interface to channel group 12 and enable link aggregation so that it can be selected for aggregation by the local system.
R2(config-if)#exit	Exit interface mode.
R2(config)#interface sa12	Enter interface mode.
R2(config-if)#no switchport	Making Interface as L3 Port
R2(config-if)#ip address 2.2.2.2/24	Assigning IP Address to PO Interface
R2(config-if)#exit	Exit interface mode.

Validation

show etherchannel detail, show etherchannel summary

```
#sh etherchannel summary
% Aggregator po10 100010
```

```
% Admin Key: 0010 - Oper Key 0010
%   Link: xe1 (10049) sync: 1
%   Link: xe2 (10050) sync: 1
%   Link: xe3 (10051) sync: 1

#sh etherchannel detail
% Aggregator po10 100010
%  Mac address: 14:18:77:5d:5c:01
%  Admin Key: 0010 - Oper Key 0010
%  Actor LAG ID- 0x4e20,14-18-77-01-5c-00,0x000a
%  Receive link count: 3 - Transmit link count: 3
```



```
%  Individual: 0 - Ready: 1
%  Partner LAG ID- 0x4e20,14-18-77-01-73-00,0x000a
%   Link: xe1 (10049) sync: 1
%   Link: xe2 (10050) sync: 1
%   Link: xe3 (10051) sync: 1

#sh etherchannel 10
% Aggregator po10 100010 Admin Key: 0010 - Oper Key 0010
% Partner LAG ID: 0x4e20,14-18-77-01-73-00,0x000a
% Partner Oper Key 0010

#sh etherchannel
% Lacp Aggregator: po10
% Member:xe1xe2xe3
```

CHAPTER 9 Static Routes

This chapter contains basic static routing configuration examples.

This example shows the complete configuration to enable static routing in a simple network topology. A static route is composed of a network prefix (host address) and a nexthop (gateway). Static routes are useful in small networks. They are simple solutions for making a few destinations reachable. Large networks use dynamic routing protocols.

For details about the commands used in these examples, see the *Unicast Routing Information Base Command Reference*.

Topology

Router R1 is configured with these static routes:

- The remote network 10.10.12.0/24
- The loopback address (host addresses) of router R2
- The loopback address of router R3

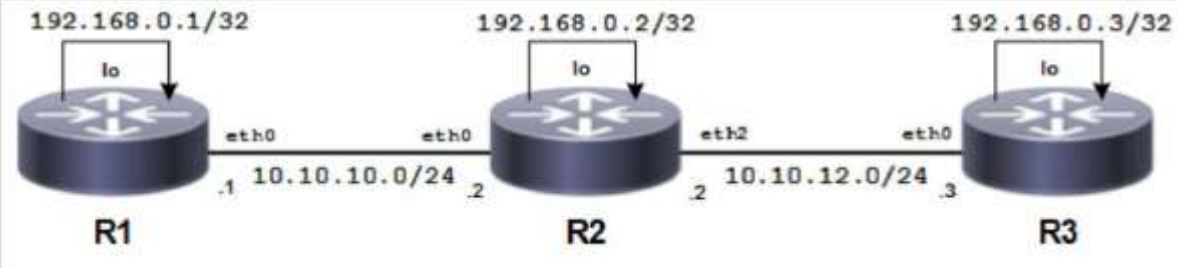


Figure 15-93: Basic Static Route

In all three routes, interface `eth0` of router R2 is the gateway. Router R3 is configured with a default static route that is equivalent to configuring separate static routes with the same gateway or nexthop address. Router R2 has two routes, one for each of the remote routers' loopback address.

Configuration

R1

`#configure terminal`	Enter configure mode.
`(config)#interface lo`	Enter interface mode.
`(config-if)#ip address 192.168.0.1/32`	Configure the IP address on this interface, and specify a 32bit mask, making it a host address.
`(config-if)#exit`	Exit interface mode.

`(config)#ip route 10.10.12.0/24 10.10.10.2`
`(config)#ip route 192.168.0.2/32 10.10.10.2`
`(config)#ip route 192.168.0.3/32 10.10.10.2`
	Specify the destination prefix and mask for the network and a gateway.
	Because R2 is the only next hop available, you can configure a default route instead of configuring the same static route for individual addresses. See the configuration of R3.

R2

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 192.168.0.2/32	Configure the IP address on this interface, and specify a 32bit mask, making it a host address.
(config-if)#exit	Exit Interface mode.
(config)#ip route 192.168.0.1/32 10.10.10.1 (config)#ip route 192.168.0.3/32 10.10.12.3	Specify the destination and mask for the network and a gateway.

R3

#configure terminal	Enter configure mode.
(config)#interface lo	Enter interface mode.
(config-if)#ip address 192.168.0.3/32	Configure the IP address on this interface, and specify a 32bit mask, making it a host address.
(config-if)#exit	Exit Interface mode.
(config)#ip route 0.0.0.0/0 10.10.12.2	Specify 10.10.12.2 as a default gateway to reach any network. Because 10.10.12.2 is the only available route, you can specify it as the default gateway instead of specifying it as the gateway for an individual network or host address.

Validation

show ip route, show ip route summary, show ip route database

R1

```
#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 10.12.4.1 to network 0.0.0.0

K*      0.0.0.0/0 [0/0] via 10.12.4.1, eth0
C       10.10.10.0/24 is directly connected, eth1
S10.10.12.0/24 [1/0] via 10.10.10.2, eth1
C10.12.4.0/24 is directly connected, eth0
C127.0.0.0/8 is directly connected, lo
C192.168.0.1/32 is directly connected, lo
S192.168.0.2/32 [1/0] via 10.10.10.2, eth1
S192.168.0.3/32 [1/0] via 10.10.10.2, eth1

#show ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths   : 8
```

```
Total number of IPv4 routes       : 8
Total number of IPv4 paths        : 8
Route Source    Networks
kernel          1 connected
4 static          3 Total
8
FIB              0

ECMP statistics (active in ASIC):
 ---------------------------------
  Total number of IPv4 ECMP routes   : 0
  Total number of IPv4 ECMP paths    : 0

 ---------------------------------

#show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
K    *> 0.0.0.0/0 [0/0] via 10.12.4.1, eth0
C    *> 10.10.10.0/24 is directly connected, eth1
S*> 10.10.12.0/24 [1/0] via 10.10.10.2, eth1
C*> 10.12.4.0/24 is directly connected, eth0
C*> 127.0.0.0/8 is directly connected, lo
C*> 192.168.0.1/32 is directly connected, lo
S*> 192.168.0.2/32 [1/0] via 10.10.10.2, eth1
S*> 192.168.0.3/32 [1/0] via 10.10.10.2, eth1

Gateway of last resort is not set
```

R2

```
#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 10.12.4.1 to network 0.0.0.0

K*      0.0.0.0/0 [0/0] via 10.12.4.1, eth0
C       10.10.10.0/24 is directly connected, eth1
C10.10.12.0/24 is directly connected, eth2
C10.12.4.0/24 is directly connected, eth0
```

```
C       127.0.0.0/8 is directly connected, lo
S       192.168.0.1/32 [1/0] via 10.10.10.1, eth1
C       192.168.0.2/32 is directly connected, lo
S       192.168.0.3/32 [1/0] via 10.10.12.3, eth2

#sh ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths    : 8
Total number of IPv4 routes       : 9
Total number of IPv4 paths        : 9
Route Source    Networks
kernel          1 connected
5 static          3 Total
9
FIB              0

ECMP statistics (active in ASIC):
 --------------------------------
 Total number of IPv4 ECMP routes   : 0
 Total number of IPv4 ECMP paths    : 0

--------------------------------

#sh ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
K    *> 0.0.0.0/0 [0/0] via 10.12.4.1, eth0
C    *> 10.10.10.0/24 is directly connected, eth1
C*> 10.10.12.0/24 is directly connected, eth2
C*> 10.12.4.0/24 is directly connected, eth0
C*> 127.0.0.0/8 is directly connected, lo
S*> 192.168.0.1/32 [1/0] via 10.10.10.1, eth1
C*> 192.168.0.2/32 is directly connected, lo
S*> 192.168.0.3/32 [1/0] via 10.10.12.3, eth2

Gateway of last resort is not set
```

R3

```
#sh ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default
```

```
    IP Route Table for VRF "default"
    Gateway of last resort is 10.12.4.1 to network 0.0.0.0

    K*       0.0.0.0/0 [0/0] via 10.12.4.1, eth0
C       10.10.12.0/24 is directly connected, eth2
C       10.12.4.0/24 is directly connected, eth0
C       127.0.0.0/8 is directly connected, lo
C       192.168.0.3/32 is directly connected, lo

#sh ip route summary
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths    : 8
Total number of IPv4 routes       : 6
Total number of IPv4 paths        : 6
Route Source    Networks kernel
2 connected       4 Total
6
FIB             0

ECMP statistics (active in ASIC):
---------------------------------
 Total number of IPv4 ECMP routes    : 0
 Total number of IPv4 ECMP paths     : 0
---------------------------------


#sh ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2        E1 -
OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       > - selected route, * - FIB route, p - stale info

IP Route Table for VRF "default"
K    *> 0.0.0.0/0 [0/0] via 10.12.4.1, eth0
S       0.0.0.0/0 [1/0] via 10.10.12.2 inactive
C*> 10.10.12.0/24 is directly connected, eth2
C*> 10.12.4.0/24 is directly connected, eth0
C*> 127.0.0.0/8 is directly connected, lo
C*> 192.168.0.3/32 is directly connected, lo

Gateway of last resort is not set
```

CHAPTER 10 Static Route Discard Configuration

This chapter show how to configure the static route discard feature.

Overview

If you identify some routers/attackers distributing invalid/bogus routes just to use the resources of the device or to make the device unstable, you can configure route-map rules, discard all routes, and black hole traffic corresponding to those routes.

To so this, you add “discard” route entries for a prefix in a route map with the “set interface null0” command. You then apply that route map to a BGP neighbor.

IPv4 Route Discard

Figure 16-94 shows the configuration required to enable static route discard for IPv4.

Topology

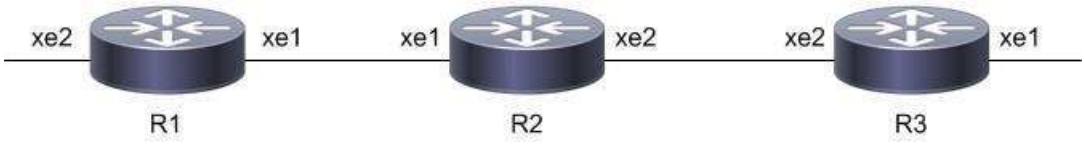


Figure 16-94: Static route discard topology

Configuration

R1

`R1#configure terminal`	Enter Configure mode
`R1(config)#interface xe1`	Enter interface mode for xe1
`R1(config-if)#ip address 2.2.2.2/24`	Assign an IP address to the interface
`R1(config-if)#exit`	Exit interface mode.
`R1(config)#interface xe2`	Enter interface mode for xe1
`R1(config-if)#ip address 1.1.1.2/24`	Assign an IP address to the interface
`R1(config-if)#exit`	Exit interface mode
`R1(config)#router bgp 2`	Enter BGP router mode
`R1(config-router)#neighbor 2.2.2.3 remote-as 3`	Create static BGP neighbor 2.2.2.3 with remote autonomous system value 3
`R1(config-router)#redistribute connected`	Advertise the connected network into BGP
`R1(config-router)#end`	Exit BGP router mode

R2

R2#configure terminal	Enter configure mode
R2(config)#ip prefix-list p1 permit any	Configure IP prefix list
R2(config)#route-map r1	Enter route-map mode
R2(config-route-map)#match ip address prefix-list p1	Configure match ip prefix list p1
R2(config-route-map)#set interface null0	Set the interface to null0
R2(config-route-map)#exit	Exit route-map mode.
R2(config)#interface xe1	Enter interface mode for xe1
R2(config-if)#ip address 2.2.2.3/24	Assign an IP address to the interface
R2(config-if)#exit	Exit interface mode.
R2(config)#interface xe2	Enter interface mode for xe2
R2(config-if)#ip address 3.3.3.2/24	Assign an IP address to the interface
R2(config-if)#exit	Exit interface mode
R2(config)#router bgp 3	Enter into BGP router mode
R2(config-router)#neighbor 2.2.2.2 remote-as 2	Create static BGP neighbor 2.2.2.2 with remote autonomous system value 2
R2(config-router)#neighbor 3.3.3.3 remote-as 4	Create static BGP neighbor 3.3.3.3 with remote autonomous system value 4
R2(config-router)#redistribute connected	Advertise the connected network into BGP
R2(config-router)#neighbor 2.2.2.2 route-map r1 in	Attach the route-map with route discard configured for the neighbor 2.2.2.2 in IN direction
R2(config-router)#end	Exit BGP router mode

R3

R3#configure terminal	Enter configure mode.
R3(config)#interface xe2	Enter interface mode for xe2
R3(config-if)#ip address 3.3.3.3/24	Assign an IP address to the interface
R3(config-if)#exit	Exit interface mode
R3(config)#interface xe1	Enter interface mode for xe1
R3(config-if)#ip address 4.4.4.2/24	Assign an IP address to the interface
R3(config-if)#exit	Exit interface mode.
R3(config)#router bgp 4	Enter into BGP router mode
R3(config-router)#neighbor 3.3.3.2 remote-as 3	Create static BGP neighbor 3.3.3.2 with remote autonomous system value 3
R3(config-router)#redistribute connected	Advertise the connected network into BGP
R3(config-router)#end	Exit BGP router.

Validation

```
R2#show running-config bgp !
```

```
router bgp 3  redistribute connected
neighbor 2.2.2.2 remote-as 2  neighbor
2.2.2.2 route-map r1 in  neighbor
3.3.3.3 remote-as 4 !

R2#show ip bgp
BGP table version is 3, local router ID is 2.2.2.3
Status  codes:  s  suppressed,  d damped, h  history,  *  valid, >  best,  i - internal,
l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric    LocPrf      Weight Path
*>    1.1.1.0/24       2.2.2.2                  0          100             0        2? *>
2.2.2.0/24        0.0.0.0             0         100           32768     ?
*                     2.2.2.2                  0          100              0        2 ?*>
                      3.3.3.0/24       0.0.0.0             0         100          32768
                      ?
*                     3.3.3.3               0         100           0       4 ?
*>    4.4.4.0/24      3.3.3.3               0         100           0       4 ?

Total number of prefixes 4


R2#show running-config prefix-list !
ip prefix-list p1 seq 5 permit any !

R2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2        E1
- OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
v - vrf leaked        * - candidate default

IP Route Table for VRF "default"
B     1.1.1.0/24 [20/0] is a summary, Null, 00:00:01
C     2.2.2.0/24 is directly connected, xe1, 00:09:57
C     3.3.3.0/24 is directly connected, xe2, 00:09:50
B     4.4.4.0/24 [20/0] via 3.3.3.3, xe2, 00:00:03
C     127.0.0.0/8 is directly connected, lo, 01:18:30

Gateway of last resort is not set

R2#show hsl nh-table
IPv4 FIB 0
  , Null, 00:00:00:00:00:00, Valid  ,
                      1.1.1.0/24, Installed FORWARD
2.2.2.2, xe1, 00:18:23:de:ee:cf, Valid , lport:0x8000034, Egress object id:100003,
refcnt 0, rulecnt 0

3.3.3.3, xe2, ec:f4:bb:84:78:1b, Valid , lport:0x8000032, Egress object id:100004,
refcnt 1, rulecnt 0,
```

```
                    4.4.4.0/24, Installed FORWARD

IPv4 FIB 1
10.12.29.1, eth0, 00:00:00:00:00:00, Invalid, ,
Not Installed TO_CPU
```

IPv6 Route Discard

Figure 16-94 shows the configuration required to enable static route discard for IPv6.

Configuration

R1

`R1#configure terminal`	Enter Configure mode.
`R1(config)#interface lo`	Enter interface mode for loopback
`R1(config-if)#ip address 1.1.1.2/24 secondary`	Assign an IPv4 address to the interface
`R1(config-if)#exit`	Exit interface mode
`R1(config)#interface xe1`	Enter interface mode for xe1
`R1(config-if)#ipv6 address 2001::2/64`	Assign an IPv6 address to the interface
`R1(config-if)#exit`	Exit interface mode
`R1(config)#interface xe2`	Enter interface mode for xe2
`R1(config-if)#ipv6 address 1001::2/64`	Assign an IPv6 address to the interface
`R1(config-if)#exit`	Exit interface mode
`R1(config)#router bgp 2`	Enter BGP router mode
`R1(config-router)#neighbor 2001::3 remote-as 3`	Create static BGP neighbor 2001::3 with remote autonomous system value 3
`R1(config-router)#address-family ipv6 unicast`	Enter address family IPv6 unicast mode
`R1(config-router-af)#neighbor 2001::3 activate`	Activate neighbor in IPv6 address family
`R1(config-router-af)#redistribute connected`	Advertise the connected network into BGP
`R1(config-router)#end`	Exit BGP router mode

R2

`R2#configure terminal`	Enter configure mode
`R2(config)#interface lo`	Enter Interface mode for loopback
`R2(config-if)#ip address 2.2.2.2/24 secondary`	Assign an IPV4 address
`R2(config-if)#exit`	Exit Interface mode
`R2(config)#ipv6 prefix-list p1 permit any`	Configure IPv6 prefix list.

R2(config)#route-map r1	Enter route-map mode.
R2(config-route-map)#match ipv6 address prefix-list p1	Configure match IPv6 prefix list p1
R2(config-route-map)#set interface null0	Set the interface to null0
R2(config-route-map)#exit	Exit route-map mode
R2(config)#interface xe1	Enter interface mode for xe1
R2(config-if)#ipv6 address 2001::3/64	Assign ipv6 address to the interface
R2(config-if)#exit	Exit interface mode
R2(config)#interface xe2	Enter interface mode for xe2
R2(config-if)#ipv6 address 3001::2/64	Assign an IPv6 address to the interface
R2(config-if)#exit	Exit interface mode
R2(config)#router bgp 3	Enter BGP router mode
R2(config-router)#neighbor 2001::2 remote-as 2	Create static BGP neighbor 2001::2 with remote autonomous system value 2
R2(config-router)#neighbor 3001::3 remote-as 4	Create static BGP neighbor 3001::3 with remote autonomous system value 4
R2(config-router)#address-family ipv6 unicast	Enter address family IPv6 unicast mode
R2(config-router-af)#redistribute connected	Advertise the connected network into BGP
R2(config-router-af)#neighbor 2001::2 activate	Activate the neighbor in IPv6 address family
R2(config-router-af)#neighbor 3001::3 activate	Activate the neighbor in IPv6 address family
R2(config-router-af)#neighbor 2001::2 routemap r1 in	Attach the route-map with route discard configured for the neighbor 2001::2 in IN direction
R2(config-router)#end	Exit BGP router mode

R3

R3#configure terminal	Enter configure mode
R3(config)#interface lo	Enter interface mode for loopback
R3(config-if)#ip address 3.3.3.2/24 secondary	Assign an IPV4 address to the interface
R3(config-if)#exit	Exit interface mode
R3(config)#interface xe1	Enter interface mode for xe1
R3(config-if)#ipv6 address 4001::2/64	Assign an IPv6 address to the interface
R3(config-if)#exit	Exit interface mode
R3(config)#interface xe2	Enter interface mode for xe2
R3(config-if)#ipv6 address 3001::3/64	Assign an IPv6 address to the interface
R3(config-if)#exit	Exit interface mode
R3(config)#router bgp 4	Enter into BGP router mode

R3(config-router)#neighbor 3001::2 remote-as 3	Create static BGP neighbor 3001::2 with remote autonomous system value 3
R3(config-router)#address-family ipv6 unicast	Enter address family IPv6 unicast mode
R3(config-router-af)#neighbor 3001::2 activate	Activate neighbor in IPv6 address family
R3(config-router-af)#redistribute connected	Advertise the connected network into BGP
R3(config-router)#end	Exit BGP router mode.

Validation

```
R2#sh running-config bgp !
router bgp 3
 neighbor  2001::2  remote-as  2    neighbor
3001::3 remote-as 4
 !  address-family ipv6 unicast
redistribute connected neighbor 2001::2
activate neighbor 2001::2 route-map r1
in neighbor 3001::3 activate exit-
address-family

R2#show  bgp ipv6
BGP table version is 3, local router ID is 2.2.2.3
Status  codes:  s suppressed,  d  damped,  h  history,  *  valid, >  best,  i -  internal,
l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network          Next Hop             Metric    LocPrf       Weight Path
*>    1001::/64       2001::2(fe80::218:23ff:fede:eecf)
                                          0         100           0       2 ?
*>    2001::/64       ::                   0         100          32768     ?
*                     2001::2(fe80::218:23ff:fede:eecf)
0          100          0        2 ?
*>    3001::/64       ::                   0         100          32768     ?
*                     3001::3(fe80::eef4:bbff:fe84:781b)
0          100          0        4 ?
*>    4001::/64       3001::3(fe80::eef4:bbff:fe84:781b)
                                          0         100           0       4 ?

Total number of prefixes 4

R2#show running-config ipv6 prefix-list !
ipv6 prefix-list p1 seq 5 permit any !
R2#
R2#show ipv6 route
IPv6 Routing Table
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
       IA - OSPF inter area, E1 - OSPF external type 1,
       E2 - OSPF external type 2, N1 - OSPF NSSA external type 1,
```

```
       N2 - OSPF NSSA external type 2, I - IS-IS, B - BGP Timers:
Uptime

IP Route Table for VRF "default"
C      ::1/128 via ::, lo, 00:56:44
B      1001::/64 [20/0] via ::, Null, 00:00:04
C      2001::/64 via ::, xe1, 00:13:03
C      3001::/64 via ::, xe2, 00:12:56
B       4001::/64 [20/0] via fe80::eef4:bbff:fe84:781b, xe50, 00:00:02 C
fe80::/64 via ::, xe50, 00:46:14

R2#show hsl nh-table
IPv4 FIB 0

IPv4 FIB 1
10.12.29.1,  eth0,  00:00:00:00:00:00,  Invalid,
, Not Installed TO_CPU

IPv6 FIB 0
  , Null, 00:00:00:00:00:00, Valid  ,
                      1001::/64, Installed FORWARD
2001::2, xe1, 00:18:23:de:ee:cf, Valid , lport:0x8000034, Egress object id:100003,
refcnt 0, rulecnt 0

3001::3, xe2, ec:f4:bb:84:78:1b, Valid , lport:0x8000032, Egress object id:100004,
refcnt 0, rulecnt 0

fe80::218:23ff:fede:eecf, xe52, 00:18:23:de:ee:cf, Valid  , lport:0x8000034, Egress
object id:100003, refcn t 0, rulecnt 0
fe80::eef4:bbff:fe84:781b, xe50, ec:f4:bb:84:78:1b, Valid  , lport:0x8000032, Egress
object id:100004, refc nt 1, rulecnt 0,
                      4001::/64, Installed FORWARD

IPv6 FIB 1
```

CHAPTER 11 RIP

This chapter contains basic Router Information Protocol (RIP) configuration examples.

For details about the commands used in these examples, see the *Routing Information Protocol Command Reference*.

Enable RIP

This example shows the minimum configuration required to enable RIP on an interface. R1 and R2 are two routers connecting to network 10.10.11.0/24. R1 and R2 are also connected to networks 10.10.10.0/24 and 10.10.12.0/24, respectively. To enable RIP, first define the RIP routing process, then associate a network with the routing process.

Topology

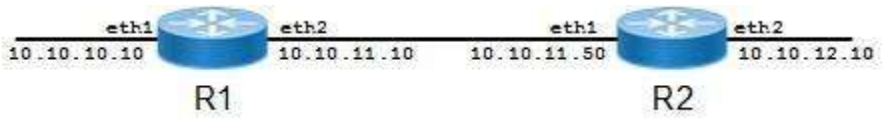


Figure 17-95: Enable RIP Topology

R1

`#configure terminal`	Enter Configure mode.
`(config)#router rip`	Define a RIP routing process, and enter Router mode.
`(config-router)#network 10.10.10.0/24` `(config-router)#network 10.10.11.0/24`	Associate networks with the RIP process.

R2

`#configure terminal`	Enter Configure mode.
`(config)#router rip`	Define a RIP routing process, and enter Router mode.
`(config-router)#network 10.10.11.0/24` `(config-router)#network 10.10.12.0/24`	Associate networks with the RIP process.

Validation

show ip rip, show running-config, show ip protocols rip, show ip rip interface, show ip route

R1

```
    #show ip rip

    Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
           C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP,
    X - Default

       Network            Next Hop         Metric From            If     Time
    Rc 10.10.10.0/24                           1                  eth1
    Rc 10.10.11.0/24                           1                  eth2
#show running-config
```

```
!
no service password-encryption
!
hostname rtr1
!
logging monitor 7
!
ip vrf management
! ip domain-lookup
spanning-tree mode provider-rstp data-center-
bridging enable feature telnet feature ssh no
feature tacacs+ snmp-server view all .1
included ntp enable sFlow disable
software-watchdog keep-alive-time 30
!
ip pim register-rp-reachability
! interface lo mtu 65536 ip address 127.0.0.1/8
ip address 192.168.0.2/32 secondary ipv6 address
::1/128
! interface eth0  ip address
10.12.4.108/24
! interface eth1 ip address
10.10.10.10/24
! interface eth2 ip address
10.10.11.10/24
!
router rip network 10.10.10.0/24
network 10.10.11.0/24
!
line con 0 login line vty
0 39 login
! end

#show ip protocols rip
RIP Database for VRF (default)
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 14 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1 Redistributing:

  Default version control: send version 2, receive version 2
    Interface        Send  Recv   Key-chain
eth1             2     2     eth2             2
2
  Routing for Networks:
    10.10.10.0/24
    10.10.11.0/24
  Routing Information Sources:
```

```
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
  Number of routes (including connected): 2
  Distance: (default is 120)

#show ip rip interface
svlan0.1 is down, line protocol is down   RIP is
not enabled on this interface eth2 is up, line
protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:        10.10.11.10/24
eth1 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:        10.10.10.10/24
eth0 is up, line protocol is up    RIP is not
enabled on this interface lo is up, line
protocol is up   RIP is not enabled on this
interface

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2        E1
- OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 10.12.4.1 to network 0.0.0.0

K*      0.0.0.0/0 [0/0] via 10.12.4.1, eth0
C       10.10.10.0/24 is directly connected, eth1
C10.10.11.0/24 is directly connected, eth2
C10.12.4.0/24 is directly connected, eth0
C127.0.0.0/8 is directly connected, lo
C192.168.0.2/32 is directly connected, lo
```

R2

```
    #show ip rip

    Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
           C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP,
    X - Default

       Network            Next Hop         Metric From            If     Time
```

```
    Rc  10.10.11.0/24                          1               eth1
    Rc  10.10.12.0/24                          1               eth2

    2#show running-config
    !
    no service password-encryption
    !
    hostname rtr2
    !
    logging monitor 7
    !
    ip vrf management
    ! ip domain-lookup
    spanning-tree mode provider-rstp data-
    center-bridging enable feature telnet
    feature ssh no feature tacacs+
    snmp-server view all .1 included ntp
    enable sFlow disable
    software-watchdog keep-alive-time 30
    !
    ip pim register-rp-reachability
    ! interface lo mtu 65536 ip address
    127.0.0.1/8 ip address 192.168.0.3/32
    secondary ipv6 address ::1/128
!
    interface eth0 ip address
    10.12.4.183/24
!
    interface eth1 ip address
    10.10.11.50/24
    ! interface eth2  ip address
    10.10.12.10/24
    ! router rip network
    10.10.11.0/24 network
    10.10.12.0/24
    ! line con 0 login
    line vty 0 39
    login
! end

#show ip protocols rip
RIP Database for VRF (default)
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 5 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set   Default
redistribution metric is 1
  Redistributing:
  Default version control: send version 2, receive version 2
```

```
    Interface        Send  Recv    Key-chain
eth1             2      2    eth2              2
2
  Routing for Networks:
    10.10.11.0/24
    10.10.12.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update   Bad Packets  Bad Routes
  Number of routes (including connected): 2
  Distance: (default is 120)

#show ip rip interface
svlan0.1 is down, line protocol is down    RIP is
not enabled on this interface eth2 is up, line
protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:        10.10.12.10/24
eth1 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:        10.10.11.50/24
eth0 is up, line protocol is up    RIP is not
enabled on this interface lo is up, line
protocol is up   RIP is not enabled on this
interface

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2        E1
- OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default
    IP Route Table for VRF "default"
    Gateway of last resort is 10.12.4.1 to network 0.0.0.0

    K*      0.0.0.0/0 [0/0] via 10.12.4.1, eth0
    C       10.10.11.0/24 is directly connected, eth1
    C10.10.12.0/24 is directly connected, eth2
    C10.12.4.0/24 is directly connected, eth0
    C127.0.0.0/8 is directly connected, lo
    C192.168.0.3/32 is directly connected, lo
```

Specify RIP Version

Configure a router to receive and send specific versions of packets on an interface. In this example, router R2 is configured to receive and send RIP version 1 and version 2 information on both eth1 and eth2 interfaces.

Topology

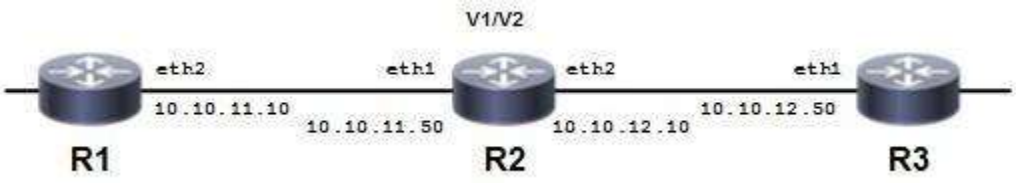


Figure 17-96: RIP Version Topology

R2

`#configure terminal`	Enter Configure mode.
`(config)#router rip`	Enable the RIP routing process.
`(config-router)#exit`	Quit Router mode, and return to Configure mode.
`(config)#interface eth1`	Specify interface `eth1` as an interface you want to configure.
`(config-if)#ip rip send version 1 2`	Allow sending RIP version 1 and version 2 packets out of this interface.
`(config-if)#ip rip receive version 1 2`	Allow receiving RIP version 1 and version 2 packets from the `eth1` interface.
`(config-if)#quit`	Quit Interface mode, and return to Configure mode to configure the next interface.
`(config)#interface eth2`	Specify interface `eth2` as the interface you want to configure.
`(config-if)#ip rip send version 1 2`	Allow sending RIP version 1 and version 2 packets out of this interface.
`(config-if)#ip rip receive version 1 2`	Allow receiving RIP version 1 and version 2 packets from the `eth2` interface.

Validation

show ip rip, show running-config, show ip protocols rip, show ip rip interface, show ip route

R2

```
#sh ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP,
X - Default

   Network            Next Hop          Metric From            If     Time
Rc 10.10.11.0/24                          1                   eth1
Rc 10.10.12.0/24                          1                   eth2
```

```
    #sh running-config
    !
    no service password-encryption
    !
    logging monitor 7
    !
    ip vrf management
    ! ip domain-lookup
    spanning-tree mode provider-rstp data-
    center-bridging enable feature telnet
    feature ssh no feature tacacs+
    snmp-server view all .1 included ntp
    enable sFlow disable
    software-watchdog keep-alive-time 30
    !
    ip pim register-rp-reachability
    ! interface lo mtu 65536 ip address
    127.0.0.1/8 ip address 192.168.0.2/32
    secondary ipv6 address ::1/128
    ! interface eth0  ip address
    10.12.4.108/24
    !
    interface eth1  ip address
    10.10.11.50/24  ip rip send
    version 1 2  ip rip receive
    version 1 2
    ! interface eth2 ip address
    10.10.12.10/24 ip rip send
    version 1 2 ip rip receive
    version 1 2
    ! router rip  network
    10.10.11.0/24  network
    10.10.12.0/24
    ! line con 0
    login line vty 0
    39 login
! end

#show ip protocols rip
RIP Database for VRF (default)
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 29 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set Default
redistribution metric is 1
  Redistributing:
  Default version control: send version 2, receive version 2
    Interface        Send  Recv   Key-chain     eth1
1 2   1 2     eth2             1 2   1 2
```

```
  Routing for Networks:
    10.10.11.0/24
    10.10.12.0/24
  Routing Information Sources:
    Gateway           Distance Last Update   Bad Packets Bad Routes
    10.10.11.10            120 00:00:31                 0          0
    10.10.12.50            120 00:00:08                 0          0
  Number of routes (including connected): 2
  Distance: (default is 120)

#show ip rip interface
svlan0.1 is down, line protocol is down    RIP is not
enabled on this interface eth2 is up, line protocol
is up   Routing Protocol: RIP
    Receive RIPv1 and RIPv2 packets
    Send RIPv1 and RIPv2 packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:        10.10.12.10/24
eth1 is up, line protocol is up    Routing Protocol:
RIP
    Receive RIPv1 and RIPv2 packets
    Send RIPv1 and RIPv2 packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:        10.10.11.50/24
eth0 is up, line protocol is up    RIP is not
enabled on this interface lo is up, line protocol
is up   RIP is not enabled on this interface

#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF
external type 1, E2 - OSPF external type 2
           i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
           * - candidate default

    IP Route Table for VRF "default"
    Gateway of last resort is 10.12.4.1 to network 0.0.0.0

    K*      0.0.0.0/0 [0/0] via 10.12.4.1, eth0
    C       10.10.11.0/24 is directly connected, eth1
    C10.10.12.0/24 is directly connected, eth2
    C10.12.4.0/24 is directly connected, eth0
    C127.0.0.0/8 is directly connected, lo
    C192.168.0.2/32 is directly connected, lo
```

Authentication with a Single Key

SWMRE RIP provides a choice of configuring authentication with a single key or with multiple keys. This example shows authenticating routing information exchange using a single key.

Topology

Routers R1 and R2 are running RIP and exchanging routing updates. To configure single-key authentication on R1, specify an interface, then define a key or password for that interface. Next, specify an authentication mode. Any receiving RIP packet on this specified interface should have the same string as the password. For an exchange of updates between R1 and R2, define the same password and authentication mode on R2.

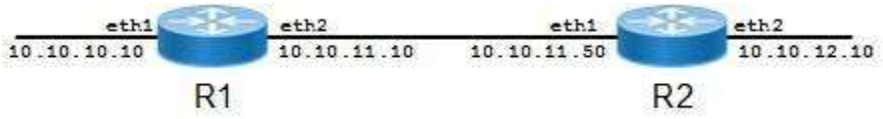


Figure 17-97: Single-key Topology

R1

`#configure terminal`	Enter Configure mode.
`(config)#router rip`	Define a RIP routing process, and enter Router mode.
`(config-router)#network 10.10.10.0/24`	Associate network `10.10.10.0/24` with the RIP process.
`(config-router)#redistribute connected`	Enable redistributing from connected routes.
`(config-router)#exit`	Quit Router mode, and return to Configure mode.
`(config)#interface eth1`	Specify the interface (`eth1`) for authentication.
`(config-if)#ip rip authentication string ABC`	Specify the authentication string (`ABC`) for this interface.
`(config-if)#ip rip authentication mode md5`	Specify the authentication mode to be MD5.

R2

`#configure terminal`	Enter Configure mode.
`(config)#router rip`	Define a RIP routing process, and enter Router mode.
`(config-router)#network 10.10.10.0/24`	Associate network `10.10.10.0/24` with the RIP process.
`(config-router)#redistribute connected`	Enable redistributing from connected routes.
`(config-router)#exit`	Quit Router mode, and return to Configure mode.
`(config)#interface eth2`	Specify the interface (`eth2`) for authentication.
`(config-if)#ip rip authentication string ABC`	Specify the authentication string (`ABC`) on this interface.
`(config-if)#ip rip authentication mode md5`	Specify the authentication mode to be MD5.

Validation

show running-config, show ip rip, show ip protocol rip, show ip rip interface, show ip route

R1

```
    #show running-config
    !
    no service password-encryption
    !
    hostname rtr1
    !
    logging monitor 7
    !
    ip vrf management
    ! ip domain-lookup spanning-tree mode provider-rstp
    data-center-bridging enable feature telnet feature
    ssh no feature tacacs+ snmp-server view all .1
    included ntp enable sFlow disable software-watchdog
    keep-alive-time 30
!
    ip pim register-rp-reachability
    ! interface lo mtu 65536 ip address 127.0.0.1/8 ip
    address 192.168.0.1/32 secondary ipv6 address ::1/128
    ! interface eth0  ip address 10.12.4.92/24
    ! interface eth1  ip address
    10.10.10.10/24  ip rip
    authentication mode md5
 ip rip authentication string 0x5c5b790e25d29287
! interface eth2 ip address
10.10.11.10/24
! router rip  network
10.10.10.0/24  redistribute
connected
! line con 0 login
line vty 0 39 login
! end

#show ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP,        X
- Default

   Network            Next Hop         Metric From            If     Time
Rc 10.10.10.0/24                         1                   eth1
C  10.10.11.0/24                         1                   eth2
R  10.10.12.0/24      10.10.10.50        2  10.10.10.50      eth1   02:33
C  10.12.4.0/24                          1                   eth0
C  192.168.0.1/32                       1                   lo
R  192.168.0.2/32     10.10.10.50        2  10.10.10.50      eth1   02:33

#show ip protocol rip
RIP Database for VRF (default)
Routing Protocol is "rip"
```

```
  Sending updates every 30 seconds with +/-50%, next due in 26 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing: connected
  Default version control: send version 2, receive version 2
    Interface        Send  Recv   Key-chain     eth1
2     2
  Routing for Networks:
    10.10.10.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
    10.10.10.50           120  00:00:31               0           0
  Number of routes (including connected): 6
  Distance: (default is 120)

#show ip rip interface
svlan0.1 is down, line protocol is down   RIP is
not enabled on this interface eth2 is up, line
protocol is up   RIP is not enabled on this
interface eth1 is up, line protocol is up
      Routing Protocol: RIP
        Receive RIP packets
        Send RIP packets
        Passive interface: Disabled
        Split horizon: Enabled with Poisoned Reversed
        IP interface address:
    10.10.10.10/24
    eth0 is up, line protocol is up   RIP is
    not enabled on this interface lo is up,
    line protocol is up   RIP is not enabled
    on this interface

    #show ip route
    Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
           O - OSPF, IA - OSPF inter area
           N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
    E1 - OSPF external type 1, E2 - OSPF external type 2
           i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
           * - candidate default

    IP Route Table for VRF "default"
    Gateway of last resort is 10.12.4.1 to network 0.0.0.0

    K*      0.0.0.0/0 [0/0] via 10.12.4.1, eth0
    C       10.10.10.0/24 is directly connected, eth1
    C10.10.11.0/24 is directly connected, eth2
    R10.10.12.0/24 [120/2] via 10.10.10.50, eth1, 00:04:05
    C10.12.4.0/24 is directly connected, eth0
```

```
    C       127.0.0.0/8 is directly connected, lo
    C       192.168.0.1/32 is directly connected, lo
    R       192.168.0.2/32 [120/2] via 10.10.10.50, eth1, 00:04:05
```

R2

```
    #sh running-config
    !
    no service password-encryption
    !
    logging monitor 7
    !
    ip vrf management
    ! ip domain-lookup
    spanning-tree mode provider-rstp
    data-center-bridging enable feature
    telnet feature ssh no feature
    tacacs+
    snmp-server view all .1 included ntp
    enable sFlow disable
    software-watchdog keep-alive-time 30
    !
    ip pim register-rp-reachability
    !
    interface lo
 mtu 65536  ip address 127.0.0.1/8  ip
address 192.168.0.2/32 secondary  ipv6
address ::1/128
! interface eth0 ip address
10.12.4.108/24
! interface eth1 ip address
10.10.12.50/24
! interface eth2  ip address
10.10.10.50/24  ip rip authentication
mode md5
 ip rip authentication string 0x5c5b790e25d29287
! router rip network
10.10.10.0/24  redistribute
connected
! line con 0 login
line vty 0 39 login
! end

#show ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP,        X
- Default

   Network            Next Hop         Metric From            If     Time
Rc 10.10.10.0/24                           1                  eth2
```

```
R  10.10.11.0/24      10.10.10.10           2 10.10.10.10     eth2    02:58
C  10.10.12.0/24                            1                 eth1
C  10.12.4.0/24                             1                 eth0
R  192.168.0.1/32     10.10.10.10           2 10.10.10.10     eth2    02:58
C  192.168.0.2/32                           1                 lo

#show ip protocol rip
RIP Database for VRF (default)
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 5 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing: connected
  Default version control: send version 2, receive version 2
    Interface        Send  Recv    Key-chain     eth2
2     2
  Routing for Networks:
    10.10.10.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
        10.10.10.10           120   00:00:01               0            0
      Number of routes (including connected): 6
      Distance: (default is 120)

    #show ip rip interface
    svlan0.1 is down, line protocol is down
    RIP is not enabled on this interface eth2
    is up, line protocol is up
      Routing Protocol: RIP
        Receive RIP packets
        Send RIP packets
        Passive interface: Disabled
        Split horizon: Enabled with Poisoned Reversed
        IP interface address:
    10.10.10.50/24
    eth1 is up, line protocol is up   RIP
    is not enabled on this interface eth0
    is up, line protocol is up    RIP is not
    enabled on this interface lo is up,
    line protocol is up
      RIP is not enabled on this interface

    #show ip route
    Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
           O - OSPF, IA - OSPF inter area
           N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
    E1 - OSPF external type 1, E2 - OSPF external type 2
           i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
```

```
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 10.12.4.1 to network 0.0.0.0

K*      0.0.0.0/0 [0/0] via 10.12.4.1, eth0
C       10.10.10.0/24 is directly connected, eth2
R       10.10.11.0/24 [120/2] via 10.10.10.10, eth2, 00:07:36
C10.10.12.0/24 is directly connected, eth1
C10.12.4.0/24 is directly connected, eth0
C127.0.0.0/8 is directly connected, lo
R192.168.0.1/32 [120/2] via 10.10.10.10, eth2, 00:07:36
C192.168.0.2/32 is directly connected, lo
```

Text Authentication with Multiple Keys

This example illustrates text authentication of the routing information exchange process for RIP using multiple keys. Routers R1 and R2 are running RIP, and exchanging routing updates. To configure authentication on R1, define a key chain, specify keys in the key chain, then define the authentication string or passwords to use by the keys. Set the time period during which it is valid to receive or send the authentication key by specifying the accept and send lifetimes. After defining the key string, specify the key chain (or set of keys) that will be used for authentication on each interface, and the authentication mode to use.

R1 receives all packets that contain any key string that matches one of the key strings included in the specified key chain (within the accept lifetime) on that interface. The key ID is not considered for matching. For additional security, the accept lifetime and send lifetime are configured such that every fifth day, the key ID and key string changes. To maintain continuity, the accept lifetimes should be configured to overlap. This will accommodate different time setup on machines. However, the send lifetime is not required to overlap, and Symanitron recommends configuring no overlapping for the send lifetime.

Topology

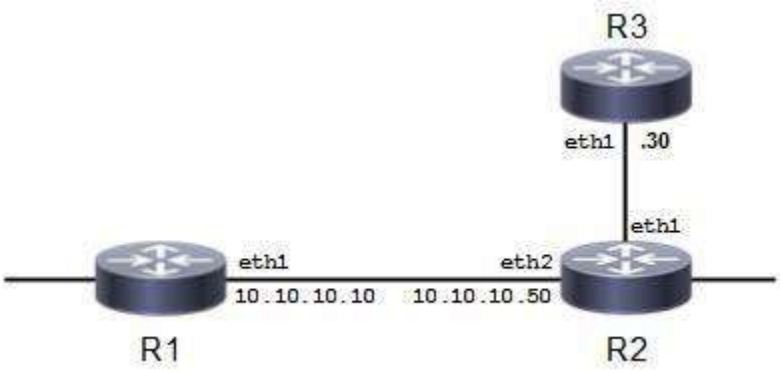


Figure 17-98: Multiple-key Topology

R1

`#configure terminal`	Enter Configure mode.
`(config)#router rip`	Define a RIP routing process, and enter Router mode.

(config-router)#network 10.10.10.0/24	Associate network 10.10.10.0/24 with the RIP process.
(config-router)#redistribute connected	Enable redistributing from connected routes.
(config-router)#exit	Quit Router mode, and return to Configure mode.
(config)#key chain SUN	Enter Keychain management mode to add keys to the key chain SUN.
(config-keychain)#key 10	Add authentication key ID (10) to the key chain SUN.
(config-keychain-key)#key-string ABC	Specify a password (ABC) to use by the specified key.
(config-keychain-key)#accept-lifetime 12:00:00 Mar 2 2003 14:00:00 Mar 7 2003	Specify the time period during which the authentication key can be received. In this case, key string ABC can be received from noon of March 2 to 2 pm March 7, 2003.
(config-keychain-key)#send-lifetime 12:00:00 Mar 2 2003 12:00:00 Mar 7 2003	Specify the time period during which the authentication key can be sent. In this case, key string ABC can be sent from noon of March 2 to noon of March 7, 2003.
(config-keychain-key)#exit	Exit Keychain-Key mode, and return to Keychain mode.
(config-keychain)#key 20	Add another authentication key (20) to the key chain SUN.
(config-keychain-key)#key-string Earth	Specify a password (Earth) to use by the specified key.
(config-keychain-key)#accept-lifetime 12:00:00 Mar 7 2003 14:00:00 Mar 12 2003	Specify the time period during which authentication key string Earth can be received. In this case, key string Earth can be received from noon of March 7 to 2 pm March 12, 2003.
(config-keychain-key)#send-lifetime 12:00:00 Mar 7 2003 12:00:00 Mar 12 2003	Specify the time period during which the authentication key can be sent. In this case, key string Earth can be sent from noon of March 7 to noon of March 12, 2003.
(config-keychain-key)#end	Enter Privileged Exec mode.
#configure terminal	Enter Configure mode.
(config)#interface eth1	Specify interface eth1 as the interface you want to configure.
(config-if)#ip rip authentication key chain SUN	Enable RIPv2 authentication on eth1 interface and specify the key chain SUN to use for authentication.
(config-if)#ip rip authentication mode text	Specify text authentication mode to use for RIP packets. This step is optional, because text is the default mode.
R2	
#configure terminal	Enter Configure mode.
(config)#router rip	Define a RIP routing process, and enter Router mode.
(config-router)#network 10.10.10.0/24	Associate network 10.10.10.0/24 with the RIP process.
(config-router)#redistribute connected	Enable redistributing from connected routes.
(config-router)#exit	Quit Router mode, and return to Configure mode.

(config)#key chain MOON	Enter Keychain management mode to add keys to the key chain MOON.
(config-keychain)#key 30	Add authentication key ID (30) to the key chain MOON.
(config-keychain-key)#key-string ABC	Specify a password (ABC) to use by the specified key.
(config-keychain-key)#accept-lifetime 12:00:00 Mar 2 2003 14:00:00 Mar 7 2003	Specify the time period during which the authentication key can be received. In this case, key string ABC can be received from noon of March 2 to 2 pm March 7, 2003.
(config-keychain-key)#send-lifetime 12:00:00 Mar 2 2003 12:00:00 Mar 7 2003	Specify the time period during which the authentication key can be sent. In this case, key string ABC can be sent from noon of March 2 to noon of March 7, 2003.
(config-keychain)#key 40	Add another authentication key (40) to the key chain MOON.
(config-keychain-key)#key-string Earth	Specify a password (Earth) to use by the specified key.
(config-keychain-key)#accept-lifetime 12:00:00 Mar 7 2003 14:00:00 Mar 12 2003	Specify the time period during which authentication key string Earth can be received. In this case, key string Earth can be received from noon of March 7 to 2 pm March 12, 2003.
(config-keychain-key)#send-lifetime 12:00:00 Mar 7 2003 12:00:00 Mar 12 2003	Specify the time period during which the authentication key can be sent. In this case, key string Earth can be sent from noon of March 7 to noon of March 12, 2003.
(config-keychain-key)#end	Enter Privileged Exec mode.
#configure terminal	Enter Configure mode.
(config)#interface eth2	Specify interface eth2 as the interface you want to configure.
(config-if)#ip rip authentication key chain MOON	Enable RIPv2 authentication on the eth1 interface, and specify the key chain MOON to use for authentication.
(config-if)#ip rip authentication mode text	Specify the authentication mode to use for RIP packets. This step is optional, because text is the default mode.

Validation

show running-config, show ip rip, show ip protocol rip, show ip rip interface, show ip route

R1

```
#sh running-config
!
no service password-encryption
!
hostname rtr1
!
logging monitor 7
!
ip vrf management
! key chain SUN  key 10
```

```
      key-string 0x5c5b790e25d29287
      accept-lifetime 12:00:00 Mar 02 2003 14:00:00 Mar 07 2003   send-lifetime
    12:00:00 Mar 02 2003 12:00:00 Mar 07 2003  key 20
      key-string 0x51b2c401dd313187
      accept-lifetime 12:00:00 Mar 07 2003 14:00:00 Mar 12 2003   send-lifetime
    12:00:00 Mar 07 2003 12:00:00 Mar 12 2003
    ! ip domain-lookup spanning-tree mode provider-rstp
    data-center-bridging enable feature telnet feature
    ssh no feature tacacs+ snmp-server view all .1
    included ntp enable sFlow disable software-watchdog
    keep-alive-time 30
!
    ip pim register-rp-reachability
    ! interface lo mtu 65536 ip address 127.0.0.1/8 ip
    address 192.168.0.1/32 secondary ipv6 address ::1/128
!
    interface eth0  ip address 10.12.4.92/24
    ! interface eth1  ip address 10.10.10.10/24
    ip rip authentication mode text  ip rip
    authentication key-chain chain SUN
!
interface eth2
! router rip  network
10.10.10.0/24  redistribute
connected
! line con 0 login
line vty 0 39 login
! end

#show ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP,        X -
Default

   Network            Next Hop         Metric From            If     Time
Rc 10.10.10.0/24                           1                  eth1
C  10.12.4.0/24                            1                  eth0
C  192.168.0.1/32                          1                  lo

#show ip protocol rip
RIP Database for VRF (default)
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 16 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing: connected
```

```
  Default version control: send version 2, receive version 2
Interface        Send   Recv   Key-chain     eth1              2     2
chain SUN
  Routing for Networks:
    10.10.10.0/24
  Routing Information Sources:
    Gateway          Distance Last Update  Bad Packets  Bad Routes
  Number of routes (including connected): 3
  Distance: (default is 120)

#show ip rip interface
svlan0.1 is down, line protocol is down   RIP is
not enabled on this interface eth2 is down, line
protocol is down   RIP is not enabled on this
interface eth1 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
         IP interface address:
    10.10.10.10/24
    eth0 is up, line protocol is up   RIP is
    not enabled on this interface lo is up,
    line protocol is up   RIP is not enabled
    on this interface

    #show ip route
    Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
           O - OSPF, IA - OSPF inter area
           N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
    E1 - OSPF external type 1, E2 - OSPF external type 2
           i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
           * - candidate default

    IP Route Table for VRF "default"
    Gateway of last resort is 10.12.4.1 to network 0.0.0.0

    K*      0.0.0.0/0 [0/0] via 10.12.4.1, eth0
    C       10.10.10.0/24 is directly connected, eth1
    C10.12.4.0/24 is directly connected, eth0
    C127.0.0.0/8 is directly connected, lo
    C192.168.0.1/32 is directly connected, lo
```

R2

```
    #sh running-config
    !
    no service password-encryption
    !
    logging monitor 7
    !
```

```
    ip vrf management
    ! key chain
    MOON key 30
      key-string 0x5c5b790e25d29287
      accept-lifetime 12:00:00 Mar 02 2003 14:00:00 Mar 07 2003
    send-lifetime 12:00:00 Mar 02 2003 12:00:00 Mar 07 2003 key 40
      key-string 0x51b2c401dd313187
      accept-lifetime 12:00:00 Mar 07 2003 14:00:00 Mar 12 2003 send-lifetime
    12:00:00 Mar 07 2003 12:00:00 Mar 12 2003
    ! ip domain-lookup
    spanning-tree mode provider-rstp
    data-center-bridging enable feature
    telnet feature ssh no feature
    tacacs+
    snmp-server view all .1 included ntp
    enable sFlow disable
    software-watchdog keep-alive-time 30
    !
    ip pim register-rp-reachability !
interface lo  mtu 65536  ip address
127.0.0.1/8  ip address 192.168.0.2/32
secondary  ipv6 address ::1/128
! interface eth0 ip address
10.12.4.108/24
!
interface eth1
! interface eth2 ip address 10.10.10.50/24 ip rip
authentication mode text ip rip authentication key-
chain chain MOON
! router rip  network
10.10.10.0/24  redistribute
connected
! line con 0 login
line vty 0 39 login
! end

#sh ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP,        X -
Default

   Network            Next Hop         Metric From            If     Time
Rc 10.10.10.0/24                         1                    eth2
C  10.12.4.0/24                          1                    eth0
C  192.168.0.2/32                        1                    lo

#show ip protocol rip
RIP Database for VRF (default)
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 5 seconds
```

```
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing: connected
  Default version control: send version 2, receive version 2
Interface        Send  Recv   Key-chain     eth2              2    2
chain MOON
  Routing for Networks:
    10.10.10.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
  Number of routes (including connected): 3
  Distance: (default is 120)
    #show ip rip interface
    svlan0.1 is down, line protocol is down
    RIP is not enabled on this interface eth2
    is up, line protocol is up
      Routing Protocol: RIP
        Receive RIP packets
        Send RIP packets
        Passive interface: Disabled
        Split horizon: Enabled with Poisoned
        Reversed IP interface address:
    10.10.10.50/24
    eth1 is down, line protocol is down
    RIP is not enabled on this interface
    eth0 is up, line protocol is up   RIP
    is not enabled on this interface lo is
    up, line protocol is up
      RIP is not enabled on this interface

    #show ip route
    Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
           O - OSPF, IA - OSPF inter area
           N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
    E1 - OSPF external type 1, E2 - OSPF external type 2
           i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
           * - candidate default

    IP Route Table for VRF "default"
    Gateway of last resort is 10.12.4.1 to network 0.0.0.0

    K*      0.0.0.0/0 [0/0] via 10.12.4.1, eth0
    C       10.10.10.0/24 is directly connected, eth2
    C10.12.4.0/24 is directly connected, eth0
    C127.0.0.0/8 is directly connected, lo
    C192.168.0.2/32 is directly connected, lo
```

MD5 Authentication with Multiple Keys

This example illustrates the MD5 authentication of the routing information exchange process for RIP using multiple keys. Routers R1 and R2 are running RIP, and exchanging routing updates. To configure authentication on R1, define a key chain, specify keys in the key chain, then define the authentication string or passwords to use by the keys. Then, set the time period during which it is valid to receive or send the authentication key by specifying the accept and send lifetimes. After defining the key string, specify the key chain (or the set of keys) that will be used for authentication on the interface, and the authentication mode to use. Configure R2 and R3 to have the same key ID and key string as R1 for the time that updates are to be exchanged.

In MD5 authentication, both the key ID and key string are matched for authentication. R1 will receive only packets that match both the key ID and the key string in the specified key chain (within the accept lifetime) on that interface. In the following example, R2 has the same key ID and key string as R1. For additional security, the accept lifetime and send lifetime are configured such that every fifth day, the key ID and key string changes. To maintain continuity, the accept lifetimes should be configured to overlap; however, the send lifetime should not overlap.

Topology

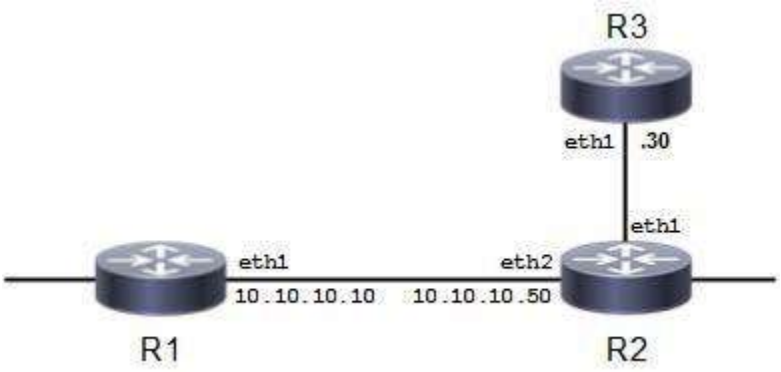


Figure 17-99: MD5 Multiple-key Topology

R1

`#configure terminal`	Enter Configure mode.
`(config)#router rip`	Define a RIP routing process, and enter Router mode.
`(config-router)#network 10.10.10.0/24`	Associate network `10.10.10.0/24` with the RIP process.
`(config-router)#redistribute connected`	Enable redistributing from connected routes.
`(config-router)#exit`	Quit Router mode, and return to Configure mode.
`(config)#key chain SUN`	Enter Keychain management mode to add keys to the key chain `SUN`.
`(config-keychain)#key 1`	Add authentication key ID (`1`) to the key chain `SUN`.
`(config-keychain-key)#key-string ABC`	Specify a password (`ABC`) to use by the specified key.
`(config-keychain-key)#accept-lifetime 12:00:00 Mar 2 2003 14:00:00 Mar 7 2003`	Specify the time period during which the authentication key can be received. In this case, key string `ABC` can be received from noon of March 2 to 2 pm March 7, 2003.
`(config-keychain-key)#send-lifetime 12:00:00 Mar 2 2003 12:00:00 Mar 7 2003`	Specify the time period during which the authentication key can be sent. In this case, key string `ABC` can be sent from noon of March 2 to noon of March 7, 2003.

(config-keychain-key)#exit	Exit Keychain-Key mode, and return to Keychain mode.
(config-keychain)#key 2	Add another authentication key (2) to the key chain SUN.
(config-keychain-key)#key-string Earth	Specify a password (Earth) to use by the specified key.
(config-keychain-key)#accept-lifetime 12:00:00 Mar 7 2003 14:00:00 Mar 12 2003	Specify the time period during which authentication key string Earth can be received. In this case, key string Earth can be received from noon of March 7 to 2 pm March 12, 2003.
(config-keychain-key)#send-lifetime 12:00:00 Mar 7 2003 12:00:00 Mar 12 2003	Specify the time period during which the authentication key can be sent. In this case, key string Earth can be sent from noon of March 7 to noon of March 12, 2003.
(config-keychain-key)#end	Enter Privileged Exec mode.
#configure terminal	Enter Configure mode.
(config)#interface eth1	Specify interface eth1 as the interface you want to configure.
(config-if)#ip rip authentication key chain SUN	Enable RIPv2 authentication on the eth1 interface, and specify the key chain SUN to use for authentication.
(config-if)#ip rip authentication mode md5	Specify MD5 authentication mode to use for RIP packets.

R2

#configure terminal	Enter Configure mode.
(config)#router rip	Define a RIP routing process, and enter Router mode.
(config-router)#network 10.10.10.0/24	Associate network 10.10.10.0/24 with the RIP process.
(config-router)#redistribute connected	Enable redistributing from connected routes.
(config-router)#exit	Quit Router mode, and return to Configure mode.
(config)#key chain MOON	Enter Keychain management mode to add keys to the key chain MOON.
(config-keychain)#key 1	Add authentication key ID (1) to the key chain MOON.
(config-keychain-key)#key-string ABC	Specify a password (ABC) to use by the specified key.
(config-keychain-key)#accept-lifetime 12:00:00 Mar 2 2003 14:00:00 Mar 7 2003	Specify the time period during which the authentication key can be received. In this case, key string ABC can be received from noon of March 2 to 2 pm March 7, 2003.
(config-keychain-key)#send-lifetime 12:00:00 Mar 2 2003 12:00:00 Mar 7 2003	Specify the time period during which the authentication key can be sent. In this case, key string ABC can be sent from noon of March 2 to noon of March 7, 2003.
(config-keychain)#key 2	Add another authentication key (2) to the key chain MOON.
(config-keychain-key)#key-string Earth	Specify a password (Earth) to use by the specified key.

`(config-keychain-key)#accept-lifetime 12:00:00 Mar 7 2003 14:00:00 Mar 12 2003`	Specify the time period during which the authentication key can be received. In this case, key string `Earth` can be received from noon of March 7 to 2 pm March 12, 2003.
`(config-keychain-key)#send-lifetime 12:00:00 Mar 7 2003 12:00:00 Mar 12 2003`	Specify the time period during which the authentication key can be sent. In this case, key string `Earth` can be sent from noon of March 7 to noon of March 12, 2003.
`(config-keychain-key)#end`	Enter Privileged Exec mode.
`#configure terminal`	Enter Configure mode.
`(config)#interface eth2`	Specify interface `eth2` as the interface you want to configure.
`(config-if)#ip rip authentication key chain MOON`	Enable RIPv2 authentication on the `eth1` interface, and specify the key chain `MOON` to use for authentication.
`(config-if)#ip rip authentication mode md5`	Specify the authentication mode to use for RIP packets.

Validation

show running-config, show ip rip, show ip protocol rip, show ip rip interface

R1

```
#sh running-config
!
no service password-encryption
!
hostname rtr1
!
logging monitor 7
!
ip vrf management
! key chain SUN  key 1
  key-string 0x5c5b790e25d29287
  accept-lifetime 12:00:00 Mar 02 2003 14:00:00 Mar 07 2003   send-lifetime
12:00:00 Mar 02 2003 12:00:00 Mar 07 2003  key 2
  key-string 0x51b2c401dd313187
  accept-lifetime 12:00:00 Mar 07 2003 14:00:00 Mar 12 2003   send-lifetime
12:00:00 Mar 07 2003 12:00:00 Mar 12 2003
! ip domain-lookup spanning-tree mode provider-rstp
data-center-bridging enable feature telnet feature
ssh no feature tacacs+ snmp-server view all .1
included ntp enable sFlow disable
software-watchdog keep-alive-time 30
!
ip pim register-rp-reachability
! interface lo  mtu 65536  ip address 127.0.0.1/8  ip
address 192.168.0.1/32 secondary  ipv6 address ::1/128
! interface eth0  ip address 10.12.4.92/24
```

```
    ! interface eth1 ip address 10.10.10.10/24 ip rip
    authentication mode md5 ip rip authentication key-chain chain
    SUN
!
    interface eth2
    ! router rip  network 10.10.10.0/24
    redistribute connected
! line con 0 login
line vty 0 39 login
! end

#show ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP,        X -
Default

   Network            Next Hop         Metric From            If     Time
Rc 10.10.10.0/24                         1                    eth1
C  10.12.4.0/24                          1                    eth0
C  192.168.0.1/32                        1                    lo

#show ip protocol rip
RIP Database for VRF (default)
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 19 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing: connected
  Default version control: send version 2, receive version 2
Interface        Send  Recv   Key-chain     eth1              2     2
chain SUN
  Routing for Networks:
    10.10.10.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
  Number of routes (including connected): 3
  Distance: (default is 120)

#show ip rip interface
svlan0.1 is down, line protocol is down   RIP is
not enabled on this interface eth2 is down, line
protocol is down   RIP is not enabled on this
interface eth1 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
```

```
    IP interface address:       10.10.10.10/24
eth0 is up, line protocol is up RIP is not
enabled on this interface lo is up, line
protocol is up RIP is not enabled on this
interface
```

R2

```
    #sh running-config
    !
    no service password-encryption
    !
    logging monitor 7
    !
    ip vrf management
    ! key chain MOON key 1 key-
      string 0x5c5b790e25d29287
      accept-lifetime 12:00:00 Mar 02 2003 14:00:00 Mar 07 2003   send-lifetime
    12:00:00 Mar 02 2003 12:00:00 Mar 07 2003  key 2
      key-string 0x51b2c401dd313187
      accept-lifetime 12:00:00 Mar 07 2003 14:00:00 Mar 12 2003   send-lifetime
    12:00:00 Mar 07 2003 12:00:00 Mar 12 2003
    ! ip domain-lookup spanning-tree mode provider-rstp
    data-center-bridging enable feature telnet feature
    ssh no feature tacacs+ snmp-server view all .1
    included ntp enable sFlow disable software-watchdog
    keep-alive-time 30
!
    ip pim register-rp-reachability
    ! interface lo mtu 65536 ip address 127.0.0.1/8 ip
    address 192.168.0.2/32 secondary ipv6 address ::1/128
    ! interface eth0 ip address 10.12.4.108/24
    !
    interface eth1
    !
    interface eth2 ip address 10.10.10.50/24 ip rip authentication
    mode md5 ip rip authentication key-chain chain MOON

    ! router rip network 10.10.10.0/24
    redistribute connected
    ! line con 0 login line vty 0 39
    login
! end

#show ip rip

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP,        X
- Default

   Network            Next Hop         Metric From            If     Time
Rc 10.10.10.0/24                           1                  eth2
```

```
C  10.12.4.0/24                              1                 eth0
R  192.168.0.1/32      10.10.10.10          16 10.10.10.10     eth2    01:29
C  192.168.0.2/32                            1                 lo


#show ip protocol rip
RIP Database for VRF (default)
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 9 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing: connected
  Default version control: send version 2, receive version 2
Interface        Send  Recv    Key-chain    eth2             2      2
chain MOON
  Routing for Networks:
    10.10.10.0/24
  Routing Information Sources:
    Gateway          Distance  Last Update  Bad Packets  Bad Routes
  Number of routes (including connected): 4
  Distance: (default is 120)

#show ip rip interface
svlan0.1 is down, line protocol is down   RIP is
not enabled on this interface eth2 is up, line
protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:        10.10.10.50/24
eth1 is down, line protocol is down   RIP is
not enabled on this interface eth0 is up, line
protocol is up   RIP is not enabled on this
interface lo is up, line protocol is up   RIP
is not enabled on this interface
```

Border Gateway Protocol Command Reference

Contents

This document contains these chapters and appendices:

- Chapter 1, *BGP Commands*
- Chapter 3, *BGP Virtual Private Network Commands*
- Chapter 4, *BGP Show Commands*
- Appendix A, *Regular Expressions*

CHAPTER 1 BGP Commands

This chapter describes the BGP configuration commands.

- address-family
- aggregate-address
- auto-summary
- bgp additional-paths
- bgp additional-paths select
- bgp aggregate-nexthop-check
- bgp always-compare-med
- bgp as-local-count
- bgp bestpath as-path ignore
- bgp bestpath as-path multipath-relax
- bgp bestpath compare-confed-aspath
- bgp bestpath compare-routerid
- bgp bestpath dont-compare-originator-id
- bgp bestpath med
- bgp bestpath tie-break-on-age
- bgp client-to-client reflection
- bgp cluster-id
- bgp confederation identifier
- bgp confederation peers
- bgp config-type
- bgp dampening
- bgp default ipv4-unicast
- bgp default local-preference
- bgp deterministic-med
- bgp enforce-first-as
- bgp extended-asn-cap
- bgp fast-external-failover
- bgp graceful-restart
- bgp g-shut
- bgp g-shut-capable
- bgp g-shut-local-preference
- bgp log-neighbor-changes
- bgp multiple-instance
- bgp nexthop-trigger delay
- bgp nexthop-trigger enable

- bgp rfc1771-path-select
- bgp rfc1771-strict
- bgp router-id
- bgp scan-time
- bgp table-map
- bgp update-delay
- clear bgp (A.B.C.D|X:X::X:X)
- clear bgp *
- clear bgp <1-4294967295>
- clear bgp dampening
- clear bgp external
- clear bgp flap-statistics
- clear bgp peer-group
- clear bgp statistics
- clear bgp view
- clear ip bgp A.B.C.D
- clear ip bgp A.B.C.D vrf
- clear ip bgp table-map
- debug bgp
- distance bgp
- exit-address-family
- ip as-path access-list
- ip community-list <1-99>
- ip community-list <100-500>
- ip community-list expanded
- ip community-list standard
- ip community-list WORD
- ip extcommunity-list <1-99>
- ip extcommunity-list <100-500>
- ip extcommunity-list expanded
- ip extcommunity-list standard
- match ip peer
- max-paths
- neighbor additional-paths
- neighbor advertise additional-paths
- neighbor activate
- neighbor advertisement-interval
- neighbor allowas-in

- neighbor as-origination-interval
- neighbor attribute-unchanged
- neighbor capability dynamic
- neighbor capability graceful-restart
- neighbor capability orf prefix-list
- neighbor capability route-refresh
- neighbor collide-established
- neighbor connection-retry-time
- neighbor default-originate
- neighbor description
- neighbor disallow-infinite-holdtime
- neighbor distribute-list
- neighbor dont-capability-negotiate
- neighbor ebgp-multihop
- neighbor enforce-multihop
- neighbor filter-list
- neighbor g-shut
- neighbor g-shut-timer
- neighbor limit
- neighbor maximum-prefix
- neighbor next-hop-self
- neighbor optional-as
- neighbor override-capability
- neighbor passive
- neighbor password
- neighbor peer-group
- neighbor peer-group range
- neighbor prefix-list
- neighbor remote-as
- neighbor remove-private-AS
- neighbor restart-time
- neighbor route-map
- neighbor route-reflector-client
- neighbor route-server-client
- neighbor send-community
- neighbor send-label explicit-null
- neighbor shutdown
- neighbor soft-reconfiguration inbound

- neighbor strict-capability-match
- neighbor timers
- neighbor transparent-as
- neighbor transparent-nexthop
- neighbor unsuppress-map
- neighbor update-source
- neighbor version
- neighbor weight
- neighbor WORD peer-group
- network
- network synchronization
- redistribute
- restart bgp gracefull
- router bgp
- snmp restart bgp
- synchronization
- timers bgp
- undebug bgp

address-family

Use the address family command to enter the IPv4 or VPNv4 address family mode allowing configuration of addressfamily specific parameters. To leave the address family mode and return to the Configure mode use the `exitaddress-family` command.

This command configures the routing exchange between Provider Edge (PE) and Customer Edge (CE) devices. The BGP sessions between PE routers can carry different types of routes (VPN-IPv4 and IPv4 routes). Address families are used to control the type of BGP session. Configure a BGP address family for each VRF configured on the PE router and a separate address family to carry VPN-IPv4 routes between PE routers. All non VPN BGP neighbors are defined using router mode. All VPN BGP neighbors are defined under its associated address family mode. The BGP process with no address-family specified is the default address-family, where any sessions are configured that either are not associated with a VRF or are used to carry IPv4 routes.

Use the `no` parameter with this command to disable the address-family configurations.

Command Syntax `address-family ipv4 address-family ipv4 (unicast|multicast) address-family ipv4 vrf NAME address-family l2vpn evpn address-family rtfilter unicast address-family vpn4 address-family vpn4 unicast no address-family ipv4 vrf NAME no address-family ipv4 multicast no address-family l2vpn evpn no address-family rtfilter unicast no address-family vpnv4 no address-family vpnv4 unicast`

Parameters

`ipv4`	IPv4 address family
`unicast`	Unicast address prefixes
`multicast`	Multicast address prefixes
`vrf`	Virtual Private Network (VPN) routing/forwarding instance
`NAME`	VPN routing/forwarding instance name
`unicast`	Unicast address prefixes
`l2vpn evpn`	Layer 2 VPN routing sessions with EVPN endpoint information distributed to BGP peers
`rtfilter`	Route target filter: on an iBGP peer or Route Reflector (RR), only send IPv4 and IPv6 prefixes to PE routers when a PE has a VRF that imports those specific prefixes.
`unicast`	Unicast address prefixes
`vpnv4`	VPN version 4 address family
`unicast`	Unicast address prefixes

Applicability

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 7657
(config-router)#neighbor 3ffe:506::1 remote-as 7657
(config-router)#neighbor 3ffe:506::1 interface eth1
```

```
#configure terminal
(config)#router bgp 7657
(config-router)#address-family ipv4 (config-
router-af)#neighbor 3ffe:506::1 activate
(config-router-af)#exit-address-family
```

aggregate-address

Use this command to configure BGP aggregate entries.

Aggregates are used to minimize the size of routing tables. Aggregation combines the characteristics of several different routes and advertises a single route.The `aggregate-address` command creates an aggregate entry in the BGP routing table if any more-specific BGP routes are available in the specified range. Using the `summary-only` parameter advertises the prefix only, suppressing the more-specific routes to all neighbors. In the following example Router1 will propagate network 172.0.0.0 and suppresses the more specific route 172.10.0.0.

The `as-set` parameter creates an aggregate entry advertising the path for this route, consisting of all elements contained in all paths being summarized. Use this parameter to reduce the size of information by listing the AS path number only once, even if it was included in multiple paths that were aggregated. `as-set` parameter is useful when The aggregation of information results in an incomplete path information.

Use the `no` parameter with this command to disable this function.

Command Syntax `aggregate-address A.B.C.D/M aggregate-address A.B.C.D/M as-set aggregate-address A.B.C.D/M as-set summary-only aggregate-address A.B.C.D/M summary only aggregate-address A.B.C.D/M summary-only as-set no aggregate-address A.B.C.D/M no aggregate-address A.B.C.D/M as-set no aggregate-address A.B.C.D/M as-set summary-only no aggregate-address A.B.C.D/M summary only no aggregate-address A.B.C.D/M summary-only as-set`

Parameters

`A.B.C.D/M` Aggregate prefix `as-set`

Generate AS set path information

`summary-only` Filter more specific routes from updates

Default

By default, aggregate address A.B.C.D/M is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
    #configure terminal
    (config)#router bgp 100
    (config-router)#aggregate-address 10.0.0.0/8 as-set summary-only
(config)#router bgp 100
```

```
(config-router)#no aggregate-address 10.0.0.0/8 as-set summary-only
```

auto-summary

Use this command to enable sending summarized routes by a BGP speaker to its peers in the router configuration mode or in the address-family configuration mode. Auto-summary is used by a BGP router to advertise summarized routes to its peers. Auto-summary can be enabled if certain routes have already been advertised: in this case, configuring auto-summary advertises the summarized routes first, then corresponding non-summarized routes are withdrawn. If certain routes have already been advertised, and auto-summary is disabled, non-summarized routes are first advertised, then the corresponding summarized routes are withdrawn from all the connected peers.

Use the `no` parameter with this command to disable this function.

Command Syntax `auto-summary no auto-summary`

Parameters

None

Default

By default, auto-summary is disabled

Command Mode

Router mode and Address Family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example enables auto-summary in Router mode.

```
#configure terminal
(config)#router bgp 11
(config-router)#auto-summary
```

The following example enables auto-summary using the IPv4 address family.

```
#configure terminal
(config)#router bgp 1
(config)#address-family ipv4
(config-af)#auto-summary
```

bgp additional-paths

Use this command to enable BGP add-path.

Use the `no` parameter with this command to disable BGP add-path.

Command Syntax `bgp additional-paths (send|receive|send-receive) no bgp additional-paths (send|receive|send-receive)`

Parameters `send` Send additional paths to neighbors `receive` Receive additional paths from neighbors

`send-receive` Send and Receive additional paths from neighbors

Default

By default, bgp additional-paths is disabled

Command Mode

Router BGP Address Family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 2
(config-router)#address-family ipv4 unicast
(config-router)#bgp additional-paths send

(config-router)#no bgp additional-paths send
```

bgp additional-paths select

Use this command to enable BGP add-path advertisement.

Use the `no` parameter with this command to disable BGP add-path advertisement.

Command Syntax `bgp additional-paths select (all|best <2-3>) no bgp additional-paths select (all|best <2-3>)`

Parameters `all` Select all available paths `best` Select best N paths

`<2-3>` Number of best paths in additional paths to be selected

Default

By default, bgp additional-paths select is disabled

Command Mode

Router BGP Address Family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 2
(config-router)#address-family ipv4 unicast
(config-router)#bgp additional-paths select all

(config-router)#no bgp additional-paths select all
```

bgp aggregate-nexthop-check

Use this command to set the BGP option to perform aggregation only when next-hop matches the specified IP address.

Use the `no` parameter with this command to disable this functionality.

Command Syntax `bgp aggregate-nexthop-check` `no bgp aggregate-nexthop-check`

Parameters

None

Default

By default, bgp aggregate nexthop check is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#bgp aggregate-nexthop-check
```

bgp always-compare-med

Use this command to compare the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems. Multi Exit Discriminator (MED) is used in best path selection by BGP. MED is compared after BGP attributes weight, local preference, AS-path and origin have been compared and are equal. MED comparison is done only among paths from the same autonomous system (AS). Use `bgp always-compare-med` command to allow comparison of MEDs from different ASs. The MED parameter is used to select the best path. A path with lower MED is preferred. If the bgp table shows the following and the always-compare-med is enabled:

```
Route1: as-path 400, med 300
Route2: as-path 200, med 200
Route3: as-path 400, med 250
```

Route1 is compared to Route2. Route2 is best of the two (lower MED). Next, Route2 is compared to Route3 and Route2 is chosen best path again (lower MED). If always-compare-med was disabled, MED is not taken into account when Route1 and Route2 are compared, because of different ASs and MED is compared for only Route1 and Route3. In this case, Route3 would be the best path. The selected route is also affected by the `bgp deterministic-med` command. Please see `bgp deterministic-med` command for details. If this command is used to compare MEDs for all paths, it should be configured on every BGP router in the AS. Use the `no` parameter with this command to disallow the comparison.

Command Syntax `bgp always-compare-med` `no bgp always-compare-med`

Parameters

None

Default

By default, bgp always compare med is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp always-compare-med
```

bgp as-local-count

Use this command to set the number of times the local-AS (Autonomous System) is to be prepended.

Use the `no` parameter with this command to stop prepending the local AS count.

Command Syntax `bgp as-local-count <2-64> no bgp as-local-count <2-64>`

Parameter

`<2-64>`	The number of times the local-AS is to be prepended

Default

By default, bgp as local count is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp as-local-count 55

(config)#router bgp 100
(config-router)#no bgp as-local-count 55
```

bgp bestpath as-path ignore

Use this command to prevent the router from considering the autonomous system (AS) path length as a factor in the algorithm for choosing a best path route.

Use the `no` parameter with this command to allow the router to consider the AS path length in choosing a best path route.

Command Syntax `bgp bestpath as-path`

```
ignore  no  bgp  bestpath  as-path
ignore
```

Parameters

None

Default

By default, bgp bestpath as-path ignore is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp bestpath as-path ignore

(config)#router bgp 100 (config-router)#no bgp
bestpath as-path ignore
```

bgp bestpath as-path multipath-relax

Use this command to relax the “same AS-Path” requirement so any candidate eBGP AS-Path with the same AS-path length might be used for eBGP load-balancing.

Note: This feature does not load-balance between eBGP and iBGP paths.

Normally eBGP load-balancing requires the candidate routes to be equal-cost paths with identical BGP attributes having the same weight, Local-Pref, AS-Path (both the AS numbers and the AS path length), origin, MED, and different next-hop.

Use the `no` parameter with this command to return to normal operation.

Command Syntax `bgp bestpath as-path multipath-relax no bgp bestpath as-path multipath-relax`

Parameters

None

Default

By default, as-path multipath-relax is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp bestpath as-path multipath-relax

(config)#router bgp 100
(config-router)#no bgp bestpath as-path multipath-relax
```

bgp bestpath compare-confed-aspath

Use this command to allow comparing of the confederation AS path length. This command specifies that the AS confederation path length must be used when available in the BGP best path decision process. It is effective only when bgp bestpath as-path ignore command has not been used.

Use the `no` parameter with this command to ignore consideration of AS confederation path length in BGP best path selection.

Command Syntax `bgp bestpath compare-confed-aspath no bgp bestpath compare-confed-aspath`

Parameters

None

Default

BGP receives routes with identical eBGP paths from eBGP peers and selects the first route received as the best path.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp bestpath compare-confed-aspath

(config)#router bgp 100
(config-router)#no bgp bestpath compare-confed-aspath
```

bgp bestpath compare-routerid

Use this command to compare router IDs for identical eBGP paths. When comparing similar routes from peers, the BGP router does not consider the router ID of the routes. By default, it selects the first received route. Use this command to include router ID in the selection process; similar routes are compared and the route with the lowest router ID is selected. The router IS is the highest IP address on the router, with preference given to loopback addresses. Router ID can be manually set by using the bgp router-id command.

Use the `no` parameter with this command to disable this functionality.

Command Syntax `bgp bestpath compare-routerid no bgp bestpath compare-routerid`

Parameters

None

Default

BGP receives routes with identical eBGP paths from eBGP peers and selects the first route received as the best path.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp bestpath compare-routerid

(config)#router bgp 100
(config-router)#no bgp bestpath compare-routerid
```

bgp bestpath dont-compare-originator-id

Use this command to change the default bestpath selection by not comparing an originator-ID for an identical EBGP path.

Use the `no` parameter with this command to disable this functionality.

Command Syntax `bgp bestpath dont-compare-originator-id no bgp bestpath dont-compare-originator-id`

Parameters

None

Default

BGP receives routes with identical eBGP paths from eBGP peers and selects the first route received as the best path.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp bestpath dont-compare-originator-id

(config)#router bgp 100
(config-router)#no bgp bestpath dont-compare-originator-id
```

bgp bestpath med

Use this command to specify two MED (Multi Exit Discriminator) attributes, `confed` and `missing-as-worst`.

The `confed` attribute enables MED comparison along paths learned from confederation peers. The MEDs are compared only if there is no external Autonomous System (an AS not within the confederation) in the path. If there is an external autonomous system in the path, the MED comparison is not made. For example in the following paths, the MED is not compared with Route3 as it is not in the confederation. MED is compared for Route1 and Route2 only.

```
Path1 = 32000 32004, med=4
Path2 = 32001 32004, med=2
Path3 = 32003 1, med=1
```

The `missing-as-worst` attribute to consider a missing MED attribute in a path as having a value of infinity, making the path without a MED value the least desirable path. If `missing-as-worst` is disabled, the missing MED is assigned the value of 0, making the path with the missing MED attribute the best path.

Use the `no` parameter with this command to prevent BGP from considering the MED attribute in comparing paths.

Command Syntax `bgp bestpath med confed missing-as-worst bgp bestpath med (confed|missing-as-worst|remove-recv-med|remove-send-med) bgp bestpath med missing-as-worst confed no bgp bestpath med confed missing-as-worst no bgp bestpath med (confed|missing-as-worst|remove-recv-med|remove-send-med) no bgp bestpath med missing-as-worst confed`

Parameters `confed` Compare MED along confederation paths

`missing-as-worst`

Treat missing MED as the least preferred one

`remove-recv-med`

Remove received MED attribute

`remove-send-med`

Remove sent MED attribute

Command Mode

Router mode

Default

By default, MED value is zero.

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
```

```
(config)#router bgp 100
(config-router)#bgp bestpath med missing-as-worst

(config)#router bgp 100
(config-router)#bgp bestpath med remove-recv-med
(config-router)#no bgp bestpath med remove-recv-med

(config)#router bgp 100
(config-router)#bgp bestpath med remove-send-med
(config-router)#no bgp bestpath med remove-send-med
```

bgp bestpath tie-break-on-age

Use this command to always select a preferred older route even when the `bgp bestpath compare-routerid` command is configured.

Use the `no` parameter with this command to disable this functionality.

Command Syntax `bgp bestpath tie-break-on-age no bgp bestpath tie-break-on-age`

Parameters

None

Default

By default, tie-break-on-age is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp bestpath tie-break-on-age

(config)#router bgp 100
(config-router)#no bgp bestpath tie-break-on-age
```

bgp client-to-client reflection

Use this command to configure routers as route reflectors. Route reflectors are used when all Interior Border Gateway Protocol (iBGP) speakers are not fully meshed. If the clients are fully meshed the route reflector is not required, use `no bgp client-to-client reflection` command to disable the client-to-client route reflection.

Use the `no` parameter with this command to turn off client-to-client reflection.

Command Syntax `bgp client-to-client reflection no bgp client-to-client reflection`

Parameters

None

Default

When a router is configured as a route reflector, client-to-client reflection is enabled by default.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp client-to-client reflection

(config)#router bgp 100
(config-router)#no bgp client-to-client reflection
```

bgp cluster-id

Use this command to configure the cluster ID if the BGP cluster has more than one route reflector. A cluster includes route reflectors and its clients. Usually, each cluster is identified by the router ID of its single route reflector but to increase redundancy sometimes a cluster may have more than one route reflector. All router reflectors in such a cluster are then identified by a cluster ID. The `bgp cluster-id` command is used to configure the 4 byte cluster ID for clusters with more than one route reflectors.

Use the `no` parameter with this command (without any arguments) to remove a previously configured route reflector cluster ID.

Command Syntax `bgp cluster-id <1-4294967295> bgp cluster-id A.B.C.D no bgp cluster-id`

Parameters

`<1-4294967295>`	Route reflector ID as a 32-bit quantity
`A.B.C.D`	Route reflector ID in an IPv4 address format

Default

By default, cluster id is set bgp cluster id

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following configuration creates a cluster-id 5 including two route-reflector-clients.

```
#configure terminal
(config)#router bgp 100
(config-router)#neighbor 2.2.2.2 remote-as 200
(config-router)#neighbor 3.3.3.3 remote-as 200
(config-router)#neighbor 3.3.3.3 route-reflector-client
(config-router)#neighbor 5.5.5.5 remote-as 200
(config-router)#neighbor 5.5.5.5 route-reflector-client
(config-router)#neighbor 6.6.6.6 remote-as 200
(config-router)#bgp cluster-id 5
```

bgp confederation identifier

Use this command to specify a BGP confederation identifier.

Use the `no` parameter with this command to remove a BGP confederation identifier.

Command Syntax `bgp confederation identifier <1-65535> no bgp confederation identifier`

Parameter

`<1-65535>`	Routing domain confederation AS number

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp confederation identifier 1
```

bgp confederation peers

Use this command to configure the Autonomous Systems (AS) that belong to a confederation. A confederation allows an AS to be divided into several ASs. The AS is given a confederation identifier. External BGP (eBGP) routers view only the whole confederation as one AS. Each AS is fully meshed within itself and is visible internally to the confederation.

Use the `no` parameter with this command to remove an autonomous system from the confederation.

Command Syntax `bgp confederation peers`

`<1-65535> no bgp confederation peers`

`<1-65535>`

Parameter

`<1-65535>` AS numbers of eBGP peers that are in the same confederation

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

In the following configuration example, the neighbor 172.210.30.2 and 172.210.20.1 have iBGP connection within AS 100, neighbor 173.213.30.1 is a BGP connection with a confederation peer 200 and neighbor 6.6.6.6 has an eBGP connection to external AS 300.

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp confederation identifier 300
(config-router)#bgp confederation peers 200
(config-router)#neighbor 172.210.30.2 remote-as 100
(config-router)#neighbor 172.210.20.1 remote-as 100
(config-router)#neighbor 173.213.30.1 remote-as 200
(config-router)#neighbor 6.6.6.6 remote-as 300
```

In this configuration, the neighbor 5.5.5.4 has an eBGP connection to confederation 300.

```
#configure terminal
(config)#router bgp 500
(config-router)#neighbor 5.5.5.4 remote-as 300
```

bgp config-type

Use this command to set the BGP configuration to the `standard` type. After setting the configuration to the `standard` type, use the neighbor send-community command to send out BGP community attributes. The `SWMRE` configuration type is the default and requires no specific configuration for sending out BGP standard community and extended community attributes.

For the `standard` type, the `no synchronization` command is always shown in the configuration, whereas for the `SWMRE` type, this command is the default.

Use the `no` parameter with this command to remove this configuration.

Command Syntax bgp config-type (standard|SWMRE) no bgp config-type

Parameters standard Standard style configuration SWMRE SWMRE style configuration

Default

The default configuration type is: bgp config-type SWMRE

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#bgp config-type standard
```

bgp dampening

Use this command to enable BGP route dampening and set various parameters. Route dampening minimizes the instability caused by route flapping. A penalty is added for every flap in a flapping route. As soon as the total penalty reaches the suppress limit the advertisement of the route is suppressed. This penalty is decayed according to the configured half time value. Once the penalty is lower than the reuse limit, the route advertisement is unsuppressed. The dampening information is purged from the router once the penalty becomes less than half of the reuse limit.

Use the no parameter with this command to unset BGP dampening parameters.

Command Syntax bgp dampening bgp dampening <1-45> bgp dampening <1-45> <1-20000> <1-20000> <1-255> bgp dampening <1-45> <1-20000> <1-20000> <1-255> <1-45> bgp dampening route-map WORD no bgp dampening no bgp dampening <1-45> no bgp dampening <1-45> <1-20000> <1-20000> <1-255> no bgp dampening <1-45> <1-20000> <1-20000> <1-255> <1-45> no bgp dampening route-map no bgp dampening route-map WORD

Parameters

<1-45>	Reachability half-life time for the penalty in minutes. The time for the penalty to decrease to one-half of its current value.

<1-20000>	Value to start reusing a route. When the penalty for a suppressed route decays below the reuse value, the routes become unsuppressed.
<1-20000>	Value to start suppressing a route. When the penalty for a route exceeds the suppress value, the route is suppressed
<1-255>	Maximum duration to suppress a stable route in minutes.
<1-45>	Un-reachability half-life time for the penalty in minutes.
route-map	Route map to specify criteria for dampening.
WORD	Route-map name.

Defaults

The default reachability half-life is 15 minutes.

The default reuse limit is 750.

The default suppress limit is 2000.

The default max-suppress value is 4 times the half-life time, or 60 minutes.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 11
                                    (config-router)#bgp dampening 20 800 2500 80 25
```

bgp default ipv4-unicast

Use this command to configure BGP defaults and activate IPv4-unicast for a peer by default. This affects the BGP global configuration.

Use the `no` parameter with this command to disable the default behavior of the BGP routing process of exchanging IPv4 addressing information with BGP neighbor routers.

Command Syntax `bgp default ipv4-unicast no bgp default ipv4-unicast`

Parameters

None

Default

IPv4 unicast is the default BGP behavior.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp default ipv4-unicast
```

bgp default local-preference

Use this command to change the default local preference value.Local preference indicates the preferred path when there are multiple paths to the same destination. The path having a higher preference is preferred. The preference is sent to all routers and access servers in the local autonomous system.

Use the `no` parameter with this command to revert to the default value for local preference.

Command Syntax `bgp default local-preference <0-4294967295> no bgp default local-preference no bgp default local-preference <0-4294967295>`

Parameter

`<0-4294967295>` Local preference value

Default

By default, local preference value is 100

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp default local-preference 2345555
```

bgp deterministic-med

Use this command to compare the Multi Exit Discriminator (MED) variable when choosing among routes advertised by different peers in the same autonomous system. MED is compared after BGP attributes weight, local preference, ASpath and origin have been compared and are equal.

For a correct comparison result, enable this command on all routers in a local AS. After enabling this command, all paths for the same prefix are grouped together and arranged according to their MED value. Based on this comparison, the best path is then chosen. This command compares MED variable when choosing routes advertised by different peers in the same AS, to compare MED, when choosing routes from neighbors in different ASs use the bgp alwayscompare-med command.

When the bgp deterministic-med command is enabled, routes from the same AS are grouped together, and the best routes of each group are compared. If the BGP table showed:

```
Route1: as-path 200, med 300, internal
Route2: as-path 400, med 200, internal
Route3: as-path 400, med 250, external
```

BGP would have a group of Route1 and a second group of Route2 and Route3 (the same ASs). The best of each group is compared. Route1 is the best of its group because it is the only route from AS 200. Route1 is compared to the Route2, the best of group AS 400 (the lower MED). Since the two routes are not from the same AS, the MED is not considered in the comparison. The external BGP route is preferred over the internal BGP route, making Route3 the best route; the preferred route would be different if `always-compare-med` command is enabled (See `alwayscompare-med` command).

Use the `no` parameter with this command to disallow this setting.

Command Syntax		
`bgp deterministic-med`	`no`	`bgp deterministic-med`

Parameters

None

Default

By default, bgp deterministic med is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp deterministic-med

(config)#router bgp 100
(config-router)#no bgp deterministic-med
```

bgp enforce-first-as

Use this command to enforce the first AS for eBGP routes. This command specifies that any updates received from an external neighbor that do not have the neighbor's configured Autonomous System (AS) at the beginning of the AS_PATH in the received update must be denied. Enabling this feature adds to the security of the BGP network by not allowing traffic from unauthorized systems.

Using the `no` parameter with this command to disable this feature.

Command Syntax `bgp enforce-first-as no bgp enforce-first-as`

Parameters

None

Default

By default, enforce-first-as is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp enforce-first-as

(config)#router bgp 100
(config-router)#no bgp enforce-first-as
```

bgp extended-asn-cap

Use this command to configure a BGP router to send 4-octet ASN capabilities. If attempting to change the AS capability from 2 to 4 or 4 to 2, a prompt occurs to remove the VRF configuration (if it exists), and reconfiguration is required, because the route distinguisher (RD) configuration would have been created with the current (2 octet or 4 octet) capability, and must be reconfigured before attempting to change the capability.

While loading from a saved configuration with AS4 capability and BGP VRF configuration, the capability will not be changed because of the above described reason.

Use the `no` parameter with this command to prevent a BGP router from sending 4-octet ASN capabilities.

Command Syntax `bgp extended-asn-cap no bgp extended-asn-cap`

Parameters

None

Default

By default, the bgp extended ASN capability and Four-octet capabilities are disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#bgp extended-asn-cap
```

bgp fast-external-failover

Use this command to reset a BGP session immediately, if the interface used for BGP connection goes down.

Use the `no` parameter with this command to disable this feature.

Command Syntax `bgp fast-external-failover`

`no bgp fast-external-failover`

Parameters

None

Default

By default, fast-external failover is enabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp fast-external-failover
```

bgp graceful-restart

Use this command to enable BGP graceful-restart capabilities. The restart-time parameter is used for setting the maximum time that a graceful-restart neighbor waits to come back up after a restart. This value is applied to all neighbors unless you explicitly override it by configuring the corresponding value on the neighbor. The stalepath-time parameter is used to set the maximum time to preserve stale paths from a gracefully restarted neighbor. All stalepaths, unless reinstated by the neighbor after a re-establishment, will be deleted at the expiration of this timer.

Use the `no` parameter with this command to restore the router to its default state.

Command Syntax `bgp graceful-restart bgp graceful-restart graceful-reset bgp graceful-restart restart-time <1-3600> bgp graceful-restart stalepath-time <1-3600> no bgp graceful-restart no bgp graceful-restart graceful-reset no bgp graceful-restart restart-time no bgp graceful-restart stalepath-time`

Parameters

`graceful-reset` The BGP daemon is not restarted, so that any changes in network configurations that cause BGP reset do not affect packet forwarding.

`restart-time` Maximum time needed for neighbors to restart. Default is 90 seconds.

`<1-3600>` Delay value in seconds. `stalepath-time` Maximum time to retain stale paths from restarting neighbors. Default is 360 seconds.

`<1-3600>` Delay value in seconds.

Default

By default, the maximum time for neighbors to restart is 90 seconds.

By default, the maximum time to retain stale paths from restarting neighbors is 360 seconds.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
    #configure terminal
    (config)#router bgp 10
    (config-router)#bgp graceful-restart

    #configure terminal
    (config)#router bgp 10
(config-router)#no bgp graceful-restart
```

bgp g-shut

Use this command to gracefully shut down all BGP IPv4 sessions under this router. The BGP graceful shutdown feature reduces packet loss during maintenance activity.

Use the `no` parameter with this command to bring up all the sessions under this router after completion of activity using the `bgp g-shut` maintenance command.

Command Syntax `bgp g-shut no bgp g-shut`

Parameters

None

Default

By default, bgp g-shut is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp g-shut
```

```
#configure terminal
(config)#router bgp 100
(config-router)#no bgp g-shut
```

bgp g-shut-capable

Use this command to enable the graceful shutdown capability at the router level and make available the gracefulshutdown related commands at the router and BGP neighbor levels.

Use the `no` parameter with this command to disable the graceful shutdown capability on a router.

Note: The graceful shutdown capability cannot be disabled on a router that is in a graceful shutdown state until it comes out this state--after the graceful shutdown has been initiated and the impacted BGP sessions are up again.

Command Syntax `bgp g-shut-capable no bgp g-shut-capable`

Parameters

None

Default

By default, the graceful shutdown capability is disabled at the router level

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp g-shut-capable

#configure terminal
(config)#router bgp 100
(config-router)#no bgp g-shut-capable
```

bgp g-shut-local-preference

Use this command to sets the local preference of the router to use during graceful shutdown. The local preference value indicates the preferred path when there are multiple paths to the same destination in a single routing database. The path with a higher preference value is the preferred one. The preferred path is sent to all routers and access servers in the local autonomous system.

Use the `no` parameter with this command to revert to the default setting.

Command Syntax `bgp g-shut-local-preference <0-4294967295> no bgp g-shut-local-preference`

Parameters

`<0-4294967295>` Local preference value

Default

By default, the local preference value is set to 0

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
```

```
(config)#router bgp 100 (config-router)#bgp g-
shut-local-preference 22
```

bgp log-neighbor-changes

Use this command to enable logging of status change messages without turning on debug bgp commands. SWMRE has many logging services for neighbor status, including `debug bgp fsm` and `debug bgp events`. However, these commands cause system performance degradation. If you need to log neighbor status changes only, Symanitron recommends turning off all debug commands and using the `bgp log-neighbor-changes` command instead. A sample output of the log is:

```
%Protocol-Severity-Events: Message-text
```

A sample output of the log for an `interface down` event is:

```
%BGP-5-ADJCHANGE: neighbor 10.10.0.24 Down Interface flap
```

This command logs the following events:

- BGP Notification Received
- Erroneous BGP Update Received
- User reset request
- Peer time-out
- Peer Closing down the session
- Interface flap
- Router ID changed
- Neighbor deleted
- Member added to peer group
- Administrative shutdown
- Remote AS changed
- RR client configuration modification
- Soft reconfiguration modification

Use the `no` parameter with this command to disable this feature.

Command Syntax `bgp log-neighbor-changes no bgp log-neighbor-changes`

Parameters

None

Default

By default, bgp log neighbor changes is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
(config)#router bgp 100
                                        (config-router)#bgp log-neighbor-changes
```


© Symanitron Proprietary

bgp multiple-instance

Use this command to enable BGP multiple instance support.

Use the `no` parameter with this command to disable this function.

Note: The `no bgp multiple-instance` command is not valid when any BGP instances are present.

Command Syntax `bgp multiple-instance (allow-same-peer|)` `no bgp multiple-instance (allow-same-peer|)`

Parameters `allow-same-peer`

Allow the same peer in multiple instances

Default

By default, there is no multiple-instance support in BGP

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows the use of the `bgp multiple-instance` command allowing the configuration of two instances.

```
(config)#bgp multiple-instance

(config)#quit #show
running-config

Current configuration:
hostname SWMRE
password zebra
log stdout
! debug bgp debug
bgp events debug
bgp updates
debug bgp fsm
!
bgp multiple-instance
! router bgp
11
```

```
 bgp router-id 10.10.10.50
neighbor 10.10.10.51 remote-as 11
!
```

bgp nexthop-trigger delay

Use this command to set the delay time for nexthop address tracking. This command configures the delay interval between routing table walks for nexthop delay tracking, after which BGP does a routing table scan on receiving a nexthop change trigger from NSM. The time period determines how long BGP waits before it walks the full BGP table to determine which prefixes are affected by the nexthop changes, after it receives the trigger from NSM about one or more nexthop changes.

Use the `no` parameter with this command to reset the timer value to the default value.

Command Syntax `bgp nexthop-trigger delay <1-100> no bgp nexthop-trigger delay`

Parameter

`<1-100>`	Nexthop trigger delay interval in seconds

Default

By default, nexthop-trigger delay time is 5 seconds

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#bgp nexthop-trigger delay 6

#configure terminal
(config)#no bgp nexthop-trigger delay
```

bgp nexthop-trigger enable

Use this command to enable nexthop address tracking. Nexthop address tracking is an event-driven notification system that monitors the status of routes installed in the Routing Information Base (RIB) and reports nexthop changes that affect internal BGP (iBGP) or external BGP (eBGP) prefixes directly to the BGP process. This improves the overall BGP convergence time, by allowing BGP to respond rapidly to nexthop changes for routes installed in the RIB.

If nexthop tracking is enabled after certain routes are learned, the registration of all nexthops for selected BGP routes is done after the nexthop tracking feature is enabled. If nexthop tracking is disabled, and if there are still some selected BGP routes, BGP de-registers the nexthops of all selected BGP routes from NSM.

Use the `no` parameter with this command to disable this feature. If the `no` command is given when nexthop tracking is in the process of execution, an error appears and nexthop tracking is not disabled. However, if the nexthop tracking timer is running at the time of negation, the nexthop tracking timer is stopped, and nexthop tracking is disabled.

Command Syntax `bgp nexthop-trigger enable` `no bgp nexthop-trigger enable`

Parameters

None

Default

By default, nexthop address tracking is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#bgp nexthop-trigger enable
```

bgp rfc1771-path-select

Use this command to set RFC 1771 compatible path selection.

Use the `no` parameter with this command to revert this setting.

Command Syntax `bgp rfc1771-path-select` `no bgp rfc1771-path-select`

Parameters

None

Default

Standard compatible path selection mechanism.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#bgp rfc1771-path-select
```

bgp rfc1771-strict

Use this command to set the origin path attribute to “IGP” when the origin is a protocol such as RIP, OSPF, or ISIS as specified in RFC 1771. Otherwise, the origin is always set to “incomplete” which is the industry standard.

Use the `no` parameter with this command to revert this setting.

Command Syntax `bgp rfc1771-strict no bgp rfc1771-strict`

Parameters

None

Default

By default, bgp rfc1771 strict is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#bgp rfc1771-strict
```

bgp router-id

Use this command to manually configure a fixed router ID as a BGP router identifier. When this command is used to configure a fixed router ID, the current router identifier is overridden and the peers are reset.

Use the `no` parameter with this command to remove a manually configured fixed router ID.

Command Syntax `bgp router-id A.B.C.D no bgp router-id no bgp router-id A.B.C.D`

Parameter

`A.B.C.D`	Router ID in an IPv4 address format

Default

Once the BGP router-id is elected, it may be re-elected in the following cases:

a. When an explicit BGP router-id is configured/un-configured

b. When the router's (global) router-id is set/unset (holds true when (a) is not applicable),

c. When the BGP process is cleared (holds true when both (a) & (b) are not applicable and the IP address(es) on the active interfaces are updated, which may result in a change in the router's router-id).

If no loopback interface is configured, the highest IP address is the BGP router-id.

When a loopback interface is configured, the BGP router-id is set to the IP address of the loopback interface.

Note: Symanitron recommends that you always configure a router identifier to avoid unpredictable behavior if the address of a loopback interface changes.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp router-id 10.1.2.7

(config)#router bgp 100
(config-router)#no bgp router-id 10.1.2.7
```

bgp scan-time

Use this command to configure scanning intervals of BGP routers. This interval is the period after which router checks the validity of the routes in its database. To disable BGP scanning, set the scan-time interval to 0 seconds.

Use the `no` parameter with this command to disable this function.

Command Syntax `bgp scan-time <0-60> no bgp scan-time no bgp scan-time <0-60>`

Parameter

`<0-60>`	Scanning interval in seconds

Default

By default, scan-time interval is 60 seconds.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp scan-time 10
```

bgp table-map

Use this command to enable or disable suppression/modification of incoming BGP updates to IP RIB/FIB table installation.

In a dedicated route reflector, all the routes it receives may not be required to be stored or only few selected routes need to be stored, because it may not lie in the data path.

Table maps are particularly useful to attain this restriction. Table-map command can be used in two ways:

- When a simple table-map command is given, the route map referenced in the table-map command shall be used to set certain properties (such as the traffic index) of the routes for installation into the RIB. The route is always downloaded, regardless of whether it is permitted or denied by the route map.
- When the option ‘filter’ is given in the table map command, the route map referenced is used to control whether a BGP route is to be downloaded to the IP RIB (hence the filter). A BGP route is not downloaded to the RIB if it is denied by the route map.

Use this command in Router mode to set the table map rule for all address families. Use this command in Address Family mode to set the table map rule per an IPv4 or IPv6 family.

Use the `no` parameter with this command to remove the table-map rule.

Command Syntax `table-map`

```
WORD (|filter)
```

Parameter

`WORD`	Specify the route-map name to apply.
`filter`	Filer the routes. If present, the incoming routes are pruned as per the rule specified in route-map-name. If not, it is used to alter the incoming packet information.

Default

All BGP routes will be downloaded to IP RIB

Command Mode

Router mode, Address Family IPv4 mode, and Address Family IPv6 mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows how to set the table-map command without filter for BGP for all address families.

```
#configure terminal
(config)#router bgp 100
(config-router)#table-map abc
```

The following example shows how to set the table-map command with filter for BGP for all address families.

```
#configure terminal
(config)#router bgp 100
(config-router)#table-map abc filter
```

The following example shows how to set the table-map command without filter for BGP for an IPv6 address family.

```
(config)#router bgp 100
(config-router)#address family ipv6
(config-router-af)# table-map abc
```

The following example shows how to set the table-map command with filter for BGP for an IPv6 address family.

```
(config)#router bgp 100
(config-router)#address family ipv6
(config-router-af)# table-map abc filter
```

bgp update-delay

Use this command to set the update delay for a graceful-restart capable router. The update-delay value is the maximum time a graceful-restart capable router, which is restarting, will defer route-selection and advertisements to all its graceful-restart capable neighbors. This maximum time starts from the instance the first neighbor attains established state after restart. The restarting router prematurely terminates this timer when end-of-RIB markers are received from all its graceful-restart capable neighbors.

Use the `no` form of this command to set to the update delay to its default value.

Command Syntax `bgp update-delay <1-3600> no bgp update-delay no bgp update-delay <1-3600>`

Parameters

`<1-3600>` Delay interval in seconds

Default

By default, update-delay value is 120 seconds

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#bgp update-delay 345
```

clear bgp (A.B.C.D|X:X::X:X)

Use this command to reset a BGP neighbor address.

Command Syntax `clear bgp (A.B.C.D|X:X::X:X) clear bgp (A.B.C.D|X:X::X:X) in clear bgp (A.B.C.D|X:X::X:X) in prefix-filter clear bgp (A.B.C.D|X:X::X:X) out`

Parameters

`A.B.C.D` IPv4 neighbor address. `X:X::X:X` IPv6 neighbor address.

`in` Clear incoming advertised routes.

`prefix-filter` Push out prefix-list ORF and do inbound soft reconfig.

`out` Clear outgoing advertised routes.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear bgp 3.3.3.3
```

clear bgp *

Use this command to reset the BGP connection for all peers.

Command Syntax `clear bgp * clear bgp * in clear bgp * in prefix-filter clear bgp * out clear bgp * soft clear bgp * soft in clear bgp * soft out clear ip bgp * clear ip bgp * in clear ip bgp * in prefix-filter clear ip bgp * out clear ip bgp * soft clear ip bgp * soft in clear ip bgp * soft out clear ip bgp * ipv4 (unicast|multicast) in clear ip bgp * ipv4 (unicast|multicast) in prefix-filter clear ip bgp * ipv4 (unicast|multicast) out clear ip bgp * ipv4 (unicast|multicast) soft clear ip bgp * ipv4 (unicast|multicast) soft in clear ip bgp * ipv4 (unicast|multicast) soft out`

Parameters

`in` Incoming advertised routes should be cleared.

`prefix-filter` Push out prefix-list ORF and do inbound soft reconfig.

`out` Clear outgoing advertised routes.

`soft` Clear both incoming and outgoing routes.

- `in` Soft reconfig inbound update.
- `out` Soft reconfig outbound update.

`ipv4` Clear incoming advertised routes.

- `multicast` Multicast prefixes.
- `unicast` Unicast prefixes.
  - `in` Clear incoming advertised routes.
  - `prefix-filter` Push out prefix-list ORF and do inbound soft reconfig.
  - `out` Clear outgoing advertised routes.
  - `soft` Clear both incoming and outgoing routes.
  - `in` Soft reconfig inbound update.
  - `out` Soft reconfig outbound update.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear bgp *
#clear ip bgp * ipv4 unicast in prefix-filter
```

clear bgp <1-4294967295>

Use this command to reset a BGP connection for all peers in a specified Autonomous System.

Command Syntax `clear bgp <1-4294967295> clear bgp <1-4294967295> in clear bgp <1-4294967295> in prefix-filter clear bgp <1-4294967295> out clear bgp <1-4294967295> soft clear bgp <1-4294967295> soft in clear bgp <1-4294967295> soft out clear ip bgp <1-4294967295> clear ip bgp <1-4294967295> in clear ip bgp <1-4294967295> in prefix-filter clear ip bgp <1-4294967295> out clear ip bgp <1-4294967295> soft clear ip bgp <1-4294967295> soft in clear ip bgp <1-4294967295> soft out clear ip bgp <1-4294967295> ipv4 (unicast|multicast) in clear ip bgp <1-4294967295> ipv4 (unicast|multicast) in prefix-filter clear ip bgp <1-4294967295> ipv4 (unicast|multicast) out clear ip bgp <1-4294967295> ipv4 (unicast|multicast) soft clear ip bgp <1-4294967295> ipv4 (unicast|multicast) soft in clear ip bgp <1-4294967295> ipv4 (unicast|multicast) soft out`

Parameters

`in`	Clear incoming advertised routes.
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.
`ipv4`	Clear incoming advertised routes.
`multicast`	Multicast prefixes.
`unicast`	Unicast prefixes.
	Clear incoming advertised routes.
`in`	Clear incoming advertised routes.
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear bgp 4294967277
#clear ip bgp 4294967277
```

clear bgp dampening

Use this command to reset BGP route flap dampening information.

Command Syntax `clear bgp ipv4 (unicast|multicast) dampening clear bgp ipv4 (unicast|multicast) dampening A.B.C.D/M clear ip bgp dampening clear ip bgp dampening A.B.C.D/M clear ip bgp ipv4 (unicast|multicast) dampening clear ip bgp ipv4 (unicast|multicast) dampening A.B.C.D/M`

Parameters

`ipv4`	IPv4 address family.
`multicast`	Multicast prefixes
`unicast`	Unicast prefixes
`A.B.C.D/M`	IP prefix (network/length), for example, 35.0.0.0/8

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear ip bgp dampening 10.10.0.121/24
#clear ip bgp ipv4 unicast dampening
```

clear bgp external

Use this command to reset the BGP connection for all external peers.

Command Syntax `clear bgp external clear bgp external in clear bgp external in prefix-filter clear bgp external out clear bgp external soft clear bgp external soft in clear bgp external soft out clear ip bgp external clear ip bgp external in clear ip bgp external in prefix-filter clear ip bgp external out clear ip bgp external soft clear ip bgp external soft in clear ip bgp external soft out clear ip bgp external ipv4 (unicast|multicast) in clear ip bgp external ipv4 (unicast|multicast) in prefix-filter clear ip bgp external ipv4 (unicast|multicast) out clear ip bgp external ipv4 (unicast|multicast) soft clear ip bgp external ipv4 (unicast|multicast) soft in clear ip bgp external ipv4 (unicast|multicast) soft out`

Parameters

`in`	Clear incoming advertised routes.
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.

`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.
`ipv4`	Clear incoming advertised routes.
`multicast`	Multicast prefixes.
`unicast`	Unicast prefixes.
`in`	Clear incoming advertised routes.
`prefix-filter`	

Push out prefix-list ORF and do inbound soft reconfig.

`out`	Clear outgoing advertised routes.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear ip bgp external
```

clear bgp flap-statistics

Use this command to reset BGP flap statistics.

Command Syntax `clear bgp ipv4 (unicast|multicast) flap-statistics`

`clear bgp ipv4 (unicast|multicast) flap-statistics A.B.C.D/M vrf (all | default | VRFNAME) clear bgp ipv4 (unicast|multicast) flap-statistics A.B.C.D/M clear ip bgp flap-statistics clear ip bgp flap-statistics A.B.C.D/M clear ip bgp ipv4 (unicast|multicast) flap-statistics clear ip bgp ipv4 (unicast|multicast) flap-statistics A.B.C.D/M vrf (all | default | VRFNAME) clear ip bgp ipv4 (unicast|multicast) flap-statistics A.B.C.D/M`

Parameters

`ipv4`	IPv4 address family.
`multicast`	Multicast prefixes.
`unicast`	Unicast prefixes.
`A.B.C.D/M`	IP prefix (network/length), for example, 35.0.0.0/8
`VRFNAME`	VPN routing or forwarding instance name
`all`	All VRF's
`default`	Default VRF

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear ip bgp flap-statistics
#clear ip bgp ipv4 unicast flap-statistics
```

clear bgp peer-group

Use this command to reset the BGP connection for all members of a peer group.

Command Syntax `clear bgp peer-group WORD clear bgp peer-group WORD in clear bgp peer-group WORD in prefix-filter clear bgp peer-group WORD out clear bgp peer-group WORD soft clear bgp peer-group WORD soft in clear bgp peer-group WORD soft out clear ip bgp peer-group WORD clear ip bgp peer-group WORD in clear ip bgp peer-group WORD in prefix-filter clear ip bgp peer-group WORD out clear ip bgp peer-group WORD soft clear ip bgp peer-group WORD soft in clear ip bgp peer-group WORD soft out clear ip bgp peer-group`

```
WORD ipv4 (unicast|multicast) in clear ip bgp peer-group WORD ipv4
(unicast|multicast) in prefix-filter clear ip bgp peer-group WORD ipv4
(unicast|multicast) out clear ip bgp peer-group WORD ipv4 (unicast|multicast) soft
clear ip bgp peer-group WORD ipv4 (unicast|multicast) soft in clear ip bgp peer-
group WORD ipv4 (unicast|multicast) soft out
```

Parameters

WORD	BGP peer-group name.
in	Clear incoming advertised routes.
prefix-filter	Push out prefix-list ORF and do inbound soft reconfig.
out	Clear outgoing advertised routes.
soft	Clear both incoming and outgoing routes.
in	Soft reconfig inbound update.
out	Soft reconfig outbound update.
ipv4	Clear incoming advertised routes.
multicast	Multicast prefixes.
unicast	Unicast prefixes.
	Clear incoming advertised routes.
in	Clear incoming advertised routes.
prefix-filter	Push out prefix-list ORF and do inbound soft reconfig.
out	Clear outgoing advertised routes.
soft	Clear both incoming and outgoing routes.
in	Soft reconfig inbound update.
out	Soft reconfig outbound update.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear ip bgp peer-group P1
```

clear bgp statistics

Use this command to reset all BGP statistics.

Command Syntax `clear bgp statistics`

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear bgp statistics
```

clear bgp view

Use this command to reset all peers in a BGP view.

Command Syntax `clear bgp view WORD * clear bgp view WORD * soft clear bgp view WORD * soft in clear bgp view WORD * soft out clear ip bgp view WORD * clear ip bgp view WORD * in prefix-filter clear ip bgp view WORD * soft clear ip bgp view WORD * soft in clear ip bgp view WORD * soft out clear ip bgp view WORD * ipv4 (unicast|multicast) in prefix-filter clear ip bgp view WORD * ipv4 (unicast|multicast) soft clear ip bgp view WORD * ipv4 (unicast|multicast) soft in clear ip bgp view WORD * ipv4 (unicast|multicast) soft out`

Parameters

`WORD` BGP peer group name.

`in` Clear incoming advertised routes.

`prefix-filter`

Push out prefix-list ORF and do inbound soft reconfig.

`soft` Clear both incoming and outgoing routes.

`in` Soft reconfig inbound update.

`out` Soft reconfig outbound update. `ipv4` IPv4 address family. `multicast` Multicast prefixes. `unicast` Unicast prefixes.

`in` Clear incoming advertised routes.

`prefix-filter`

Push out prefix-list ORF and do inbound soft reconfig.

`soft` Clear both incoming and outgoing routes.

`in` Soft reconfig inbound update. `out` Soft reconfig outbound update.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear ip bgp view myview *
```

clear ip bgp A.B.C.D

Use this command to reset an IPv4 BGP neighbor address.

Command Syntax `clear ip bgp A.B.C.D in clear ip bgp A.B.C.D in prefix-filter clear ip bgp A.B.C.D out clear ip bgp A.B.C.D soft clear ip bgp A.B.C.D soft in clear ip bgp A.B.C.D soft out clear ip bgp A.B.C.D ipv4 (unicast|multicast) in clear ip bgp A.B.C.D ipv4 (unicast|multicast) in prefix-filter clear ip bgp A.B.C.D ipv4 (unicast|multicast) out clear ip bgp A.B.C.D ipv4 (unicast|multicast) soft clear ip bgp A.B.C.D ipv4 (unicast|multicast) soft in clear ip bgp A.B.C.D ipv4 (unicast|multicast) soft out`

Parameters `in` Clear incoming advertised routes.

`prefix-filter`

Push out prefix-list ORF and do inbound soft reconfig.

`out` Clear outgoing advertised routes.

`soft` Clear both incoming and outgoing routes.

`in` Soft reconfig inbound update.

`out` Soft reconfig outbound update.

`ipv4` Clear incoming advertised routes.

`multicast` Multicast prefixes. `unicast` Unicast prefixes.

`in` Clear incoming advertised routes.

`prefix-filter`

Push out prefix-list ORF and do inbound soft reconfig.

`out` Clear outgoing advertised routes.

`soft` Clear both incoming and outgoing routes.

`in` Soft reconfig inbound update. `out` Soft reconfig outbound update.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear ip bgp 35.0.0.1 in
```

clear ip bgp A.B.C.D vrf

Use this command to reset the VPN Routing/Forwarding (VRF) instance for a peer address.

Command Syntax `clear ip bgp A.B.C.D vrf WORD clear ip bgp A.B.C.D vrf WORD in clear ip bgp A.B.C.D vrf WORD out clear ip bgp A.B.C.D vrf WORD soft clear ip bgp A.B.C.D vrf WORD soft in clear ip bgp A.B.C.D vrf WORD soft out`

Parameters

`A.B.C.D`	IPv4 address
`WORD`	VPN routing/forwarding instance name
`in`	Clear incoming advertised routes
`out`	Clear outgoing advertised routes
`soft`	Clear both incoming and outgoing routes
`in`	Soft reconfig inbound update
`out`	Soft reconfig outbound update

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear ip bgp 35.0.0.1 vrf
```

clear ip bgp table-map

Use this command to apply the modified table map or route map rules to the BGP routes in the existing IP routing table.

Command Syntax `clear ip bgp table-map (vrf (VRFNAME|all|default))`

`clear ip bgp ipv4 (unicast | multicast) table-map(vrf (VRFNAME|all|default))`

Parameters

`vrf`	Select a VPN Routing/Forwarding Instance.
`VRFNAME`	Specify a VPN Routing/Forwarding instance name.
`all`	Select all VRFs.
`default`	Select default VRFs.
`unicast`	Unicast prefixes.
`multicast`	Multicast prefixes.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear ip bgp table-map vrf all
```

debug bgp

Use this command to enable all BGP troubleshooting functions. Use this command without any parameters to turn on normal bgp debug information.

Use the `no` parameter with this command to disable this function.

Command Syntax `debug bgp (all|) debug bgp bfd debug bgp dampening debug bgp events debug bgp filters debug bgp fsm debug bgp keepalives debug bgp mpls debug bgp nht debug bgp nsm debug bgp updates debug bgp updates (in|out) debug bgp vpls no debug bgp (all|) no debug bgp bfd no debug bgp dampening no debug bgp events no debug bgp filters no debug bgp fsm no debug bgp keepalives no debug bgp mpls no debug bgp nht no debug bgp nsm no debug bgp updates no debug bgp vpls undebug bgp (all|) undebug bgp bfd undebug bgp dampening undebug bgp events undebug bgp filters undebug bgp fsm undebug bgp keepalives`

```
undebug bgp mpls undebug bgp nht undebug bgp nsm undebug bgp
updates undebug bgp vpls
```

Parameters

`all`	Used only with the `no` form; turns off all debugging for BGP
`bfd`	Enable debugging for BGP Bidirectional Forwarding Detection
`dampening`	Enable debugging for BGP dampening
`events`	Enable debugging for BGP events
`filters`	Enable debugging for BGP filters
`fsm`	Enable debugging for BGP Finite State Machine (FSM)
`keepalives`	Enable debugging for BGP keepalives
`mpls`	Enable debugging for BGP Multiprotocol Label Switching (MPLS)
`nht`	Enable debugging for BGP NHT
`nsm`	Enable debugging for NSM messages
`updates`	Enable debugging for BGP updates
`in`	Debug inbound updates
`out`	Debug outbound updates
`vpls`	Enable debugging for BGP Virtual Private LAN Service (VPLS)

Command Mode

Privileged Exec mode and Configure Mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#debug bgp
#debug bgp events
```

distance bgp

Use this command to define an administrative distance. A distance is a rating of trustworthiness of a router. The higher the distance the lower the trust rating. Administrative distances can be set for external, internal and local routes. External paths are routes learned from a neighbor outside of the AS. Internal routes are routes learned from another router within the same AS. Local routes are for a router that is redistributed from another process.

If the administrative distance is changed, it could create inconsistency in the routing table and obstruct routing. Use this command in Router mode to set the administrative distance for all address families. Use this command in Address Family mode to set the administrative distance per an IPv4 family.

Use the `no` parameter with this command to remove an administrative distance.

Command Syntax `distance bgp <1-255> <1-255> <1-255> no distance bgp`

```
no distance bgp <1-255> <1-255> <1-255>
```

Parameters

<1-255>	Distance for BGP external routes
<1-255>	Distance for BGP internal routes
<1-255>	Distance for BGP local routes

Command Mode

Router mode, Address Family IPv4 mode

Defaults

Default distance for external routes is 20.

Default distance for internal routes is 200.

Default distance for local routes is 200.

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows how to set the administrative distance for BGP for all address families.

```
#configure terminal
(config)#router bgp 100
(config-router)#distance bgp 34 23 15
```

exit-address-family

Use this command to exit Address-Family-vrf, Address-Family-vpnv4 mode.

For information on how to enter the address family mode (IPv4, VPNv4), see address-family.

Command Syntax `exit-address-family`

Parameters

None

Default

No default value is specified

Command Mode

Address Family-vrf and Address Family-vpnv4 mode.

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following examples shows the change in the prompt after using this command.

```
#configure terminal
(config)#router bgp 100 (config-
router)#address-family ipv4 multicast
(config-router-af)#exit-address-family
(config-router)#
```

ip as-path access-list

Use this command to define a BGP Autonomous System (AS) path access list. A named community list is a filter based on regular expressions. If the regular expression matches the specified string representing the AS path of the route, then the permit or deny condition applies. Use this command to define the BGP access list globally; use the neighbor router configuration command to apply a specific access list.

Use the no parameter with this command to disable use of the access list.

Command Syntax `ip as-path access-list WORD (deny|permit) LINE no ip as-path access-list WORD`

`no ip as-path access-list WORD (deny|permit) LINE`

Parameters

`WORD`	Access list name
`deny`	Reject packets
`permit`	Forward packets
`LINE`	An ordered list as a regular expression

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip as-path access-list mylist deny ^65535$
```

ip community-list <1-99>

Use this command to specify a standard community list (1 to 99) that specifies BGP community attributes.

Use the `no` parameter with this command to delete the community list entry.

Command Syntax `ip community-list <1-99> (deny|permit) ip community-list <1-99> (deny|permit) [AA:NN|internet|local-AS|no-advertise|no-export]`

`no ip community-list <1-99> (deny|permit) no ip community-list <1-99> (deny|permit) [AA:NN|internet|local-AS|no-advertise|no-export]`

Parameters

`deny`	Reject the community
`permit`	Accept the community
`AA:NN`	Community number
`internet`	Advertise routes to the internet community
`local-AS`	Do not advertise routes to external BGP peers
`no-advertise`	Do not advertise routes to other BGP peers
`no-export`	Do not advertise routes outside of Autonomous System boundary

Default

By default, ip community list is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip community-list 55 permit 7675:80 7675:90
```

```
(config)#no ip community-list 55 permit 7675:80 7675:90
```

ip community-list <100-500>

Use this command to specify an expanded community list (100 to 500) that specifies BGP community attributes.

Use the `no` parameter with this command to delete the community list entry.

Command Syntax `ip community-list <100-500> (deny|permit) ip community-list <100-500> (deny|permit) LINE no ip community-list <100-500> no ip community-list <100-500> (deny|permit) LINE`

Parameters

`deny`	Reject community
`permit`	Accept community
`LINE`	An ordered list as a regular expression

Default

By default, ip community list is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip community-list 225 permit 6789906
(config)#ip community-list expanded CLIST permit .*
```

ip community-list expanded

Use the community-lists to specify BGP community attributes. The community attribute is used for implementing policy routing. It is an optional, transitive attribute and facilitates transfer of local policies through different autonomous systems. It includes community values that are 32-bits long.

There are two kinds of community-lists: expanded and standard. The standard community-list defines the community attributes in a specified format and not with regular expressions. The expanded community-list defines the community attributes with regular expressions.Use the `no` parameter with this command to delete the community list entry.

Command Syntax `ip community-list expanded WORD (deny|permit) LINE no ip community-list expanded WORD no ip community-list expanded WORD (deny|permit) LINE`

Parameters

`WORD`	Community list name

deny	Reject community
permit	Accept community
LINE	An ordered list as a regular expression

Default

By default, ip community list is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip community-list 125 permit 6789906
(config)#ip community-list expanded CLIST permit .*
```

ip community-list standard

Use the community-lists to specify BGP community attributes. The community attribute is used for implementing policy routing. It is an optional, transitive attribute and facilitates transfer of local policies through different autonomous systems. It includes community values that are 32-bits long. There are two kinds of community-lists: expanded and standard. The standard community-list defines the community attributes in a specified format without regular expressions. The expanded community-list defines the community attributes with regular expressions.

Use this command to add a standard community-list entry. The standard community-list is compiled into binary format and is directly compared with the BGP communities attribute in the BGP updates. The comparison is faster than the expanded community-list. Any community value that does not match the standard community value is automatically treated as expanded.

Use the `no` parameter with this command to delete the standard community-list entry.

Command Syntax `ip community-list standard WORD (deny|permit) ip community-list standard WORD (deny|permit) [AA:NN|internet|local-AS|no-advertise|no-export]`

```
no ip community-list standard WORD (deny|permit) [AA:NN|internet|local-AS|no-advertise|no-export]
```

Parameters

WORD	Community list name
deny	Reject the community
permit	Accept the community
AA:NN	Community number
internet	Advertise routes to the internet community
local-AS	Do not advertise routes to external BGP peers
no-advertise	Do not advertise routes to other BGP peers

no-export	Do not advertise routes outside of Autonomous System boundary

Default

By default, ip community list is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip community-list standard CLIST permit 7675:80 7675:90 no-export
(config)#ip community-list 34 permit 5675:50 no-advertise
```

ip community-list WORD

Use the community-list commands to specify BGP community attributes. The community attribute is used for implementing policy routing. It is an optional, transitive attribute and facilitates transfer of local policies through different
autonomous systems. There are two kinds of community-lists: the expanded and standard. The `standard community-list` defines the community attributes in a specified format and not with regular expressions. The `expanded community-list` defines the community attributes with regular expressions.

Use the `no` parameter with this command to delete the community list entry.

Command Syntax

```
ip community-list WORD (deny|permit) ip community-list WORD
(deny|permit) [AA:NN|internet|local-AS|no-advertise|no-
  export]
no ip community-list WORD no ip community-list WORD (deny|permit)
[AA:NN|internet|local-AS|no-advertise|no-
  export]
```

Parameters

WORD	Community list name
deny	Reject the community
permit	Accept the community
AA:NN	Community number
internet	Advertise routes to the internet community
local-AS	Do not advertise routes to external BGP peers
no-advertise	Do not advertise routes to other BGP peers
no-export	Do not advertise routes outside of Autonomous System boundary

Default

By default, ip community list is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip community-list mylist permit 7675:80 7675:90

(config)#no ip community-list mylist permit 7675:80 7675:90
```

ip extcommunity-list <1-99>

Use this command to create an entry for a standard extended community list.

Use the `no` parameter with this command to delete the community-list entry.

Command Syntax `ip extcommunity-list <1-99> (deny|permit) LINE (rt|soo) no ip extcommunity-list <1-99> (deny|permit) LINE (rt|soo)`

Parameters

`deny`	Reject community
`permit`	Accept community
`LINE`	One of the following:
`rt`	Route target extended community in aa:nn or IPaddr:nn format
`soo`	Site-of-origin extended community in aa:nn or IPaddr:nn format

Default

By default, ip extcommunity list is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
           (config)#ip extcommunity-list 3 permit rt 10.10.23.123:67

(config)#ip extcommunity-list 25 deny soo 1465:22
```

ip extcommunity-list <100-500>

Use this command to create an extended community list.

Use the `no` parameter with this command to delete the community-list entry.

Command Syntax `ip extcommunity-list <100-500> (deny|permit) LINE no ip extcommunity-list <100-500> (deny|permit) LINE`

Parameters

`<100-500>`	Extended community list number (expanded)
`deny`	Reject the community
`permit`	Accept the community
`LINE`	Any regular expression:

Default

By default, ip extcommunity list is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
                                (config)#ip extcommunity-list 125 permit 4567:335

(config)#ip extcommunity-list 231 deny *.
```

ip extcommunity-list expanded

Use this command to create an expanded community list.

Use the `no` parameter with this command to delete the expanded community-list entry.

Command Syntax `ip extcommunity-list expanded WORD ip extcommunity-list expanded WORD (deny|permit) LINE no ip extcommunity-list expanded WORD no ip extcommunity-list expanded WORD (deny|permit) LINE`

Parameters

`WORD`	Expanded community list name
`deny`	Reject the community
`permit`	Accept the community
`LINE`	One of the following:
`rt`	Route target extended community in aa:nn or IPaddr:nn format
`soo`	Site-of-origin extended community in aa:nn or IPaddr:nn format

Default

By default, ip extcommunity list is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip extcommunity-list 125 permit 4567335
(config)#ip extcommunity-list expanded CLIST permit .*
```

ip extcommunity-list standard

Use this command to create and delete a standard extended-community list. The extended community attribute is 8 bytes in 2 formats. The sub-type can be route target (`rt`) or site of origin (`soo`). Thus, the sub-type of each community must be specified when creating the extended community list. Regarding the formats, an extended community is based on a 6-byte value. These 6-bytes are represented in 4-btye:2-byte format, and may be entered in one of the following forms:

- Format 1, aa.nn: The 16-bit value of the AS (aa) number is represented in the higher-order 4-bytes. If the extended ASN capability is enabled, the AS number is represented using higher-order 4-bytes. The nn assigned value is represented in the low-order 2-bytes in both cases.
- Format 2, IPaddr:nn: In this format, the higher-order 4-bytes are used to represent the IP address, and the loworder 2-bytes are used to represent the assigned value.

Use the `no` parameter with this command to delete the extended-community-list entry.

Command Syntax `ip extcommunity-list standard WORD (deny|permit) (rt|soo) (aa:nn) no ip extcommunity-list standard WORD (deny|permit) (rt|soo) (aa:nn)`

Parameters

`WORD`	Extended community list name
`deny`	Reject the community
`permit`	Accept the community
`rt`	Route target extended community in aa:nn or IPaddr:nn format
`soo`	Site-of-origin extended community in aa:nn or IPaddr:nn format

Default

By default, ip extcommunity list is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip extcommunity-list standard 36 permit rt 5675:50
(config)#ip extcommunity-list standard CLIST permit soo 10.10.32.15:70
```

match ip peer

Use this command to apply policies based on the route source of which the BGP TCP/IP session formed using an IPv4 address in the update message.

Use the `no` parameter with this command to disable this function.

Command Syntax `match ip peer (<1-199>|<1300-2699>|WORD) no match ip peer (<1-199>|<1300-2699>|WORD)`

Parameters

`<1-199>`	IP access-list number
`<1300-2699>`	IP access-list number (expanded range)
`WORD`	Access-list name

Default

By default, import bgp route is disabled

Command Mode

Route-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#route-map in-A permit 10
(route-map)#match ip peer 1
```

max-paths

Use this command to set the number of equal-cost multi-path (ECMP) routes for eBGP or iBGP. You can install multiple BGP paths to the same destination to balance the load on the forwarding path.

Use the `no` parameter with this command to disable this feature.

Command Syntax `max-paths (ebgp|ibgp|) <2-64> no max-paths ebgp (<2-64>|) no max-paths ibgp (<2-64>|)`

Parameters

`ebgp`	eBGP ECMP session
`ibgp`	iBGP ECMP session
`<2-64>`	Number of routes

Default

Available for the default BGP instance and for IPv4 and IPv6 unicast addresses

Command Mode

Router mode and Address Family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example configures 7 routes for ECMP for iBGP.

```
#configure terminal
(config)#router bgp 11
(config-router)#max-paths ibgp 7
```

neighbor additional-paths

Use this command to enable neighbour BGP add-path.

Use the `no` parameter with this command to disable neighbour BGP add-path.

Command Syntax `neighbor A.B.C.D additional-paths (send|receive|send-receive|disable) no neighbor A.B.C.D additional-paths (send|receive|send-receive|disable)`

Parameters `send` Send additional paths to neighbors `receive` Receive additional paths from neighbors `send-receive` Send and Receive additional paths from neighbors `disable` Disable additional paths

Default

By default additional-path is disabled

Command Mode

Router BGP Address Family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 2
(config-router)#address-family ipv4 unicast
(config-router)#neighbor 1.1.1.2 additional-paths send

(config-router)#no neighbor 1.1.1.2 additional-paths send
```

neighbor advertise additional-paths

Use this command to enable BGP add-path at neighbor level.

Use the `no` parameter with this command to disable BGP add-path at neighbor level.

Command Syntax `neighbor A.B.C.D advertise additional-paths (all|best <2-3>) no neighbor A.B.C.D advertise additional-paths (all|best <2-3>)`

Parameters `all` Select all available paths `best` Select best N paths

`<2-3>` Number of best paths in additional paths to be selected

Default

By default, neighbor advertise additional path is disabled

Command Mode

Router BGP Address Family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 2
(config-router)#address-family ipv4 unicast
(config-router)#neighbor  1.1.1.2 advertise additional-paths all

(config-router)#no neighbor  1.1.1.2 advertise additional-paths all
```

neighbor activate

Use this command to enable the exchange of specific address family routes with a neighboring router. After a TCP connection is opened with a neighboring router, use this command to enable or disable the exchange of address family information. To enable the exchange of multicast and VPNv4 address prefix types, activate neighbors using this command in address family mode.

Use the `no` parameter with this command to disable exchange of information with a neighbor.

Command Syntax `neighbor (A.B.C.D|WORD)`

`activate no neighbor (A.B.C.D|WORD)`

`activate`

Parameters

`A.B.C.D` Address of the BGP neighbor in an IPv4 format

`WORD` Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

A neighbor under address-family IPv4 is activated by default. For all other address-families, use this command to enable a neighbor to exchange routing information of a specific address-family with a neighbor.

Command Mode

Address Family mode and Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 1.2.3.4 activate

(config)#router bgp 100
(config-router)#neighbor 10.10.20.1 remote-as 100
(config-router)#address-family vpnv4 unicast
(config-router-af)#neighbor 10.10.20.1 activate
```

neighbor advertisement-interval

Use this command to set a minimum interval between the sending of BGP routing updates. To reduce the flapping of routes, set a minimum advertisement interval so that the BGP routing updates are sent only per interval seconds. BGP dampening can also be used to control the effects of flapping routes. Use the `no` parameter with this command to set the interval time to default.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) advertisement-interval <0-65535> no neighbor (A.B.C.D|X:X::X:X|WORD) advertisement-interval no neighbor (A.B.C.D|X:X::X:X|WORD) advertisement-interval <0-65535>`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`<0-65535>`	Advertisement interval value in seconds

Default

By default, neighbor value for ebgp peer is 30 seconds and IBGP peer is 5 seconds

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.3 advertisement-interval 45
```

neighbor allowas-in

Use this command to advertise prefixes (routes) even when the source of the prefixes is from the same Autonomous System (AS) number.

Use this command in a scenario where two routers at different locations use the same Autonomous System number and are connected via an ISP. Once prefixes arrive from one branch at the ISP, they are tagged with the customer's AS number. By default, when the ISP passes the prefixes to the other router, the prefixes are dropped if the other router

uses the same AS number. Use this command to advertise the prefixes at the other side. Control the number of times an AS number is advertised by specifying a number.

In a hub and spoke configuration in a VPN, a PE (Provider Edge) router advertises all prefixes containing duplicate AS numbers. Use this command to configure two VRFs on each PE router to receive and advertise prefixes. One of the VRFs receives prefixes with AS numbers from all PE routers and then advertises them to neighboring PE routers. The other VRF receives prefixes with AS numbers from the CE (Customer Edge) router and advertises them to all PE routers in the hub and spoke configuration.

Use the `no` parameter with this command to reset to default.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) allowas-in neighbor (A.B.C.D|X:X::X:X|WORD) allowas-in <1-10> no neighbor (A.B.C.D|X:X::X:X|WORD) allowas-in`

Parameters

`A.B.C.D`	IPv4 neighbor address.
`X:X::X:X`	IPv6 neighbor address.
`WORD`	Name of peer group.

Note: For information on how to create peer groups, refer to the neighbor peer-group and neighbor remoteas commands. When this parameter is used with a command, the command applies on all peers in the specified group.

`<1-10>`	Number of times to allow the advertisement of an AS number

Default

By default, when the ISP passes the prefixes to the other router, the prefixes are dropped if the other router uses the same AS number, default number of local AS is 3

Command Mode

Router mode and Address Family mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.3 allowas-in 4

#configure terminal
```

```
(config)#router bgp 7657
(config-router)#address-family ipv4 vrf VRF_A
(config-router-af)#neighbor 10.10.0.1 allowas-in 3

#configure terminal
(config)#router bgp 7657
(config-router)#address-family ipv6 vrf VRF_A
(config-router-af)#neighbor 3ffe:15:15:15:15::0 allowas-in 3
```


© Symanitron Proprietary

neighbor as-origination-interval

Use this command to set the minimum interval between sending of AS-origination routing updates.

Use the `no` parameter with this command to disable this function.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) as-origination-interval <1-65535> no neighbor (A.B.C.D|X:X::X:X|WORD) as-origination-interval no neighbor (A.B.C.D|X:X::X:X|WORD) as-origination-interval <1-65535>` **Parameters**

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`<1-65535>`	AS origination interval in seconds

Default

By default, neighbor as origination interval is 15 seconds

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.75 as-origination-interval 555
```

neighbor attribute-unchanged

Use this command to advertise unchanged BGP attributes to the specified neighbor.

Use the `no` parameter with this command to disable this function.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) attribute-unchanged ({ as-path|next-hop|med }|) no neighbor (A.B.C.D|X:X::X:X|WORD) attribute-unchanged (({ as-path|next-hop|`

`med }|)`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format

WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
as-path	AS path attribute
next-hop	Nexthop attribute
med	Multi-exit discriminator attribute

Default

By default, the neighbor attribute-unchanged is disabled

Command Mode

Router mode and Address Family mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.75 attribute-unchanged as-path med
```

neighbor capability dynamic

Use this command to enable the dynamic capability for a specific peer. This command allows a BGP speaker to advertise or withdraw an address family capability to a peer in a non-disruptive manner.

Use the no parameter with this command to disable the dynamic capability.

Command Syntax neighbor (A.B.C.D|X:X::X:X|WORD) capability dynamic

no neighbor (A.B.C.D|X:X::X:X|WORD) capability dynamic

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, neighbor capability dynamic is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.10.1 capability dynamic
```

neighbor capability graceful-restart

Use this command to advertise the graceful restart capability to its neighbor. This configuration indicates that the BGP speaker has the ability to preserve its forwarding state for the address family when BGP restarts. You must first specify a neighbor's `remote-as` identification number assigned by the neighbor router.

Note: The graceful restart capability is advertised only when the graceful restart capability has been enabled using the bgp graceful-restart command.

Use the `no` parameter with this command to not advertise the graceful restart capability to its neighbor.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) capability graceful-restart no neighbor (A.B.C.D|X:X::X:X|WORD) capability graceful-restart`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, the graceful-restart is disabled

Command Mode

Router mode and Address Family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.10.50 capability graceful-restart
```

neighbor capability orf prefix-list

Use this command to enable Outbound Router Filtering (ORF) and advertise the ORF capability to its neighbors. The ORFs send and receive capabilities to lessen the number of updates exchanged between neighbors. By filtering updates, this option minimizes generating and processing of updates.

The two routers exchange updates to maintain the ORF for each router:

- The local router advertises the ORF capability in `send` mode.
- The remote router receives the ORF capability in `receive` mode, applying the filter as outbound policy.

Only an individual router or a peer group can be configured to be in `receive` or `send` mode. A peer-group member cannot be configured to be in `receive` or `send` mode.

Use the `no` parameter with this command to disable this function.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) capability orf prefix-list (both|receive|send) no neighbor (A.B.C.D|X:X::X:X|WORD) capability orf prefix-list (both|receive|send)`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`both`	The local router can send ORF entries to its peer, as well as receive ORF entries from its peer.
`receive`	The local router is willing to receive ORF entries from its peer
`send`	The local router is willing to send ORF entries to its peer

Default

By default, the orf prefix-list is disabled

Command Mode

Router mode and Address Family (IPv4 unicast, IPv4 multicast, IPv6) mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.5 capability orf prefix-list both (config-
router)#neighbor effe:2897::0003:3ed5 capability orf prefix-list receive
```

neighbor capability route-refresh

Use this command to advertise to peer about route refresh capability. If route refresh capability is supported, then router can dynamically request that the peer re-advertises its Adj-RIB-Out. Use the `no` parameter with this command to disable this function

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) capability route-refresh no neighbor (A.B.C.D|X:X::X:X|WORD) capability route-refresh`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, neighbor capability route refresh is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.10.1 capability route-refresh
```

neighbor collide-established

Use this command to include a neighbor already in an established state for conflict resolution when a TCP connection collision is detected. This command is not required for most network deployments, so users should only use this command when required.

Note: The associated functionality of including an “established” neighbor into TCP connection collision conflict resolution is automatically enabled when a neighbor is configured for BGP graceful-restart.

Use the `no` option with this command to turn this feature off.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) collide-established no neighbor (A.B.C.D|X:X::X:X|WORD) collide-established`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, neighbor collide is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 3.3.3.3 collide-established
```

neighbor connection-retry-time

Use this command to set the connection retry time for a specific BGP neighbor.

Use the `no` parameter with this command to clear the connection retry time for a specific BGP neighbor.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) connection-retry-time <1-65535> no neighbor (A.B.C.D|X:X::X:X|WORD) connection-retry-time no neighbor (A.B.C.D|X:X::X:X|WORD) connection-retry-time <1-65535>` **Parameters**

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`<1-65535>`	Connection retry time in seconds

Default

By default, connection retry time is 120 seconds

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 connection-retry-time 125
```

neighbor default-originate

Use this command to allow a BGP local router to send the default route 0.0.0.0 to a neighbor to use as a default route. This command can be used with standard or extended access lists.

Use the `no` parameter with this command to send no route as a default.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) default-originate neighbor (A.B.C.D|X:X::X:X|WORD) default-originate route-map WORD no neighbor (A.B.C.D|X:X::X:X|WORD) default-originate`

`no neighbor (A.B.C.D|X:X::X:X|WORD) default-originate route-map WORD` **Parameters**

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`WORD`	Route map name

Default

By default, neighbor default originate is disabled

Command Mode

Router mode and Address Family

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.10.1 default-originate route-map myroute
```

neighbor description

Use this command to associate a description with a neighbor. This command helps to identify a neighbor quickly. This command is useful for an ISP that has multiple neighbor relationships.

Use the no parameter with this command to remove the description.

Command Syntax neighbor (A.B.C.D|X:X::X:X|WORD) description

LINE no neighbor (A.B.C.D|X:X::X:X|WORD) description no

neighbor (A.B.C.D|X:X::X:X|WORD) description LINE

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
LINE	Neighbor description (up to 80 characters)

Default

By default, the neighbor description is disabled

Command Mode

Router mode and Address Family

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 1.2.3.4 description Backup router for sales

(config)#router bgp 100 (config-
router)#address-family ipv4 vrf VRF_A
(config-router-af)#neighbor 10.10.0.1 description Bank of America

(config)#router bgp 100 (config-
router)#address-family ipv6 vrf VRF_A
(config-router-af)#neighbor 3ffe:15:15:15:15::0 description Bank of America
```

neighbor disallow-infinite-holdtime

Use this command to disallow configuration of infinite hold-time. This command enables the local BGP speaker to reject a hold-time of “0” seconds from a peer (during exchange of open messages) or a user (during configuration). The no form of this command allows the BGP speaker to accept a hold-time of “0” from a peer or during configuration.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) disallow-infinite-holdtime no neighbor (A.B.C.D|X:X::X:X|WORD) disallow-infinite-holdtime`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, neighbor disallow infinite holdtime is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config-router)#neighbor 10.11.4.26 disallow-infinite-holdtime
(config-router)#neighbor 3ffe::45 disallow-infinite-holdtime
```

neighbor distribute-list

Use this command to filter route updates from a particular BGP neighbor. Use only one distribute list per BGP neighbor.

Use the `no` parameter with this command to remove an entry.

Command Syntax

`neighbor (A.B.C.D|X:X::X:X|WORD) distribute-list (<1-199>|<1300-2699>|WORD) (in|out) no neighbor (A.B.C.D|X:X::X:X|WORD) distribute-list (<1-199>|<1300-2699>|WORD) (in|out)`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`<1-199>`	IP access-list number

<1300-2699>	IP access-list number (expanded-range)
WORD	Access-list name
in	Filter incoming advertised routes
out	Filter outgoing advertised routes

Default

By default, neighbor distribute list is disabled

Command Mode

Router mode and Address Family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 1.2.3.4 distribute-list mylist out
```

neighbor dont-capability-negotiate

Use this command to disable capability negotiation. This command is used to allow compatibility with older BGP versions that have no capability parameters used in open messages between peers.

Use the no parameter with this command to enable capability negotiation.

Command Syntax neighbor (A.B.C.D|X:X::X:X|WORD) dont-capability-negotiate no neighbor (A.B.C.D|X:X::X:X|WORD) dont-capability-negotiate

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, capability negotiation is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.34 dont-capability-negotiate
```

neighbor ebgp-multihop

Use this command to accept and try BGP connections to external peers on indirectly connected networks. Multihop is not established if the only route to the multihop peer is a default route. This avoids loop formation.

Use the `no` parameter with this command to return to the default.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) ebgp-multihop`

`neighbor (A.B.C.D|X:X::X:X|WORD) ebgp-multihop <1-255> no`

`neighbor (A.B.C.D|X:X::X:X|WORD) ebgp-multihop no neighbor (A.B.C.D|X:X::X:X|WORD) ebgp-multihop <1-255>`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`<1-255>`	Maximum hop count

Default

By default, maximum hop count is 255

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.10.34 remote-as 20
(config-router)#neighbor 10.10.10.34 ebgp-multihop 5
```

neighbor enforce-multihop

Use this command to enforce BGP neighbors to perform multihop.

Use the `no` parameter with this command to turn off this feature.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) enforce-multihop` `no neighbor (A.B.C.D|X:X::X:X|WORD) enforce-multihop`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, the maximum hop count is 255

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.34 remote-as 20
(config-router)#neighbor 10.10.0.34 enforce-multihop
```

neighbor filter-list

Use this command to set up a BGP filter. This command specifies an access list filter on updates based on the BGP autonomous system paths. Each filter is an access list based on regular expressions.

Use the `no` parameter with this command to disable this function.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) filter-list WORD (in|out)` `no neighbor (A.B.C.D|X:X::X:X|WORD) filter-list WORD (in|out)`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`WORD`	Name of an autonomous system path access list

in	Filter incoming advertised routes
out	Filter outgoing advertised route

Default

By default, filter list is disabled

Command Mode

Router mode and Address Family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.34 remote-as 20
(config-router)#neighbor 10.10.0.34 filter-list out in
```

neighbor g-shut

Use this command to start a graceful shutdown for the BGP session of the specified BGP neighbor. The BGP session for this neighbor is shut down after the graceful shutdown timer expires.

If there is no alternate path available for traffic to flow prior the actual shutdown of the BGP session, this path is made available for 60 seconds or for configured time after which the path is no longer available and traffic is dropped.

Use the `no` parameter with this command to bring up the session again for the specified BGP neighbor whose BGP session had been shut down using the `neighbor g-shut` command. Note: The graceful shutdown capability is not supported on iBGP sessions.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) g-shut no neighbor (A.B.C.D|X:X::X:X|WORD) g-shut`

Parameters

A.B.C.D	Neighbor IPv4 address
X:X::X:X|	Neighbor IPv6 address
WORD	Neighbor tag

Default

By default, neighbor g-shut is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#neighbor 1.1.1.2 g-shut

#configure terminal
(config)#router bgp 100
(config-router)#no neighbor 1.1.1.2 g-shut
```

neighbor g-shut-timer

Use this command to configure the value of the graceful shutdown timer. After the timer expires, the BGP session initiated for graceful shutdown is shut down.

Use the `no` parameter with this command to revert to the default setting.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) g-shut-timer <10-65535> no neighbor (A.B.C.D|X:X::X:X|WORD) g-shut-timer <10-65535>`

Parameters

`A.B.C.D`	Neighbor IPv4 address
`X:X::X:X`	Neighbor IPv6 address
`WORD`	Neighbor tag
`<10-65535>`	Graceful shutdown timer in seconds

Default

By default, the timer value is set to 60 seconds

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#neighbor 1.1.1.2 g-shut-timer 120
```

neighbor limit

Use this command to specify the maximum number of peers that can be configured in the BGP dynamic peer-group.

Use the `no` parameter with this command to disable this function.

Command Syntax `neighbor WORD limit <1-200> no neighbor WORD (limit <1-200>|)`

Parameters

`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command.
`<1-200>`	The maximum number of peers that can be configured in a BGP dynamic peer-group.

Default

By default, neighbor word limit is disabled

Command Mode

Router mode and Address Family VRF mode

Applicability

This command was introduced in SWMRE version 1.3.4.

Example

```
#configure terminal
(config)#router bgp 11
(config-router)#neighbor group1 limit 120
```

neighbor local-as

Use this command to specify an AS (autonomous system) number to use with BGP neighbor.

Use the `no` parameter with this command to disable this command.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) local-as <1-4294967295> no neighbor (A.B.C.D|X:X::X:X|WORD) local-as <1-4294967295>`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`<1-4294967295>`	Neighbor's AS number when extended capabilities are configured

Note: The AS number 23456 is a reserved 2-byte AS number. An old BGP speaker (2-byte implementation) should be configured with 23456 as its remote AS number while peering with a non-mappable new BGP speaker (4-byte implementation).

Default

By default, local as is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router bgp 11
(config-router)#neighbor 10.10.0.34 local-as 12345
```

neighbor maximum-prefix

Use this command to set the number of prefixes that can be received from a neighbor.

Use the `no` parameter with this command to disable this function.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) maximum-prefix <1-4294967295> neighbor (A.B.C.D|X:X::X:X|WORD) maximum-prefix <1-4294967295> <1-100> neighbor (A.B.C.D|X:X::X:X|WORD) maximum-prefix <1-4294967295> <1-100> warning-only neighbor (A.B.C.D|X:X::X:X|WORD) maximum-prefix <1-4294967295> warning-only no neighbor (A.B.C.D|X:X::X:X|WORD) maximum-prefix no neighbor (A.B.C.D|X:X::X:X|WORD) maximum-prefix <1-4294967295>`

`no neighbor (A.B.C.D|X:X::X:X|WORD) maximum-prefix <1-4294967295> warning-only`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`<1-4294967295>`	Maximum number of prefixes accepted from this peer
`<1-100>`	Threshold value percent <1-100>
`warning-only`	Only give a warning message when the limit is exceeded. When this parameter is not

specified and extra prefixes are received, the router ends the peering. A terminated peer remains down until the `clear ip bgp A.B.C.D` command is given.

Default

By default, neighbor maximum prefix is disabled

Command Mode

Router mode and Address Family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.72 maximum-prefix 1244 warning-only
```

neighbor next-hop-self

Use this command to make the router the next hop for a BGP-speaking neighbor or peer group. This command allows a BGP router to change the nexthop information that is sent to the iBGP peer. The nexthop information is set to the IP address of the interface used to communicate with the neighbor.

Use the `no` parameter with this command to disable this feature.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) next-hop-self no neighbor (A.B.C.D|X:X::X:X|WORD) next-hop-self`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, next hop self is disabled

Command Mode

Router mode and Address Family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.72 remote-as 100
(config-router)#neighbor 10.10.0.72 next-hop-self
```

neighbor optional-as

Use this command to specify an AS (autonomous system) number to use with BGP dynamic peer-group.

Use the `no` parameter with this command to disable this function.

Command Syntax `neighbor WORD optional-as <1-4294967295> no neighbor WORD optional-as <1-4294967295>`

Parameters

`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`<1-4294967295>`	The range from which the optional AS number must be configured.

Default

By default, neighbor optional as is disabled

Command Mode

Router mode and Address Family VRF mode

Applicability

This command was introduced in SWMRE version 1.3.4.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor group1 optional-as 400
```

neighbor override-capability

Use this command to ignore received capabilities and use locally configured values.

Use the `no` parameter with this command to disable this function.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) override-capability no neighbor (A.B.C.D|X:X::X:X|WORD) override-capability`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, override-capability is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 override-capability
```

neighbor passive

Use this command to make a BGP neighbor passive.

Use the `no` parameter with this command to disable this function.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) passive no neighbor (A.B.C.D|X:X::X:X|WORD) passive`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, neighbor passive is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 passive
```

neighbor password

Use this command to enable message digest5 (MD5) authentication on a TCP connection between two BGP peers. Configuring MD5 authentication between two BGP peers, means that each segment sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both BGP peers; otherwise, the connection between them will not be established.

Use the `no` parameter with this command to delete the MD5 authentication

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) password`

```
<WORD> no neighbor (A.B.C.D|X:X::X:X|WORD) password
<WORD>
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of the BGP peer group
`WORD`	Password (Maximum length is 80 characters)

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
```

```
(config)#router bgp 11
(config-router)#neighbor 10.10.0.73 password myPass

(config-router)#no neighbor 10.10.0.73 password myPass
```

neighbor peer-group

Use this command to add a neighbor to an existing peer group. Neighbors with the same update policies are grouped into peer groups. This facilitates the updates of various policies, such as distribute and filter lists. The peer group is then configured easily with any of the neighbor commands. Any changes made to the peer group affect all members.

To create a peer group, use the `neighbor WORD peer-group` command, and then use this command to add neighbors to the group.

Use the no parameter with this command to remove a neighbor from a named peer group.

Command Syntax `neighbor (A.B.C.D|X:X::X:X) peer-group WORD`

`no neighbor (A.B.C.D|X:X::X:X) peer-group WORD`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Peer group name

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor group1 peer-group
```

neighbor peer-group range

Use this command to create a dynamic peer group.

Use the no parameter with this command to remove a peer group.

Command Syntax `neighbor WORD peer-group range (A.B.C.D/M|X:X::X:X/M) no neighbor WORD peer-group range (A.B.C.D/M|X:X::X:X/M)`

Parameters

`A.B.C.D/M`	IP Prefix
`X:X::X:X/M`	IPv6 Prefix
`WORD`	Peer group name

Default

No default value is specified

Command Mode

Router mode and Address Family VRF mode.

Applicability

This command was introduced in SWMRE version 1.3.4.

Example

```
#configure terminal
(config)#router bgp 10
                    (config-router)#neighbor group1 peer-group range 10.10.10.0/24
```

neighbor port

Use this command to set the BGP port number of a neighbor.

Use the `no` parameter with this command to remove a port number from a BGP neighbor.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) port <0-65535> no neighbor (A.B.C.D|X:X::X:X|WORD) port no neighbor (A.B.C.D|X:X::X:X|WORD) port <0-65535>`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`<0-65535>`	Port number

Default

By default, neighbor port is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 port 643
```

neighbor prefix-list

Use this command to specify a prefix list for filtering BGP advertisements.

Filtering by prefix list matches the prefixes of routes with those listed in the prefix list. If there is a match, the route is used. An empty prefix list permits all prefixes. If a given prefix does not match any entries of a prefix list, the route is denied access. When multiple entries of a prefix list match a prefix, the entry with the smallest sequence number is considered to be a real match.

The router begins the search at the top of the prefix list, with the sequence number 1. Once a match or deny occurs, the router does not need to go through the rest of the prefix list. For efficiency the most common matches or denies are listed at the top. The neighbor distribute-list command is an alternative to this command and only one of them can be used to filter the same neighbor in any direction.

Use the `no` parameter with this command to remove an entry.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) prefix-list WORD (in|out)`

```
no neighbor (A.B.C.D|X:X::X:X|WORD) prefix-list WORD (in|out)
```

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`WORD`	Name of an access list
`in`	Apply access list to incoming advertisements
`out`	Apply access list to outgoing advertisements

Default

By default, neighbor prefix list is disabled

Command Mode

Router mode and Address Family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip prefix-list list1 deny 30.0.0.0/24
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 prefix-list list1 in
```

neighbor remote-as

Use this command to establish a BGP peering relationship with a customer edge router.

The specified neighbor only exchanges unicast address prefixes, unless the neighbor is also activated using the neighbor activate command, which allows the exchange of other routing information.

Use the `no` parameter with this command to delete this peering.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) remote-as <1-4294967295>` `no neighbor (A.B.C.D|X:X::X:X|WORD) remote-as <1-4294967295>`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`<1-4294967295>`	Neighbor's autonomous system number (ASN) when extended capabilities are configured. If the specified ASN matches the ASN number specified in the router BGP global configuration, the neighbor is identified as internal. If the ASN does no match, the neighbor is identified as external to the local AS.

Default

By default, neighbor remote is disabled

Command Mode

Router mode and Address Family-vrf mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router bgp 11
(config-router)#neighbor 10.10.0.73 remote-as 345
(config-router)#neighbor 11.11.0.74 remote-as 23456
```

Note: The last command in the example above should be used when the local speaker is OBGP and the neighbor is NBGP with a 4-octet ASN.

```
(config)#router bgp 100
(config-router)#address-family ipv4 vrf VRF_A
(config-router-af)#neighbor 10.10.0.1 remote-as 65000
```

```
(config)#router bgp 100 (config-
router)#address-family ipv6 vrf VRF_A
(config-router-af)#neighbor 3ffe:15:15:15:15::0 remote-as 65000
```


© Symanitron Proprietary

neighbor remove-private-AS

Use this command to remove the private autonomous system number (ASN) from outbound updates. Private ASNs are not advertised to the Internet. This command is used with external BGP peers only. The router removes the ASNs only if the update includes private ASNs. If the update includes both private and public ASNs, the system treats it as an error.

Use the `no` parameter with this command to revert to default.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) remove-private-AS no neighbor (A.B.C.D|X:X::X:X|WORD) remove-private-AS`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, neighbor remove private AS is disabled

Command Mode

Router mode and Address Family mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.63 remove-private-AS
```

neighbor restart-time

Use this command to set a different restart-time than the global restart-time configured using the bgp graceful-restart command.

Use the `no` parameter with this command to restore the router to its default state.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) restart-time <1-3600> no neighbor (A.B.C.D|X:X::X:X|WORD) restart-time <1-3600>`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format

X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
<1-3600>	The maximum time that a graceful-restart neighbor waits to come back up after a restart. Make sure that this value does not exceed the stalepath-time specified in router mode.

Default

By default, restart time is 90 seconds

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 3.3.3.3 restart-time 45
```

neighbor route-map

Use this command to apply a route map to incoming or outgoing routes. This command filters updates and modifies attributes. A route map is applied to inbound or outbound updates. Only the routes that pass the route map are sent or accepted in updates.

Use the `no` parameter with this command to a route map.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) route-map WORD (in|out)
no neighbor (A.B.C.D|X:X::X:X|WORD) route-map WORD (in|out)
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
WORD	Name of the route map
in	Apply access list to incoming advertisements
out	Apply access list to outgoing advertisements

Default

No default value is specified

Command Mode

Router mode and Address Family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows the configuration of the route map named `rmap2` and then the use of this map name in the `neighbor route-map` command.

```
#configure terminal
(config)#route-map rmap2 permit 6
(config-route-map)#match origin incomplete
(config-route-map)#set metric 100
(config-route-map)#exit
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 route-map rmap2 in
```

neighbor route-reflector-client

Use this command to make the router a BGP route reflector and set a specified neighbor as its client.

Using route reflectors reduces the number of iBGP peers within an AS. An AS can have more than one route reflector. A route reflector treats other route reflectors as other iBGP speakers.

Use the `no` parameter with this command to indicate that the neighbor is not a client.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) route-reflector-client no neighbor (A.B.C.D|X:X::X:X|WORD) route-reflector-client`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

No default value is specified

Command Mode

Router mode and Address Family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

In the following configuration, Router1 is the route reflector for clients 3.3.3.3 and 2.2.2.2; it also has a non-client peer 6.6.6.6.

```
#configure terminal
(config)#router bgp 200
(config-router)#neighbor 3.3.3.3 remote-as 200
(config-router)#neighbor 3.3.3.3 route-reflector-client
(config-router)#neighbor 2.2.2.2 remote-as 200
(config-router)#neighbor 2.2.2.2 route-reflector-client
(config-router)#neighbor 6.6.6.6 remote-as 200
```

neighbor route-server-client

Use this command to make a neighbor a route server client.

Use the `no` parameter with this command to remove the configuration of a neighbor as route server client.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) route-server-client no neighbor (A.B.C.D|X:X::X:X|WORD) route-server-client`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.72 route-server-client
```

```
#configure terminal
(config)#router bgp 10
(config-router)#no neighbor 10.10.0.72 route-server-client
```

neighbor send-community

Use this command to send that a community attribute to a BGP neighbor.

The community attribute groups destinations in a certain community and applies routing decisions according to those communities. On receiving community attributes, the router reannounces them to the neighbor.

By default, both `standard` and `extended` community attributes are sent to a neighbor. To explicitly send only the `standard` or `extended` community attribute, run the bgp config-type command with the `standard` parameter before running this command.

Use the `no` parameter with this command to not announce community attributes to the neighbor. Use the `extended` and `no` parameters to remove extended communities. Specifying no other parameter with `no` removes standard communities only.

See also neighbor send-community in Chapter 3, *BGP Virtual Private Network Commands*.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) send-community neighbor (A.B.C.D|X:X::X:X|WORD) send-community (both|extended|standard) no neighbor (A.B.C.D|X:X::X:X|WORD) send-community no neighbor (A.B.C.D|X:X::X:X|WORD) send-community (both|extended|standard)`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`both`	Send Standard and Extended Community attributes
`extended`	Send Extended Community attributes
`standard`	Send Standard Community attributes

Default

Both `standard` and `extended` community attributes are sent to a neighbor.

Command Mode

Router mode and Address Family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#bgp config-type standard
(config)#router bgp 10
(config-router)#neighbor 10.10.0.72 send-community extended
```

neighbor send-label explicit-null

Use this command to exchange explicit –null label for the specific AF routes advertised between the neighbors. The AFI, SAFI combination of [1, 4] is the associated capability parameter (labelled-unicast) and is enabled by this command. This command is viable only on the ipv4 unicast and ipv4 vrf address families. This command has to be configured on both the neighbors for the capability to be negotiated.

Use the no parameter with this command to disable exchange of labels and remove the associated capability parameter.

Command Syntax `neighbor (WORD|x.x.x.x) send-label explicit-null no neighbor (WORD|x.x.x.x) send-label explicit-null`

Parameters

`x.x.x.x` Address of the BGP neighbor in IPv4 format `WORD`

Specify the neighbor router.

Default

By default, only the IPV4 unicast capability is enabled. Only configuration of this command on both neighbors will enable the Labelled Unicast capability.

Command mode

Address family and router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
# configure terminal
(config)# router bgp 100
(config-router)#neighbor 192.168.0.1 send-label explicit-null

# configure terminal
(config)#router bgp 100
(config-router)#address-family ipv4 vrf VRF-1
    (config-router-af)#neighbor 192.168.0.3 send-label explicit-null
```

neighbor shutdown

Use this command to terminate active sessions for a specified neighbor and clear all related routing information.

If a peer group is specified, a large number of peering sessions might be terminated. The `show ip bgp summary` command displays a summary of BGP neighbors and their connections.

Use the `no` parameter with this command to re-enable a neighbor.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) shutdown no neighbor (A.B.C.D|X:X::X:X|WORD) shutdown`

Parameters

`A.B.C.D` Address of the BGP neighbor in an IPv4 format

X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, neighbor shutdown is enabled

Command Mode

Router mode and Address Family-vrf mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.72 shutdown

(config)#router bgp 100
(config-router)#address-family ipv6 vrf VRF_A
(config-router-af)#neighbor 3ffe:15:15:15:15::0 shutdown
```

neighbor soft-reconfiguration inbound

Use this command to store updates for inbound soft reconfiguration.

Soft-reconfiguration can be used instead of BGP route refresh capability. Using this command enables local storage of all the received routes and their attributes. This requires additional memory. When a soft reset (inbound) is done on this neighbor, the locally stored routes are re-processed according to the inbound policy. The BGP neighbor connection is not affected.

Use the `no` parameter with this command to disable this function.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) soft-reconfiguration inbound no neighbor (A.B.C.D|X:X::X:X|WORD) soft-reconfiguration inbound`

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, the neighbor soft reconfiguration inbound is disabled

Command Mode

Router mode and Address Family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 soft-reconfiguration inbound
```

neighbor strict-capability-match

Use this command to close the BGP connection if a capability value does not match the remote peer.

Use the `no` parameter with this command to disable this function.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) strict-capability-match no neighbor (A.B.C.D|X:X::X:X|WORD) strict-capability-match`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, strict capability match is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 strict-capability-match
```

neighbor timers

Use this command to set the timers for a specific BGP neighbor.

Use the `no` parameter with this command to clear the timers for a BGP neighbor.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) timers <0-65535> <0-65535> neighbor (A.B.C.D|X:X::X:X|WORD) timers connect <1-65535> no neighbor (A.B.C.D|X:X::X:X|WORD) timers no neighbor (A.B.C.D|X:X::X:X|WORD) timers connect`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`<0-65535>`	Keepalive interval. Keepalive messages are sent by a router to inform another router that the BGP connection between the two is still active. The keepalive interval is the period of time between each keepalive message sent by the router.
`<0-65535>`	Holdtime interval which is the time the router waits to receive a keepalive message. If the router does not receive a message in this period, the router declares the neighbor dead. The holdtime value should be at least 3 times the keepalive time.
`connect`	BGP connect timer
`<1-65535>`	Connect timer

Defaults

By default, keepalive timer value is 30 seconds

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 timers 60 230
(config-router)#neighbor 10.10.10.10 timers connect 10

(config-router)#no neighbor 10.10.10.10 timers
```

neighbor transparent-as

Use this command to not to append the AS path number even when the peer is an eBGP peer.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) transparent-as`

Parameters

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, transparent as is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.7.1 transparent-as
```

neighbor transparent-nexthop

Use this command to keep the nexthop value of the route even when the peer is an eBGP peer.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) transparent-nexthop`

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 transparent-nexthop
```

neighbor unsuppress-map

Use this command to selectively leak more-specific routes to a particular neighbor.

When the aggregate-address command is used with the `summary-only` option, the more-specific routes of the aggregate are suppressed to all neighbors. Use the `neighbor unsuppress-map` command to selectively leak morespecific routes to a particular neighbor.

Use the `no` parameter with this command to restore the setting to the default level.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) unsuppress-map WORD no neighbor (A.B.C.D|X:X::X:X|WORD) unsuppress-map WORD`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`WORD`	Name of the route map used to select routes to unsuppress

Default

By default, neighbor unsuppress map is disabled

Command Mode

Router mode and Address Family mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.73 unsuppress-map mymap

#configure terminal
(config)#router bgp 10
(config-router)#address-family ipv4 unicast
(config-router-af)#neighbor 10.10.0.70 unsuppress-map mymap
```

neighbor update-source

Use this command to allow internal BGP sessions to use any operating interface for TCP connections.

A loopback interface is most commonly used with this command. The use of loopback interface eliminates a dependency and BGP does not have to rely on the availability of a particular interface for making TCP connections.

Use the `no` parameter with this command to restore the interface assignment to the closest interface.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) update-source WORD no neighbor (A.B.C.D|X:X::X:X|WORD) update-source`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`WORD`	Interface name

Default

By default, neighbor update source is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#neighbor 10.10.0.72 update-source myif
```

neighbor version

Use this command to accept only a particular BGP version.

By default, the system uses BGP version 4 and on request dynamically negotiates down to version 2. Using this command disables the router's version-negotiation capability and forces the router to use only a specified version with the neighbor.

Use the `no` parameter with this command to use the default version level of a neighbor.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) version 4 no neighbor (A.B.C.D|X:X::X:X|WORD) version`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format

X:X::X:X	Address of the BGP neighbor in an IPv6 format
WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
4	BGP version number

Default

By default, the system uses BGP version 4 and on request dynamically negotiates down to version 2

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 version 4

(config)#router bgp 12
(config-router)#no neighbor 10.10.10.10 version
```

neighbor weight

Use this command to specify a weight value, per address-family, for all routes learned from a neighbor.

The route with the highest weight gets preference when the same prefix is learned from more than one peer. Unlike the local-preference attribute, the weight attribute is relevant only to the local router. The weights assigned using the `set weight` command override the weights assigned using this command.

Use this command in router mode to specify a weight value for all address families. Use this command in address family mode to specify a weight value per IPv4/IPv6/VPNv4/6PE address family,

When the weight is set for a peer group, all members of the peer group get the same weight. This command can also be used to assign a different weight to an individual peer-group member. When an individually-configured weight of a peer-group member is removed, its weight is reset to its peer group's weight.

Use the `no` parameter with this command to remove a weight assignment.

Command Syntax

```
neighbor (A.B.C.D|X:X::X:X|WORD) weight <0-65535> no neighbor (A.B.C.D|X:X::X:X|WORD) weight no neighbor (A.B.C.D|X:X::X:X|WORD) weight <0-65535>
```

Parameters

A.B.C.D	Address of the BGP neighbor in an IPv4 format
X:X::X:X	Address of the BGP neighbor in an IPv6 format

WORD	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
<0-65535>	Weight value

Default

By default, neighbor weight value is 0

Command Mode

Router mode, Address-Family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#neighbor 10.10.10.10 weight 60

(config-router)#no neighbor 10.10.10.10 weight 60
```

neighbor WORD peer-group

Use this command to create a peer group.

Use the no parameter with this command to remove a peer group.

Command Syntax neighbor WORD peer-group no neighbor WORD peer-group

Parameters

WORD	Name of BGP peer group

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

This example shows how to create a peer group named group1.

```
#configure terminal
(config)#router bgp 10
                                        (config-router)#neighbor group1 peer-group
```

network

Use this command to specify the networks to be advertised by the BGP routing process. A unicast network address without a mask is accepted if it falls into the natural boundary of its class. A class-boundary mask is derived if the address matches its natural class-boundary.

Use the `backdoor` parameter to specify a backdoor route to a BGP border router that will provide better information about the network. For data to be advertised by BGP, its routing table must include a route to the specified network. This command specifies the networks to be advertised. The network command works if the network being advertised is known to the router.

The `backdoor` parameter enables a route to be the preferred route even if it has a greater distance. A network that is specified as a backdoor network is dynamically assigned an administrative distance of 200 ensuring that IGP learned routes are preferred. If a backdoor network is not sourced by the local router, the network is learned from the external routers. If the route is learned from eBGP for a backdoor network, the distance is set to 20 or 200.

Use the `no` form of this command to remove a network route entry.

Command Syntax `network A.B.C.D (backdoor|) network A.B.C.D/M (backdoor|) network A.B.C.D mask A.B.C.D (backdoor|) network A.B.C.D mask A.B.C.D route-map WORD (backdoor|) network A.B.C.D route-map WORD (backdoor|) network A.B.C.D/M route-map WORD (backdoor|) no network A.B.C.D (backdoor|) no network A.B.C.D/M (backdoor|) no network A.B.C.D mask A.B.C.D (backdoor|) no network A.B.C.D mask A.B.C.D route-map WORD (backdoor|) no network A.B.C.D route-map WORD (backdoor|) no network A.B.C.D/M route-map WORD (backdoor|)`

Parameters

`A.B.C.D`	IP prefix <network>, for example, 35.0.0.0
`A.B.C.D/M`	IP prefix <network>/<length>, for example., 35.0.0.0/8
`backdoor`	BGP backdoor route
`routemap`	Route map used to modify the attributes
`WORD`	Name of the route map
`mask`	Network mask, for example, 255.255.0.0
`A.B.C.D`	Network mask, e.g., 255.255.0.0

Default

No default value is specified

Command Mode

Router mode and Address-family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example illustrates a Class-A address configured as a network route. The natural Class-A network prefix mask length of 8 is internally derived, that is, 2.0.0.0/8.

```
(config)#router bgp 1
(config-router)#network 2.0.0.0
```


© Symanitron Proprietary

network synchronization

Use this command to enable IGP synchronization for BGP static network routes.

Use this no parameter with this command to disable synchronization of BGP static routes.

Command Syntax `network synchronization` `no network synchronization`

Parameters

None

Default

By default, network synchronization is disabled

Command Mode

Router mode and Address Family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example enables IGP synchronization of BGP static network routes in the router configuration mode.

```
#configure terminal
(config)#router bgp 11
(config-router)#network synchronization
```

The following example enables IGP synchronization of BGP static network routes in the IPv6 unicast address-family mode.

```
#configure terminal
(config)#router bgp 11
(config)#address-family ipv6 unicast
(config-af)#network synchronization
```

redistribute

Use this command to inject routes from one routing process into another. Redistribution is used by routing protocols to advertise routes that are learned by some other means, such as by another routing protocol or by static routes. Since all internal routes are dumped into BGP, careful filtering is applied to make sure that only routes to be advertised reach the internet, not everything. This command allows redistribution by injecting prefixes from one routing protocol into another routing protocol.

Use the `no` parameter with this command to disable this function.

Command Syntax `redistribute [connected|isis|kernel|ospf|rip|static] redistribute [connected|isis|kernel|ospf|rip|static] route-map WORD no redistribute [connected|isis|kernel|ospf|rip|static] no redistribute`

```
[connected|isis|kernel|ospf|rip|static]    route-map    no    redistribute
[connected|isis|kernel|ospf|rip|static] route-map WORD
```

Parameters

`connected`	Redistribute connected routes
`isis`	Redistribute connected ISO IS-IS routes
`kernel`	Redistribute connected kernel routes
`ospf`	Redistribute OSPFv2 routes
`rip`	Redistribute RIP routes
`static`	Redistribute static routes
`route-map`	Route map reference
`WORD`	Route map entries

Default

By default, redistribute is disabled

Command Mode

Router mode and Address Family-vrf mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows the configuration of the route-map name `rmap1` and then the use of this map name in the `redistribute route-map` command.

```
#configure terminal
(config)#route-map rmap1 permit 1
(config-route-map)#match origin incomplete
(config-route-map)#set metric 100
(config-route-map)#exit
(config)#router bgp 12
```

```
(config-router)#redistribute ospf route-map rmap1

(config)#router bgp 100 (config-
router)#address-family ipv4 vrf VRF_A
(config-router-af)#redistribute static

(config)#router bgp 100 (config-
router)#address-family ipv6 vrf VRF_A
(config-router-af)#redistribute static
```

restart bgp graceful

Use this command to enable a BGP-speaker router for graceful restart. This command stops the whole BGP process and makes SWMRE retain the BGP routes and mark them as stale. Receiving BGP speakers, retain and mark as stale all BGP routes received from the restarting speaker for all address families received in the Graceful Restart Capability exchange.

Command Syntax `restart`

`bgp graceful`

Parameters

None

Default

By default, bgp graceful is disabled

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#restart bgp graceful
```

router bgp

Use this command to start a BGP process.

Use the `no` parameter with this command to disable an existing routing process.

Command Syntax `router bgp <1-4294967295> no`

`router bgp <1-4294967295>`

Parameters

`<1-4294967295>`

Associate the routing process with this autonomous system number

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 12
(config-router)#
```

snmp restart bgp

Use this command to restart SNMP in Border Gateway Protocol (BGP)

Command Syntax `snmp restart bgp`

Parameters

None

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#snmp restart bgp
```

synchronization

Use this command to enable IGP synchronization of Internal BGP (iBGP) learned routes with the Internal Gateway Protocol (IGP) system in the router configuration mode or in the address-family configuration mode.

Synchronization is used when a BGP router should not advertise routes learned from iBGP neighbors, unless those routes are also present in an IGP (for example, OSPF). Synchronization may be enabled when all the routers in an autonomous system do not speak BGP, and the autonomous system is a transit for other autonomous systems.

The `no synchronization` command is used when BGP router can advertise routes learned from its iBGP neighbors without waiting for the IGP reachability to be present.

Command Syntax

```
synchronization  no
synchronization
```

Parameters

None

Default

No default value is specified

Command Mode

Router mode and Address Family modes

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example enables IGP synchronization of iBGP routes in Router mode.

```
#configure terminal
(config)#router bgp 11
(config-router)#synchronization
```

The following example enables IGP synchronization of iBGP routes in the IPv6-Unicast address family.

```
#configure terminal
(config)#router bgp 11
(config-router)#address-family ipv6 unicast
```

```
(config-af)#synchronization
```

timers bgp

Use this command to globally set or reset the keepalive and holdtime values for all the neighbors.

Use the `no` parameter with this command to reset timers to default value.

Command Syntax `timers bgp <0-65535> <0-65535>`

`no timers bgp <0-65535> <0-65535>`

Parameters

`<0-65535>`	Frequency with which keepalive messages are sent to the neighbors
`<0-65535>`	Interval after which a neighbor is considered dead if keepalive messages are not received

Default

By default, keepalive timer value is 30 seconds

By default, holdtime value is 90 seconds

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 10
(config-router)#timers bgp 40 120
```

undebug bgp

Use this command to disable BGP debugging options.

Command Syntax `undebug bgp (all|bfd|dampening|events|filters|fsm|keepalives|mpls|nht|nsm|updates)` **Parameters**

`all`	Disable all debugging for BGP

`bfd`	Disable debugging for BGP Bidirectional Forwarding Detection (BFD)
`dampening`	Disable debugging for BGP dampening
`events`	Disable debugging for BGP events
`filters`	Disable debugging for BGP filters
`fsm`	Disable debugging for BGP Finite State Machine (FSM)
`keepalives`	Disable debugging for BGP keepalives
`mpls`	Disable debugging for BGP MPLS
`nht`	Disable debugging for BGP NHT messages
`nsm`	Disable debugging for NSM messages
`updates`	Disable debugging for BGP updates

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#undebug bgp events
```

© Symanitron Proprietary

CHAPTER 2 BGP4+ Commands

This chapter describes the BGP4+ configuration commands.

- address-family ipv6 (see address-family in Chapter 1, *BGP Commands*)
- aggregate-address X:X::X:X/M
- bgp g-shut (see bgp g-shut in n Chapter 1, *BGP Commands*)
- clear bgp * ipv6
- clear bgp ipv6 (A.B.C.D|X:X::X:X)
- clear bgp ipv6 <1-4294967295>
- clear bgp ipv6 external
- clear bgp ipv6 peer-group
- clear bgp ipv6 unicast dampening
- clear bgp ipv6 unicast flap-statistics
- clear ipv6 bgp * vrf
- clear ipv6 bgp X:X::X:X vrf
- clear ip bpg ipv6 unicast table-map
- neighbor activate (see neighbor activate in Chapter 1, *BGP Commands*)
- neighbor attribute-unchanged (see neighbor attribute-unchanged in Chapter 1, *BGP Commands*)
- neighbor capability dynamic (see neighbor capability dynamic in Chapter 1, *BGP Commands*)
- neighbor capability route-refresh (see neighbor capability route-refresh in Chapter 1, *BGP Commands*)
- neighbor default-originate (see neighbor default-originate in Chapter 1, *BGP Commands*)
- neighbor distribute-list (see neighbor distribute-list in Chapter 1, *BGP Commands*)
- neighbor filter-list (see neighbor filter-list in Chapter 1, *BGP Commands*)
- neighbor maximum-prefix (see neighbor maximum-prefix in Chapter 1, *BGP Commands*)
- neighbor next-hop-self (see neighbor next-hop-self in Chapter 1, *BGP Commands*)
- neighbor peer-group (see neighbor peer-group in Chapter 1, *BGP Commands*)
- neighbor prefix-list (see neighbor prefix-list in Chapter 1, *BGP Commands*)
- neighbor remove-private-AS (see neighbor remove-private-AS in Chapter 1, *BGP Commands*)
- neighbor route-map (see neighbor route-map in Chapter 1, *BGP Commands*)
- neighbor route-reflector-client (see neighbor route-reflector-client in Chapter 1, *BGP Commands*)
- neighbor send-community (see neighbor send-community in Chapter 1, *BGP Commands*)
- neighbor soft-reconfiguration inbound (see neighbor soft-reconfiguration inbound in Chapter 1, *BGP Commands*)
- neighbor unsuppress-map (see neighbor unsuppress-map in Chapter 1, *BGP Commands*)
- network X:X::X:X
- redistribute (see redistribute in Chapter 1, *BGP Commands*)

aggregate-address X:X::X:X/M

Use this command to configure BGP aggregate entries.

Aggregates are used to minimize the size of routing tables. Aggregation combines the characteristics of several different routes and advertises a single route. This command creates an aggregate entry in the BGP routing table if any more-specific BGP routes are available in the specified range. Using the `summary-only` parameter advertises the prefix only, suppressing more-specific routes to neighbors.

The `as-set` parameter creates an aggregate entry advertising the path for this route, consisting of all elements contained in all paths being summarized. Use the `as-set` parameter to reduce the size of path information by listing the AS number only once, even if it was included in multiple paths that were aggregated. The `as-set` parameter is useful when aggregation of information results in an incomplete path information.

Use the `no` parameter with this command to disable this function.

Command Syntax `aggregate-address X:X::X:X/M aggregate-address X:X::X:X/M as-set aggregate-address X:X::X:X/M as-set summary-only aggregate-address X:X::X:X/M summary-only aggregate-address X:X::X:X/M summary-only as-set no aggregate-address X:X::X:X/M no aggregate-address X:X::X:X/M as-set no aggregate-address X:X::X:X/M as-set summary-only no aggregate-address X:X::X:X/M summary-only no aggregate-address X:X::X:X/M summary-only as-set`

Parameters

`X:X::X:X/M` Aggregate IPv6 prefix `as-set`

Generate AS set path information

`summary-only` Filter more specific routes from updates

Command Mode

Address Family mode

Default

By default, aggregate address is disabled

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100 (config-
router)#neighbor 2.2.2.2 remote-as 100
(config-router)#neighbor 3.3.3.3 remote-as 200
(config-router)#address-family ipv6 (config-router-af)#aggregate-
address 3ffe::/32 as-set summary-only
```

clear bgp * ipv6

Use this command to reset the BGP IPv6 connection for all peers.

Command Syntax `clear bgp ipv6 * clear bgp ipv6 * in clear bgp ipv6 * in prefix-filter clear bgp ipv6 * out clear bgp ipv6 * soft clear bgp ipv6 * soft in clear bgp ipv6 * soft out clear ip bgp * ipv6 unicast in clear ip bgp * ipv6 unicast out clear ip bgp * ipv6 unicast soft clear ip bgp * ipv6 unicast soft in clear ip bgp * ipv6 unicast soft out`

Parameters

`in`	Clear incoming advertised routes.
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.
`unicast`	Unicast prefixes
`in`	Clear incoming advertised routes.
`out`	Soft reconfig outbound update
`soft`	Clear both incoming and outgoing routes
`in`	Soft reconfig inbound update
`out`	Clear outgoing advertised routes

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear ip bgp * ipv6 unicast soft out
```

clear bgp ipv6 (A.B.C.D|X:X::X:X)

Use this command to reset the BGP neighbor addresses (IPv4 or IPv6) for IPv6 peers.

Command Syntax `clear bgp ipv6 (A.B.C.D|X:X::X:X) clear bgp ipv6 (A.B.C.D|X:X::X:X) in clear bgp ipv6 (A.B.C.D|X:X::X:X) in prefix-filter clear bgp ipv6 (A.B.C.D|X:X::X:X) out clear bgp ipv6 (A.B.C.D|X:X::X:X) soft clear bgp ipv6 (A.B.C.D|X:X::X:X) soft in clear bgp ipv6 (A.B.C.D|X:X::X:X) soft out`

Parameters

`in`	Clear incoming advertised routes
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig
`out`	Clear outgoing advertised routes
`soft`	Clear both incoming and outgoing routes
`in`	Soft reconfig inbound update
`out`	Soft reconfig outbound update

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear bgp ipv6 10.5.2.7
```

clear bgp ipv6 <1-4294967295>

Use this command to reset the BGP connection with a specified AS (Autonomous System) number for IPv6 peers.

Command Syntax `clear bgp ipv6 <1-4294967295> clear bgp ipv6 <1-4294967295> in clear bgp ipv6 <1-4294967295> in prefix-filter clear bgp ipv6 <1-4294967295> out clear bgp ipv6 <1-4294967295> soft clear bgp ipv6 <1-4294967295> soft in clear bgp ipv6 <1-4294967295> soft out`

Parameters

`in`	Clear incoming advertised routes.
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig.
`out`	Clear outgoing advertised routes.
`soft`	Clear both incoming and outgoing routes.
`in`	Soft reconfig inbound update.
`out`	Soft reconfig outbound update.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear bgp ipv6 12345
```

clear bgp ipv6 external

Use this command to reset the BGP connection for all external IPv6 peers or for a specified external IPv6 peer.

Command Syntax `clear bgp ipv6 external clear bgp ipv6 external in prefix-filter clear bgp ipv6 external soft clear bgp ipv6 external soft in clear bgp ipv6 external soft out clear bgp ipv6 external WORD in clear bgp ipv6 external WORD out`

Parameters

`in`	Clear incoming advertised routes
`prefix-filter`	Push out prefix-list ORF and do inbound soft reconfig
`soft`	Clear both incoming and outgoing routes
`in`	Soft reconfig inbound update
`out`	Soft reconfig outbound update
`WORD`	Name of external IPv6 peer
`in`	Soft reconfig inbound update
`out`	Soft reconfig outbound update

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear bgp ipv6 external soft in
```

clear bgp ipv6 peer-group

Use this command to reset the BGP connection for all members of a peer group.

Command Syntax `clear bgp ipv6 peer-group WORD clear bgp ipv6 peer-group WORD in clear bgp ipv6 peer-group WORD in prefix-filter clear bgp ipv6 peer-group WORD out clear bgp ipv6 peer-group WORD soft clear bgp ipv6 peer-group WORD soft in clear bgp ipv6 peer-group WORD soft out`

Parameters `in` Clear incoming advertised routes `prefix-filter` Push out prefix-list ORF and do inbound soft reconfig

`out`	Clear outgoing advertised routes
`soft`	Clear both incoming and outgoing routes
`in`	Soft reconfig inbound update
`out`	Soft reconfig outbound update
`WORD`	BGP peer-group name

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear ip bgp peer-group P1
```

clear bgp ipv6 unicast dampening

Use this command to reset IPv6 BGP dampening information.

Command Syntax `clear bgp ipv6 unicast dampening clear bgp ipv6 unicast dampening X:X::X:X clear bgp ipv6 unicast dampening X:X::X:X/M clear ip bgp ipv6 unicast dampening clear ip bgp ipv6 unicast dampening X:X::X:X clear ip bgp ipv6 unicast dampening X:X::X:X/M`

Parameters

`unicast`	Unicast prefixes
`X:X::X:X`	IP prefix (network) for example, 2003::
`X:X::X:X/M`	IP prefix (network and length) for example, 2003::/16

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear ip bgp ipv6 unicast dampening 1:2::3:4/7
```

clear bgp ipv6 unicast flap-statistics

Use this command to reset IPv6 BGP route flap statistics.

Command Syntax `clear bgp ipv6 unicast flap-statistics clear bgp ipv6 unicast flap-statistics X:X::X:X clear bgp ipv6 unicast flap-statistics X:X::X:X/M clear ip bgp ipv6 unicast flap-statistics clear ip bgp ipv6 unicast flap-statistics X:X::X:X clear ip bgp ipv6 unicast flap-statistics X:X::X:X/M`

Parameters

X:X::X:X	IP prefix (network) for example, 35.0.0.0
X:X::X:X/M	IP prefix (network and length) for example, 35.0.0.0/8

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear ip bgp ipv6 unicast flap-statistics 1:2::3:4/7
```

clear ipv6 bgp * vrf

Use this command to reset an IPv6 BGP connection for all virtual routing forwarding addresses.

Command Syntax `clear ipv6 bgp * vrf WORD clear ipv6 bgp * vrf WORD in clear ipv6 bgp * vrf WORD out clear ipv6 bgp * vrf WORD soft clear ipv6 bgp * vrf WORD soft in clear ipv6 bgp * vrf WORD soft out`

Parameters

in	Clear incoming advertised routes
out	Clear outgoing advertised routes
soft	Clear both incoming and outgoing routes
in	Soft reconfig inbound update
out	Soft reconfig outbound update
WORD	BGP peer-group name

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear ipv6 bgp * vrf BGPpeer7
```

clear ipv6 bgp X:X::X:X vrf

Use this command to reset the specified VPNv6 Routing/Forwarding (VRF) instance for BGP connections. If the neighbor address is specified with this command, it clears the specified connection. If no address is specified, this command clears all the BGP routes.

Command Syntax `clear ipv6 bgp (X:X::X:X) vrf WORD clear ipv6 bgp X:X::X:X vrf WORD in clear ipv6 bgp X:X::X:X vrf WORD out clear`

```
ipv6 bgp X:X::X:X vrf WORD soft in clear
ipv6 bgp X:X::X:X vrf WORD soft out
```

Parameters

vrf	Specify a VPN routing/forwarding instance for IPv6
WORD	VPN routing/forwarding instance name
in	Clear incoming advertised routes
out	Clear outgoing advertised routes
soft	Clear both incoming and outgoing routes
in	Soft reconfig inbound update
out	Soft reconfig outbound update

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear ipv6 bgp vrf 10:10::0:12 vrf vrfname
```

clear ip bpg ipv6 unicast table-map

Use this command to apply the modified table map or route map rules to the BGP routes in the existing IP routing table.

Command Syntax `clear ip bpg ipv6 unicast table-map (vrf (VRFNAME|all|default))`

Parameters

vrf	Select a VPN Routing/Forwarding Instance.
VRFNAME	Specify a VPN Routing/Forwarding instance name.
all	Select all VRFs.
default	Select default VRFs.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear ip bgp ipv6 unicast table-map vrf all
```

network X:X::X:X

Use this command to specify the networks to be advertised by the BGP routing process. A unicast network address without a mask is accepted if it falls into the natural boundary of its class. A class-boundary mask is derived if the address matches its natural class-boundary.

Use the `backdoor` parameter to specify a backdoor route to a BGP border router that will provide better information about the network. For data to be advertised by BGP, its routing table must include a route to the specified network. This command specifies the networks to be advertised. The network command works if the network being advertised is known to the router.

The `backdoor` parameter enables a route to be the preferred route even if it has a greater distance. A network that is specified as a backdoor network is dynamically assigned an administrative distance of 200 ensuring that IGP learned routes are preferred. If a backdoor network is not sourced by the local router, the network is learned from the external routers. If the route is learned from eBGP for a backdoor network, the distance is set to 20 or 200.

Use the `no` parameter with this command to remove an entry.

Command Syntax `network X:X::X:X/M network X:X::X:X/M backdoor network X:X::X:X/M route-map WORD (backdoor|) no network X:X::X:X/M no network X:X::X:X/M backdoor`

`no network X:X::X:X/M route-map WORD (backdoor|)`

Parameters

`X:X::X:X` IPv6 prefix <network>, for example, 3ffe::

`backdoor` Specify a BGP backdoor route `WORD`

Name of the route map

Default

No default value is specified

Command Mode

Router mode and Address Family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#router bgp 10
(config-router)#network 172.26.0.0/16
```

If Router1 receives updates from 172.10.0.0 via two routing protocols RIP (distance 120) and eBGP (distance 20), router1 chooses the shorter route. Use the `backdoor` parameter to allow Router1 to learn about 172.10.0.0 via RIP.

```
(config)#router rip
(config)#network 172.10.0.0
(config)#router bgp 200
```

```
(config)#neighbor 3.3.3.3 remote-as 500
(config)#network 172.10.0.0 backdoor (config-
router)#network 172.16.1.0/24 route-map myRM
```

CHAPTER 3 BGP Virtual Private Network Commands

This chapter describes the BGP Virtual Private Network (VPN) configuration commands.

- address-family (see address-family in Chapter 1, *BGP Commands*)
- bgp inbound-route-filter
- clear bgp * l2vpn vpls
- clear ip bgp * vpnv4
- clear bgp <1-4294967295> l2vpn vpls
- clear ip bgp <1-4294967295> vpnv4
- clear bgp A.B.C.D l2vpn vpls
- clear ip bgp A.B.C.D vpnv4
- debug bgp mpls
- exit-address-family (see exit-address-family in Chapter 1, *BGP Commands*)
- import map
- ip vrf
- neighbor activate (see neighbor activate in Chapter 1, *BGP Commands*)
- neighbor allow-ebgp-vpn
- neighbor allowas-in (see neighbor allowas-in in Chapter 1, *BGP Commands*)
- neighbor as-origination-interval (see neighbor as-origination-interval in Chapter 1, *BGP Commands*)
- neighbor as-override
- neighbor description (see neighbor description in Chapter 1, *BGP Commands*)
- neighbor remote-as (see neighbor remote-as in Chapter 1, *BGP Commands*)
- neighbor send-community (see neighbor send-community in Chapter 1, *BGP Commands*)
- neighbor shutdown (see neighbor shutdown in Chapter 1, *BGP Commands*)

- neighbor soo
- redistribute (see redistribute in Chapter 1, *BGP Commands*)
- rd (route distinguisher)
- route-target

bgp inbound-route-filter

Use this command to enable the MPLS (Multiprotocol Label Switching) VPN/BGP inbound route filter. This command is used to control the installation of routing information into the BGP table.

When a router runs MPLS VPN/BGP PE, it exchanges routing information with a routing distinguisher. By default, SWMRE does not install routing information that does not match the configured routing distinguisher value. When the local box has two VRFs where each routing distinguisher value is 10:100 and 20:200, routing information with routing distinguisher 10:200 is not installed into BGP table.

When `no bgp inbound-route-filter` is configured, all of routing information is installed into the BGP table.

Command Syntax `bgp inbound-route-filter` `no bgp inbound-route-filter`

Parameter

None

Default

By default, the router performs the routing distinguisher value check is enabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 100
(config-router)#bgp inbound-route-filter
```

clear bgp * l2vpn vpls

Use this command to reset the session with all neighbors for VPLS address family

Command Syntax `clear bgp * l2vpn vpls`

Parameters

None

Command Mode

Exec and Privileged Exec Modes

Applicability

This command was introduced in version SWMRE version 1.3.

Example

```
#clear bgp * l2vpn vpls
```

clear ip bgp * vpnv4

Use this command to reset a VPNv4 BGP connection for all peers. This command clears the BGP connection and dynamically resets the outbound routing table. This frees up additional memory required for storing updates to generate new updates.

Command Syntax `clear ip bgp * vpnv4 unicast`

`in clear ip bgp * vpnv4 unicast out clear`

`ip bgp * vpnv4 unicast soft clear ip bgp`

`* vpnv4 unicast soft in clear ip bgp *`

`vpnv4 unicast soft out`

Parameters

`in`	Clear incoming advertised routes
`out`	Clear outgoing advertised routes
`soft`	Clear both incoming and outgoing routes
`in`	Soft reconfig inbound update
`out`	Soft reconfig outbound update

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear ip bgp *
#clear ip bgp * vpnv4 unicast out
```

clear bgp <1-4294967295> l2vpn vpls

Use this command to reset the session for the neighbors with a specific ASN number for L2VPN VPLS.

Command Syntax

`Clear bgp <1-4294967295> l2vpn vpls`

Parameters

`<1-4294967295>`	Autonomous System number of the BGP neighbor.

Command Mode

Exec and Privileged Exec Modes

Applicability

This command was introduced in version SWMRE version 1.3.

Example

```
#clear bgp 100 l2vpn vpls
```

clear ip bgp <1-4294967295> vpnv4

Use this command to reset a BGP connection for all VPN peers in a specified Autonomous System.

Command Syntax `clear ip bgp <1-4294967295> vpnv4 unicast in clear ip bgp <1-4294967295> vpnv4 unicast out clear ip bgp <1-4294967295> vpnv4 unicast soft clear ip bgp <1-4294967295> vpnv4 unicast soft in clear ip bgp <1-4294967295> vpnv4 unicast soft out`

Parameters

`<1-4294967295>` Clear peers with this AS number

`in` Clear incoming advertised routes `out` Clear outgoing advertised routes

`soft` Clear both incoming and outgoing routes `in` Soft reconfig inbound update `out` Soft reconfig outbound update

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear ip bgp 500 vpnv4 unicast soft out
```

clear bgp A.B.C.D l2vpn vpls

Use this command to reset the session for neighbor with address A.B.C.D.

Command Syntax `clear bgp A.B.C.D l2vpn vpls`

Parameters

`A.B.C.D` BGP neighbor address.

Command Mode

Exec and Privileged Exec Modes

Applicability

This command was introduced in version SWMRE version 1.3.

Example

```
#clear bgp 192.168.0.3 l2vpn vpls
```

clear ip bgp A.B.C.D vpnv4

Use this command to reset an VPNv4 BGP connection for a specific IPv4 address.

Command Syntax `clear ip bgp A.B.C.D vpnv4 unicast in clear ip bgp A.B.C.D vpnv4 unicast out clear ip bgp A.B.C.D vpnv4 unicast soft clear ip bgp A.B.C.D vpnv4 unicast soft in clear ip bgp A.B.C.D vpnv4 unicast soft out`

Parameters

`in`	Clear incoming advertised routes
`out`	Clear outgoing advertised routes
`soft`	Clear both incoming and outgoing routes
`in`	Soft reconfig inbound update
`out`	Soft reconfig outbound update

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear ip bgp 10.10.0.12 vpnv4 unicast soft
#clear ip bgp 10.10.0.10 vpnv4 unicast out
```

debug bgp mpls

Use this command to enable the display of MPLS related information.

Use the `no` parameter with this command to disable this function.

Note: This command is available only when `vrf` option is enabled.

Command Syntax `debug bgp mpls no debug bgp mpls`

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
debug bgp mpls
```

import map

This command assigns a route map to the VRF. This map is applied for routing information imported from another PE or VRF.

Use this command when an application requires finer control over the routes imported into a VRF than provided by the import and export extended communities. You can filter routes that are eligible for import into a VRF through the use of a route map.The route map can deny access to selected routes from a community that is on the import list.

Use the `no` option with this command to remove the map.

Command Syntax

```
import map WORD
no import map
```

Parameter

`WORD`	Route map

Default

No default value is specified

Command Mode

VRF mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#ip vrf myVRF
(config-vrf)#import map set-pref
(config-vrf)#
```

ip vrf

Use this command to assign a VPN Routing Forwarding (VRF) instance.

Use the `no` option with this command to remove the VRF from the instance.

Command Syntax `ip vrf WORD no ip vrf WORD`

Parameter

`WORD`	Name of the VRF instance

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Command Example

```
(config)#ip vrf myVRF
(config-vrf)#
```

neighbor allow-ebgp-vpn

Use this command to allow an eBGP neighbor to be a VPN peer. By default, BGP VPN functionality is allowed only for iBGP peers.

Use the `no` parameter with this command to remove the configuration.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) allow-ebgp-vpn`

`no neighbor (A.B.C.D|X:X::X:X|WORD) allow-ebgp-vpn`

Parameters

`A.B.C.D`	Address of the BGP neighbor in IPv4 format
`X:X::X:X`	Address of the BGP neighbor in IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, BGP VPN functionality is allowed only for iBGP peers

Command Mode

Address Family-vpnv4 mode and Address Family-vpnv6 mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#router bgp 200
(config-router)#neighbor 66.66.66.66 remote-as 100
(config-router)#neighbor 66.66.66.66 update-source lo
(config-router)#address-family vpnv4 unicast
(config-router-af)#neighbor 66.66.66.66 allow-ebgp-vpn
(config-router-af)#neighbor 66.66.66.66 activate
(config-router-af)#exit-address-family
```

neighbor as-override

Use this command to configure a provider edge (PE) router to override the autonomous system number (ASN) of a site with the ASN of a provider. BGP normally ignores routes from the same autonomous system. However, this command is used so that the Customer Edge (CE) routers router accepts and installs routes from the same autonomous system.

Typically, this command is used when CE routers have the same ASN in some or all sites. As per BGP requirement, a BGP speaker rejects a route that has the same ASN as itself in the `AS_PATH` attribute. Thus the CE routers having the same ASN do not accept routes from each other. Giving this command on the PE router removes the CE neighbor's ASN from the `AS_PATH` attribute allowing CE routers with the same ASN to accept routes from each other.

Use the `no` parameter with this command to remove VPN IPv4 prefixes from a specified router.

Command Syntax

`neighbor (A.B.C.D|X:X::X:X|WORD)`

`as-override no neighbor (A.B.C.D|X:X::X:X|WORD)`

`as-override`

Parameters

`A.B.C.D`	Address of the BGP neighbor in IPv4 format
`X:X::X:X`	Address of the BGP neighbor in IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.

Default

By default, neighbor as override is disabled

Command Mode

Address Family-vrf mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router bgp 7657
(config-router)#address-family ipv4 vrf VRF_A
(config-router-af)#neighbor 10.10.0.1 as-override

#configure terminal
(config)#router bgp 7657
(config-router)#address-family ipv6 vrf VRF_A
(config-router-af)#neighbor 3ffe:15:15:15:15::0 as-override
```

neighbor send-community

Use this command to send the extended-community attribute to a customer edge router. In VPN, the routedistinguisher and route-target are encoded in BGP extended-community.

See also neighbor send-community in Chapter 1, *BGP Commands*.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) send-community neighbor (A.B.C.D|X:X::X:X|WORD) send-community (both|extended|standard) no neighbor (A.B.C.D|X:X::X:X|WORD) send-community`

`no neighbor (A.B.C.D|X:X::X:X|WORD) send-community (both|extended|standard)`

Parameters

`A.B.C.D`	Address of the BGP neighbor in an IPv4 format
`X:X::X:X`	Address of the BGP neighbor in an IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`both`	Send standard and extended community attributes
`extended`	Send extended community attributes
`standard`	Send standard community attributes

Default

By default, no extended-community attribute is sent to a customer router is disabled

Command Mode

Router mode and Address Family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#router bgp 100
(config-router)#address-family ipv4 vrf VRF_A
(config-router-af)#neighbor 10.10.10.1 remote-as 200
(config-router-af)#neighbor 10.10.0.1 send-community extended
```

neighbor soo

Use this command to enable the site-of-origin (SOO) feature. If the customer AS is multi-homed to the ISP, this command ensures that the PE does not advertise the routes back to the same AS.

Use the `no` parameter with this command to disable this feature.

Command Syntax `neighbor (A.B.C.D|X:X::X:X|WORD) soo AS:nn_or_IP:nn no neighbor (A.B.C.D|X:X::X:X|WORD) soo`

Parameters

`A.B.C.D`	Address of the BGP neighbor in IPv4 format
`X:X::X:X`	Address of the BGP neighbor in IPv6 format
`WORD`	Name of a BGP peer group created with the neighbor WORD peer-group command. When you specify this parameter, the command applies to all peers in the group.
`ASN:nn_or_IP-address:nn`	An AS number and an arbitrary number (for example, 100:1), or a 32-bit IP address and an arbitrary number (for example, 192.16.10.1:1).

Default

By default, the site-of-origin (SOO) feature is disabled.

Command Mode

Address Family VRF mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#router bgp 100
(config-router)#address-family ipv4 vrf VRF_A
(config-router-af)#neighbor 1.1.1.1 remote-as 200
(config-router-af)#neighbor 10.10.0.1 soo 100:1
```

rd (route distinguisher)

Use this command to assign a route distinguisher (RD) for the VRF. The route distinguisher value must be a unique value on the router.

This command creates routing and forwarding tables and specifies the default RD for a VPN. The RD is added to the customer's IPv4 prefixes, changing them into globally unique VPN-IPv4 prefixes.

Command Syntax `rd`

`ASN:nn_or_IP-address:nn`

Parameters

`ASN:nn_or_IP-address:nn`

AS number and an arbitrary number (for example, 100:1). Otherwise, specify a 32-bit IP address and an arbitrary number (for example, 192.16.10.1:1).

Default

No default value is specified

Command Mode

VRF mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#ip vrf VRF_A
(config-vrf)#rd 100:1
```

route-target

Use this command to add a list of import and export route-target extended communities to the VRF.

This command creates lists of import and export route-target extended communities for the VRF. It specifies a target VPN extended community. Execute the command once for each community. All routes with the specific route-target extended community are imported into all VRFs with the same extended community as an import route-target.

Use the `no` parameter with this command to delete a route target.

Command Syntax `route-target (import|export|both) ASN:nn_or_IP-address:nn no route-target (import|export|both) ASN:nn_or_IP-address:nn`

Parameters

`import`	Import routing information
`export`	Export routing information
`both`	Import and export routing information
`ASN:nn_or_IP-address:nn`	AS number and an arbitrary number (for example, 100:1). Otherwise, specify a 32-bit IP address and an arbitrary number (for example, 192.16.10.1:1).

Default

No default value is specified

Command Mode

VRF mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#ip vrf VRF_A
(config-vrf)#route-target both 100:10
```

```
(config)#ip vrf VRF_A
(config-vrf)#route-target import 100:20
```

© Symanitron Proprietary

CHAPTER 4 BGP Show Commands

This chapter describes the BGP show commands.

- show bgp
- show bgp A.B.C.D
- show bgp A.B.C.D/M
- show bgp client
- show bgp community
- show bgp community-list
- show bgp dampening dampened-paths
- show bgp dampening flap-statistics
- show bgp dampening parameters
- show bgp filter-list
- show bgp inconsistent-as
- show bgp ipv6
- show bgp l2vpn vpls
- show bgp neighbors
- show bgp neighbors advertised-routes
- show bgp neighbors received prefix-filter
- show bgp neighbors received-routes
- show bgp neighbors routes
- show bgp nexthop-tracking
- show bgp nexthop-tree-details
- show bgp paths
- show bgp prefix-list
- show bgp quote-regexp
- show bgp regexp
- show bgp route-map
- show bgp statistics
- show bgp summary
- show bgp view
- show bgp X:X::X:X
- show bgp X:X::X:X/M longer prefixes
- show debugging bgp
- show ip bgp

- show ip bgp attribute-info
- show ip bgp cidr-only
- show ip bgp community-info
- show ip bgp peer-group
- show ip bgp peer-group vrf all
- show ip bgp rtfilter all
- show ip bgp scan
- show ip bgp vpnv4
- show ip extcommunity-list
- show ip extcommunity-list
- show ip protocols
- show ip vrf

show bgp

Use this command to display the status of BGP routes.

Command Syntax `show bgp show bgp (ipv6) show bgp (ipv4|ipv6) (unicast|multicast) show ip bgp show ip bgp ipv4 (unicast|multicast) show bgp (vrf (VRFNAME|all|default)) show ip bgp (vrf (VRFNAME|all|default))`

Parameters

`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show bgp
```

show bgp A.B.C.D

Use this command to display BGP route information for a network.

Command Syntax `show bgp (ipv4) (unicast|multicast) A.B.C.D show`

`ip bgp A.B.C.D`

`show ip bgp ipv4 (unicast|multicast) A.B.C.D`

Parameters

`ipv4`	IPv4 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`A.B.C.D`	IP prefix (network), for example, 35.0.0.0

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show ip bgp 80.80.80.0

BGP routing table entry for 80.80.80.0/24
Paths: (1 available, no best path)
 Not advertised to any peer
 300
  15.15.15.1 (inaccessible) from 11.11.11.2 (15.15.15.2)
   Origin incomplete, metric 0, localpref 100, valid, internal   rx path_id: 0
 tx path_id: -1
   Last update: Wed May 11 15:22:36 2016
```

Table 4-96 explains the output fields.

Table 4-96: show ip bgp output details

Field	Description
Paths	The paths listed in the routing table, along with path information, and whether the path are being advertised.
Metric	If shown, the value of the inter-autonomous system metric.
LocalPref	Local preference value as set with the set local-preference route-map configuration command.

rx path_id	Autonomous system receive path to the source network. There can be one entry in this field for each autonomous system in the path.

Table 4-96: show ip bgp output details

Field	Description
tx path_id	Autonomous system transmit path to the destination network. There can be one entry in this field for each autonomous system in the path.
Last update	Last time since the neighbor transitioned to or from the established state.

show bgp A.B.C.D/M

Use this command to display BGP route information for a network prefix.

Command Syntax `show bgp ipv4 (unicast|multicast) A.B.C.D/M show ip bgp A.B.C.D/M show ip bgp ipv4 (unicast|multicast) A.B.C.D/M show ip bgp A.B.C.D/M (vrf (VRFNAME|all|default)) show ip bgp A.B.C.D/M longer-prefixes show ip bgp ipv4 (unicast|multicast) A.B.C.D/M longer-prefixes show ip bgp A.B.C.D/M longer-prefixes (vrf (VRFNAME|all|default))`

Parameters

`ipv4`	IPv4 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`A.B.C.D/M`	IP prefix (network/length), for example, 35.0.0.0/8
`longer-prefixes`	Display route and more specific routes
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show bgp ipv4 unicast 35.0.0.1/8
```

show bgp client

Use this command to display BGP client information.

Command Syntax `show bgp client`

Parameters

None

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show bgp client
```

show bgp community

Use this command to display BGP routes that match a community.

Command Syntax `show bgp ip (unicast|multicast) community show bgp ip (unicast|multicast) community (vrf (VRFNAME|all|default)) show bgp ip (unicast|multicast) community [AA:NN|local-AS|no-advertise|no-export] (exact-match|) show ip bgp community show ip bgp community [AA:NN|local-AS|no-advertise|no-export|internet] (exact-match|)`

`show ip bgp community (vrf (VRFNAME|all|default)) show ip bgp community [AA:NN|local-AS|no-advertise|no-export|internet] (exact-match|)`

`show ip bgp community-list WORD (exact-match|) (vrf (VRFNAME|all|default))`

`show ip bgp ipv4 (unicast|multicast) community`

`show ip bgp ipv4 (unicast|multicast) community (vrf (VRFNAME|all|default))`

Parameters

`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF
`AA:NN`	Community number
`local-AS`	Do not send outside local AS (well-known community)
`no-advertise`	Do not advertise to any peer (well-known community)
`no-export`	Do not export to next AS (well-known community)
`internet`	Internet community (well-known community)
`exact-match`	Exact match of the communities

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
    #show bgp community local-as no-export
#show bgp community local-AS exact-match
#show ip bgp ipv4 multicast community 12:34 exact-match
```

show bgp community-list

Use this command to display BGP routes that match a community list.

Command Syntax `show bgp community-list WORD (exact-match|) show bgp ip (unicast|multicast) community-list WORD (exact-match|) show bgp ip (unicast|multicast) community-list WORD (exact-match|) show bgp (ipv4|ipv6) (unicast|multicast) community-list WORD (exact-match|) show bgp (ipv6) community-list WORD (exact-match|) show ip bgp community-list WORD (exact-match|) show ip bgp ipv4 (unicast|multicast) community-list WORD (exact-match|)`

Parameters

`WORD`	Community list name
`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`exact-match`	Only routes that exactly match the community

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip bgp community-list mylist exact-match
#show ip bgp ipv4 multicast community-list mylist exact-match
```

show bgp dampening dampened-paths

Use this command to display detailed information about paths suppressed due to dampening.

Command Syntax `show bgp dampening dampened-paths show bgp (ipv4|ipv6) (unicast|multicast) dampening dampened-paths show bgp (ipv6) dampening dampened-paths show ip bgp dampening dampened-paths show ip bgp dampening dampened-paths (vrf (VRFNAME|all|default)) show ip bgp ipv4 (unicast|multicast) dampening dampened-paths`

Parameters

`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs

default	Default VRF

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show bgp dampening dampened-paths
```

show bgp dampening flap-statistics

Use this command to display BGP dampening flap statistics.

Command Syntax `show bgp dampening flap-statistics show bgp (ipv4|ipv6) (unicast|multicast) dampening flap-statistics show bgp (ipv6) dampening flap-statistics show ip bgp dampening flap-statistics show ip bgp dampening flap-statistics (vrf (VRFNAME|all|default)) show ip bgp ipv4 (unicast|multicast) dampening flap-statistics`

Parameters

ipv4	IPv4 routes
ipv6	IPv6 routes
unicast	Unicast prefixes
multicast	Multicast prefixes
VRFNAME	VPN routing/forwarding instance name
all	All VRFs
default	Default VRF

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

This sample output shows that the internal route (`i`), has flapped 3 times and is now categorized as history (`h`).

```
#show ip bgp dampening flap-statistics
BGP table version is 1, local router ID is 30.30.30.77
Status codes: s suppressed, d damped, h history, * valid, > best, i
- internal, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network            From               Flaps   Duration   Reuse    Path
hi1.1.1.0/24     10.100.0.62        3  00:01:20       i
```

Header

```
BGP table version is 1, local router ID is 30.30.30.77
```

- BGP table version
- BGP router ID is `30.30.30.77`

`Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S stale` Table 4-96 shows the status codes displayed at the start of a route entry.

Table 4-97: status details

Status Code	Description	Comments
s	suppressed	Whether the route is suppressed and is not advertised to neighbors.
d	damped	When the penalty of a flapping route exceeds the suppress limit, the route is damped and remains in a withdrawn state until its penalty decreases below the reuse limit.
h	history	When the penalty of a flapping route does not exceed the suppress limit, the route is not damped and BGP maintains a history of the flapping route.
p	stale	When the BGP neighbor from which a route is learned is in graceful restart, the route is retained in the BGP routing table, but marked as stale .
*	valid	Whether the route is valid. When a route is not suppressed, damped, or present in the history, it is valid.
>	best	The selected route to be installed in the kernel routing table.
i	internal	The prefix was learned from an iBGP peer.

`Origin codes: i - IGP, e - EGP, ? - incomplete`

Table 4-98 shows the codes at the end of each route entry that indicate where the route originated.

Table 4-98: origin details

Origin Code	Description	Comments
i	IGP	The route is from an Interior Gateway Protocol.
e	EGP	The route is from an Exterior Gateway Protocol.
?	incomplete	Origin not known. Typically, these are routes redistributed from an IGP.

Table 4-99 explains the output fields.

Table 4-99: show bgp dampening flap-statistics output details

Field	Description
Network	Internet address of a network.
From	IP address of the advertising peer.
Flaps	Number of times this route has failed and returned (flapped).

Table 4-99: show bgp dampening flap-statistics output details

Field	Description
Duration	Elapsed time since the first penalty points were assessed.
Reuse	The amount of time remaining until this route will be un-suppressed and can be used again.

show bgp dampening parameters

Use this command to display the BGP dampening parameters.

Command Syntax `show bgp dampening parameters show bgp (ipv4|ipv6) (unicast|multicast) dampening parameters show bgp (ipv6) dampening parameters show ip bgp dampening parameters show ip bgp ipv4 (unicast|multicast) dampening parameters (vrf (VRFNAME|all|default)) show ip bgp dampening parameters (vrf (VRFNAME|all|default))`

Parameters

`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show ip bgp dampening parameters
```

show bgp filter-list

Use this command to display routes that match a regular expression filter list.

Command Syntax `show bgp filter-list WORD show bgp (ipv4|ipv6) (unicast|multicast) filter-list WORD show bgp (ipv6) filter-list WORD show ip bgp filter-list WORD show ip bgp ipv4 (unicast|multicast) filter-list WORD show ip bgp filter-list WORD (exact-match) show ip bgp filter-list WORD (exact-match) (vrf (VRFNAME|all|default)) show ip bgp filter-list WORD (vrf (VRFNAME|all|default)) show ip bgp ipv4 (unicast|multicast) filter-list WORD (exact-match)(vrf (VRFNAME|all|default))`

Parameters

`WORD`	Regular-expression filter list
`ipv4`	IPv4 routes
`ipv6`	IPv6 routes

`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`exact-match`	Exact match of the filter list
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF
`vrf`	VPN Routing/Forwarding instance name

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip bgp filter-list mylist
```

show bgp inconsistent-as

Use this command to display routes with inconsistent AS paths.

Command Syntax `show bgp inconsistent-as show bgp (ipv4|ipv6) (unicast|multicast) inconsistent-as show bgp (ipv6) inconsistent-as show ip bgp inconsistent-as show ip bgp ipv4 inconsistent-as`

`show ip bgp ipv4 (unicast|multicast) inconsistent-as`

Parameters

`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show bgp inconsistent-as
```

show bgp ipv6

Use this command to display the BGP routing table.

Command Syntax `show bgp ipv6 (unicast|multicast|labeled|)`

`show bgp ipv6 (unicast|multicast|labeled|) X:X::X:X/M`

Parameters

`multicast`	IPv6 multicast address prefixes
`unicast`	IPv6 unicast address prefixes
`labeled`	Labeled IPv6 routes
`X:X::X:X/M`	IPv6 prefix network/length, such as 3ffe:a::/64

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example: iBGP and eBGP Routes

This example shows routes learned from both iBGP and eBGP.

```
#show bgp ipv6
BGP table version is 0, local router ID is 10.100.0.77
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal S stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network                                    Metric LocPrf Weight  Path *>
2001:58::/32                                                 0   20 ?
fe80::202:b3ff:fec8:9fdb
*>  2002:58::/32                                                              0   20  i
fe80::202:b3ff:fec8:9fdb
*>i2003:58::/32                                  100     0  i    fe80::208:a1ff:fe16:797d
```

Header

```
BGP table version is 0, local router ID is 10.100.0.77
```

- BGP table version
- BGP router ID is `10.100.0.77`

```
Status codes: s suppressed, d damped, h history, p stale, * valid, > best, i - internal
```

Table 4-96 shows the status codes displayed at the start of a route entry.

Table 4-100: status details

Status Code	Description	Comments
s	suppressed	Whether the route is suppressed and is not advertised to neighbors.
d	damped	When the penalty of a flapping route exceeds the suppress limit, the route is damped and remains in a withdrawn state until its penalty decreases below the reuse limit.

h	history	When the penalty of a flapping route does not exceed the suppress limit, the route is not damped and BGP maintains a history of the flapping route.
p	stale	When the BGP neighbor from which a route is learned is in graceful restart, the route is retained in the BGP routing table, but marked as stale .
*	valid	Whether the route is valid. When a route is not suppressed, damped, or present in the history, it is valid.
>	best	The selected route to be installed in the kernel routing table.
i	internal	The prefix was learned from an iBGP peer.

```
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Table 4-101 shows the codes at the end of each route entry that indicate where the route originated.

Table 4-101: origin codes

Origin Code	Description	Comments
i	IGP	The route is from an Interior Gateway Protocol.
e	EGP	The route is from an Exterior Gateway Protocol.
?	incomplete	Origin not known. Typically, these are routes redistributed from an IGP.

Route Entry Examples

```
*> 2002:58::/32     fe80::202:b3ff:fec8:9fdb                              0 20 i
```

- This route entry shows that this route is learned from eBGP.
- The origin code “i” means that the prefix is added by the network statement at originating AS.
- The path 20 indicates that the prefix advertisement originated from AS20.
- The administrative weight parameter applies only to routes within an individual router.
- Since this route was learned from a peer, it has a default weight of 0. All routes generated by the local router have a weight of 32,768.

```
*> 2001:58::/32      fe80::202:b3ff:fec8:9fdb                             0 20 ?
```

- This route entry shows that the prefix is learnt from eBGP.The origin code i indicates that the prefix is added by network statement at originating AS.The path attribute 20 indicates that the route advertisement originated from AS20.The administrative weight parameter applies only to routes within an individual router. Since this route was learned from a peer, it has a default weight of 0. All routes generated by the local router have a weight of 32,768.The origin code “?” means the route was learned through redistribution.

```
*>i2003:58::/32      fe80::208:a1ff:fe16:797d                    100     0 i
```

- The status code “i” means that the route was learned through iBGP. The Local Preference attribute of the route, which is used only with the local AS, is set to 100 (the default value).

Example: IPv6 Prefix Routes

This example shows labeled routes for a given IPv6 prefix:

```
#show bgp ipv6 labeled 3ffe:a::/64
           BGP routing table entry for 3ffe:a::/64
           Paths: (1 available, best #1, table Default-IP-Routing-Table)
           Not advertised to any peer
           Local
           ::ffff:114:1414 from 20.20.20.1 (92.92.92.92)
           Origin   incomplete   metric    0,   localpref    100,   label            5420,
valid, internal, best
           Last update: Mon May 26 17:48:18 2008
```

Table 4-102 explains the output fields.

Table 4-102: show bgp ipv6 output details

Field	Description
Paths	The paths listed in the routing table, along with path information, and whether the path are being advertised.
Metric	If shown, the value of the inter-autonomous system metric.
LocalPref	Local preference value as set with the set local-preference route-map configuration command.
rx path_id	Autonomous system receive path to the source network. There can be one entry in this field for each autonomous system in the path.
tx path_id	Autonomous system transmit path to the destination network. There can be one entry in this field for each autonomous system in the path.
Last update	Last time since the neighbor transitioned to or from the established state.

show bgp l2vpn vpls

Command Syntax `show bgp l2vpn vpls (rr|) (detail|)`

Parameters `rr` Display the information of auto-discovered peers at Route reflector node. `detail` Display the detailed information of auto-discovered peers.

Command Mode

Exec and Privileged Exec Modes

Applicability

This command was introduced in version SWMRE version 1.3.

Example

```
#show bgp l2vpn vpls
VPLS-ID   VE-ID    Discovered-Peers   Route-Target
10        3        1                    10:100


#show bgp l2vpn vpls  detail

VPLS ID: 10
VE-ID: 3
Discovered Peers: 1
Route-Target: 10:100 Local RD:
10:100  Mesh Peers:
  Address:3.3.3.3, RD:10:100, VE-ID:4
  VC Details: VC-ID:34
  Remote (LB:52480,VBO:1,VBS:64)  Local (LB:52480,VBO:1,VBS:64)
  LB sent on known VEID:Yes
  In Label:52483, Out Label:52482
  PW Status:Established
```

Table 4-103 explains the output fields.

Table 4-103: show bgp l2vpn vpls output details

Field	Description
VPLS-ID	L2VPN address family database information for the Virtual Private LAN Service (VPLS).
VE-ID	L2VPN address family database information for the Virtual Expansion.
Discovered Peers	Peer discovery is used to find peers that are available for data using LLDP.
Route-Target	An identifier prepended to IP addresses to assure the uniqueness of the address.

Table 4-103: show bgp l2vpn vpls output details

Field	Description
Local RD	The Local Route Descriptor – the first two numbers of the Route-Target.
Mesh Peers	Internal BGP peers – devices that do not re-advertise routes to other IBGP devices.

Address	Mesh session information for the peer specified with the ip-address argument.
RD	Mesh peer's Route-Descriptor.
VC Details	The virtual circuit session information with the ip-address for the Provider Edge (PE) routers.
Remote	•LB (Label Base) – the first label value of a free set of labels that can be reserved by the PE router to be used for this VPLS domain. •VBO (VE Block Offset) – the offset value to be used when multiple label blocks must be created by a PE router. •VBS (VE Block Size) – the size of the label block.
Local	•LB (Label Base) – the first label value of a free set of labels that can be reserved by the PE router to be used for this VPLS domain. •VBO (VE Block Offset) – the offset value to be used when multiple label blocks must be created by a PE router. •VBS (VE Block Size) – the size of the label block.
LB sent on known VEID	Whether the Label Base came on a known Virtual Expansion Identifier – yes or no.
In Label	The ingress (incoming interface) label for this segment.
Out Label	Label received from downstream neighbor for route.
PW Status	The status of the VPLS Pseudo-Wire. Values can be: Idle, Active, Open, or Established.

```
#show bgp l2vpn vpls rr
RD          RR-Clients      Non-Clients           Route-Target
10:100        2                  0                   10:100
10:100        2                  0                   10:100


#show bgp l2vpn vpls rr detail

Route-Target: 10:100
  Peer:1.1.1.1
    RR Client   : Yes
    VE-ID:3  LB:52480  VBO:1  VBS:64

Route-Target: 10:100
  Peer:3.3.3.3
    RR Client   : Yes
    VE-ID:4  LB:52480  VBO:1  VBS:64
```

Table 4-104 explains the output fields.

Table 4-104: show bgp l2vpn vpls rr output details

Field	Description
Route-Target	An identifier prepended to IP addresses to assure the uniqueness of the address.
Peer	Internal BGP peers – devices that do not re-advertise routes to other IBGP devices.
RR Client	Device is a client of the Route Reflector – yes or no.
VE-ID	L2VPN address family database information for the Virtual Expansion.
LB	LB (Label Base) – the first label value of a free set of labels that can be reserved by the PE router to be used for this VPLS domain.
VBO	VBO (VE Block Offset) – the offset value to be used when multiple label blocks must be created by a PE router.
VBS	VBS (VE Block Size) – the size of the label block.

show bgp neighbors

Use this command to display information about BGP neighbor connections.

Command Syntax `show bgp neighbors` `show bgp ipv6 neighbors` `show ip bgp ipv4 (unicast|multicast) neighbors` `show ip bgp neighbors` `show ip bgp neighbors (A.B.C.D|X:X::X:X)(advertise-routes|)` `show ip bgp ipv4 (unicast|multicast) neighbors (A.B.C.D|X:X::X:X)` `show ip bgp neighbors (A.B.C.D|X:X::X:X) (hold-time|keepalive-interval|connection-retrytime)`

`show ip bgp neighbors (A.B.C.D|X:X::X:X) (sent-msgs|rcvd-msgs|notification|update|open|keepalive)`

Parameters

`ipv4` IPv4 neighbors `ipv6` IPv6 neighbors

`unicast` Unicast prefixes `multicast` Multicast prefixes

`A.B.C.D` IPv4 neighbor `X:X::X:X` IPv6 neighbor `advertised-routes` Routes advertised to a BGP neighbor

`hold-time` Hold time `keepalive-interval` Keepalive interval

`connection-retrytime` Connection retry time

`sent-msgs`	Sent packets
`rcvd-msgs`	Received packets
`notification`	Notification messages
`update`	Update messages
`open`	Open messages
`keepalive`	Keepalive messages

Command Mode

Privileged Exec and Exec modes

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show bgp neighbors
BGP neighbor is 2.2.2.2, remote AS 200, local AS 200, internal link
```

```
 Member of peer-group myPeer for session parameters
  BGP version 4, remote router ID 10.12.7.155
  BGP state = Established, up for 00:04:55
  Last read 00:04:55, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
  Received 11 messages, 0 notifications, 0 in queue
  Sent 11 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv4 IPv4
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2 myPeer peer-group member
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 1; dropped 0
Local host: 2.2.2.1, Local port: 33865
Foreign host: 2.2.2.2, Foreign port: 179
Nexthop: 2.2.2.1
Nexthop global: 1111::1
Nexthop local: fe80::a00:27ff:fecc:47a6
BGP connection: non shared network
Last Reset: 00:32:48, due to BGP Notification sent
Notification Error Message: (OPEN Message Error/Bad Peer AS.)
```

BGP Neighbor Fields

Table 4-105 explains the output fields.

Table 4-105: show bgp neighbor output details

Field	Description
BGP neighbor	BGP session information for the neighbor with the ip-address argument.
remote AS	Remote Autonomous system used to exchange exterior routing information between neighboring ASs.
local AS	Local Autonomous system used to exchange internal routing information within AS.

Field	Description
internal link external link	Internal link is used to forward route advertisements received from an external BGP router through the internal network (in the same AS). External link is used for exchanging routing information between Autonomous Systems (AS) and routing traffic across the Internet (eBGP neighbor).
member of peer-group	Peer group information for the peer group specified with the peer-group argument.
BGP version	Negotiated BGP version for this session.
remote router ID	IP address of the neighbor. BGP uses the highest loopback address as the Router ID. If no loopback interface is configured, BGP uses the highest configured IP address on a system.
BGP state	Session state as explained in Table 4-110. The exchange of routing information begins between peers only after the neighbor session is in an Established state.
up for	Time that the underlying TCP connection has been up.
last read	Time since BGP last received a message from this neighbor.
hold time	Time, in seconds, that BGP will maintain the session with this neighbor without receiving messages. The maximum time that can elapse between successive messages from this neighbor is 180 seconds. If no message is received for 180 seconds, this neighbor will be declared dead.
last write	Time since BGP last sent a message to this neighbor.
keepalive interval	Time interval, in seconds, at which keepalive messages are transmitted to this neighbor. The time interval between successive keepalive messages is 60 seconds. Typically, the hold time value is set to three times the keepalive interval.
neighbor capabilities	BGP capabilities advertised and received from this neighbor. “Advertised and received” is displayed when a capability is successfully exchanged between two routers.
received	Total number of received messages. notifications: Number of notification (error) messages received. in queue: Number of messages in the input queue
sent	Total number of sent messages. notifications: Number of notification (error) messages sent. in queue: Number of messages in the output queue
route refresh request	Number of route refresh request messages sent and received.
minimum time between advertisement runs.	The minimum time gap, in seconds, between successive route updates sent to the neighbor. Generally, a jitter (of 25%) is applied to this time interval, which means that if the time between advertisements is configured as 30, successive advertisements can have a time gap of as low as 22.5 (after applying a 25% jitter to the 30 seconds, which is 7.5 seconds).

for address family	The peers have exchanged address family capability.
BGP table version	For each of the address families agreed upon, BGP maintains a separate table.
neighbor version	Tracks prefixes that have been sent and those that need to be sent.
connections established	The number of times the router has established a TCP connection and the two peers have agreed to speak BGP with each other. “Dropped” means the number of time the connection has failed or gone down.
local host foreign host	Local host is the IP address and the port number of the local system used for the peering session. Foreign host is the IP address and the port of the neighbor. BGP always uses the TCP port number 179 for the peer originating the session.
nexthop	The IP address of the next hop used to reach the neighbor. eBGP or iBGP peers do not need to be directly connected. Peering sessions can be set up across multiple hops. If the neighbors are directly connected, the IP address of the local system is listed as the next hop.
nexthop global	The global IPv6 address of the next hop
nexthop local	The link-local IPv6 address of the next hop
non shared network	The peering session is running on a non shared network.
last reset	Time since this peering session was last reset. The reason for the reset is displayed on this line.
notification error message	Last error message sent.

show bgp neighbors advertised-routes

Use this command to display the routes advertised to a BGP neighbor.

Command Syntax `show bgp neighbors (A.B.C.D|X:X::X:X) advertised-routes`

`show ip bgp neighbors (A.B.C.D|X:X::X:X) advertised-routes (vrf (VRFNAME|all|default)) show ip bgp neighbors (A.B.C.D|X:X::X:X) advertised-routes`

`show ip bgp ipv4 (unicast|multicast) neighbors (A.B.C.D|X:X::X:X) advertised-routes`

Parameters

`A.B.C.D`	IPv4 neighbor
`X:X::X:X`	IPv6 neighbor
`ipv4`	IPv4 addresses
`multicast`	Multicast prefixes
`unicast`	Unicast prefixes
`vrf`	VPN Routing/Forwarding instance name

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip bgp ipv4 multicast neighbors 1.2.3.4 advertised-routes
```

show bgp neighbors received prefix-filter

Use this command to display the prefix list filter.

Command Syntax `show bgp neighbors (A.B.C.D|X:X::X:X) received prefix-filter show ip bgp neighbors (A.B.C.D|X:X::X:X) received prefix-filter show ip bgp ipv4 (unicast|multicast) neighbors (A.B.C.D|X:X::X:X) received prefix-filter`

Parameters

`A.B.C.D`	IPv4 address
`X:X::X:X`	IPv6 address
`ipv4`	IPv4 addresses
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show bgp neighbors 1.2.3.4 received prefix-filter
```

show bgp neighbors received-routes

Use this command to display the received routes from a neighbor.

To display all the received routes from a neighbor, perform a BGP soft reconfigure first.

Command Syntax `show bgp neighbors (A.B.C.D|X:X::X:X) received-routes show ip bgp ipv4 (unicast|multicast) neighbors (A.B.C.D|X:X::X:X) received-routes show ip bgp neighbors (A.B.C.D|X:X::X:X) received-routes`

Parameters

`A.B.C.D`	IPv4 address
`X:X::X:X`	IPv6 address
`ipv4`	IPv4 addresses
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show bgp neighbors 10.10.10.2 received-routes
```

show bgp neighbors routes

Use this command to display all accepted routes learned from neighbors.

Command Syntax `show bgp neighbors (A.B.C.D|X:X::X:X) routes show ip bgp neighbors (A.B.C.D|X:X::X:X) routes`

`show ip bgp ipv4 (unicast|multicast) neighbors (A.B.C.D|X:X::X:X) routes`

Parameters

`A.B.C.D`	IPv4 address
`X:X::X:X`	IPv6 address
`ipv4`	IPv4 addresses
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following output displays detailed information about the neighbor.

```
#show bgp neighbors 10.10.10.2 routes
BGP neighbor is fe80::203:47ff:feb0:d72b, remote AS 10, local AS 10, internal
link
  BGP version 4, remote router ID 10.10.10.50
  BGP state = Established, up for 00:02:01
  Last read 00:00:01, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv6 Unicast: advertised and received
  Received 3 messages, 0 notifications, 0 in queue
  Sent 5 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv4 Unicast
  Community attribute sent to this neighbor (both)
```

```
                                                                    0
accepted prefixes
  0 announced prefixes
```

Table 4-106 explains the output fields.

Table 4-106: show bgp neighbors routes output details

Field	Description
BGP neighbor	Neighbor identifier along with the local and remote Autonomous System numbers.
BGP version	The version of BGP being used by the neighbor device, along with the remote router ID number.
BGP state	The current state of the neighbor connection and length of time within the current state. Possible states are: Idle, Connect, Active, and Established.
Last read	The amount of time in Hours**:** Minutes**:** Seconds since this device last checked the Hold Time parameters.
hold time	The amount of time this device waits for a Keepalive or Update message before the BGP connection is closed.
Keepalive interval	KEEPALIVE messages are sent periodically to ensure that the connection is live.
Neighbor capabilities	New or optional parameters called “Capabilities.” Provides a graceful way to advertise new or unique options without causing peering to terminate. The capabilities are communicated in TLV fields. (see RFC 3392). In the example output above, the following capabilities were advertised by the neighbor and were received and understood by this device: •Route refresh •Address family IPv4 Unicast •Address family IPv6 Unicast
Route refresh	This helps to identify that and synchronize the peers without a hard reset.
For address family	Address Family Identifier (AFI) IPv4 Unicast.
Received messages	Information received from the neighbors.
notifications	Passes information to a router about sessions.

in que	Number of messages currently residing in the queue awaiting action.
Route refresh request	Information received and sent.
Minimum time between advertisement runs	Interval between exchange of messages.
For address family: IPv4 Unicast	The following three values are subordinate to the IPv4 Unicast Address Family.
Community attributes sent to this neighbor	Both the standard and the extended community information has been sent to the neighbor.
accepted prefixes	Configure a limit to the number of prefixes that can be accepted in a BGP peer session.
announced prefixes	A prefix announced in BGP consists of the IPV4 or IPV6 address block being announced.

show bgp nexthop-tracking

Use this command to display BGP nexthop-tracking status.

Command Syntax `show bgp nexthop-tracking`

Parameters

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show bgp nexthop-tracking

Configured NHT: ENABLED
NHT Delay time-interval : 6
BGP VRF: (Default) VRF_ID 0
BGP Instance: (Default), AS: 100, router-id 4.4.4.40
NHT is Enabled
Recvd Msg count from RIB: 0 NHT delay-timer remaining
 seconds: 0
BGP nexthop(s):
Total number of IPV4 nexthops : 0
Total number of IPV6 nexthops : 0
```

```
                                                                BGP VRF:
VRF_A VRF_ID 2
BGP Instance: (Default), AS: 100, router-id 4.4.4.40
NHT is Enabled
Recvd Msg count from RIB: 0 NHT delay-timer remaining
 seconds: 0
BGP nexthop(s):
Total number of IPV4 nexthops : 0
Total number of IPV6 nexthops : 0
```

Table 4-107 explains the output fields.

Table 4-107: show bgp nexthop-tracking output details

Field	Description
Configured NHT	Whether Next Hop Tracking (NHT) is enabled or disabled.
NHT Delay time-interval	A delay timer that indicates how long this device waits before checking its RIB for changes.

Table 4-107: show bgp nexthop-tracking output details

Field	Description
BGP VRF	Name and ID number of this BGP VRF.
BGP Instance	Autonomous System number and router ID.
NHT is Enabled	NHT Network enables the measurement and comparison of performance.
Recvd Msg count from RIB	Number of received change-messages from the RIB.
NHT delay-timer remaining seconds	Time remaining until the next decision cycle.
BGP nexthop(s)	Nexthop in the BGP to reach a certain destination.
Total number of IPV4 nexthops	Number of nexthops in the IPv4 Address Family.
Total number of IPV6 nexthops	Number of nexthops in the IPv6 Address Family.

show bgp nexthop-tree-details

Use this command to display BGP nexthop-tree details.

Command Syntax `show bgp nexthop-tree-details`

Parameters

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show bgp nexthop-tree-details
BGP Instance: (Default), AS: 65534, router-id 51.1.1.3
AFI_IP Nexthop count : 0
AFI_IP6 Nexthop count : 0

BGP Instance: (Default), AS: 0, router-id 51.1.1.3
AFI_IP Nexthop count : 0
AFI_IP6 Nexthop count : 0
```

Table 4-108 explains the output fields.

Table 4-108: show bgp nexthop-tree-details output details

Field	Description
Bgp Instance	The Autonomous System number and router ID.
AFI_IP Nexthop count	Nexthop count for the IPv4 Address Family
AFI_IP6 Nexthop count	Nexthop count for the IPv6 Address Family

show bgp paths

Use this command to display BGP path information.

Command Syntax `show bgp paths show bgp (ipv6) paths show ip bgp paths`

`show ip bgp ipv4 (unicast|multicast) paths`

Parameters

`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show bgp paths

Address         Refcnt    Path
[0x1af8ee0:0]    (21)
[0x1b3ceb0:345]  (14)      64602
[0x1c71d40:821]  (12008)   64602 65500
[0x1d03fb0:822]  (12008)   64602 65501
```

Table 4-109 explains the output fields.

Table 4-109: show bgp paths output details

Field	Description
Address	Hash and hash key separated by the colon character.
Refcnt	Number of routed using that path.
Path	Autonomous System Number (ASN) for the route.

show bgp prefix-list

Use this command to display routes matching the prefix-list.

Command Syntax `show bgp prefix-list WORD show bgp (ipv4|ipv6) (unicast|multicast|) prefix-list WORD (vrf (VRFNAME|all|default|)) show ip bgp prefix-list WORD show ip bgp prefix-list WORD (exact-match) show ip bgp prefix-list WORD (exact-match) (vrf (VRFNAME|all|default)) show ip bgp ipv4 (unicast|multicast) prefix-list WORD show ip bgp ipv4 (unicast|multicast) prefix-list WORD (exact-match)`

Parameters

`WORD`	Name of the IP prefix list
`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`exact-match`	Exact match of the prefix list
`vrf`	VPN Routing/Forwarding instance
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show bgp prefix-list mylist
```

show bgp quote-regexp

Use this command to display route matching an AS path quoted regular expression.

Command Syntax `show bgp quote-regexp WORD show bgp (ipv4|ipv6) (unicast|multicast|) quote-regexp WORD show ip bgp quote-regexp WORD show ip bgp ipv4 (unicast|multicast) quote-regexp WORD`

Parameters

`WORD`	A regular expression to match the AS paths. Use quotes to enclose the regular expression.
`ipv4`	IPv4 route information
`ipv6`	IPv6 route information
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show bgp quote-regexp "myPath"
```

show bgp regexp

Use this command to display routes matching the AS path regular expression.

Command Syntax `show bgp regexp LINE show bgp (ipv4|ipv6) (unicast|multicast) regexp LINE show bgp (ipv6) regexp LINE show ip bgp regexp LINE show ip bgp regexp LINE (vrf (VRFNAME|all|default)) show ip bgp ipv4 (unicast|multicast) regexp LINE`

Parameters

`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`LINE`	A regular expression to match the AS paths
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show bgp regexp myPath
```

show bgp route-map

Use this command to display routes that match the specified route map.

Command Syntax `show bgp route-map WORD show bgp (ipv4|ipv6) (unicast|multicast) route-map WORD show bgp (ipv6) route-map WORD show ip bgp route-map WORD show ip bgp route-map WORD (vrf (VRFNAME|all|default)) show ip bgp ipv4 (unicast|multicast) route-map WORD`

Parameters

WORD	Routes matching the route-map
ipv4	IPv4 routes
ipv6	IPv6 routes
unicast	Unicast prefixes
multicast	Multicast prefixes
vrf	VPN routing/forwarding instance
VRFNAME	VPN routing/forwarding instance name
all	All VRFs
default	Default VRF

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show bgp route-map myRM
```

show bgp statistics

Use this command to display BGP statistics.

Command Syntax `show bgp statistics`

Parameters

None

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show bgp statistics
```

show bgp summary

Use this command to display a summary of BGP neighbor status.

Command Syntax `show bgp summary show bgp (ipv4|ipv6) (unicast|multicast|) summary show ip bgp summary show ip bgp summary (vrf (VRFNAME|all|default)) show ip bgp ipv4 (unicast|multicast) summary`

Parameters

`ipv4`	IPv4 routes
`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show bgp summary

BGP router identifier 6.6.6.6, local AS number 64601

BGP table version is 1

1 BGP AS-PATH entries

0 BGP community entries

Neighbor V    AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down  State/PfxRcd

*12.1.1.24  64902    7          7       1      0      0   00:02:54       0

* Dynamically created based on a listen range

command BGP dynamic peer-group: group1
```

```
listen range:  12.1.0.0/16
Total number of dynamically created neighbors/limit: 1/(200)
Total number of dynamically created neighbors: 1
Total number of activated dynamic peer-groups for IPv4 Unicast address-family:
Total number of neighbors 1
Total number of Established sessions 1

BGP  dynamic  peer-group:  group2  listen
range:  12.2.0.0/16
Total number of dynamically created neighbors/limit: 0/(200)
Total number of dynamically created neighbors: 0
Total number of activated dynamic peer-groups for IPv4 Unicast address-family: 1
```

Header

```
BGP router identifier 10.10.15.50, local AS number
65000 1 BGP AS-PATH entries
0 BGP community entries
```

- The BGP router identifier is 10.10.15.50 and the local router AS number is 65000.
- The BGP table version tracks the local BGP table version. Any time the BGP best path algorithm executes, the table version increments.
- There is one BGP AS-PATH entry and no community entries.

Neighbor Entry Fields

Table 4-110 explains the fields for each neighbor entry.

Table 4-110: neighbor entry fields

Field	Description
Neighbor	IP address of peer.
V	BGP version of peer.
AS	Autonomous system number of peer.
MsgRcvd	Messages received since the BGP connection was established.
MsgSent	Messages sent since the BGP connection was established.
TblVer	Last version of the local router's BGP database advertised to the peer.
InQ	Received messages waiting in the input queue for further processing.

OutQ	Messages waiting in the output queue to be sent.

Table 4-110: neighbor entry fields (Continued)

Field	Description
Up/Down	Connection up time and down time.
State/PfxRcd	If the TCP session is up and the BGP peers have formed an adjacency, this field shows how many prefixes have been received from the remote neighbor. Other states: Idle: The local router has not allocated resources for the peer connection, so incoming connection requests are refused Idle (Admin): The peer has shut down Idle (PfxCt): Prefix overflow Idle (G-shut): Graceful shutdown Connect: BGP is waiting for the TCP connection to complete Active: the local router is trying to establish a TCP connection to the remote peer. You might see this if the local peer has been configured, but the remote peer is unreachable or has not been configured. OpenSent: BGP is waiting for an open message from its peer OpenConfirm: BGP received an open message from the peer and is now waiting for a keepalive or notification message. If BGP receives a keepalive message from the peer, the state changes to established. If the message is a notification, the state changes to idle. Established: BGP is ready to exchange update, notification, and keepalive messages with its peer Invalid: The session state is invalid

Neighbor Entry Example

```
10.10.14.51    4    100  93        120      0       0     0      00:42:16        0
```

- The neighbor has the IP address 10.10.14.51 and AS number 100.
- The neighbor uses BGP version 4.
- 93 messages have been received.
- 120 messages have been sent.
- The BGP routing table version is 0.
- There are no received messages waiting in the input queue for further processing.
- There are no messages waiting in the output queue to be sent.
- The connection has been up for 0 hours, 42 minutes and 53 seconds.

- The local router has received no prefixes from this neighbor.

show bgp view

Use this command to display information for a BGP view.

Command Syntax `show bgp ipv6 view WORD show ip bgp view WORD show ip bgp view WORD A.B.C.D show ip bgp view WORD A.B.C.D/M show ip bgp view WORD ipv4 (unicast|multicast) summary show ip bgp view WORD neighbors show ip bgp view WORD neighbors (A.B.C.D|X:X::X:X) show ip bgp view WORD summary`

Parameters

`ipv6`	IPv6 addresses
`WORD`	BGP view name
`A.B.C.D`	Network in the BGP routing table
`A.B.C.D/M`	IP prefix <network>/<length>, e.g., 35.0.0.0/8, in the BGP routing table
`ipv4`	IPv4 addresses
`multicast`	Multicast prefixes
`unicast`	Unicast prefixes
`summary`	Summary of BGP neighbor status
`neighbors`	Detailed information on TCP and BGP neighbor connections
`A.B.C.D`	IPv4 neighbor
`X:X::X:X`	IPv6 neighbor

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
    #show ip bgp view I2
    BGP table version is 0, local router ID is 10.10.10.50
    Status codes: s suppressed, d damped, h history, p stale, * valid, > best, i
    - internal
    Origin codes: i - IGP, e - EGP, ? - incomplete

       Network          Next Hop            Metric LocPrf Weight Path
    *>i100.156.70.0/24  10.10.10.52                  0      0 i
    *>i100.156.71.0/24  10.10.10.52                  0      0 i
    *>i100.156.72.0/24  10.10.10.52                  0      0 i
*>i100.156.73.0/24  10.10.10.52                  0      0 i
```

```
*>i100.156.74.0/24  10.10.10.52                       0      0 i

Total number of prefixes 5
```

show bgp X:X::X:X

Use this command to display BGP network information in an IPv6 environment.

Command Syntax `show bgp X:X::X:X show bgp (ipv6) X:X::X:X`

`show bgp (ipv6) (unicast|multicast) X:X::X:X`

Parameters

`ipv6`	IPv6 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`X:X::X:X`	IPv6 prefix (network), for example, 2003::

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show bgp ipv6 3ffe::8
```

show bgp X:X::X:X/M longer prefixes

Use this command to display BGP network information along with mask information.

Command Syntax `show bgp X:X::X:X/M longer-prefixes`

Parameters

`X:X::X:X/M`	IPv6 prefix (network/length), for example, 2003::/16

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show bgp 3ffe::8/8 longer-prefixes
```

show debugging bgp

Use this command to display BGP debugging options.

Command Syntax `show debugging bgp`

Parameters

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

This is a sample output from the show debugging bgp command.

```
#show debugging bgp BGP debugging status:
 BGP debugging is on
 BGP events debugging is on
 BGP updates debugging is on
 BGP fsm debugging is on
```

show ip bgp

Use this command to display BGP routes.

Command Syntax `show`

```
ip bgp
show ip bgp ipv4 (unicast|multicast)(vrf (VRFNAME|all|default))
```

Parameters

`ipv4`	IPv4 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes
`VRFNAME`	VPN routing/forwarding instance name
`all`	All VRFs
`default`	Default VRF

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

This example shows routes learned from both iBGP and eBGP peers.

```
#show ip bgp
BGP table version is 0, local router ID is 10.100.0.77
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S stale,
       Origin codes: i - IGP, e - EGP,? - incomplete
    Network              Next Hop      Metric LocPrf   Weight   Path
   *> 172.16.1.0/24       10.10.10.78                        0       1 4 i *>
   192.16.1.0          10.10.10.78       200              0       1  4 ?
   *                      10.100.0.62       100              0       3  4  ?
   *>i 192.17.1.0         10.100.0.62               100       0       i

Total number of prefixes 2
```

Header

```
BGP table version is 0, local router ID is 10.100.0.77
```

- The BGP table version tracks the local BGP table version. Any time the BGP best path algorithm executes, the table version increments.
- The Router ID of the local router is `10.100.0.77`.

```
Status codes: s suppressed, d damped, h history, p stale, * valid, > best, i - internal
```

Table 4-111 explains the status codes in the header.

Table 4-111: status codes

```
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Field	Description
Network	Network prefix installed in BGP. If multiple routes exist for the same prefix, only the first prefix is identified and others have blank spaces. The status codes are explained in Table 4-111.
Next Hop	IP address of the nexthop for this route.
Metric	Multiple-Exit Discriminator (MED). If there are multiple paths to the same destination from a single routing protocol, then the multiple paths have the same administrative distance and the best path is selected based on this metric. The path with the lowest metric is selected as the optimal path and installed in the routing table.

Table 4-112 explains the codes are at the end of each routing entry that show where the route originated.

Table 4-112: origin codes

Origin code	Description	Comments
i	IGP	The route originated from an Interior Gateway Protocol.
e	EGP	The route originated from an Exterior Gateway Protocol.
?	incomplete	Origin not known. Typically, these are routes redistributed from an Interior Gateway Protocol.
s	suppressed	Whether the route is suppressed and will not be advertised to the neighbors.
d	damped	When the penalty of a flapping route exceeds the suppress limit, the route is damped and remains in a withdrawn state until its penalty decreases below the reuse limit.
h	history	When the penalty of a flapping route does not exceed the suppress limit, the route is not damped and BGP maintains a history of the flapping route.
p	stale	When the BGP neighbor from which a route is learned is in graceful restart, the route is retained in the BGP routing table, but marked as stale.
*	valid	Whether the route is valid. When a route is not suppressed, damped, or present in the history, it is valid.
>	best	The route selected as the best path and installed in the kernel routing table.
i	internal	Whether the route is learned from an iBGP peer. If this symbol is not present, the route was learned from an eBGP peer.

Table 4-113: route entry fields

Field	Description
LocPrf	Local preference set with the `set local-preference` command. This value is used only with iBGP sessions within the local autonomous system to determine if a route towards a destination is the “best” one. The path with the highest local preference is preferred.
Weight	This field applies only to routes within an individual router. If a route was learned from a peer, it has a default weight of 0. All routes generated by the local router have a weight of 32,768.
Path and origin	The autonomous systems through which the prefix advertisement passed. The origin codes are explained in Table 4-112

Route Entry Examples

```
*> 172.16.1.0/24    10.10.10.78                          0    1 4 i
```

- The absence of status code “i” means the route is external and was learned from an eBGP peer.
- The “>” means this route is selected to be installed in the kernel routing table. Its network address is 172.16.1.0/24.
- The IP address of the nexthop for this route is 10.10.10.78.
- This route was learned from a peer, so it has a default weight of 0.
- The path “1 4” means the prefix advertisement passed through AS1 and AS4.
- The origin code “i” means the prefix was added by a network statement at an originating AS.

```
*>  192.16.1.0       10.10.10.78            200            0    1 4 ?
*                    10.100.0.62            100            0    3 4 ?
```

- The same prefix was learned from two different ASs, AS1 and AS3.
- The route learned from AS1 is chosen as the best route because AS1 has a lower Router ID (10.10.10.78) than AS2 (10.100.0.62). Although the metric of the route learned from AS1 is higher (200) than the route learned from AS3 (100), this attribute is not used in the best path selection decision because the metrics are compared only if the first (neighboring) AS is the same in the two paths.
- The origin code “?” indicates that the routes were learned through redistribution.

```
*>i192.17.1.0       10.100.0.62                    100     0    i
```

- The route is learned through an iBGP peer as indicated by the status code “i”.
- The preference of the route, used only with the local AS, is 100 (the default value).

show ip bgp attribute-info

Use this command to show internal attribute hash information.

Command Syntax `show ip bgp attribute-info`

Parameters

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

This is a sample output from the `show ip bgp attribute-info` command displaying internal attribute information.

```
#show ip bgp attribute-info
attr[1] nexthop 0.0.0.0 attr[1]
nexthop 10.10.10.10
```

show ip bgp cidr-only

Use this command to display routes with non-natural network masks.

Command Syntax `show ip bgp cidr-only`

`show ip bgp ipv4 (unicast|multicast) cidr-only`

Parameters

`ipv4`	IPv4 routes
`unicast`	Unicast prefixes
`multicast`	Multicast prefixes

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

This is a sample output from the `show ip bgp cidr-only` command.

```
#show ip bgp cidr-only
BGP table version is 0, local router ID is 10.10.10.50
Status codes: s suppressed, d damped, h history, p stale, * valid, > best, i
- internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 3.3.3.0/24       10.10.10.10                           0 11 i
Total number of prefixes 2
```

show ip bgp community-info

Use this command to list all BGP community information.

Command Syntax `show ip bgp community-info`

Parameters

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip bgp community-info
```

```
Address Refcnt Community
```

show ip bgp peer-group

Use this command to list the BGP peer group information.

Command Syntax `show ip bgp peer-group <name>`

Parameters

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.4.

Example

```
#show ip bgp peer-group group1
BGP dynamic peer-group is group1, EBGP, remote AS 64902
  BGP dynamic peer-group group1 listen range group
  members: 12.1.0.0/16 BGP version 4
Minimum time between advertisement runs is 30 seconds For address family:
IPv4 Unicast
  Peer-group member:
  *12.1.1.2
  Index 0, Offset 0, Mask 0x1
  0 accepted prefixes, 0 announced prefixes
```

show ip bgp peer-group vrf all

Use this command to list all BGP peer group VRF information.

Command Syntax `show ip bgp peer-group vrf all`

Parameters

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.4.

Example

```
#show ip bgp peer-group vrf all
% VRF: VRF1

BGP dynamic peer-group is group2, EBGP, remote AS 64902
```

```
  BGP dynamic peer-group group2 listen range group members:
  12.2.0.0/16   BGP version 4
Minimum time between advertisement runs is 30 seconds
% VRF: management
Peer-Group not found

% VRF: default


BGP dynamic peer-group is group1, EBGP, remote AS 64902
  BGP dynamic peer-group group1 listen range group
  members: 12.1.0.0/16 BGP version 4
Minimum time between advertisement runs is 30 seconds For address family:
IPv4 Unicast
  Peer-group member:
  *12.1.1.2
  Index 0, Offset 0, Mask 0x1
  0 accepted prefixes, 0 announced prefixes
```

show ip bgp rtfilter all

Use this command to display route target filters sent and received.

Command Syntax `show ip bgp rtfilter all`

Parameters

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip bgp rtfilter all
```

show ip bgp scan

Use this command to display BGP scan status.

Command Syntax `show ip bgp scan`

Parameters

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip bgp scan
BGP scan is running
BGP scan interval is 60
BGP instance: AS is 11,DEFAULT
Current BGP nexthop cache:
BGP connected route:
 10.10.10.0/24
 10.10.11.0/24
```

show ip bgp vpnv4

Use this command to display information relating to VPNv4.

Command Syntax `show ip bgp vpnv4 all show ip bgp vpnv4 all A.B.C.D show ip bgp vpnv4 all neighbors show ip bgp vpnv4 all neighbors A.B.C.D show ip bgp vpnv4 all summary show ip bgp vpnv4 all tags show ip bgp vpnv4 rd WORD show ip bgp vpnv4 rd WORD A.B.C.D show ip bgp vpnv4 rd WORD label show ip bgp vpnv4 rd WORD neighbors show ip bgp vpnv4 rd WORD neighbors A.B.C.D show ip bgp vpnv4 rd WORD summary show ip bgp vpnv4 view WORD all show ip bgp vpnv4 vrf NAME show ip bgp vpnv4 vrf NAME A.B.C.D show ip bgp vpnv4 vrf NAME label show ip bgp vpnv4 vrf NAME summary`

Parameters

`all`	Displays information about all VPNv4 NLRIs
`A.B.C.D`	Network
`neighbors`	TCP and BGP neighbor connections
`A.B.C.D`	Network
`summary`	Summary display
`tags`	BGP tags for prefixes
`rd`	Route distinguisher

WORD	BGP view name
A.B.C.D	Network
label	MPLS Labels for prefixes
neighbors	TCP and BGP neighbor connections
A.B.C.D	Network
summary	Summary display
view	VPNv4 NLRI-specific information
WORD	BGP view name

`vrf` VRF VPNv4 NLRIs

`NAME` VPN Routing/Forwarding instance name

`A.B.C.D` Network `label` MPLS Labels

for prefixes `summary` Summary display

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

This is a sample output from the `show ip bgp vpnv4 all` command displaying VPNv4 specific information

```
#show ip bgp vpnv4 all
   Network           Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (VRF1)
* i  10.10.9.0/24     10.10.0.1                0   141      0  65000 ?
*>   10.10.9.0/24     10.10.14.50              0            0  65000 ?
*>   10.10.10.0/24    10.10.14.50                           0  65000 ?
* i  10.10.15.0/24    10.10.0.1                    141      0  65000 ?
*>   10.10.15.0/24    10.10.14.50              0            0  65000 ?

#show ip bgp vpnv4 all neighbors

BGP neighbor is 24.10.10.2, remote AS 65000, local AS 65000, internal link
  BGP version 4, remote router ID 179.112.0.1
  BGP state = Established, up for 10:04:14
  Last read 10:04:14, hold time is 90, keepalive interval is 30 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (new)
    Address family IPv4 Unicast: advertised and received
    Address family IPv4 Multicast: received
    Address family IPv6 Unicast: received
  Received 1641 messages, 0 notifications, 0 in queue
  Sent 1280 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5
 seconds For address family: IPv4 Unicast
  BGP table version 676, neighbor version 676
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  60000 accepted prefixes
  0 announced prefixes

 Connections established 2; dropped 1
Local host: 24.10.10.1, Local port: 179
```

```
Foreign host: 24.10.10.2, Foreign port: 32959
Nexthop: 24.10.10.1 Nexthop global: :: Nexthop
local: ::
BGP connection: non shared network
```

Table 4-114 explains the fields shows for each route.

Table 4-114: show ip bgp vpnv4 all neighbors output details

Field	Description
BGP neighbor	Router ID of the BGP neighbor.
remote AS	Autonomous system number of the neighbor.
local AS	Autonomous system number of the local system.
internal link	internal link: iBGP neighbor (in the same AS).
BGP version	The version of BGP being used by the neighbor device.
BGP state	The current state of the neighbor connection and length of time within the current state.Possible states are: Idle, Connect, Active, and Established.
Last read	The amount of time in Hours **:** Minutes **:** Seconds since this device last checked the Hold Time parameters.
hold time	The amount of time this device waits for a Keepalive or Update message before the BGP connection is closed.
Keepalive interval	KEEPALIVE messages are sent periodically to ensure that the connection is live.
Neighbor capabilities	New or optional parameters called “Capabilities.” Provides a graceful way to advertise new or unique options without causing peering to terminate. The capabilities are communicated in TLV fields. (see RFC 3392). In the example output above, the following capabilities were advertised by the neighbor and were received and understood by this device: •Route refresh •Address family IPv4 Unicast •Address family IPv6 Unicast
Received	Message count, notification count, number of messages waiting in the queue.

Sent	Message count, notification count, number of messages waiting in the queue.
Route refresh request	Route requests sent and received.
For address family	As stated – in this case IPv4 Unicast.
BGP table version	For each of the address families agreed upon, BGP maintains a separate table.
neighbor version	Tracks prefixes that have been sent and those that need to be sent.
connections established	The number of times the router has established a TCP connection and the two peers have agreed to speak BGP with each other. "Dropped" means the number of time the connection has failed or gone down.
local host foreign host	Local host is the IP address and the port number of the local system used for the peering session. Foreign host is the IP address and the port of the neighbor. BGP always uses the TCP port number 179 for the peer originating the session.

Table 4-114: show ip bgp vpnv4 all neighbors output details (Continued)

Field	Description
nexthop	The IP address of the next hop used to reach the neighbor. eBGP or iBGP peers do not need to be directly connected. Peering sessions can be set up across multiple hops. If the neighbors are directly connected, the IP address of the local system is listed as the next hop.
nexthop global	The global IPv6 address of the next hop
nexthop local	The link-local IPv6 address of the next hop
non shared network	The peering session is running on a non shared network.
last reset	Time since this peering session was last reset. The reason for the reset is displayed on this line.
notification error message	Last error message sent.

show ip extcommunity-list

Use this command to display BGP routes that match an extended community list.

Command Syntax `show ip extcommunity-list (WORD | ) show ip extcommunity-list (<1-199>|WORD)`

`show ip bgp extcommunity-list WORD (exact-match|)(vrf VRFNAME|)`

Parameters

`WORD`	Name of extended community list
`<1-199>`	Number of extended community list
`VRFNAME`	VPN routing/forwarding instance name

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip extcommunity-list 33
```

show ip protocols

Use this command to display information about the IP protocols such as IP routing process parameters and statistics.

Command Syntax `show ip protocols show ip protocols bgp`

Parameters

`bgp`	BGP information

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip protocols bgp
Routing Protocol is "bgp 100"
Sending updates every 30 seconds with +/-50%, next due in 12 seconds
Timeout after 180 seconds, garbage collect after 120 seconds
Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set
```

```
Default redistribution metric is 1
Redistributing: connected static
Default version control: send version 2, receive version 2
Interface        Send  Recv   Key-chain    eth0
2     2
Routing for Networks:
  10.10.0.0/24
Routing Information Sources:
  Gateway          BadPackets BadRoutes  Distance Last Update  Distance:
(default is 120)
```

Table 4-115 explains the fields shows for each route.

Table 4-115: show ip protocols output details

Field	Description
Routing Protocol is "bgp 100"	Specifies the routing protocol used.
Sending updates every 30 seconds	Specifies the time between sending updates.
Next due in 12 seconds	Precisely when the next update is due to be sent.
Timeout after 180 seconds	Specifies the value of the timeout parameter.
Redistributing	Lists the protocol that is being redistributed.

Table 4-115: show ip protocols output details

Field	Description
Routing for Networks	Specifies the networks for which the routing process is currently injecting routes.
Routing Information Sources	Lists all the routing sources the Symanitron Networks software is using to build its routing table.

show ip vrf

Use this command to display the routing information of the VRF, such as interface, route distinguisher, route-target, and so on.

Command Syntax `show ip vrf show ip vrf WORD`

Parameter

`WORD`	VRF name

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip vrf VRF_A
VRF VRF_A; (table=1)
```

Appendix A Regular Expressions

Table A-116 shows the regular expression special characters used in BGP commands. You can use these characters in combination to build complex regular expressions.

Table A-116: Regular expression characters

Symbol	Character	Meaning
^	Caret	Matches the beginning of the input string. When used at the beginning of a string of characters, it negates a pattern match.
$	Dollar sign	Matches the end of the input string.
.	Period	Matches a single character (including white spaces).
*	Asterisk	Matches none or more sequences of a pattern.
+	Plus sign	Matches one or more sequences of a pattern.
?	Question mark	Matches none or one occurrence of a pattern.
_	Underscore	Matches spaces, commas, braces, parenthesis, or the beginning and end of an input string.
[]	Brackets	A range of single-characters.
-	Hyphen	Separates the end points of a range.

© Symanitron Proprietary

Open Shortest Path First Command Reference

Contents

This document contains these chapters and appendices:

- Chapter 1, *OSPFv2 Commands*
- Chapter 2, *OSPFv3 Commands*
- Chapter 3, *OSPF VPN Commands*
- Chapter 4, *CSPF-TE Commands*

CHAPTER 1 OSPFv2 Commands

This chapter provides an alphabetized reference for each of the OSPFv2 commands. It includes the following commands:

- area authentication
- area default-cost
- area filter-list
- area nssa
- area range
- area stub
- area virtual-link
- auto-cost reference bandwidth
- bfd all-interfaces
- capability cspf
- capability lls
- capability opaque
- capability restart
- capability te/traffic-engineering
- capability vrf-lite
- clear ip ospf
- compatible rfc1583
- debug ospf
- debug ospf database-timer rate-limit
- debug ospf events
- debug ospf ifsm
- debug ip ospf graceful-restart
- debug ip ospf lfa
- debug ip ospf redist
- debug ip ospf retransmission
- debug ospf lsa
- debug ospf nfsm
- debug ospf nsm
- debug ospf packet
- debug ospf rib
- debug ospf route
- default-information originate
- default-metric

- distance
- distribute-list
- enable db-summary-opt
- fast-reroute keep-all-paths
- fast-reroute tie-break
- host area
- ip ospf authentication
- ip ospf authentication-key
- ip ospf bfd
- ip ospf cost
- ip ospf database-filter
- ip ospf dead-interval
- ip ospf disable
- ip ospf fast-reroute per-prefix candidate disable
- ip ospf flood-reduction
- ip ospf hello-interval
- ip ospf multi-area
- ip ospf message-digest-key
- ip ospf mtu
- ip ospf mtu-ignore
- ip ospf network
- ip ospf priority
- ip ospf retransmit-interval
- ip ospf transmit-delay
- log-adjacency-changes
- max-concurrent-dd
- maximum-area
- neighbor
- network
- ospf abr-type
- ospf flood-reduction
- ospf restart helper • ospf router-id
- overflow database
- overflow database external
- passive-interface
- redistribute
- restart ospf graceful
- router ospf

- show debugging ospf
- show ip ospf
- show ip ospf border-routers
- show ip ospf database brief
- show ip ospf database detail
- show ip ospf igp-shortcut-lsp
- show ip ospf igp-shortcut-route
- show ip ospf interface
- show ip ospf multi-area-adjacencies
- show ip ospf neighbor
- show ip ospf route
- show ip ospf valid
- show ip ospf virtual-links
- show ip protocols
- show ip route fast-reroute
- shutdown
- snmp restart ospf
- summary-address
- timers lsa arrival
- timers spf exp
- timers throttle lsa

area authentication

Use this command to enable authentication for an OSPF area. Specifying the area authentication sets the authentication to Type 1 authentication or simple text password authentication (details in RFC 2328). Setting up a Type 1 authentication configures a 64-bit field for that particular network. All packets sent on this network must have this configured value in their OSPF header. This allows only routers that have the same passwords to join the routing domain. Give all routers that are to communicate with each other through OSPF the same authentication password.

Use the ip ospf authentication-key command to specify a simple text password.

Use the ip ospf message-digest-key command to specify an MD5 password.

Use the `no` parameter to remove the authentication specification for an area.

Command Syntax `area (A.B.C.D|<0-4294967295>) authentication`

```
area (A.B.C.D|<0-4294967295>) authentication message-digest
no area (A.B.C.D|<0-4294967295>) authentication
```

Parameters

`A.B.C.D`	OSPF Area ID in IPv4 address format.
`<0-4294967295>`	OSPF Area ID as 4-octet unsigned integer value.
`message-digest`	Enables MD5 authentication in the specified area ID.

Default

Null authentication

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#area 1 authentication message-digest

(config)#router ospf 100
(config-router)#no area 1 authentication
```

area default-cost

Use this command to specify a cost for the default summary route sent into a stub or NSSA area. This command provides the metric for the summary default route, generated by the area border router, into the NSSA or stub area. Use this option only on an area border router that is attached to the NSSA or stub area. Refer to the RFC 3101 for information on NSSA.

Use the `no` form of this command to remove the assigned default-route cost.

Command Syntax `area (A.B.C.D|<0-4294967295>) default-cost <0-16777215> no area (A.B.C.D|<0-4294967295>) default-cost`

Parameters

`A.B.C.D`	OSPF Area ID in IPv4 address format.
`<0-4294967295>`	OSPF Area ID as a decimal value.
`default-cost`	Indicates the cost for the default summary route used for a stub or NSSA area.
`<0-16777215>`	Stub's advertised default summary cost. The default is 1.

Default

By default, route cost is 1

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

This example sets the default-cost to 10 for area 1.

```
#configure terminal
(config)#router ospf 100
(config-router)#area 1 default-cost 10

(config)#router ospf 100
(config-router)#no area 1 default-cost
```

area filter-list

Use this command to configure a filter to advertise summary routes on an Area Border Router (ABR).

This command suppresses incoming and outgoing summary routes between this area and other areas. You use this command in conjunction with the `prefix-list` and `access-list` commands.

Use the `no` form of this command to remove a filter.

Command Syntax `area (A.B.C.D|<0-4294967295>) filter-list prefix WORD (in|out) area (A.B.C.D|<0-4294967295>) filter-list access WORD (in|out) no area (A.B.C.D|<0-4294967295>) filter-list prefix WORD (in|out) no area (A.B.C.D|<0-4294967295>) filter-list access WORD (in|out)`

Parameters

`A.B.C.D` OSPF area ID as an IPv4 address.

`<0-4294967295>` OSPF area ID as a decimal value. `prefix` Use prefix list to filter summary.

`WORD` Name of the prefix list.

`access` Use access list to filter summary.

`WORD` Name of the access list.

`in` Filter routes from other areas into this area. `out` Filter routes from this area into other areas.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#access-list 1 deny 172.22.0.0
(config)#router ospf 100
(config-router)#area 1 filter-list access 1 in
```

area nssa

Use this command to set an area as a Not-So-Stubby-Area (NSSA). There are no external routes in an OSPF stub area, so you cannot redistribute from another protocol into a stub area. An NSSA allows external routes to be flooded within the area. These routes are then leaked into other areas. However, the external routes from other areas still do not enter the NSSA. You can configure an area to be a stub area or an NSSA, but not both.

This command simplifies administration when connecting a central site using OSPF to a remote site that is using a different routing protocol. You can extend OSPF to cover the remote connection by defining the area between the central router and the remote router as a NSSA.

Use the `no` form of this command to remove this designation.

Command Syntax

`area (A.B.C.D|<0-4294967295>) nssa {translator-role (candidate|always)|`

```
stabilityinterval < 0-2147483647>|no-redistribution|default-information-
originate

(metric < 0-16777214>|metric-type <1-2>|metric <0-16777214> metric-type <1-
2>|metric-type< 1-2> metric <0-16777214>|)|no-summary} area (A.B.C.D|<0-
4294967295>) nssa {translator-role (candidate|always|never)| stabilityinterval <
0-2147483647>|no-redistribution|default-information-originate
(metric < 0-16777214>|metric-type <1-2>|metric <0-16777214> metric-type <1-
2>|metric-type< 1-2> metric <0-16777214>|)|no-summary} no area
(A.B.C.D|<0-4294967295>) nssa no area (A.B.C.D|<0-4294967295>) nssa
{translator-role|stability-interval|no-
redistribution |default-information-originate (route-map |) |no-summary}
```

Parameters

`A.B.C.D` OSPF Area ID in IPv4 address format.

`<0-4294967295>` OSPF Area ID as a decimal value.

`translator-role`

NSSA-ABR translator role

`candidate` Translate NSSA-LSA to Type-5 LSA if router is elected.

`never` Do not translate NSSA-LSA to Type-5 LSA. `always`

Always translate NSSA-LSA to Type-5 LSA.

`stability-interval`

Stability timer for a NSSA area. If an elected translator determines its services are no longer required, it continues to perform its duties for this time interval. This minimizes excess flushing of translated Type-7 LSAs and provides a more stable translator transition.

`<0-2147483647>`

Stability interval in seconds.

`no-redistribution`

Do not redistribute into the NSSA.

`default-information-originate`

Originate Type-7 default LSA into the NSSA.

`metric` Specify metric for default routes.

`<0-16777214>`

Specify metric value.

`metric-type` Specify metric type (see RFC 3101).

`<1-2>` Specify metric type:

1: Type 1 external route

2: Type 2 external route

`route-map` OSPF default Route map reference.

`WORD` Pointer to route-map entries.

no-summary	Do not inject inter-area routes into the NSSA.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#router ospf 100
(config-router)#area 3 nssa translator-role candidate no-redistribution
default-information-originate metric 34 metric-type 2
```

area range

Use this command to summarize OSPF routes at an area boundary. A single summary route is then advertised to other areas by the Area Border Routers (ABRs). Routing information is condensed at area boundaries and outside the area. If the network numbers in an area are assigned in a way such that they are contiguous, the ABRs can be configured to advertise a summary route that covers all the individual networks within the area that fall into the specified range.

Use the no parameter with this command to disable this function.

Command Syntax area (A.B.C.D|<0-4294967295>) range (A.B.C.D/M | A.B.C.D A.B.C.D) area (A.B.C.D|<0-4294967295>) range (A.B.C.D/M | A.B.C.D A.B.C.D) advertise area (A.B.C.D|<0-4294967295>) range (A.B.C.D/M | A.B.C.D A.B.C.D) not-advertise area (A.B.C.D|<0-4294967295>) range A.B.C.D A.B.C.D (advertise|non-advertise) no area (A.B.C.D|<0-4294967295>) range (A.B.C.D/M | A.B.C.D A.B.C.D) no area (A.B.C.D|<0-4294967295>) range (A.B.C.D/M | A.B.C.D A.B.C.D) (advertise|not-advertise)

Parameters

A.B.C.D	Area range prefix or length e.g. X.X.X.X/length
A.B.C.D	Area range prefix e.g. A.B.C.D <0-4294967295>
OSPF Area ID as a decimal value. A.B.C.D/M	The area
range prefix and length.	
advertise	Advertises this range. not-advertise
Does not advertise this range.	

Default

By default, area range is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#area 1 range 192.16.0.0/24

(config)#router ospf 100 (config-router)#no
area 1 range 192.16.0.0/24
```

area stub

Use this command to define an area as a stub area. There are two stub area router configuration commands: the `stub` and `default-cost` commands. In all routers attached to the stub area, configure the area by using the `stub` option of the area command. For an area border router (ABR) attached to the stub area, use the `area default-cost` command.

Use the `no-summary` parameter with this command to define a totally stubby area. Define an area as a totally stubby area when routers in the area do not need to learn about summary LSAs from other areas.

Use the `no` form of this command to disable this function.

Command Syntax `area (A.B.C.D|<0-4294967295>) stub`

`area (A.B.C.D|<0-4294967295>) stub no-summary`

`no area (A.B.C.D|<0-4294967295>) stub no area (A.B.C.D|<0-4294967295>) stub no-summary`

Parameters

`A.B.C.D` OSPF Area ID in IPv4 address format.

`<0-4294967295>` OSPF Area ID as a decimal value. `no-summary` Stops an ABR from sending summary link advertisements into the stub area.

Default

By default, no stub area is defined.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
```

```
(config)#router ospf 100
(config-router)#area 1 stub no-summary
```

area virtual-link

Use this command to configure a link between two backbone areas that are physically separated through other nonbackbone area.

In OSPF, all non-backbone areas must be connected to a backbone area. If the connection to the backbone is lost, the virtual link repairs the connection. Configure virtual links between any two backbone routers that have an interface to a common non-backbone area. The protocol treats these routers joined by a virtual link as if they were connected by an unnumbered point-to-point network.

Configure the hello-interval to be the same for all routers attached to a common network. A short hello-interval results in the router detecting topological changes faster but also an increase in the routing traffic. The retransmit-interval is the expected round-trip delay between any two routers in a network. Set the value to be greater than the expected round-trip delay to avoid needless retransmissions.

The transmit-delay is the time taken to transmit a link state update packet on the interface. Before transmission, the link state advertisements in the update packet, are incremented by this amount. Set the transmit-delay to be greater than zero. Also, take into account the transmission and propagation delays for the interface. Include the transit area ID and the corresponding virtual link neighbor's router ID in each virtual link neighbor to properly configure a virtual link.

Use the `no` parameter with this command to remove a virtual link.

Command Syntax `area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D {authentication (message-digest|null|)|authentication-key LINE|message-digest-key <1-255> md5 LINE|deadinterval <1-65535>|hello-interval <1-65535>|retransmit-interval <1-3600>|transmit-delay <1-3600>} area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D {fall-over bfd} no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D {authentication (messagedigest| null|)|authentication-key LINE|message-digest-key <1-255> md5 LINE|deadinterval <1-65535>|hello-interval <1-65535>|retransmit-interval <1-3600>|transmit-delay <1-3600>} no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D {fall-over bfd}`

Parameters

`A.B.C.D`	OSPF Area ID in IPv4 address format.
`<0-4294967295>`	OSPF Area ID as a decimal value.
`A.B.C.D`	Specify IP address of the virtual link neighbor.
`authentication`	Enable authentication on this virtual link `message-digest` Cryptographic authentication.
`null`	Null authentication.
`authentication-key`	

Set authentication key.

LINE Authentication key ID of 8 characters.

message-digest-key
Set message digest key. <1-255> Set message digest key. md5 Specify the MD5 key.

LINE MD5 key.

dead-interval The interval during which no packets are received and after which the router acknowledges a neighboring router as off-line.

<1-65535> The interval in seconds. The default is 40 seconds. hello-interval The interval the router waits before it sends a hello packet. <1-65535> The interval in seconds. The default is 10 seconds.

retransmit-interval
The interval the router waits before it retransmits a packet.

<1-3600> The interval in seconds. The default is 5 seconds. transmit-delay The interval the router waits before it transmits a packet.

<1-3600> The interval in seconds. The default is 1 second fall-over
Specify fall-over detection. bfd Bidirectional Forwarding Detection (BFD)

Default

Default intervals:

Dead interval : 40 seconds

Hello interval: 10 seconds

Retransmit interval: 5 seconds

Transmit delay: 1 second

Command Mode

Router mode

SWMRE version 1.3

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#area 1 virtual-link 10.10.11.50 hello 5 dead 10
```

auto-cost reference bandwidth

Use this command to control how OSPF calculates the default metric for the interface.

Use the `no` form of this command to assign cost based only on the interface bandwidth.

Command Syntax `auto-cost reference-bandwidth <1-4294967>`

`no auto-cost reference-bandwidth`

Parameters

`<1-4294967>`	The reference bandwidth in Mbps per second. The default is 100 Mbps.

Default

By default, OSPF calculates the OSPF metric for an interface by dividing the reference bandwidth by the interface bandwidth. The default value for the reference bandwidth is 100Mbps. The auto-cost command is used to differentiate high bandwidth links. For multiple links with high bandwidth, specify a larger reference bandwidth value to differentiate cost on those links.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#auto-cost reference-bandwidth 50

(config)#router ospf 100 (config-router)#no
auto-cost reference-bandwidth
```

bfd all-interfaces

Use this command to enable Bidirectional Forwarding Detection (BFD) on all interfaces.

Use the `no` form of this command to disable BFD.

Command Syntax `bfd all-interfaces no bfd all-interfaces`

Parameters

None

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#bfd all-interfaces

(config)#router ospf 100
(config-router)#no bfd all-interfaces
```

capability cspf

Use this command to enable the CSPF (Constrained Shortest Path First) feature for an OSPFv2 or OSPFv3 instance.

Use the `no` parameter with this command to disable CSPF functionality for the OSPFv2 or OSPFv3 instance.

Command Syntax

```
capability cspf no
capability cspf
```

Parameters

None

Default

By default, CSPF functionality for the OSPFv2 or OSPFv3 instance is enabled.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#capability cspf

(config)#router ospf 100
(config-router)#no capability cspf
```

capability lls

Use this command to enable link-local signaling feature on OSPF router.

Use no parameter to disable link-local signaling feature on OSPF router.

Command Syntax `capability lls no capability lls`

Parameters

None

Default

By default, capability lls is enabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#capability lls

(config-router)#no capability lls
```

capability opaque

Use this command to enable opaque-LSAs which are Type 9, 10 and 11 LSAs that deliver information used by external applications.

Use the `no` form of this command to disable the feature.

Command Syntax

```
capability opaque no
capability opaque
```

Parameters

None

Default

By default, opaque-LSA is enabled.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#capability opaque

(config)#router ospf 100
(config-router)#no capability opaque
```

capability restart

Use this command to enable OSPF graceful restart or restart signaling. If a router is not restart-enabled, it cannot enter graceful restart mode and act as a helper.

Use the `no` parameter with this command to disable the features.

Command Syntax `capability restart`

```
graceful no capability restart
graceful
```

Parameters `graceful` Specify enabling OSPF graceful restart feature.

Default

By default, OSPF graceful restart or restart signaling is enabled.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#capability restart graceful

(config)#router ospf 100 (config-router)#no
capability restart graceful
```

capability te/traffic-engineering

Use this command to enable traffic engineering feature on OSPF router.

Use `no` parameter to disable traffic engineering feature on OSPF router.

Command Syntax `capability traffic-engineering capability te no capability traffic-engineering no capability te`

Parameters

None

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf
               (config-router)#capability traffic-engineering

                                (config-router)#no capability traffic-engineering
```

capability vrf-lite

Use this command to apply multi-VRF capability to OSPF process or to decouple the PE router from the VPN backbone.

Use `no` parameter to deny multi-VRF capability to OSPF process or to avoid decoupling the PE router from the VPN backbone.

Command Syntax `capability`

`vrf-lite no capability`

`vrf-lite`

Parameters

None

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf
(config-router)#capability vrf-lite

(config-router)#no capability vrf-lite
```

clear ip ospf

Use this command to clear and restart all OSPF routing processes or a given OSPF routing process.

Command Syntax `clear ip ospf (<0-65535>|) process`

Parameter

`<0-65535>`	Specify the process ID.

Command Mode

Privileged Exec Mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear ip ospf process
#clear ip ospf 555 process
```

compatible rfc1583

Use this command to restore the method used to calculate summary route costs per RFC.

RFC 1583 specified a method for calculating the metrics for summary routes based on the minimum metric of the component paths available. RFC 2328 specifies a method for calculating metrics based on maximum cost. With this change, it is possible that all of the ABRs in an area might not be upgraded to the new code at the same time. This command addresses this issue and allows the selective disabling of RFC 2328 compatibility.

Use the `no` parameter with this command to disable RFC 1583 compatibility.

Command Syntax `compatible`

`rfc1583 no compatible`

`rfc1583`

Parameters

None

Default

By default, OSPF is RFC 2328 compatible

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#compatible rfc1583

(config)#router ospf 100
(config-router)#no compatible rfc1583
```

debug ospf

Use this command to specify debugging options for OSPF.

Use the `no` parameter with this command to disable this function.

Command Syntax `debug ospf (all|bfd|database-timer|events|ifsm|lsa|nfsm|nsm| packet|route|sr|) debug ospf rib ({interface|redistribute}|) no debug ospf (all|bfd|database-timer|events|ifsm|lsa|nfsm|nsm| packet|route|sr|) undebug ospf (all|bfd|database-timer|events|ifsm|lsa|nfsm|nsm| packet|route|) no debug all ospf`

```
undebug all ospf no debug all no debug ospf rib ({interface|redistribute}|)
undebug all
```

Parameters `all` Enable or disable debugging for `ifsm`, `nsfm`, `lsa`, `nsm`, `events`, and `route`.

`bfd`	Debug Bidirectional Forwarding Detection (BFD) `database-timer`
	Debug OSPF rate-limiting values for LSA throttling (see debug ospf database-timer ratelimit)
`events ifsm`	Debug OSPF events information (see debug ospf events)
`lsa nfsm nsm`	Debug OSPF Interface State Machine (see debug ospf ifsm)
`packet route`	Debug OSPF Link State Advertisement (see debug ospf lsa)
`rib sr`	Debug OSPF Neighbor State Machine (see debug ospf nfsm)
`interface`	Debug OSPF NSM information (see debug ospf nsm)
`redistribute`	Debug OSPF packets (see debug ospf packet)
	Debug OSPF route information (see debug ospf route)
	Debug OSPF RIB information
	Debug OSPF segment routing
	information Debug OSPF RIB interface
	Debug OSPF RIB redistribute

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
  #debug ospf all

  #debug ospf bfd
#no debug ospf bfd
```


© Symanitron Proprietary

debug ospf database-timer rate-limit

Use this command to log when link-state advertisement (LSA) rate-limiting timers will expire. These messages are logged only when debug ospf lsa `generate` or debug ospf lsa `refresh` is enabled Use the `no` parameter with this command to disable this function.

Command Syntax `debug ospf database-timer rate-limit`

```
no debug ospf database-timer rate-limit undebug
ospf database-timer rate-limit
```

Parameters

None

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#debug ospf database-timer rate-limit

#undebug ospf database-timer rate-limit
```

debug ospf events

Use this command to specify debugging options for OSPF event troubleshooting. Use this command without parameters to turn on all the options.

Use the `no` parameter with this command to disable this function.

Command Syntax `debug ospf events ({abr|asbr|lsa|nssa|os|router|vlink}|)`

```
no debug ospf events ({abr|asbr|lsa|nssa|os|router|vlink}|) undebug
ospf events ({abr|asbr|lsa|nssa|os|router|vlink}|)
```

Parameters

`abr`	Debug OSPF ABR events.
`asbr`	Debug ASBR events.
`lsa`	Debug LSA events.

nssa	Debug NSSA events.
os	Debug OS interaction events.
router	Debug other router events.
vlink	Debug virtual link events.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#no debug ospf event abr
#debug ospf event asbr
#debug ospf event lsa
#no debug ospf event nssa
#debug ospf event os
#debug ospf event router
#debug ospf event vl
```

debug ospf ifsm

Use this command to specify debugging options for OSPF Interface Finite State Machine (IFSM) troubleshooting.

Use the `no` parameter with this command to disable this function.

Command Syntax `debug ospf ifsm ({events|status|timers}|)`

```
no debug ospf ifsm ({events|status|timers}|) undebug
ospf ifsm ({events|status|timers}|)
```

Parameters

events	Debug IFSM event information
status	Debug IFSM status information
timers	Debug IFSM timer information

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#no debug ospf ifsm events
#debug ospf ifsm status
```

```
#debug ospf ifsm timers
```

debug ip ospf graceful-restart

Use this command to specify debugging option for OSPF graceful restart.

Use the `no` parameter with this command to disable this function.

Command Syntax `debug ip ospf graceful-restart (detail|terse|) no debug ip ospf graceful-restart (detail|terse|)`

Parameters `detail` Debug OSPF graceful restart detail information `terse` Debug OSPF graceful restart summary information

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#debug ip ospf graceful-restart detail
```

debug ip ospf lfa

Use this command to specify the debugging options for OSPFv2 Loop-free Alternate path Use the `no` parameter with this command to disable this function.

Command Syntax `debug ip ospf lfa no debug ip ospf lfa`

Parameters

None

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#debug ip ospf lfa
```

debug ip ospf redist

Use this command to display debugging option for OSPF redistribute information Use the `no` parameter with this command to disable this function.

Command Syntax `debug ip ospf redist (detail|terse|) no debug ip ospf redist (detail|terse|)`

Parameters `detail` Debug OSPF redistribute detail information `terse` Debug OSPF redistribute summary information

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#debug ip ospf redistribute detail
```

debug ip ospf retransmission

Use this command to display debug logs of OSPF retransmission information.

Use the `no` parameter with this command to disable this function.

Command Syntax `debug ip ospf retransmission no debug ip ospf retransmission`

Parameters

None

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#debug ip ospf retransmission
```

debug ospf lsa

Use this command to specify debugging options for OSPF Link State Advertisements (LSA) troubleshooting.

Use the `no` parameter with this command to disable this function.

Command Syntax `debug ospf lsa ({flooding|generate|install|maxage|refresh}|)`

`no debug ospf lsa ({flooding|generate|install|maxage|refresh}|) undebug ospf lsa ({flooding|generate|install|maxage|refresh}|)`

Parameters

`flooding`	Debug LSA flooding.
`generate`	Debug LSA generation.
`install`	Debug LSA installation.
`maxage`	Debug the maximum age processing.
`refresh`	Debug LSA refresh.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#no debug ospf lsa refresh
#debug ospf lsa flooding
#debug ospf lsa install
#debug ospf lsa maxage
#debug ospf lsa generate
```

debug ospf nfsm

Use this command to specify debugging options for OSPF Neighbor Finite State Machines (NFSMs).

Use the `no` parameter with this command to disable this function.

Command Syntax `debug ospf nfsm ({events|status|timers}|)`

`no debug ospf nfsm ({events|status|timers}|) undebug ospf nfsm ({events|status|timers}|)`

Parameters

`events`	Debug NFSM event information

status	Debug NFSM status information
timers	Debug NFSM timer information

Command Mode

Privileged Exec mode Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#debug ospf nfsm events
#no debug ospf nfsm timers
```

debug ospf nsm

Use this command to specify debugging options for OSPF NSM information.

Use the `no` parameter with this command to disable this function.

Command Syntax `debug ospf nsm ({interface|redistribute}|)`

`no debug ospf nsm ({interface|redistribute}|) undebug ospf nsm ({interface|redistribute}|)`

Parameters `interface` Debug NSM interface information. `redistribute` Debug NSM redistribute information.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The `debug ospf nsm` command enables the display of debug information related to NSM.

```
#debug ospf nsm interface
#no debug ospf nsm redistribute
```

debug ospf packet

Use this command to specify debugging options for OSPF packets.

Use the `no` parameter with this command to disable this function.

Command Syntax `debug ospf packet ({hello|dd|ls-request|ls-update|ls-ack|send|recv|detail}|)`

```
no debug ospf packet ({hello|dd|ls-request|ls-update|ls-ack|send|recv|detail}|)
undebug ospf packet ({hello|dd|ls-request|ls-update|ls-ack|send|recv|detail}|)
```

Parameters

`hello`	Debug OSPF hello packets.
`dd`	Debug OSPF database.
`ls-request`	Debug OSPF link state requests.
`ls-update`	Debug OSPF link state updates.
`ls-ack`	Debug OSPF link state acknowledgments.
`send`	Debug OSPF sent packets.
`recv`	Debug OSPF received packets.
`detail`	Debug OSPF detailed information.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#debug ospf packet detail
#debug ospf packet dd send detail
#no debug ospf packet ls-request recv detail
```

debug ospf rib

Use this command to display debug information about the interaction between the OSPF process and the Routing Information Base (RIB).

Use `no` parameter of this command to disable debugging output.

Command Syntax

```
debug ospf rib ({interface|redistribute}|)
no debug ospf rib ({interface|redistribute}|)
debug ip ospf ({client|redistribute}|)
no debug ip ospf ({client|redistribute}|)
undebug ospf rib ({interface|redistribute}|)
```

Parameters

`interface`	Debug RIB interface information.
`redistribute`	Debug RIB redistribute
information. `client`	Debug RIB client information.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.1.

Example

```
#debug ospf rib interface
#no debug ospf rib redistribute
```

debug ospf route

Use this command to debug route calculation. Use this command without parameters to turn on all the options.

Use the `no` parameter with this command to disable this function.

Command Syntax `debug ospf route ({ase|ia|install|spf}|) no debug ospf route ({ase|ia|install|spf}|) undebug ospf route ({ase|ia|install|spf}|)`

Parameters

`ase`	Debug OSPF external route calculation.
`ia`	Debug OSPF Inter-Area route calculation.
`install`	Debug OSPF route installation.
`spf`	Debug OSPF SPF calculation.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#debug ospf route
#no debug ospf route ia
#debug ospf route install
```

default-information originate

Use this command to create a default external route into an OSPF routing domain.

Use the `no` parameter with this command to disable this feature.

The system acts like an Autonomous System Boundary Router (ASBR) when you use the `default-information originate` command to redistribute routes into an OSPF routing domain. An ASBR does not by default generate a default route into the OSPF routing domain.

When you give the `default-information originate` command, also specify a `route-map` to avoid a dependency on the default network in the routing table.

Command Syntax default-

information originate

default-information originate {metric <0-16777214>|metric-type (1|2)|?route-map WORD|always} no default-

information originate

no default-information originate {metric|metric-type|?route-map|always}

Parameters

always Used to advertise the default route regardless of whether there is a default route.

metric Sets the OSPF metric used in creating the default route.

<0-16777214>

Sets the OSPF metric used in creating the default route. The default metric value is 10. The value used is specific to the protocol.

metric-type The external link type associated with the default route advertised into the OSPF routing domain (see RFC 3101).

1 Sets OSPF External Type 1 metric.

2 Sets OSPF External Type 2 metric (default). route-map Route map.

WORD Specify the name of route map.

Default

Sets the OSPF metric used in creating the default route. The default metric value is 10.

The value used is specific to the protocol. metric-type The external link type associated with the default route advertised into the OSPF routing domain (see RFC 3101).

By default, 2 Sets OSPF External Type 2 metric.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#default-information originate always metric 23 metric-type
2 route-map myinfo

(config)#router ospf 100
(config-router)#no default-information originate metric metric-type route-map
```

default-metric

Use this command to set a default metric for OSPF.

A default metric facilitates redistributing routes with incompatible metrics. If the metrics do not convert, the default metric provides an alternative. Use this command to use the same metric value for all redistributed routes. Use this command in conjunction with the redistribute command.

Use the `no` parameter with this command to return to the default state.

Command Syntax `default-metric <1-16777214>`

`no default-metric`

`no default-metric <1-16777214>`

Parameters

`<1-16777214>`	Default metric value.

Default

Built-in, automatic metric translations, as appropriate for each routing protocol.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#default-metric 100
```

distance

Use this command to set OSPF administrative distances.

The administrative distance rates the trustworthiness of a routing information source. A higher distance value means a lower trust rating. For example, an administrative distance of 255 means that the routing information source cannot be trusted and should be ignored.

Use the `no` form of this command to restore the default value (110).

Command Syntax `distance <1-255> distance <1-255> A.B.C.D/M (WORD|) distance ospf {intra-area <1-255>|inter-area <1-255>|external <1-255>} no distance <1-255> no distance <1-255> A.B.C.D/M (WORD|) no distance ospf`

Parameters

<1-255>	Used alone, this parameter specifies a default administrative distance used when no other specification exists for a routing information source.
intra-area	Routes within an area.
<1-255>	Distance for all routes within an area
inter-area	Routes from one area to another area.
<1-255>	Distance for all routes from one area to another area.
external	Routes from other routing domains learned by redistribution.
<1-255>	Distance for routes from other routing domains learned by redistribution.
A.B.C.D/M	Distance for routes to prefixes whose nexthop matches this address.
WORD	Name of access list to apply to route updates.

Default

By default, distance for each type of route (intra-, inter-, or external) is 110

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#distance ospf inter-area 20 intra-area 10 external 40
```

distribute-list

Use this command to filter networks in routing updates. This command redistributes other routing protocols into the OSPF routing table.

Use the no parameter with this command to disable this function.

Command Syntax distribute-list WORD out (kernel|connected|static|rip|bgp|isis|ospf (<1-65535>|)) distribute-list WORD in no distribute-list WORD out (kernel|connected|static|rip|bgp|isis|ospf (<1-65535>|)) no distribute-list WORD in

Parameters

WORD	Specify the name of the access list.
in	Filter incoming routing updates.
out	Filter outgoing routing updates.
kernel	Specify kernel routes.
connected	Specify connected routes.
static	Specify static routes.

`rip`	Specify RIP routes.
`bgp`	Specify BGP routes.
`isis`	Specify IS-IS routes.
`ospf`	Specify OSPF process.
`<1-65535>`	Specify OSPF process ID <1-65535>. If not specified, this command redistribute OSPF instance with process ID 0.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows the distribution of BGP routing updates based on the access list `list1` (network 172.10.0.0).

```
    #configure terminal
    (config)#access-list list1 permit 172.10.0.0
    (config)#router ospf 100
    (config-router)#distribute-list list1 out bgp
(config-router)#redistribute bgp
```

enable db-summary-opt

Use this command to enable the database summary list optimization for OSPFv2.

When this feature is enabled, the database exchange process is optimized by removing the LSA from the database summary list for the neighbor, if the LSA instance in database summary list is the same as or less recent than the listed LSA in the database description packet received from the neighbor.

Use the `no` form of this command to disable database summary list optimization.

Command Syntax `enable db-summary-opt` `no enable db-summary-opt`

Parameters

None

Default

By default, database summary list optimization for OSPFv2 is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf
(config-router)#enable db-summary-opt
(config-router)#no enable db-summary-opt
```

fast-reroute keep-all-paths

Use this command to enable fast rerouting on all OSPF interfaces.

Use the `no` parameter with this command to disable fast rerouting.

Command Syntax `fast-reroute keep-all-paths` `no fast-reroute keep-all-paths`

Parameters

None

Defaults

By default, fast rerouting is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf 200
(config-router)#fast-reroute keep-all-paths
```

fast-reroute tie-break

Use this command to set the tie-breaking policy for selecting a fast reroute repair path. You assign a priority to each type of repair path.

Use the `no` parameter with this command to set the tie-breaking policy for a specific type of repair path to its default priority. To set all types of repair paths to their default priorities, do not specify a repair path with the `no` form of this command.

Command Syntax

```
fast-reroute tie-break (primary-path|interface-disjoint|node-protecting|broadcast-
  interface-disjoint) index <1-10>
no fast-reroute tie-break no fast-reroute tie-break (primary-
path|interface-disjoint|node-
  protecting|broadcast-interface-disjoint) index <1-10>
```

Parameters `primary-path` Use a path from the Equal-Cost Multipath Path (ECMP) set. An ECMP found during the primary shortest path first (SPF) repair might not be desirable in networks where traffic exceeds the capacity of any single link.

`interface-disjoint`

Do not select point-to-point interfaces that have no alternate next hop for rerouting if the primary gateway fails, thus protecting the interface.

`node-protecting`

Bypass the `primary-path` gateway router which might not protect the router that is the next hop in the primary path.

`broadcast-interface-disjoint`

Do not use the interface if connected to a broadcast network. Repair paths protect links when a repair path and a protected primary path use *different* next-hop interfaces. However, on broadcast interfaces, if the repair path is computed via the same interface as the primary path, but their next-hop gateways are different, the router is protected but the link might not be.

`index` Tie break priority. A lower value has higher preference.

`<1-10>` Range of priority values.

Defaults

By default, LFA backup path is calculated based on interface-disjoint.

The default priority scheme is:

1. primary-path
2. interface-disjoint
3. node-protecting
4. broadcast-interface-disjoint

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf 200
                (config-router)#fast-reroute tie-break interface-disjoint index 1
```

host area

Use this command to configure a stub host entry belonging to a particular area.

Using this command, you can advertise specific host routes in the router-LSA as stub link. Since stub host belongs to the specified router, specifying cost is not important.

Use the `no` form of this command to remove the host area configuration.

Command Syntax `host A.B.C.D area (A.B.C.D|<0-4294967295>)`

`host A.B.C.D area (A.B.C.D|<0-4294967295>) cost <0-65535> no host A.B.C.D area (A.B.C.D|<0-4294967295>)`

`no host A.B.C.D area (A.B.C.D|<0-4294967295>) cost (<0-65535>|)`

Parameters

`A.B.C.D` Specify IP address of the host. `area`

Set the OSPF area ID

`A.B.C.D` OSPF Area ID in IPv4 address format.

`<0-4294967295>`

OSPF Area ID as a decimal value.

`cost` Specify cost for stub host entry. `<0-65535>` Specify cost for stub host entry.

Default

No host entry is configured

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#host 172.16.10.100 area 1
(config-router)#host 172.16.10.101 area 2 cost 10
```

ip ospf authentication

Use this command to send and receive OSPF packets with the specified authentication method on the current interface.

Use the `no` parameter with this command to disable the authentication.

Command Syntax `ip ospf authentication (null|message-digest|)`

`ip ospf A.B.C.D authentication (null|message-digest|) no ip ospf (A.B.C.D|) authentication`

Parameters

`A.B.C.D` The IP address of the interface. `null` Use no authentication. `message-digest` Use message digest authentication.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

In this example, interface `eth0` is configured to have no authentication. This will override any `text` or `MD5` authentication configured on this interface.

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf authentication null
```

ip ospf authentication-key

Use this command to specify an OSPF authentication password for neighboring routers.

This command creates a password (key) that is inserted into the OSPF header when SWMRE originates packets. Assign a separate password to each network for different interfaces. All neighboring routers on the same network with the same password exchange OSPF routing data.

The key can be used only when authentication is enabled for an area with the `area authentication` command.

Simple password authentication allows a password to be configured for each area. Configure the routers in the same routing domain with the same password.

Use the `no` parameter with this command to remove an OSPF authentication password.

Command Syntax `ip ospf (A.B.C.D|) authentication-key (0|) WORD no ip ospf (A.B.C.D|) authentication-key`

Parameters

`A.B.C.D` The IP address of the interface.

`authentication-key`

Specify the authentication password.

`0` Specify the unencrypted password (key).

`WORD` Specify the OSPF password (key) up to maximum 8 characters.

Default

By default, no password used when exchanging OSPF routing data

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

In the following example, an authentication key `test` is created on interface `eth0` in area `0`. Note that first authentication is enabled for area `0`.

```
#configure terminal
(config)#router ospf 100
(config-router)#network 10.10.10.0/24 area 0
(config-router)#area 0 authentication
(config-router)#exit
(config)#interface eth0
(config-if)#ip ospf 3.3.3.3 authentication-key test
```

ip ospf bfd

Use this command to enable Bidirectional Forwarding Detection (BFD).

Use this command with either the `no` or `disable` parameter to disable BFD.

Command Syntax `ip ospf bfd (disable|) no ip ospf bfd (disable|)`

Parameters `disable` Specify to disable BFD.

Default

By default, ip ospf bfd is disabled

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf bfd
```

ip ospf cost

Use this command to explicitly specify the cost of the link-state metric in a router-LSA.

The interface cost indicates the overhead required to send packets across an interface. This cost is stated in the Router-LSA's link. The cost is inversely proportional to the bandwidth of an interface. By default, the cost of an interface is calculated based on the bandwidth (10^8/ bandwidth). Use this command to set the cost manually.
Use the `no` parameter with this command to reset the cost to its default value.

Command Syntax `ip ospf (A.B.C.D|) cost <1-65535> no ip ospf (A.B.C.D|) cost`

Parameters

`A.B.C.D`	The IP address of the interface.
`<1-65535>`	Specify the link-state metric.

Default

By default, the cost of an interface is calculated based on the bandwidth (10^8/ bandwidth). The default cost value is 10.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows setting the cost as 10 on interface `eth0` for IP address 10.10.10.50.

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf 10.10.10.50 cost 10
```

ip ospf database-filter

Use this command to turn on the LSA database-filter for a particular interface.

OSPF floods new LSAs over all interfaces in an area, except the interface on which the LSA arrives. This redundancy ensures robust flooding. However, too much redundancy can waste bandwidth and might lead to excessive link and CPU usage in certain topologies, resulting in destabilizing the network. To avoid this, use this command to block flooding of LSAs over specified interfaces.

Use the `no` parameter with this command to turn off the filter.

Command Syntax `ip ospf (A.B.C.D|) database-filter all out no ip ospf (A.B.C.D|) database-filter`

Parameters

`A.B.C.D`	The IP address of the interface.

Default

Disabled, all outgoing LSAs are flooded to the interface.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf database-filter all out
```

ip ospf dead-interval

Use this command to set the interval during which the router waits to receive an OSPF hello packet from the neighbor before declaring the neighbor down. This value is advertised in the router's hello packets. It must be a multiple of hellointerval and be the same for all routers on a specific network.

Use the `no` parameter with this command to return to the default time. If you have configured this command specifying the IP address of the interface and want to remove the configuration, use the `no` parameter with the specified IP address (`no ip ospf dead-interval A.B.C.D`).

Command Syntax `ip ospf (A.B.C.D|) dead-interval <1-65535> no ip ospf (A.B.C.D|) dead-interval`

Parameters

`A.B.C.D`	The IP address of the interface.

`dead-interval` Specify the interval.

`<1-65535>` Specify the interval in seconds.

Default

By default, dead interval is 40 seconds

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows configuring dead-interval for 10 seconds on eth0 interface.

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf dead-interval 10
```

ip ospf disable

Use this command to completely disable OSPF packet processing on an interface.

This command overrides the network command.

Use the `no` option with this command to return to the default setting.

Command Syntax `ip ospf disable all no ip ospf disable all`

Parameters

None

Default

By default, this feature is disabled

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf disable all
```

ip ospf fast-reroute per-prefix candidate disable

Use this command to prohibit the interface from being used as the next hop in a repair path.

Use the `no` option with this command to use the interface as the next hop in a repair path.

Command Syntax `ip ospf fast-reroute per-prefix candidate disable no ip ospf fast-reroute per-prefix candidate disable`

Parameters

None

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf fast-reroute per-prefix candidate disable
```

ip ospf flood-reduction

Use this command to enable flood reduction on an interface. When this command is configured, an LSA sent out on the interface is set with the DNA bit in the LSA age field. The LSA is not refreshed every refresh interval if there is no change in LSA. Only changed LSAs are sent out on the interface

Use the `no` option with this command to disable flood reduction on an interface.

Command Syntax `ip ospf flood-reduction no ip ospf flood-reduction`

Parameters

None

Default

By default, flood reduction on an interface is disabled

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip ospf flood-reduction

(config-if)#no ip ospf flood-reduction
```

ip ospf hello-interval

Use this command to specify the interval between hello packets.

The hello-interval is advertised in the hello packets. Configure the same hello-interval for all routers on a specific network. A shorter hello interval ensures faster detection of topological changes but results in more routing traffic.

Use the `no` parameter with this command to return to the default time.

Command Syntax `ip ospf (A.B.C.D|) hello-interval <1-65535> no ip ospf (A.B.C.D|) hello-interval`

Parameters

`A.B.C.D` The IP address of the interface. `hello-interval`

Specify the interval.

`<1-65535>` Specify the interval in seconds.

Default

By default, hello interval is 10 seconds

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows setting the hello-interval for 3 seconds on interface eth0.

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf hello-interval 3
```

ip ospf multi-area

Use this command to enable multi-area adjacency on point-to-point network and other network types. Multi-area adjacency establishes adjacency between the Area Border Routers (ABRs). The interface of the ABR where this command is configured, shall be associated with multiple areas.

Use the `no` parameter to disable multi-area adjacency on the given interface on point-to-point network.

Command Syntax `ip ospf <0-65535> multi-area (A.B.C.D|<0-4294967295>)(neighbor A.B.C.D |) no ip ospf <0-65535> multi-area (A.B.C.D|<0-4294967295>)`

Parameters

`<0-65535>`	OSPF process ID.
`A.B.C.D`	OSPF area ID in IP address format.
`<0-4294967295>`	OSPF area ID as a decimal value. `A.B.C.D`
	Neighbor IP address.

Default

By default, multi-area adjacency is disabled

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#ip ospf 0 multi-area 1

(config-if)# no ip ospf 0 multi-area 1
```

ip ospf message-digest-key

Use this command to register an MD5 key for OSPF authentication.

Use the `no` parameter with this command to remove an MD5 key.

Message Digest Authentication is cryptographic authentication. A key (password) and key-id are configured on each router. The router uses an algorithm based on the OSPF packet, the key, and the key-id to generate a message digest that is appended to the packet.

Use this command for uninterrupted transitions between passwords. This is helpful for administrators who want to change the OSPF password without disrupting communication. The system begins a rollover process until all the neighbors have adopted the new password. This allows neighboring routers to continue communication while the network administrator is updating them with a new password. The router will stop sending duplicate packets once it detects that all of its neighbors have adopted the new password.

Maintain only one password per interface, removing the old password whenever you add a new one. This prevents the local system from continuing to communicate with the system that is using the old password. Removing the old password also reduces overhead during rollover. All neighboring routers on the same network must have the same password value to enable exchange of OSPF routing data.

Command Syntax `ip ospf (A.B.C.D|) message-digest-key <1-255> md5 LINE no ip ospf (A.B.C.D|) message-digest-key <1-255>`

Parameters

`A.B.C.D` IPv4 address of the interface.

`message-digest-key`

Specify a key ID.

`<1-255>` Specify a key ID. `md5`

Specify a key (password).

`LINE` Specify the OSPF password (1-16 characters).

Default

By default, MD5 key for OSPF authentication is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows OSPF authentication on the interface eth0 when IP address has not been specified.

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf authentication message-digest
(config-if)#ip ospf message-digest-key 1 md5 yourpass
```

The following example shows OSPF authentication on the interface eth0 for the IP address 1.1.1.1. (If the interface has two IP addresses assigned-- 1.1.1.1 & 2.2.2.2, OSPF authentication will be enabled only for the IP address 1.1.1.1)

```
(config)#interface eth0
(config-if)#ip ospf 1.1.1.1 authentication message-digest
(config-if)#ip ospf 1.1.1.1 message-digest-key 2 md5 yourpass
```

ip ospf mtu

Use this command to set MTU size for OSPF to construct packets based on this value. Whenever OSPF constructs packets, it uses interface MTU size as Maximum IP packet size. This command forces OSPF to use the specified value overriding the actual interface MTU size.

This command does not configure the MTU settings in the kernel. OSPF does not recognize MTU size changes made in the kernel until the MTU size is updated through this command. Use the `no` parameter with this command to return to the default value.

Command Syntax `ip ospf mtu <576-65535> no ip ospf mtu`

Parameters

`mtu` Specify an MTU size.

`<576-65535>` Specify an MTU size.

Default

By default, OSPF uses interface MTU derived from the kernel.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf mtu 1480
```

ip ospf mtu-ignore

Use this command to configure OSPF so that it does not check the MTU size during DD (Database Description) exchange.

Use the `no` form of this command to make OSPF check the MTU size during DD exchange.

Command syntax `ip ospf (A.B.C.D|) mtu-ignore no ip ospf (A.B.C.D|) mtu-ignore`

Parameters

`A.B.C.D` IP address of the interface.

Default

By default, during the DD exchange process, OSPF checks the MTU size described in DD packets received from its neighbor. If the MTU size does not match the interface MTU, the neighbor adjacency is not established. Using this command makes OSPF ignore this check and allows establishing of adjacency regardless of MTU size in the DD packet.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-router)#ip ospf mtu-ignore
```

ip ospf network

Use this command to set the OSPF network type.

Use the `no` parameter with this command to return to the default value.

Command Syntax `ip ospf network (broadcast|non-broadcast|point-to-multipoint|point-to-point) ip ospf network point-to-multipoint non-broadcast no ip ospf network`

Parameters `broadcast` Sets the network type to broadcast.

`non-broadcast` Sets the network type to NBMA.

`point-to-multipoint`

Sets the network type to point-to-multipoint.

`non-broadcast`

Sets the network type to NBMA.

`point-to-point` Sets the network type to point-to-point.

Default

By default, OSPF network type is broadcast

Command Mode interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows setting the network to `point-to-point` type on the `eth0` interface.

```
#configure terminal
(config)#interface eth0
```

```
(config-if)#ip ospf network point-to-point
```

ip ospf priority

Use this command to set the router priority to determine the designated router (DR) for the network.

A router with the higher router priority becomes the DR. If the priority is the same for two routers, the router with the higher router ID takes precedence.

Only routers with a nonzero priority value are eligible to become the designated or backup designated router. Configure router priority for broadcast or NBMA networks only and not for point-to-point networks.

Use the `no` parameter with this command to return to the default value.

Command Syntax `ip ospf (A.B.C.D|) priority <0-255> no ip ospf (A.B.C.D|) priority`

Parameters

`A.B.C.D`	The IP address of the interface.
`priority`	Specify the router priority of the interface.
`<0-255>`	Specify the router priority of the interface. The default value is 1.

Default

By default, ip ospf priority is 1

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows setting the OSPF priority value to 3 on the `eth0` interface.

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf priority 3
```

ip ospf retransmit-interval

Use this command to specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface.

After sending an LSA to a neighbor, the router keeps the LSA until it receives an acknowledgement. If the router does not receive an acknowledgement during the retransmit interval, it retransmits the LSA. Set the retransmission interval value conservatively to avoid needless retransmission. The interval should be greater than the expected round-trip delay between two routers.

Use the `no` parameter with this command to return to the default value.

Command Syntax `ip ospf (A.B.C.D|) retransmit-interval <5-65535> no ip ospf (A.B.C.D|) retransmit-interval`

Parameters

`A.B.C.D` The IPv4 address of the interface.

`retransmit-interval`

Specify the interval.

`<5-65535>` Specify the interval in seconds.

Default

By default, retransmit interval is 5 seconds

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows setting the `ospf retransmit interval` to 6 seconds on the eth0 interface.

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf retransmit-interval 6
```

ip ospf transmit-delay

Use this command to set the estimated time it takes to transmit a link-state-update packet on the interface.

The transmit delay value adds a specified time to the age field of an update. If the delay is not added, the time in which the LSA transmits over the link is not considered. This command is especially useful for low speed links. Add transmission and propagation delays when setting the transmit delay value.

Use the `no` parameter with this command to return to the default value.

Command Syntax `ip ospf (A.B.C.D|) transmit-delay <1-65535> no ip ospf (A.B.C.D|) transmit-delay`

Parameters

`A.B.C.D` The IPv4 address of the interface. `transmit-delay`

Specify the time to transmit a link-state update.

`<1-65535>` Specify the time in seconds to transmit a link-state update.

Default

By default, transmit delay is 1 second

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows setting the OSPF transmit delay time to 3 seconds on the `eth0` interface.

```
#configure terminal
(config)#interface eth0
(config-if)#ip ospf transmit-delay 3
```

log-adjacency-changes

Use this command for the router to send a SYSLOG message when an OSPF neighbor goes up or down.

Use `no` parameter of this command to stop sending SYSLOG message.

Command Syntax `log-adjacency-changes`

`(detail|)` `no log-adjacency-changes`

`(detail|)`

Parameters `detail` Sends a SYSLOG message for each state change, not just when a neighbor goes up or down.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#log-adjacency-changes
(config-router)#log-adjacency-changes detail
(config-router)#no log-adjacency-changes
(config-router)#no log-adjacency-changes detail
```

max-concurrent-dd

Use this command to limit the number of Database Descriptors (DD) that can be processed concurrently.

This command is useful when a router's performance is affected from simultaneously bringing up several OSPF adjacencies. This command limits the maximum number of DD exchanges that can occur concurrently per OSPF instance, thus allowing for all of the adjacencies to come up.

Use the `no` option with this command to remove the limit.

Command Syntax `max-concurrent-dd <1-65535> no max-concurrent-dd`

Parameters

`<1-65535>` Specify the number of DD processes.

Default

By default, max concurrent dd value is 64

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example set the `max-concurrent-dd` value to 4.

```
#configure terminal
(config)#router ospf 100
(config-router)#max-concurrent-dd 4
```

maximum-area

Use this command to configure the maximum number of OSPF areas.

Use the `no` parameter with this command to disable the limit.

Command Syntax `maximum-area <1-4294967294> no maximum-area`

Parameters

`<1-4294967294>` Specify the maximum number of OSPF areas.

Default

By default, ospf maximum area is 4294967294

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#maximum-area 5
```

neighbor

Use this command to configure OSPF routers interconnecting to NBMA (Non-Broadcast Multi-Access) networks. Include one neighbor entry for each known non-broadcast network neighbor. Configure the neighbor address on the primary address of the interface.

Use the `no` parameter with this command to remove a configuration.

Command Syntax `neighbor A.B.C.D neighbor A.B.C.D (priority <0-255>|poll-interval <1-2147483647>) no neighbor A.B.C.D`

`no neighbor A.B.C.D {priority (<0-255>|)|poll-interval (<1-2147483647>|)}`

Parameters

`A.B.C.D`	Specify the interface IP address of the neighbor.
`priority`	Specify the router priority of the non-broadcast neighbor associated with the specified IP address.This parameter does not apply to point-to-multipoint interfaces.
`<0-255>`	Specify the router priority value of the non-broadcast neighbor associated with the specified IP address.
`poll-interval`	The reduced rate at which routers continue to send hello packets when a neighboring router has become inactive.
`<1-2147483647>`	Dead neighbor polling interval in seconds. Set this value much larger than hello interval.

Default

The default priority is 0 and polling interval is 120 seconds.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

This example shows neighbor configured with a priority value and poll interval time.

```
#configure terminal
(config)#router ospf 100
(config-router)#neighbor 1.2.3.4 priority 1 poll-interval 90
```

network

Use this command to enable OSPF routing with a specified area ID (and optionally an instance ID) on interfaces with IP addresses that match the specified network address.

OSPF routing is enabled per IPv4 subnet basis. You define the network address using the prefix length or a subnet mask.

Use the `no` parameter with this command to disable OSPF routing on the interfaces.

Command Syntax

Network address defined using the prefix length:

```
network A.B.C.D/M area (A.B.C.D|<0-4294967295>) (instance-id <0-255>|) no
network A.B.C.D/M area (A.B.C.D|<0-4294967295>) (instance-id <0-255>|)
```

Network address defined using subnet mask:

```
network A.B.C.D A.B.C.D area (A.B.C.D|<0-4294967295>) (instance-id <0-255>|) no
network A.B.C.D A.B.C.D area (A.B.C.D|<0-4294967295>) (instance-id <0-255>|)
```

Parameters

`A.B.C.D/M`	IPv4 network address with prefix length.
`A.B.C.D`	IPv4 network address.
`A.B.C.D`	Subnet mask where the bits on left side are set to 1 to represent the network part and the bits on the right side are set to 0 to represent the host part.
`area`	OSPF area ID
`A.B.C.D`	OSPF area ID in IPv4 address format.
`<0-4294967295>`	OSPF area ID as a decimal value.
`instance-id`	Instance ID
`<0-255>`	Instance ID value.

Default

No network area is configured

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following the use of the `network` command with OSPF multiple-instance support disabled.

```
#configure terminal
(config-router)#network 10.0.0.0/8 area 3
(config-router)#network 10.0.0.0/8 area 1.1.1.1
```

The following shows the use of the `network` command with OSPF multiple-instance support enabled.

```
(config)#router ospf 100
(config-router)#network 10.0.0.0/8 area 3 instance-id 4
```

ospf abr-type

Use this command to set an OSPF Area Border Router (ABR) type.

Use the `no` parameter with this command to revert the ABR type to the default setting (`cisco`).

Specifying the ABR type allows better functioning in a multi-vendor environment. The ABR types are:

- Cisco (RFC 3509): A router is considered an ABR if it has more than one area actively attached and one of them is the backbone area.
- IBM (RFC 3509): A router is considered an ABR if it has more than one area actively attached and the backbone area is configured. In this case the configured backbone need not be actively connected.
- Standard (RFC 2328): A router is considered an ABR if it has more than one area actively attached to it.

Command Syntax `ospf abr-type (cisco|ibm|standard)`

`no ospf abr-type (cisco|ibm|standard|)`

Parameters `cisco` Specify an alternative ABR using Cisco implementation. This is the default ABR type.

`ibm` Specify an alternative ABR using IBM implementation. `standard` Specify a standard ABR.

Default

By default, ABR type is Cisco

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#ospf abr-type ibm
```

ospf flood-reduction

Use this command to Enable flood reduction on all OSPF interface. When this command is configured, an LSA sent out on the OSPF interface is set with the DNA bit in the LSA age field. If there is no change in LSA, it is not refreshed every refresh interval. LSAs are sent out on the interface only if there is a change in an LSA Use the `no` option with this command to disable flood reduction on all OSPF interfaces.

Command Syntax `ospf flood-reduction`

`no ospf flood-reduction`

Parameters

None

Default

By default, flood reduction on all OSPF interfaces is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#ospf flood-reduction

(config-router)#no ospf flood-reduction
```

ospf restart grace-period

Use this command to set the grace period for restarting the router.

If graceful restart is enabled, NSM is notified about the grace period. If the OSPF daemon unexpectedly shuts down, NSM sends this value to the OSPF daemon when it comes up again which uses this value to end the graceful state.

Use the `no` parameter with this command to revert to the default.

Command Syntax `ospf restart grace-period <1-1800> no ospf restart grace-period`

Parameters `grace-period` Specify the grace period.

`<1-1800>` Specify the grace period in seconds.

Default

The default grace period for restarting the OSPF router is 120 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
```

```
(config)#ospf restart grace-period 250
```

ospf restart helper

Use this command to configure the helper behavior for graceful restart.

Use the `no` parameter with this command to revert to default.

Command Syntax `ospf restart helper {only-reload|only-upgrade|max-grace-period <1-1800>} ospf restart helper never (router-id A.B.C.D|)`

`no ospf restart helper (never router-id (A.B.C.D | all) | max-grace-period|)`

Parameters `only-reload` Help only on software reloads.

`only-upgrade` Help only on software upgrades.

`max-grace-period`

Help only if received grace-period is less than this value.

`<1-1800>`

Help only if received grace-period is less than this value.

`never` Prevent the neighbor from entering helper mode.

`router-id` Neighbor to never to act as helper.

`A.B.C.D` Router ID of neighbor to never to act as helper. `all`

All neighbors to never to act as helper.

Default

By default, router behave as helper. To disable it as helper, `ospf restart helper never` command should be configured. `ospf restart helper max-grace-period` – Max-grace-period to function as helper. If not configured, value will be the grace-period in restarting node.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ospf restart helper never router-id 1.1.1.1

#configure terminal
(config)#ospf restart helper only-reload

#configure terminal
(config)#ospf restart helper only-reload max-grace-period 200

#configure terminal
(config)#no ospf restart helper never router-id all
```

ospf router-id

Use this command to specify a router ID for the OSPF process.

Configure each router with a unique router ID. In an OSPF router process which has active neighbors, a new router ID is used at the next reload or when you start the OSPF manually.

Use the `no` parameter with this command to force OSPF to use the previous router ID.

Command Syntax `ospf router-id A.B.C.D`

`router-id A.B.C.D`

`no ospf router-id no router-id (A.B.C.D|)`

Parameters

`A.B.C.D`	Specify the router ID in IPv4 address format.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows a specified router ID 2.3.4.5.

```
#configure terminal
(config)#router ospf 100
(config-router)#ospf router-id 2.3.4.5
```

overflow database

Use this command to limit the maximum number of LSAs that can be supported by the OSPF instance.

Use the `no` parameter with this command to have an unlimited number of LSAs.

Command Syntax `overflow database <0-4294967294> (hard|soft|)`

`no overflow database`

Parameters

`<0-4294967294>`	The maximum number of LSAs
`hard`	Shutdown occurs if the number of LSAs exceeds the specified value.

`soft` Warning message appears if the number of LSAs exceeds the specified value.

Default

No default value is specified. unlimited number of LSAs.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows setting the database overflow to 5 and shutting down in that event.

```
#configure terminal
(config)#router ospf 100
(config-router)#overflow database 5 hard
```

overflow database external

Use this command to limits the number of AS-external-LSAs a router can receive once it is in the wait state.

Use the `no` parameter with this command to revert to default.

Command Syntax `overflow database external <0-2147483647> <0-65535> no overflow database external`

Parameters

`<0-2147483647>` The maximum number of LSAs. This value should be the same on all routers in the AS.

`<0-65535>` The number of seconds the router waits before trying to exit the database overflow state. If this parameter is 0, the router exits the overflow state only after an explicit administrator command.

Default

The default OSPF exit overflow interval is 0 second and number of external LSDB limit is unlimited.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows setting the maximum number of LSAs to 5 and the time to recover from overflow state to be 3.

```
#configure terminal
(config)#router ospf 100
(config-router)#overflow database external 5 3
```

passive-interface

Use this command to suppress sending Hello packets on all interfaces or on a specified interface.

This command configures OSPF on simplex Ethernet interfaces. Since a simplex interface represents only one network segment between two devices, configure the transmitting interface as a passive interface. This ensures that OSPF does not send hello packets for the transmitting interface. Both the devices can see each other via the hello packet generated for the receiving interface.

Use the `no` form with this command to resume sending `hello` packets on all interfaces, or on a specified interface.

Command Syntax `passive-interface IFNAME`

```
passive-interface (IFNAME A.B.C.D |) no
passive-interface IFNAME no passive-
interface (IFNAME A.B.C.D |)
```

Parameters

`IFNAME` The name of the interface. `A.B.C.D`

IP address of the interface.

Default

The default OSPF exit overflow interval is 0 second and number of external LSDB limit is 100000.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#router ospf 100
(config-router)#passive-interface eth0
```

redistribute

This command redistributes routes from a routing protocol, static route, and kernel route into an OSPF routing table.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
redistribute (kernel|connected|static|rip|bgp|isis|ospf (<1-65535>|)) {metric <0-
  16777214>|metric-type (1|2)|?route-map WORD|tag <0-4294967295>} no
redistribute (kernel|connected|static|rip|bgp|isis|ospf (<1-65535>|))
  metric|metric-type|?route-map|tag}
```

Parameters

`kernel` Specify kernel routes.

`connected`	Specify connected routes.
`static`	Specify static routes.
`rip`	Specify RIP routes.
`bgp`	Specify BGP routes.
`isis`	Specify IS-IS routes.
`ospf`	Specify OSPF process.
`<1-65535>`	Specify an OSPF process ID to redistribute a particular OSPF instance into another OSPF instance. If not specified, this command redistribute OSPF instance with process ID 0.
`metric`	Specify the external metric.
`<0-16777214>`	Specify the external metric.
`metric-type`	Specify the external metric-type (see RFC 3101):
`1`	Set OSPF External Type 1 metrics.
`2`	Set OSPF External Type 2 metrics.
`route-map`	Specify a route map reference.
`WORD`	Specify name of the route-map.
`tag`	Tag value to use as a “match” value for controlling redistribution via route maps
`<0-4294967295>`	Specify the route tag.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#router ospf 100
(config-router)#redistribute bgp metric 12
```

The following example shows redistributing OSPF instance 2 into OSPF instance 1.

```
#configure terminal
(config)#router ospf 1
(config-router)#redistribute ospf 2
```

The following example shows redistributing OSPF instance `2` into OSPF instance `1`, with an external metric of `10`, metric type `1`, a route-map named `rmp1`, and an external route tag of `3`.

```
#configure terminal
(config)#router ospf 1
(config-router)#redistribute ospf 2 metric 10 metric-type 1 route-map rmp1 tag 3
```

restart ospf graceful

Use this command to restart OSPF gracefully.

After this command is executed, the router immediately shuts down. NSM is notified that OSPF has shut down gracefully. NSM preserves routes installed by OSPF until the grace period expires.

Command Syntax `restart ospf graceful (grace-period <1-1800>|)`

Parameters `grace-period` Specify a grace period.

`<1-1800>` Specify a grace period in seconds.

Default

No default value is specified

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#restart ospf graceful grace-period 200
```

router ospf

Use this command to enter router mode and to configure an OSPF routing process.

Specify the process ID to configure multiple instances of OSPF. When running a single instance of OSPF, you do not need to specify a process ID.

Use the `no` parameter with this command to terminate an OSPF routing process.

Command Syntax `router ospf`

```
router ospf <1-65535>

no router ospf no router
ospf <1-65535>
```

Parameters

`<1-65535>` Process ID; should be unique for each routing process.

Default

No routing process defined

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

This example shows the use of the `router ospf` command to enter router mode. Note the change in the prompt.

```
#configure terminal
(config)#router ospf 100
(config-router)#
```

show debugging ospf

Use this command to display the set OSPF debugging option.

Command Syntax `show debugging ospf`

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

This is a sample output from the `show debugging ospf` command. Some lines in this output wrap around, they might not wrap around in the actual display.

```
#show debugging ospf
OSPF debugging status:
  OSPF packet Link State Update debugging is on
  OSPF all events debugging is on
```

show ip ospf

Use this command to display general information about all OSPF routing processes.

Command Syntax `show ip ospf (<0-65535>|)`

Parameters

`<0-65535>`	The ID of the router process for which information will be displayed. If this parameter is specified, only the information for the specified routing process is displayed.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show ip ospf 1
 Routing Process "ospf 1" with ID 4.1.1.1
 Process uptime is 1 minute
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is
 disabled Supports only single TOS(TOS0) routes Supports opaque
 LSA
 Supports Graceful Restart
 This router is an ASBR (injecting external routing information)
 SPF schedule delay min 0 secs 500 msecs
 SPF schedule delay max 50 secs 0 msecs
 Refresh timer 10 secs
 Number of incomming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Initial LSA throttle delay 10 secs 0 msecs
 Minimum hold time for LSA throttle 20 secs 0 msecs
 Maximum wait time for LSA throttle 45 secs 0 msecs
 Minimum LSA arrival 1 secs 0 msecs
 Number of external LSA 5. Checksum 0x010632
 Number of opaque AS LSA 0. Checksum 0x000000    Number
of non-default external LSA 5
 External LSA database is unlimited.
 Number of LSA originated 6
 Number of  LSA  received  0   Number  of  areas
attached to this router: 1
    Area 0 (BACKBONE)
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 0
        Area has no authentication
        SPF algorithm last executed 00:00:47.558 ago
```

```
SPF algorithm executed 2 times
Number of LSA 1. Checksum 0x0041e0
```

OSPF Routing Process Fields

Table 1-117 explains the routing process fields.

Table 1-117: show ip ospf output details

Field	Description
Routing Process with ID	OSPF process identifier and router identifier.
Process is not up	OSPF process is not running.
Process uptime is	OSPF process running time.
Process bound to VRF	VRF name
Router is in Graceful Restart	When in graceful restart.
Router is in Restart Signaling	When in restart signalling.
Bidirectional Forwarding Detection is configured	When BFD is enabled.
Conforms to RFC2328, and RFC1583 Compatibility flag is enabled	RFC compatibility.
Supports only single TOS (TOS0) routes	OSPF TOS-based routing was never deployed.
Supports opaque LSA	When opaque LSAs are supported.
Do not support Restarting	When restart is not supported.
Supports Graceful Restart	Method of restart in process.
Supports Restart Signaling	Method of restart in signaling process.
Connected to MPLS VPN Super backbone	VRF is enabled and the process is connected to the MPLS VPN backbone.

This router is an ABR, ABR Type is	Type of ABR: Standard (RFC2328) Alternative Cisco (RFC3509) Alternative IBM (RFC3509) Alternative Shortcut
This router is an ASBR (injecting external routing information)	Type of router function in the process.
SPF schedule delay initial	Initial SPF schedule delay.
SPF schedule delay min	Minimum delay between receiving a change to SPF calculation.
SPF schedule delay max	Maximum delay between receiving a change to SPF calculation.
Refresh timer	LSA refresh interval.
Number of incoming current DD exchange neighbors	Incoming neighbor Database Descriptors and maximum concurrent DDs.

Table 1-117: show ip ospf output details (Continued)

Field	Description
Number of outgoing current DD exchange neighbors	Outgoing neighbor Database Descriptors and maximum concurrent DDs.
Initial LSA throttle delay	Initial delay for the generation of LSAs.
Minimum hold time for LSA throttle	Minimum hold time between generation of the same LSA.
Maximum wait time for LSA throttle	Maximum wait time between generation of the same LSA.
Minimum LSA arrival	Minimum time between reception of new LSAs during flooding.
Number of external LSA	Number of AS external LSAs and checksum.
Number of opaque AS LSA	Number of AS opaque LSAs and checksum.
Number of non-default external LSA	For database overflow, number of non-default external LSAs.
External LSA database is unlimited	When the external LSA database is unlimited.

External LSA database limit	Maximum number of LSAs in database.
Exit database overflow state interval is	Exit database overflow state interval.
Exit database overflow state interval is not configured	When the exit database overflow state interval is not set.
OSPF is [not] in database overflow state now	Whether OSPF is in database overflow state now.
Next attempt to exit database overflow state in	How long until OSPF tries to exit the database overflow state.
LSDB database overflow limit	Maximum number of LSAs that can be supported by the OSPF instance.
LSDB exceed overflow limit	Whether OSPF is exceeding the maximum number of LSAs.
Number of LSA originated	LSAs originated by the OSPF instance.
Number of LSA received	LSAs received by the OSPF instance.
Number of areas attached to this router	As stated
Next fields are repeated for each area	As stated
Area	Area identifier.
(BACKBONE)	Area is a backbone.
no-summary	Area is a stub and does no import summaries.
(Inactive)	Area is not active.
Number of interfaces in this area is	Number of interfaces in this area.
Number of fully adjacent neighbors in this area	As stated.
Number of fully adjacent virtual neighbors through this area	As stated.

Table 1-117: show ip ospf output details (Continued)

Field	**Description**

Area has no authentication	Area does not use authentication.
Area has simple password authentication	Area uses password authentication.
Area has message digest authentication	Area uses MD5 authentication.
SPF algorithm last executed	As stated.
SPF algorithm executed	As stated.
Number of LSA	Number of LSAs in area link-state database and checksum.
End of area field	As stated.
NSSA Translator Role is	candidate: Translate Type-7 LSAs to Type-5 if router is elected. never: Do not translate Type-7 LSAs to Type-5. always: Always translate Type-7 LSAs to Type-5.
NSSA Translator State is	disabled: Router is not a border router. enabled: Router is a border router. elected: Router has been elected to be an NSSA translator.
Stability Interval	If an elected translator determines its services are no longer required, how long it continues to perform its services.
Number of NSSA Translator Events	As stated.
Shortcutting mode	Shortcut ABR that installs inter-area routes through non-backbone areas if non-backbone paths are really better: Default Enabled Disabled
S-bit consensus	Whether other ABR agrees on S-bit: ok no
Dste Status	Whether DSTE is enabled or disabled.

show ip ospf border-routers

Use this command to display the ABRs and ASBRs for OSPF instances.

Command Syntax `show ip ospf (<0-65535>|) border-routers`

Parameters

`<0-65535>`	The ID of the router process for which information will be displayed.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

This is a sample output from the `show ip ospf border-routers` command.

```
#show ip ospf border-routers
OSPF process 1 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route i 10.15.0.1 [10] via 10.10.0.1,
eth0, ASBR, Area 0.0.0.0 i 172.16.10.1 [10] via 10.10.11.50, eth1, ABR, ASBR,
Area 0.0.0.0
```

Border Router Fields

Table 1-118 explains the border router fields.

Table 1-118: border router output details

Field	Description
Code	i: Intra-area route I: Inter-area route
Router ID	Router identifier of the destination
Cost	Cost of using this route.
via	Next hop IP address toward the destination.
is directly connected	Destination is directly connected.
Interface	Outgoing interface name.
Type	Router type of the destination: ABR or ASBR.
through Transit Area	Next hop is an area that carries traffic that neither originates nor terminates in the area itself.

Area	Area identifier from which this route was learned.
Transit	Area is a transit area.

show ip ospf database brief

Use this command to display a summary of the OSPF database.

Command Syntax `show ip ospf database (self-originate|max-age|adv-router A.B.C.D|) show ip ospf <0-65535> database(self-originate|max-age|adv-router A.B.C.D|)`

Parameters

`self-originate` Self-originated link states. `max-age` LSAs which have reached the maximum age (3600 seconds). `A.B.C.D` IPv4 address of the advertising router. `<0-65535>` ID of the router process

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Field	Description
Link ID	The meaning of this field depends on the type of Link-State Advertisement (LSA). Type 1: Router LSA (depends on the type of network to which the router connects): Point-to-point network: neighbor's router ID. Transit network: IP address of the designated router's interface. Stub network: IP network or subnet address Virtual link: Neighbor's Router ID. Type 2: Network LSA: The IP address of the designated router's interface. Type 3: Summary LSA: The IP address of the network or subnet being advertised.
ADV Router	The ID of the router advertising the LSA.
Age	The age of the LSA.
Seq#	The sequence number of the LSA. This number increments each time a new instance of the LSA originates. This update helps other routers identify the most recent instance of the LSA.
CkSum	The fetch checksum of the complete LSA except the Age field.

Link count	Total number of links.
Route	Summary prefix address.

Examples

```
#show ip ospf database
        OSPF Router process 100 withID (100.100.100.72)
                Router Link States (Area 0.0.0.0)
Link ID         ADV Router       Age  Seq#       CkSum  Link count
10.100.12.57       10.100.12.57        930   0x80000003  0x90de   2 100.100.100.72
100.100.100.72   933  0x80000004 0x7592  2
                Net Link States (Area 0.0.0.0)
Link ID         ADV Router       Age  Seq#       CkSum
10.100.10.72    100.100.100.72   933  0x80000001 0x0bef
                Summary Link States (Area 0.0.0.0)
Link ID         ADV Router       Age  Seq#       CkSum  Route
10.60.0.0       10.100.12.57     928  0x80000001 0x5108 10.60.0.0/24
71.87.120.0     10.100.12.57     928  0x80000001 0xc2c5 71.87.120.0/24  127.0.0.1
10.100.12.57     928  0x80000001 0x23fb 127.0.0.1/32
```

OSPF Database Fields

Table 1-119 explains the fields for each database entry.

Table 1-119: ospf database output details

show ip ospf database detail

Use this command to display details of the OSPF database.

Command Syntax

```
show ip ospf database (asbr-summary|external|network|router|summary|nssa-
    external|opaque-link|opaque-area|opaque-as) (self-originate|adv-router A.B.C.D|)
show ip ospf <0-65535> database (asbr-summary|external|network|router|summary)
  (self-originate|adv-router A.B.C.D|) show ip ospf database (asbr-
summary|external|network|router|summary|nssa-
  external|opaque-link|opaque-area|opaque-as) A.B.C.D (self-originate|adv-router
  A.B.C.D|) show ip ospf <0-65535> database (asbr-
summary|external|network|router|summary|nssa-
  external|opaque-link|opaque-area|opaque-as) A.B.C.D (self-originate|adv-router
  A.B.C.D|)
```

Parameters

`<0-65535>`	The ID of the router process for which information should be displayed.
`asbr-summary`	Type 4 ASBR summary LSAs.
`external`	Type 5 external LSAs.
`network`	Type 2 network LSAs.
`router`	Type 1 router LSAs.
`summary`	Type 3 summary LSAs.
`nssa-external`	Type 7 NSSA external LSAs.
`opaque-link`	Type 9 LSAs which are not flooded beyond the local network.
`opaque-area`	Type 10 LSAs which are not flooded beyond the borders of their area.
`opaque-as`	Type 11 LSAs which are flooded throughout the AS.
`A.B.C.D`	Link state ID as an IP address.
`self-originate`	Display self-originated link states.
`adv-router`	Advertising router link states.
`A.B.C.D`	IPv4 address of advertising router.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example: external and self-originate Parameters

This is sample output with the `external` and `self-originate` parameters.

```
#show ip ospf database external self-originate

 OSPF Router process 100 with ID (10.10.11.50)
```

```
 AS External Link States
  LS age: 298
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: AS-external-LSA
  Link State ID: 10.10.100.0 (External Network Number)
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x7033
  Length: 36
  Network Mask: /24
 Metric Type: 2 (Larger than any link state path)
 TOS: 0
 Metric: 20
 Forward Address: 10.10.11.50
 External Route Tag: 0
```

Example: opaque-as and self-originate Parameters

This is sample output with the `opaque-as` and `self-originate` parameters.

```
#show ip ospf database opaque-as self-originate
 OSPF Router process 100 with ID (10.10.11.50)
 AS-Global Opaque-LSA
  LS age: 325
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: AS-external Opaque-LSA
  Link State ID: 11.10.9.23 (AS-external Opaque-Type/ID)
  Opaque Type: 11
  Opaque ID: 657687
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0xb018
 Length: 25
```

Example: adv-router Parameter

This is a sample output with the `adv-router` parameter.

```
#show ip ospf database nssa-external adv-router 10.10.11.50 OSPF Router process
100 with ID (10.10.11.50)

 NSSA-external Link States (Area 0.0.0.0)
 NSSA-external Link States (Area 0.0.0.1 [NSSA])
  LS age: 78
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: AS-NSSA-LSA
  Link State ID: 0.0.0.0 (External Network Number For NSSA)
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0xc9b6
  Length: 36
  Network Mask: /0
 Metric Type: 2 (Larger than any link state path)
```

```
 TOS: 0
 Metric: 1
 NSSA: Forward Address: 0.0.0.0
OSPF Router process 100 with ID (10.10.11.50)
 NSSA-external Link States (Area 0.0.0.0)
 NSSA-external Link States (Area 0.0.0.1 [NSSA])
  LS age: 78
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: AS-NSSA-LSA
 Link State ID: 0.0.0.0 (External Network Number For NSSA)
```

Example: router and Link State ID Parameters

This is sample output with the `router` and link state ID parameters.

```
#show ip ospf database router 10.10.11.50
 OSPF Router process 100 with ID (10.10.11.50)
 Router Link States (Area 0.0.0.0)
  LS age: 878
  Options: 0x2 (*|-|-|-|-|-|E|-)
  Flags: 0x3 : ABR ASBR
  LS Type: router-LSA
  Link State ID: 10.10.11.50
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000004
  Checksum: 0xe39e
  Length: 36
Number of Links: 1
 Link connected to: Stub Network
 (Link ID) Network/subnet number: 10.10.10.0
 (Link Data) Network Mask: 255.255.255.0
Number of TOS metrics: 0
 TOS 0 Metric: 10
 Router Link States (Area 0.0.0.1)
  LS age: 877
  Options: 0x2 (*|-|-|-|-|-|E|-)
  Flags: 0x3 : ABR ASBR
  LS Type: router-LSA
  Link State ID: 10.10.11.50
  Advertising Router: 10.10.11.50
 LS Seq Number: 80000003
```

Example: adv-router Parameter

This is sample output using the `adv-router` parameter for flood reduction.

```
#show ip ospf database summary adv-router 10.10.11.50

 OSPF Router process 100 with ID (10.10.11.50)
 Summary Link States (Area 0.0.0.0)
  LS age: 1(DoNotAge)
  Options: 0x2 (*|-|-|-|-|-|E|-)
```

```
  LS Type: summary-LSA
  Link State ID: 10.10.11.0 (summary Network Number)
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x36ac
  Length: 28
  Network Mask: /24
 TOS: 0 Metric: 10
Summary Link States (Area 0.0.0.1)
  LS age: 989
  Options: 0x2 (*|-|-|-|-|-|E|-)
LS Type: summary-LSA
  Link State ID: 10.10.11.0 (summary Network Number)   Advertising Router:
10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x36ac
  Length: 28
  Network Mask: /24
 TOS: 0 Metric: 10

#show ip ospf database external self-originate

 OSPF Router process 100 with ID (10.10.11.50)

 AS External Link States
  LS age: 298
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: AS-external-LSA
  Link State ID: 10.10.100.0 (External Network Number)
  Advertising Router: 10.10.11.50
  LS Seq Number: 80000001
  Checksum: 0x7033
  Length: 36
  Network Mask: /24
 Metric Type: 2 (Larger than any link state path)
 TOS: 0
 Metric: 20
 Forward Address: 10.10.11.50
 External Route Tag: 0
```

Database Detail Header Fields

Table 1-120 explains the fields for each database entry.

Table 1-120: ospf database detail header fields

Field	Description

LS age	Age of the LSA in seconds. “Do Not Age” is displayed if the DNA bit is set.
Options	LSA options as explained in Table 1-121.
Flags	ABR: Area border router ASBR: AS boundary router VL-endpoint: Endpoint of an active virtual link that is using the described area as a transit area Shortcut: shortcut ABR NSSA-Translator: NSSA border router with NSSA Translate or State enabled
LS Type	Type of LSA: Router-LSA Network-LSA Summary-LSA ASBR-summary-LSA AS-external-LSA AS-NSSA-LSA Link-Local Opaque-LSA Area-Local Opaque-LSA AS-external Opaque-LSA

Table 1-120: ospf database detail header fields

Field	**Description**
Link State ID	Identifier of the router described by the LSA.
Opaque Type	Opaque type used to identify the application type of the LSA: 9: link-local scope 10: area-local scope 11: LSA flooded throughout the AS
Opaque ID	Identifier used to differentiate LSAs of the same type.
Advertising Router	Identifier of the router that originated the LSA.
LS Seq Number	Sequence number of the LSA. This number increments each time a new instance of the LSA originates. This update helps other routers identify the most recent instance of the LSA.
Checksum	Checksum of the entire LSA, except the LS age field.
Length	Length of the LSA
I LSA	Indication LSA: ASBR set the infinity metric to tell all routers in the backbone not to originate DNA LSAs.

OSPF LSA Option Bits

Table 1-121 explains the fields for each database entry.

Table 1-121: ospf LSA option bits output details

Bit	Description
DN	Used in MPLS-based L3 VPNs. When a route learned from a customer network via OSPF is advertised across a BGP/ MPLS VPN using Multiprotocol BGP and advertised back to a customer network via OSPF, a loop can happen where the OSPF route is redistributed back to the VPN service provider network via BGP. The DN-bit prevents this type of routing loop. When an OSPF router receives a Type 3, 5, or 7 LSA with the DN-bit set, it foes use that LSA for OSPF route calculations.
O	Originating router supports Type 9, 10, and 11 Opaque LSAs.
DC	Originating router supports OSPF over Demand Circuits.
L	Whether the OSPF packet contains a Link-Local Signaling (LLS) data block. This bit is set only in Hello and database description packets.
N/P	The N-bit is used only in Hello packets when the originating router supports Type-7 NSSA-External-LSAs. Neighboring routers with mismatched N-bit will not form a neighbor relationship. This restriction ensures that all OSPF routers within an area support NSSA capabilities. When the N-bit is set, the E-bit must be 0. The P-bit is used only in Type-7 NSSA-External-LSA headers. Due to this reason, the N- and P-bits share the same position in the options field. The P (Propagate) bit is set to inform an NSSA ABR to translate Type-7 LSAs into Type-5 LSAs.
MC	Originating router supports multicast extensions to OSPF (MOSPF)

Table 1-121: ospf LSA option bits output details (Continued)

Bit	Description
E	Originating router accepts AS External LSAs. The bit is set in all AS External LSAs and in all LSAs originated in the backbone and non-stub areas; and is be set to 0 in all Hellos and LSAs originated within a stub area. Additionally, this bit is used in Hello packets to indicate the capability of a router interface to send and receive Type-5 AS-External-LSAs. Neighboring routers with mismatched E-bit do not form a neighbor relationship. This restriction ensures that all OSPF routers within an area support the stub capabilities.
T	Originating router supports Multitopology OSPF (MT-OSPF.) Older OSPF specifications used this bit when the originating router support TOS-based routing. However, OSPF TOS-based routing was never deployed; therefore the Tbit was never used.

Type 1 Router LSAs (“router” Parameter)

Table 1-122 explains the fields for each database entry.

Table 1-122: router LSAs

Field	Description
Number of Links	Number of router links the LSA describes.
Link connected to	Description of the router link: another Router (point-to-point) a Transit Network Stub Network a Virtual Link
(Link ID)	Identifier of the router to which the link connects: Neighboring Router ID Designated Router address Network/subnet number Neighboring Router ID
(Link Data)	Extra information: Router Interface address Network Mask
Number of TOS metrics	Number of TOS (Type of Service) metrics for this link, not including the metric for TOS 0.
TOS 0 Metric	Cost of using this router link for TOS 0.

Type 2 Net Link States (“network” Parameter)

Table 1-123 explains the fields for each database entry.

Table 1-123: net LSAs

Field	Description
Network Mask	IP address mask for the network.
Attached Router	Identifiers of each router attached to the network.

Type 3 Summary LSAs (“summary” Parameter) and Type 4 ASBR Summary LSAs (“asbr-summary” Parameter) Table 1-124 explains the fields for each database entry.

Table 1-124: summary and ASBR summary link states

Field	Description

Network Mask	For Type 3 LSAs, the destination network's IP address mask. Not meaningful for Type 4 link state advertisements.
TOS: 0 Metric	Cost of using this router link for TOS 0.

Type 5 AS External LSAs (“external” Parameter)

Table 1-125 explains the fields for each database entry.

Table 1-125: external LSAs

Field	Description
Network Mask	IP address mask for the advertised destination
Metric Type	1: Type 1 external metric that is comparable directly (without translation) to the link state metric 2: Type 2 external metric that is considered larger than any link state path
TOS	Always zero.
Metric	The cost of this route.
Forward Address	Data traffic for the advertised destination is forwarded to this address.
External Route Tag	Custom field attached to each external route whose use is defined by the application.

Type 7 NSSA External Link States (“nssa-external” Parameter) Table 1-126 explains the fields for each database entry.

Table 1-126: NSSA external LSAs

Field	Description
Network Mask	IP address mask for the advertised destination
Metric Type	1: Type 1 external metric that is comparable directly (without translation) to the link state metric 2: Type 2 external metric that is considered larger than any link state path
Metric	The cost of this route.
NSSA: Forward Address	Data traffic for the advertised destination is forwarded to this address.

External Route Tag	Custom field attached to each external route whose use is defined by the application.

show ip ospf igp-shortcut-lsp

Use this command to show the IGP shortcut LSP used by OSPF.

Command Syntax `show ip ospf igp-shortcut-lsp`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip ospf igp-shortcut-lsp
Tunnel-endpoint      Tunnel-id     Tunnel-metric
           8.8.8.8              101           2              active
```

Table 1-127 explains the fields in the output.

Table 1-127: show ip ospf igp-shortcut-lsp output details

Field	Description
Tunnel-endpoint	Tunnel endpoint address of ospf.
Tunnel-id	Tunnel address (destination port) for the session.
Tunnel-metric	Number of tunnel-metric.
active/inactive	Whether the tunnel is active or inactive.

show ip ospf igp-shortcut-route

Use this command to show the IGP shortcut route calculated by OSPF.

Command Syntax `show ip ospf (<0-65535>|) igp-shortcut-route`

Parameters

`<0-65535>` ID of the router process.

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip ospf igp-shortcut-route
OSPF process 0:
8.8.8.8/32 [2] tunnel-id: 101, 8.8.8.8
15.15.15.15/32 [0] tunnel-id: 101, 8.8.8.8
20.20.15.0/24 [0] tunnel-id: 101, 8.8.8.8
```

Table 1-128 explains the fields in the output.

Table 1-128: show ip igp-shortcut-route output details

Field	Description
OSPF process	OSPF process identifier.
Destination	IP address of the destination port.
Metric	Number of tunnel metric.
Tunnel-ID	Tunnel address (destination port) for the session.
Tunnel-End-Point	Tunnel endpoint address of ospf.

show ip ospf interface

Use this command to display interface information for OSPF.

Command Syntax `show ip ospf interface (IFNAME|)`

Parameters

`IFNAME` Interface name.

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip ospf interface eth1 is up, line
protocol is up
 Internet Address 10.100.10.72/24, Area 0.0.0.0, MTU 1500
    Router ID 100.100.100.72, Network Type BROADCAST, Cost: 10, TE Metric
    0 Transmit Delay is 1 sec, State DR, Priority 1 LDP-OSPF Sync
    configured
    Holddown timer : 50 seconds, Remaining time =  30seconds
    Designated Router (ID) 100.100.100.72, Interface Address 10.100.10.72 Backup
    Designated Router (ID) 10.100.12.57, Interface Address 10.100.10.105 Timer
    intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:05
    Neighbor Count is 1, Adjacent neighbor count is
    1 Crypt Sequence Number is 0
    Hello received 19 sent 106, DD received 4 sent 3
    LS-Req received 1 sent 1, LS-Upd received 3 sent 3
    LS-Ack received 2 sent 3, Discarded 0
```

OSPF Interface Fields

Table 1-129 explains the fields for each interface entry.

Table 1-129: OSPF interface output details

Field	Description
Internet address	The IP address and subnet mask of the interface.
Area	The OSPF area to which the interface belongs.
MTU	The Maximum Transmission Unit (MTU) of the interface.
Transmit Delay	The transmit delay of the interface.

Table 1-129: OSPF interface output details

Field	Description
Priority	The OSPF priority of the interface used for election of Designated Router (DR) and Backup Designated Router (BDR).
Hello	The OSPF hello-interval.
Dead	The OSPF dead-interval.
Wait	The Hello wait-interval.

Retransmit	The period, in seconds, for which the router waits between retransmissions of OSPF packets that have not been acknowledged.
Hello due in	The time period for which router expects to receive hello packet.
Neighbor Count	The OSPF neighbor count.
Adjacent neighbor	The OSPF adjacent neighbor count.
Crypt Sequence Number	Used for authentication.
Hello received	Number of Hello packets and DD packets sent and received.
LS-Req	Number of LSA requests and LSA updates sent and received.
LS-Ack	Number of LSA acknowledgements sent and received number of LSA acknowledgement discards.

Example: DoNotAge

The following is sample output of this command when DoNotAge is enabled:

```
#show ip ospf interface eth1 eth1 is up, line
protocol is up
 Internet Address 1.1.1.1/24, Area 0.0.0.0, MTU 1500
 Process ID 0, Router ID 33.33.33.33, Network Type BROADCAST, Cost:
 10 Transmit Delay is 1 sec, State Waiting, Priority 1, TE Metric 0
 No designated router on this network
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
 5 Hello due in 00:00:02
 Neighbor Count is 0, Adjacent neighbor count is
 0 Crypt Sequence Number is 1106347721
 Hello received 0 sent 1, DD received 0 sent 0
 LS-Req received 0 sent 0, LS-Upd received 0 sent 0
 LS-Ack received 0 sent 0, Discarded 0
 Reduce LSA flooding
```

Example: Hello Suppression

The following is sample output of this command when Hello-Suppression is enabled:

```
#sh ip os interface p7p1 is up, line protocol is up
  Internet Address 14.1.1.2/24, Area 0.0.0.0, MTU 1500
  Process ID 1, VRF (default), Router ID 2.2.2.2, Network Type POINTOMULTIPOINT, Cost: 1
  Reduce LSA flooding.
  Transmit Delay is 1 sec,  State Point-To-Point, TE Metric 1
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    Hello due in 00:00:03
```

```
Neighbor Count is 1, Adjacent neighbor count is 1
Suppress hello for 1 neighbor(s)
Hello received 5 sent 8, DD received 8 sent 6
LS-Req received 2 sent 2, LS-Upd received 8 sent 9
LS-Ack received 6 sent 6, Discarded 0
No authentication
```

show ip ospf multi-area-adjacencies

Use this command to display multi-area adjacency information for OSPF.

Command Syntax `show ip ospf (<0-65535>|) multi-area-adjacencies`

Parameters

`<0-65535>`	The ID of the router process for which information should be displayed.

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following is a sample output of this command:

```
#show ip ospf 1 multi-area-adjacencies

Multi-area-adjacency on interface eth1 to neighbor 20.20.20.10
Internet Address 20.20.20.11/24, Area 0.0.0.1, MTU 1500
Process ID 1, Router ID 10.10.10.10, Network Type POINTOPOINT, Cost: 10
Transmit Delay is 1 sec, State Point-To-Point
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
 5 Hello due in 00:00:02
Neighbor Count is 0, Adjacent neighbor count is 0
Crypt Sequence Number is 1229928206
Hello received 0 sent 513, DD received 0 sent 0
LS-Req received 0 sent 0, LS-Upd received 0 sent 0
LS-Ack received 0 sent 0, Discarded 0
```

Table 1-130 explains the fields for each adjacency entry.

Table 1-130: show ip ospf multi-area-adjacencies output details

Field	Description
Multi-area-adjacency	Specifies the interface name and the router ID to which it is connected.
Internet Address	As Stated
Area	As Stated
MTU	Maximum Transmission Unit in bytes.

Process ID	The Process Identifier.
Router ID	As Stated
Network Type	In multi-area adjacencies, this is a point-to-point network with the neighbor.

Table 1-130: show ip ospf multi-area-adjacencies output details (Continued)

Field	Description
Cost	A reference bandwidth of 100 Mbps for cost calculation. The formula to calculate the cost is reference bandwidth divided by interface bandwidth.
Transmit Delay	A stated
State	As stated
Timer intervals configured	Hello timer = 10, Dead timer = 40, Wait timer = 40, Retransmit timer = 5
Hello due in	Countdown timer for a Hello message from the neighbor.
Neighbor Count	The number of neighbor.
Adjacent neighbor count	The number of neighbors participating in adjacencies.
Crypt Sequence Number	The 32-bit cryptographic sequence number appended on each OSPF protocol packet.
Hello received, sent	Hello packets sent and received.
DD received, sent	Database Description packets sent and received.
LS-Req received, sent	Link State Request packets sent and received.
LS-Upd received, sent	Link State Update packets sent and received.
LS-Ack received, sent, discarded	Link State Acknowledgement packets sent, received, or discarded.

show ip ospf neighbor

Use this command to display information about OSPF neighbors.

Command Syntax `show ip ospf (<0-65535>|) neighbor show ip ospf (<0-65535>|) neighbor all show ip ospf (<0-65535>|) neighbor interface A.B.C.D show ip ospf (<0-65535>|) neighbor A.B.C.D show ip ospf (<0-65535>|) neighbor A.B.C.D detail show ip ospf (<0-65535>|) neighbor detail show ip ospf (<0-65535>|) neighbor detail all`

Parameters

`<0-65535>`	The ID of the router process
`all`	Include downstatus neighbor
`A.B.C.D`	IPv4 address
`detail`	Details of neighbors

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip ospf neighbor

Total number of full neighbors: 3
OSPF process 1 VRF(default):
Neighbor ID      Pri   State       Dead Time   Address      Interface     Instance ID
1.1.1.1            1   Full/ -     inactive    14.1.1.1     p7p1                0
3.3.3.3            1   Full/ -     00:01:41    15.1.1.2     p8p1                0
3.3.3.3            1   Full/ -     inactive    15.1.1.2     VLINK0              0
```

OSPF Neighbor Fields

Table 1-131 explains the fields for each neighbor entry.

Table 1-131: OSPF neighbor output details

Field	Description
OSPF process	OSPF process identifier.
Neighbor ID	OSPF router identifier of the neighbor.

Table 1-131: OSPF neighbor output details

Field	Description

Pri	OSPF priority of the neighbor.
State	State of the OSPF neighbor: DependUpon: dummy state Down: no OSPF neighbors detected at this instant Attempt: in an NBMA environment, the router sends unicast hello packets every poll interval to the neighbor, from which hellos have not been received within the dead interval Init: hello packet received, but the receiving router's ID was not included in the hello packet 2-Way: bi-directional communication established between two routers ExStart: master and slave roles determined Exchange: database description packets (DBD) sent Loading: exchange of LSRs (link state request) and LSUs (link state update) packets Full: routers fully adjacent with each other.
Dead Time	If a new Hello is not received within this duration, the neighbor is declared dead.
Address	IP address of neighbor's interface attached to the network.
Interface	The interface attached to the network on which the neighbor is located.
Instance ID	Instance identifier for the session.

Example: Detail Parameter

This is sample output from the command when the `detail` parameter is specified:

```
#show ip ospf neighbor detail
 Neighbor 10.10.10.50, interface address
 10.10.10.50 In the area 0.0.0.0 via interface eth0
 Neighbor priority is 1, State is Full, 5 state changes
 DR is 10.10.10.50, BDR is 10.10.10.10
 Options is 0x42 (*|O|-|-|-|-|E|-)
 Dead timer due in 00:00:38
 Neighbor is up for 00:53:07
 Database Summary List 0
 Link State Request List 0
 Link State Retransmission List 0
 Crypt Sequence Number is 0
 Thread Inactivity Timer on
 Thread Database Description Retransmission off
```

OSPF Neighbor Detail Fields

Table 1-132 explains the fields for each neighbor detail entry.

Table 1-132: OSPF neighbor output detail

Field	Description
Neighbor	OSPF router identifier of the neighbor.
interface address	IP address of the neighbor interface.
In the area	Area and interface through which the OSPF neighbor is known.
Neighbor priority	OSPF priority of the neighbor.
State	OSPF state as explained in Table 1-131.
state changes	Number of state changes since the neighbor was created.
Hello is suppressed	Hello suppression is enabled.
Poll interval	Poll timer value.
DR is	Router ID of the designated router for the interface.
BDR is	Router ID of the backup designated router for the interface.
Options	LSA options as explained in Table 1-121.
LLS Options	LSDB Resynchronization (LR) Restart Signal (RS-bit) Whether link-local signalling (LLS) and out-of-band (OOB) link-state database resynchronization are performed for nonstop forwarding (NSF).
OOB-Resync in progress (receiver)/last OOBResync	Last successful OOB resynchronization with the NSF-capable neighbor. The router waits before taking a neighbor adjacency down if the OOB resynchronization has not taken place since the time a restart signal (Hello packet with RS-bit set) was received from the neighbor.
Dead timer due in	Expected time before declaring the neighbor dead.
Poll due in	Poll timer thread.
Neighbor is up for	Time since the neighbor went into the two-way state.

Database Summary List	Number of LSAs in the neighbor's database.
Link State Request List	Number of LSAs that need to be received from this neighbor to synchronize the neighbors' topological databases.
Link State Retransmission List	Number of advertisements flooded out an adjacency. To ensure flooding is reliable, advertisements are retransmitted until they are acknowledged.
Crypt Sequence Number is	MD5 cryptographic sequence number.
Thread Inactivity Timer	Off if hello suppression is enabled, on otherwise.
Thread Database Description Retransmission	Off if hello suppression is enabled, on otherwise.
Thread Link State Request Retransmission	Off if hello suppression is enabled, on otherwise.
Thread Link State Update Retransmission	Off if hello suppression is enabled, on otherwise.
Thread Poll Timer	Whether the poll timer thread is on.
Bidirectional Forwarding Detection is enabled	Status of BFD, enabled or disabled.

Example: Hello-Suppression Option

This is sample output from the command when the `detail` parameter is specified and Hello-Suppression is enabled:

```
#sh ip os neighbor detail
 Neighbor 1.1.1.1, interface address 14.1.1.1
    In the area 0.0.0.0 via interface p7p1
    Neighbor priority is 1, State is Full, 5 state
    changes Hello is suppressed
    DR is 0.0.0.0, BDR is 0.0.0.0
    Options is 0x62 (-|O|DC|-|-|-|E|-)
    Dead timer due in inactive
    Neighbor is up for 00:05:03
    Database Summary List 0
    Link State Request List 0
    Link State Retransmission List 0
    Crypt Sequence Number is 0
    Thread Inactivity Timer off
    Thread Database Description Retransmission off
    Thread Link State Request Retransmission off
    Thread Link State Update Retransmission off
```

show ip ospf route

Use this command to display the OSPF routing table.

Command Syntax `show ip ospf (<0-65535>|) route ( A.B.C.D |A.B.C.D/M |summary |)`

`show ip ospf (<0-65535>|) route ( A.B.C.D |A.B.C.D/M |summary | fast-reroute |)`

Parameters

`<0-65535>`	Router process identifier.
`A.B.C.D`	Single route.
`A.B.C.D/M`	Single exact match route.
`summary`	Route counts.
`fast-reroute`	Fast-reroute routes.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip ospf route OSPF
process 10:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
C 50.0.0.0/24 [10] is directly connected, eth1, Area 0.0.0.10
C 60.0.0.0/24 [10] is directly connected, eth3, Area 0.0.0.10
OSPF process 15:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
C 80.0.0.0/24 [1] is directly connected, eth4, Area 0.0.0.15 Header
```

Each entry in this table has a code preceding it indicating the source of the routing entry.

Table 1-133 explains the fields of route codes.

Table 1-133: route codes

Code	Meaning	Description
C	connected	Routes directly connected to the local device that were not distributed via IGP. The device inherently knows of these networks, so there is no need to learn about these from another device. Connected routes are preferred over routes for the same network learned from routing protocols.

O	OSPF	Modifiers: IA - OSPF inter area N1 - OSPF NSSA external type 1 N2 - OSPF NSSA external type 2 E1 - OSPF external type 1 E2 - OSPF external type 2
D	discard	An ABR or ASBR performing summarization installs a discard route in its routing table for the summarized network range to prevent routing loops where portions of the summarized network range do not have a more specific route in the RIB. External and internal discard route entries are installed by default. During route summarization, routing loops can happen if data sent to a nonexisting network appears to be a part of the summary, and the router doing the summarization has a less specific route that points back to the sending router for the network.

Route Entry Fields

Table 1-134 shows the route entry fields.

Table 1-134: route entry output details

Field	Description
Codes	As explained in Table 1-133.
IP address	IP address of the remote network.
Metric	For OSPF the metric is cost, which indicates the best quality path to use to forward packets.
Next hop router IP address	This route is available through the next hop router located at this IP address. This identifies exactly where packets go when they match this route.
Outgoing interface name	Interface used to get to the next-hop address for this route.
Area	OSPF area identifier

Example: Process Identifier

The following is a sample output with the process identifier parameter.

```
#show ip ospf 10 route
OSPF process 10:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
C 50.0.0.0/24 [10] is directly connected, eth1, Area 0.0.0.10
C 60.0.0.0/24 [10] is directly connected, eth3, Area 0.0.0.10
```

show ip ospf valid

Use this command to display information about opaque LSAs.

Command Syntax `show ip ospf (<0-65535>|) opaque-link valid`

Parameters

`<0-65535>`	The ID of the router process for which information will be displayed.
`opaque-link`	Displays information about the opaque link-local LSAs.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show ip ospf 1 opaque-link valid
```

show ip ospf virtual-links

Use this command to display virtual link information.

Command Syntax `show ip ospf (<0-65535>|) virtual-links (brief|)`

Parameters

`<0-65535>` The ID of the router process for which information will be displayed. `brief`

Display summary of OSPF virtual-links.

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following is the display of the virtual link information for two routers, one with the virtual link up and one with virtual link down.

```
ospfd#show ip ospf virtual-links
Virtual Link VLINK0 to router 10.10.0.9 is up
 Transit area 0.0.0.1 via interface eth0
 Transmit Delay is 1 sec, State Point-To-Point,
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:02
 Adjacency state Full
Virtual Link VLINK1 to router 10.10.0.123 is
 down Transit area 0.0.0.1 via interface *
 Transmit Delay is 1 sec, State Down,
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in inactive
 Adjacency state Down
```

The following is the display of the virtual link information for two routers, one with the virtual link up and one with virtual link down when flood reduction is enabled

```
ospfd#show ip ospf virtual-links
Virtual Link VLINK0 to router 10.10.0.9 is up
 Transit area 0.0.0.1 via interface eth0
 Transmit Delay is 1 sec, State Point-To-Point,
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:02
 Adjacency state Full
Virtual Link VLINK1 to router 10.10.0.123 is
 down Transit area 0.0.0.1 via interface *
 Transmit Delay is 1 sec, State Down,
```

```
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
 5 Hello due in inactive
 Adjacency state Down
DoNotAge LSA Allowed
```

If Hello-Suppression is enabled

```
M1#sh ip os virtual-links
Virtual Link VLINK0 to router 3.3.3.3 is up
  Transit area 0.0.0.1 via interface p8p1
  Hello suppression enabled
  DoNotAge LSA allowed
  Local address 15.1.1.1/32
  Remote address 15.1.1.2/32
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in inactive
  No authentication
    Adjacency state Full
M1#
```

Table 1-135 explains the fields for each virtual-links entry.

Table 1-135: show ip ospf virtual-links output details

Field	Description
Virtual Link	Virtual link name, the router ID to which it is connected, and the state of the link.
Transit area	Transit area ID, the interface it uses, and its instance ID – an Instance ID should default to 0. It is only necessary to assign a value other than 0 on those links that will contain multiple separate communities of OSPF routers.
Local address	The local IP address and subnet mask.
Remote address	The remote IP address and subnet mask.
Transmit Delay	The delay, in seconds, between link-state transmits. This value must be the same for all nodes on the network. The range is 0 to 65535. The default is 1. The state is point-to-point.
Timer intervals configured	The configured values in seconds of the following timers: Hello, Dead, Wait, Retransmit.
Hello due in	A countdown timer that indicates when the next Hello packet should arrive.
Adjacency State	Whether the adjacency state is either up or down.

show ip protocols

Use this command to display OSPF process parameters and statistics.

Command Syntax `show ip protocols show ip protocols ospf`

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

This is an example of the output from the `show ip protocols` command:

```
#show ip protocols
Routing Protocol is "ospf 200"
  Invalid after 0 seconds, hold down 0, flushed after 0
  Outgoing update filter list for all interfaces is
 Redistributed kernel filtered by filter1
  Incoming update filter list for all interfaces is   Redistributing: kernel
  Routing for Networks:
 192.30.30.0/24
 192.40.40.0/24
  Routing Information Sources:
 GatewayDistanceLast Update
  Distance: (default is 110)
 AddressMaskDistance List
```

Table 1-136 explains the fields for each ip protocol entry.

Table 1-136: show ip protocols output details

Field	Description
Routing Protocol is "ospf 200"	Specifies the routing protocol used.
Invalid after 0 seconds	Specifies the value of the invalid parameter.
Hold down 0	Specifies the current value of the hold-down parameter.

Flushed after 0	Specifies the time in seconds after which the individual routing information will be thrown (flushed) out.
Outgoing update	Specifies whether the outgoing filtering list has been set.

Table 1-136: show ip protocols output details

Field	Description
Incoming update	Specifies whether the incoming filtering list has been set.
Redistributing	Lists the protocol that is being redistributed.
Routing for Networks	Specifies the networks for which the routing process is currently injecting routes.
Routing Information Sources	Lists all the routing sources the Symanitron Networks software is using to build its routing table.

show ip route fast-reroute

Use this command to display routes with alternate next hops.

Command Syntax `show ip route fast-reroute`

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show ip route fast-reroute
```

shutdown

Use the this command to temporarily shut down a protocol in the least disruptive manner and to notify its neighbors that it is going away.

Use the no parameter of this command.

Command

Syntax

```
shutdown
no
shutdown
```

Parameters

None

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#shutdown

#configure terminal
(config)#router ospf 100
(config-router)#no shutdown
```

snmp restart ospf

Use this command restart SNMP in OSPF

Command Syntax `snmp restart ospf`

Parameter

None

Default

By default, SNMP resart is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#snmp restart ospf
```

summary-address

Use this command to summarize or suppress external routes with the specified address range.

Use the `no` option with this command to disable summary address.

An address range is a pairing of an address and a mask that is almost the same as IP network number. For example, if the specified address range is 192.168.0.0/255.255.240.0, it matches 192.168.1.0/24, 192.168.4.0/22, 192.168.8.128/ 25 and so on.

Redistributing routes from other protocols into OSPF requires the router to advertise each route individually in an external LSA. Use this command to advertise one summary route for all redistributed routes covered by a specified network address and mask. This minimizes the size of the OSPF link state database.

Command Syntax `summary-address (A.B.C.D/M | A.B.C.D A.B.C.D) (not-advertise|tag <0-4294967295>|) no summary-address (A.B.C.D/M | A.B.C.D A.B.C.D) (not-advertise|tag (<04294967295>|))`

Parameters

`A.B.C.D/M` The range of addresses given as IPv4 starting address and a mask.

`A.B.C.D` IP summary prefix e.g. i.i.i.i

`A.B.C.D` IP summary prefix mask e.g. m.m.m.m `not-advertise`

Suppress routes that match the range.

`tag` Tag value to use as a “match” value for controlling redistribution via route maps.

`<0-4294967295>`

Set a tag value.

Default

By default, tag value is 0

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example uses the `summary-address` command to aggregate external LSAs that match the network 172.16.0.0/24 and assign a tag value of 3.

```
#configure terminal
(config)#router ospf 100
(config-router)#summary-address 172.16.0.0/16 tag 3
```

timers lsa arrival

This command sets the minimum interval to accept the same link-state advertisement (LSA) from OSPF neighbors.

Use the `no` form of this command to restore the default value.

Command Syntax `timers lsa arrival <0-600000>` `no timers lsa arrival`

Parameters

`<0-600000>`	The minimum delay in milliseconds between accepting the same LSA from neighbors.

Default

By default, Minimum LSA Arrival timer is 1 sec.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#timers lsa arrival 5000
```

timers spf exp

Use this command to set the Shortest-Path First (SPF) best-path schedule minimum and maximum delay between receiving a change to SPF calculation in milliseconds.

Use no parameter of this command to unset the SPF best-path schedule.

Command Syntax `timers spf exp <0-2147483647> <0-2147483647>` `no timers spf exp`

Parameters

`<0-2147483647>`	The minimum delay in milliseconds between receiving a change to SPF calculation.
`<0-2147483647>`	The maximum delay in milliseconds between receiving a change to SPF calculation.

Default

Default minimum delay: 500 milliseconds

Default maximum delay: 50000 milliseconds (50 seconds)

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#timers spf exp 300 300
```

timers throttle lsa

This command sets the rate-limiting intervals for OSPF link-state advertisement (LSA) generation.

Use the `no` form of this command to restore the default values.

Command Syntax `timers throttle lsa all <0-600000> <1-600000> <1-600000> no timers throttle lsa all`

Parameters

`<0-600000>`	Start interval: The minimum delay in milliseconds for the generation of LSAs. The first instance of LSA is always generated immediately upon a local OSPF topology change. The generation of the next LSA is not before the start interval.
`<0-600000>`	Hold interval: The hold time in milliseconds. This value is used to calculate the subsequent rate limiting times for LSA generation.
`<0-600000>`	Maximum interval: The maximum wait time in milliseconds between generation of the same LSA.

Defaults

Default start interval: 0 milliseconds

Default hold interval: 5000 milliseconds

Default maximum interval: 5000 milliseconds

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#timers throttle lsa all 200 10000 45000
```

© Symanitron Proprietary

CHAPTER 2 OSPFv3 Commands

This chapter provides an alphabetized reference for each of the OSPFv3 commands. It includes the following commands:

- abr-type
- address-family ipv4 unicast
- area default-cost
- area nssa
- area range
- area stub
- area virtual-link
- auto-cost reference bandwidth
- capability cspf
- capability restart
- clear ipv6 ospf process
- debug ipv6 ospf
- debug ipv6 ospf bfd
- debug ipv6 ospf events
- debug ipv6 ospf ifsm
- debug ipv6 ospf lfa
- debug ipv6 ospf lsa
- debug ipv6 ospf nfsm
- debug ipv6 ospf nsm
- debug ipv6 ospf packet
- debug ipv6 ospf retransmission
- debug ipv6 ospf rib
- debug ipv6 ospf route
- default-information originate
- default-metric
- distance
- distribute-list
- enable db-summary-opt
- exit-address-family
- fast-reroute keep-all-paths
- fast-reroute tie-break
- ipv6 ospf dead-interval
- ipv6 ospf demand-circuit

- ipv6 ospf display route single-line
- ipv6 ospf link-lsa-suppression
- ipv6 ospf mtu-ignore
- ipv6 ospf neighbor
- ipv6 ospf network
- ipv6 ospf priority
- ipv6 ospf restart grace-period
- ipv6 ospf restart helper
- ipv6 ospf retransmit-interval
- ipv6 ospf transmit-delay
- ipv6 router ospf
- ipv6 te-metric
- max-concurrent-dd
- passive-interface
- redistribute
- restart ipv6 ospf graceful
- router-id
- router ipv6 ospf
- show debugging ipv6 ospf
- show ipv6 ospf
- show ipv6 ospf database
- show ipv6 ospf interface
- show ipv6 ospf neighbor
- show ipv6 ospf route
- show ipv6 route fast-reroute
- show ipv6 ospfv3 topology
- show ipv6 ospf virtual-links
- show ipv6 vrf
- snmp restart ospf6
- summary-address

abr-type

Use this command to set an OSPFv3 Area Border Router (ABR) type.

Use the `no` parameter with this command to revert the ABR type to the default setting (`cisco`).

Specifying the ABR type allows better functioning in a multi-vendor environment. The ABR types are:

- Cisco (RFC 3509): A router is considered an ABR if it has more than one area actively attached and one of them is the backbone area.

- IBM (RFC 3509): A router is considered an ABR if it has more than one area actively attached and the backbone area is configured. In this case the configured backbone need not be actively connected.
- Standard (RFC 2328): A router is considered an ABR if it has more than one area actively attached to it.

Command Syntax `abr-type (cisco|ibm|standard) no abr-type (cisco|ibm|standard|)`

Parameters `cisco` Specify an alternative ABR using Cisco implementation. This is the default ABR type.

`ibm` Specify an alternative ABR using IBM implementation. `standard` Specify a standard ABR.

Default

By default, ABR type is Cisco

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3 1.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#abr-type standard
```

address-family ipv4 unicast

Use this command to enter address family mode where you can configure IPv4 unicast addresses for OSPFv3, including:

- Summarizing intra-area IPv4 routes (area range command)
- Create a default external route (default-information originate command)
- Redistributing IPv4 routes (redistribute command)
- Summarizing IPv4 external routes (summary-address command)

RFC 5838 defines the range of instance IDs below to use for each address family in OSPFv3.

Instance ID#	Address Family
0-31	IPv6 unicast
64-95	IPv4 unicast

Multiple router processes can configured per interface, but only one instance per router per interface can be configured. Each instance ID creates a separate OSPFv3 instance with its own neighbor adjacencies, link state database, and SPF computation. A single IPv4 or IPv6 OSPFv3 process running multiple instances on the *same* interface is not supported.

To leave the address family mode and return to the configure mode, use the `exit-address-family` command.

Use the `no` form of this command to remove the address-family configuration.

Command Syntax

`address-family`

```
ipv4 unicast no address-family
```

Parameters

None

Default

By default, OSPFv3 supports only IPv6 unicast traffic.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#address-family ipv4 unicast
```

area default-cost

Use this command to specify the cost for default summary route sent into a stub area. If an area is configured as a stub, the OSPFv3 router originates one type-3 inter-area-prefix-LSA into the stub area. This command changes the metric for this LSA.

Use the `no` parameter with this command to remove the assigned default cost.

Command Syntax `area (A.B.C.D|<0-4294967295>) default-cost (<0-16777215>) no area (A.B.C.D|<0-4294967295>) default-cost (<0-16777215>|)`

Parameters

`A.B.C.D`	OSPF Area ID in IPv4 address format.
`<0-4294967295>`	OSPF Area ID as a decimal value.
`<0-16777215>`	The advertised cost for the default summary route used for a stub or NSSA area.

Default

By default, advertised cost for the default summary route is 1.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#area 1 default-cost 10
```

area nssa

Use this command to set an area as a Not-So-Stubby-Area (NSSA). There are no external routes in an OSPF stub area, so you cannot redistribute from another protocol into a stub area. An NSSA allows external routes to be flooded within the area. These routes are then leaked into other areas. However, the external routes from other areas still do not enter the NSSA. You can configure an area to be a stub area or an NSSA, but not both.

This command simplifies administration when connecting a central site using OSPF to a remote site that is using a different routing protocol. You can extend OSPF to cover the remote connection by defining the area between the central router and the remote router as a NSSA.

Use the `no` form of this command to make an area a normal area.

Command Syntax `area (A.B.C.D|<0-4294967295>) nssa area (A.B.C.D|<0-4294967295>) nssa {translator-role (candidate|always)|stabilityinterval <0-2147483647>|no-redistribution|default-information-originate (metric <0-16777214>|metric-type <1-2>|metric <0-16777214> metric-type <1-2>|metric-type`

```
  <1-2> metric <0-16777214>|)|no-summary} no area (A.B.C.D|<0-
4294967295>) nssa no area (A.B.C.D|<0-4294967295>) nssa {translator-
role|stability-interval|no-
  redistribution|default-information-originate|no-summary}
```

Parameters

`A.B.C.D` OSPF Area ID in IPv4 address format.

`<0-4294967295>` OSPF Area ID as a decimal value.

`translator-role`

NSSA-ABR translator role:

`candidate` Translate NSSA-LSA to Type-5 LSA if router is elected.

`always` Always translate NSSA-LSA to Type-5 LSA.

`stability-interval`

Stability timer for a NSSA area. If an elected translator determines its services are no longer required, it continues to perform its duties for this time interval. This minimizes excess flushing of translated Type-7 LSAs and provides a more stable translator transition.

`<0-4294967295>`

Stability interval in seconds.

`no-redistribution`

Do not redistribute into the NSSA.

`default-information-originate`

Originate Type-7 default LSA into the NSSA.

`metric` Specify metric for default routes.

`<0-16777214>`

Specify metric value.

`metric-type` Specify metric type (see RFC 3101).

`<1-2>` Specify metric type:

1: Type 1 external route 2: Type 2 external route

`no-summary` Do not inject inter-area routes into the NSSA.

`translate-candidate`

Translate NSSA-LSA to Type-5 LSA if router is elected.

`translate-always`

Always translate NSSA-LSA to Type-5 LSA.

Default

By default, the nssa option value is candidate.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#router ipv6 ospf
(config-router)#area 3 nssa translator-role candidate no-redistribution
default-information-originate metric 34 metric-type 2
```

area range

Use this command to configure the OSPF address range. This command summarizes intra-area routes for an area. The single summary route is then advertised to other areas by the Area Border Routers (ABRs). Routing information is condensed at area boundaries and outside the area. If the network numbers in an area are assigned in a way such that they are contiguous, the ABRs can be configured to advertise a summary route that covers all the individual networks within the area that fall into the specified range.

Use the `no` parameter with this command to remove the assigned area range.

Command Syntax `area (A.B.C.D|<0-4294967295>) range X:X::X:X/M area (A.B.C.D|<0-4294967295>) range A.B.C.D/M area (A.B.C.D|<0-4294967295>) range X:X::X:X/M (advertise|not-advertise) area (A.B.C.D|<0-4294967295>) range A.B.C.D/M (advertise|not-advertise) no area (A.B.C.D|<0-4294967295>) range X:X::X:X/M no area (A.B.C.D|<0-4294967295>) range A.B.C.D/M`

Parameters

`A.B.C.D` OSPF Area ID in IPv4 address format.

`<0-4294967295>` OSPF Area ID as a decimal value.

`X:X::X:X/M` The area IPv6 range prefix and length. `A.B.C.D/M`

The area IPv4 range prefix and length.

`advertise` Advertises this range. `not-advertise`

Does not advertise this range.

Default

No default value is specified

Command Mode

Router mode

Router address-family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
    #configure terminal
    (config)#router ipv6 ospf
    (config-router)#area 1 range 2000::/3

    #configure terminal
    (config)#router ipv6 ospf 10
    (config-router)#router-id 10.10.10.10
    (config-router)#address-family ipv4 unicast
    (config-router-af)#area 1 range 10.0.0.0/8
(config-router-af)#exit-address-family
```

area stub

Use this command to define an area as a stub area on all routers. There are two stub area router configuration commands: the `stub` and commands. In all routers attached to the stub area, configure the area by using the `stub` option of the area command. For an area border router (ABR) attached to the stub area, use the `area` command.

Use the `no` form of this command to make an area a normal area.

Command Syntax `area (A.B.C.D|<0-4294967295>) stub`

`area (A.B.C.D|<0-4294967295>) stub no-summary no area (A.B.C.D|<0-4294967295>) stub no area (A.B.C.D|<0-4294967295>) stub no-summary`

Parameters

`A.B.C.D` OSPF Area ID in IPv4 address format.

`<0-4294967295>` OSPF Area ID as a decimal value. `no-summary` Stops an ABR from sending summary link advertisements into the stub area.

Default

No stub area is defined.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#area 1 stub no-summary
```

area virtual-link

Use this command to configure a link between two backbone areas that are physically separated through other nonbackbone areas.

Use the `no` parameter with this command to remove the virtual link.

In OSPFv3, all non-backbone areas must be connected to a backbone area. If the connection to the backbone is lost, the virtual link repairs the connection.You can configure virtual links between any two backbone routers that have an interface to a common non-backbone area. The protocol treats these two routers joined by a virtual link as if they were connected by an unnumbered point-to-point network.

Configure the `hello-interval` to be the same for all routers attached to a common network. If the `hellointerval` is short, the router detects topological changes faster, but more routing traffic follows.

The `retransmit-interval` is the expected round-trip delay between any two routers in a network. Set the value to be greater than the expected round-trip delay to avoid needless retransmissions.

The `transmit-delay` is the time taken to transmit a link state update packet on the interface. Before transmission, the link state advertisements in the update packet are increased by this amount. Set the transmit-delay to be greater than zero. Also, take into account the transmission and propagation delays for the interface.

Command Syntax `area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D {fall-over bfd} area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D (dead-interval|hello-interval|retransmit-interval|transmit-delay) <1-65535>`

`area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D instance-id (<0-31>|<64-95>)`

`no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D {fall-over bfd} no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D (dead-interval|hello-interval|retransmit-interval|transmit-delay)`

`no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D instance-id`

Parameters

`A.B.C.D` OSPF Area ID in IP64 address format.

`<0-4294967295>` OSPF Area ID as a decimal value.

`A.B.C.D` Specify router ID associated with a virtual link neighbor.

`dead-interval` The interval in seconds during which no packets are received and after which the router acknowledges a neighboring router as off-line.

`hello-interval` The interval in seconds the router waits before it sends a hello packet.

`retransmit-interval`

The interval in seconds the router waits before it retransmits a packet.

`transmit-delay` The interval in seconds the router waits before it transmits a packet.

<1-65535> The timer interval. instance-id

The OSPFv3 instance.

<0-31> Interface instance ID for IPv6 unicast

<64-95> Interface instance ID for IPv4 unicast. fall-over bfd Fall-over Bidirectional Forwarding Detection (BFD).

Default

Default hello interval:10 seconds.

Default dead interval:40 seconds.

Default retransmit interval: 5 seconds.

Default transmit delay: 1 second

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#area 1 virtual-link 10.10.11.50 hello 5 dead 10
(config-router)#area 1 virtual-link 10.10.11.50 instance-id 1
(config-router)#area 1 virtual-link 10.10.11.50 fall-over bfd
```

auto-cost reference bandwidth

Use this command to control how OSPFv3 calculates default metrics for the interface.

By default, OSPFv3 calculates the OSPFv3 metric for an interface by dividing the reference bandwidth by the interface bandwidth. The auto-cost command is used to differentiate high bandwidth links. For multiple links with high bandwidth, specify a larger reference bandwidth value to differentiate cost on those links.

Use the `no` form of this command to assign cost based only on the interface bandwidth.

Command Syntax `auto-cost reference-bandwidth <1-4294967> no auto-cost reference-bandwidth`

Parameters

`<1-4294967>`	The reference bandwidth in Mbps per second.

Default

By default, reference bandwidth is 100Mbps

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

This example changes the reference bandwidth to 1Gbps to change the Fast Ethernet interface cost from 1 to 10.

```
#configure terminal
(config)#router ipv6 ospf 1
(config-router)#auto-cost reference-bandwidth 1000

(config)#router ipv6 ospf 1 (config-router)#no
auto-cost reference-bandwidth
```

capability cspf

Use this command to enable the CSPF (Constrained Shortest Path First) feature for an OSPFv2 or OSPFv3 instance.

Use the `no` parameter with this command to disable CSPF functionality for the OSPFv2 or OSPFv3 instance.

Command Syntax

```
capability cspf no
capability cspf
```

Parameters

None

Default

By default, capability cspf is enabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#no capability cspf
```

capability restart

Use this command to enable OSPFv3 graceful restart capability. If a router is not restart-enabled, it cannot enter graceful restart mode and act as a helper.

Use the `no` parameter with this command to disable the feature.

Command Syntax `capability restart`

```
graceful no capability restart
```

Parameter

None

Default

By default, capability restart graceful is enabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf 100
(config-router)#capability restart graceful

(config)#router ipv6 ospf 100
(config-router)#no capability restart
```

clear ipv6 ospf process

Use this command to clear and restart all OSPFv3 routing processes or a given OSPFv3 routing process.

Command Syntax `clear ipv6 ospf (WORD|) process`

Parameters

`WORD`	OSPFv3 process tag.

Command Mode

Privileged Exec Mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear ipv6 ospf Tag1 process
```

debug ipv6 ospf

Use this command to specify all debugging options for OSPFv3.

Use the `no` form of this command to disable the options.

Command Syntax `debug ipv6 ospf (all|bfd|events|ifsm|lsa|nfsm|nsm|packet|retransmission|rib|route|)`

`no debug ipv6 ospf (all|bfd|events|ifsm|lsa|nfsm|nsm|packet|retransmission|rib|route|) undebug ipv6 ospf (all|bfd|events|ifsm|lsa|nfsm|nsm|packet|rib|route) no debug all ipv6 ospf undebug all ipv6 ospf no debug all undebug all`

Parameters `all` Enables all debugging information.

`bfd` Debug OSPFv3 Bidirectional Forwarding Detection. (see debug ipv6 ospf bfd) `events` Debug OSPFv3 events (see debug ipv6 ospf events). `ifsm` Debug OSPFv3 Interface State Machines (see debug ipv6 ospf ifsm). `lsa` Debug OSPFv3 Link State Advertisements (see debug ipv6 ospf lsa). `nfsm` Debug OSPFv3 Neighbor State Machines (see debug ipv6 ospf nfsm). `nsm` Debug OSPFv3 NSM information (see debug ipv6 ospf nsm). `packet` Debug OSPFv3 packets (see debug ipv6 ospf packet). `retransmission` Debug OSPFv3 retransmission information. (see debug ipv6 ospf retransmission) `rib` Debug OSPFv3 Routing Information Base.(see debug ipv6 ospf rib) `route` Debug OSPFv3 route information (see debug ipv6 ospf route).

Command Mode

Privileged Exec and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#debug ipv6 ospf all
```

debug ipv6 ospf bfd

Use this command to specify the debugging options for OSPFv3 Bidirectional Forwarding Detection Use the `no` parameter with this command to disable this function.

Command Syntax `debug ipv6 ospf bfd no debug ipv6 ospf bfd undebug ipv6 ospf bfd`

Parameters

None

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#debug ipv6 ospf bfd
```

debug ipv6 ospf events

Use this command to display debug information related to OSPF internal events. Use this command without parameters to turn on all the options.

Use the `no` parameter with this command to disable this function.

Command Syntax `debug ipv6 ospf events {(abr|asbr|os|router|vlink|nssa)|}`

`no debug ipv6 ospf events {(abr|asbr|os|router|vlink|nssa)|}`

`undebug ipv6 ospf events {(abr|asbr|os|router|vlink|nssa)|}`

Parameters

`abr`	Debug ABR events
`asbr`	Debug ASBR events
`os`	Debug OS interaction events
`router`	Debug other router events
`vlink`	Debug virtual link events
`nssa`	Debug NSSA events

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#no debug ipv6 ospf events abr
#debug ipv6 ospf events asbr
```

debug ipv6 ospf ifsm

Use this command to specify debugging options for OSPFv3 Interface Finite State Machine (IFSM) troubleshooting.

Use the `no` parameter with this command to disable this function.

Command Syntax `debug ipv6 ospf ifsm ({events|status|timers}|)`

`no debug ipv6 ospf ifsm ({events|status|timers}|)`

`undebug ipv6 ospf ifsm ({events|status|timers}|)`

Parameters

`events`	Debug IFSM event information.
`status`	Debug IFSM status information.
`timers`	Debug IFSM timer information.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#debug ipv6 ospf ifsm status
```

debug ipv6 ospf lfa

Use this command to specify the debugging options for OSPFv3 Loop-free Alternate path Use the `no` parameter with this command to disable this function.

Command Syntax `debug ipv6 ospf lfa no debug ipv6 ospf lfa`

Parameters

None

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#debug ipv6 ospf lfa
```

debug ipv6 ospf lsa

Use this command to specify the debugging options for OSPFv3 Link State Advertisements (LSAs).

Use the `no` parameter with this command to disable this function.

Command Syntax `debug ipv6 ospf lsa {(generate|flooding|install|maxage|refresh)|} no debug ipv6 ospf lsa {(generate|flooding|install|maxage|refresh)|} undebug ipv6 ospf lsa {(generate|flooding|install|maxage|refresh)|}`

Parameters

`generate`	Debug LSA generation.
`flooding`	Debug LSA flooding.
`install`	Debug LSA installation.
`maxage`	Debug the maximum age processing.
`refresh`	Debug LSA refresh.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#debug ipv6 ospf lsa
```

debug ipv6 ospf nfsm

Use this command to specify debugging options for OSPFv3 Neighbor Finite State Machines (NFSMs).

Use the `no` parameter with this command to disable this function.

Command Syntax `debug ipv6 ospf nfsm {(events|status|timers)|} no debug ipv6 ospf nfsm {(events|status|timers)|} undebug ipv6 ospf nfsm {(events|status|timers)|}`

Parameters

`events`	Debug NFSM event information.
`status`	Debug NFSM status information.
`timers`	Debug NFSM timer information.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#debug ipv6 ospf nfsm events
#no debug ipv6 ospf nfsm timers
```

debug ipv6 ospf nsm

Use this command to specify the debugging options for OSPFv3 NSM information.

Use the `no` parameter with this command to disable this function.

Command Syntax `debug ipv6 ospf nsm {(interface|redistribute)|} no debug ipv6 ospf nsm {(interface|redistribute)|} undebug ipv6 ospf nsm {(interface|redistribute)|}`

Parameters `redistribute` Debug redistribute. `interface` Debug the NSM interface.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#debug ipv6 ospf nsm interface
```

debug ipv6 ospf packet

Use this command to specify the packet debugging options for OSPFv3 information.

Use the `no` parameter with this command to disable this function.

Command Syntax `debug ipv6 ospf packet ({hello|dd|ls-request|ls-update|ls-ack|send|recv|detail}|)`

```
no debug ipv6 ospf packet ({hello|dd|ls-request|ls-update|ls-ack|send|recv|
  detail}|)
undebug ipv6 ospf packet ({hello|dd|ls-request|ls-update|ls-ack|send|recv|detail}|)
```

Parameters

`hello`	Debug OSPFv3 hello.
`dd`	Debug OSPFv3 database description.
`ls-request`	Debug OSPFv3 link state request.
`ls-update`	Debug OSPFv3 link state update.
`ls-ack`	Debug OSPFv3 link state acknowledgment.
`send`	Debug packets sent
`recv`	Debug packets received.
`detail`	Debug detail information.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#debug ipv6 ospf packet ls-request
```

debug ipv6 ospf retransmission

Use this command to specify the debugging options for OSPFv3 retransmission information.

Use the `no` parameter with this command to disable this function.

Command Syntax `debug ipv6 ospf retransmission no debug ipv6 ospf retransmission`

Parameters

None

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#debug ipv6 ospf retransmission
```

debug ipv6 ospf rib

Use this command to specify the debugging options for OSPFv3 RIB information.

Use the `no` parameter with this command to disable this function.

Command Syntax `debug ipv6 ospf rib {(interface|redistribute)|}`

`no debug ipv6 ospf rib {(interface|redistribute)|} undebug ipv6 ospf rib {(interface|redistribute)|}`

Parameters `redistribute` Debug redistribute. `interface` Debug the NSM interface.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#debug ipv6 ospf rib interface
```

debug ipv6 ospf route

Use this command to specify which route calculation to debug. Use this command without parameters to turn on all the options.

Use the `no` parameter with this command to disable this function.

Command Syntax `debug ipv6 ospf route {(ase|ia|install|spf)|} no debug ipv6 ospf route {(ase|ia|install|spf)|} undebug ipv6 ospf route {(ase|ia|install|spf)|}`

Parameters

`ase`	Debug external route calculations.
`ia`	Debug inter-area route calculations.
`install`	Debug the route installation.
`spf`	Debug the SPF calculation.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#no debug ipv6 ospf route
#debug ipv6 ospf route ia
```

default-information originate

Use this command to create a default external route into an OSPF routing domain.

The system acts like an Autonomous System Boundary Router (ASBR) when you use the `default-information originate` command to redistribute routes into an OSPF routing domain. An ASBR does not by default generate a default route into the OSPF routing domain.

When you give the `default-information originate` command, also specify a `route-map` to avoid a dependency on the default network in the routing table.

Use the `no` parameter with this command to disable this feature.

Command Syntax `default-information originate`

`default-information originate {metric <0-16777214>|metric-type (1|2)|route-map WORD|always}`

`no default-information originate`

`no default-information originate {metric|metric-type|route-map|always}`

Parameters `always` Used to advertise the default route regardless of whether there is a default route.

`metric <0-16777214>` Sets the OSPF metric used in creating the default route. Sets the OSPF metric used in creating the default route. The value used is specific to the protocol.

`metric-type` The external link type associated with the default route advertised into the OSPF routing domain (see RFC 3101).

`1` Sets OSPF External Type 1 metric.

`2` Sets OSPF External Type 2 metric (default).

`route-map` Route map.

`WORD` Specify the name of route map.

Default

Sets the OSPF metric used in creating the default route. The default metric value is 10. The value used is specific to the protocol. metric-type The external link type associated with the default route advertised into the OSPF routing domain (see RFC 3101).

By default, 2 sets OSPF External Type 2 metric

Command Mode

Router mode

Router address-family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#default-information originate always metric 23 metric-type
2 route-map myinfo

(config)#router ipv6 ospf
(config-router)#no default-information originate metric metric-type route-map
```

default-metric

Use this command to set a default metric for OSPF.

A default metric facilitates redistributing routes with incompatible metrics. If the metrics do not convert, the default metric provides an alternative. Use this command to use the same metric value for all redistributed routes. Use this command in conjunction with the redistribute command.

Use the `no` parameter with this command to return to the default state.

Command Syntax `default-metric <1-16777214> no default-metric`

`no default-metric <1-16777214>`

Parameter

`<1-16777214>` Default metric value.

Default

Built-in, automatic metric translations, as appropriate for each routing protocol.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#default-metric 100
```

distance

Use this command to define OSPFv3 route administrative distances based on route type. This command sets the distance for an entire group of routes rather than a specific route that passes an access list.

The administrative distance rates the trustworthiness of a routing information source. A higher distance value means a lower trust rating. For example, an administrative distance of 254 means that the routing information source cannot be trusted and should be ignored.

Use the `no` form of this command to restore the default value.

Command Syntax `distance <1-254> distance ospfv3 {intra-area <1-254>|inter-area <1-254>|external <1-254>} no distance (<1-254>|) no distance ospfv3`

Parameters

`<1-254>` Used alone, this parameter specifies a default administrative distance used when no other specification exists for a routing information source.

intra-area	Routes within an area.
<1-254>	Distance for all routes within an area
inter-area	Routes from one area to another area.
<1-254>	Distance for all routes from one area to another area.
external	Routes from other routing domains learned by redistribution.
<1-254>	Distance for routes from other routing domains learned by redistribution.

Default

By default, distance value for each type of route is 110

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router ipv6 ospf 100
(config-router)#distance ospfv3 inter-area 20 intra-area 10 external 40
```

distribute-list

Use this command to filter networks in routing updates. This command redistributes other routing protocols into the OSPF routing table.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
distribute-list WORD out ((kernel|connected|static|rip|bgp|isis|ospf (WORD|<1-
  65535>|))) distribute-list WORD in no distribute-list WORD out
((kernel|connected|static|rip|bgp|isis|ospf (WORD|<1-
  65535>|)))   no   distribute-
list WORD in
```

Parameters

WORD	Specify the name of the access list.
in	Filter incoming routing updates.
out	Filter outgoing routing updates.
kernel	Specify kernel routes.
connected	Specify connected routes.
static	Specify static routes.
rip	Specify RIP routes.
bgp	Specify BGP routes.
isis	Specify IS-IS routes.

`ospf`	Specify OSPF routes.
`WORD`	Specify the OSPF process tag. If not specified, redistribute OSPF process with tag "null".
`<1-65535>`	Specify OSPF process ID <1-65535>. If not specified, redistribute OSPF instance with process ID 0.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows the distribution of BGP routing updates based on the access list `list1` (network 172.10.0.0).

```
    #configure terminal
    (config)#access-list list1 permit 172.10.0.0/16
(config)#router ipv6 ospf 100 (config-
router)#distribute-list list1 out bgp (config-
router)#redistribute bgp
```

enable db-summary-opt

Use this command to enable the database summary list optimization for OSPFv3.

When this feature is enabled, the database exchange process is optimized by removing the LSA from the database summary list for the neighbor if the LSA instance in the summary list is the same as or less recent than the LSA in the database description packet received from the neighbor.

Use the `no` form of the command to disable database summary list optimization.

Command Syntax `enable db-summary-opt no enable db-summary-opt`

Parameters

None

Default

By default, db summary opt is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#enable db-summary-opt
(config-router)#no enable db-summary-opt
```

fast-reroute keep-all-paths

Use this command to enable fast rerouting on all OSPFv3 interfaces.

Use the `no` parameter with this command to disable fast rerouting.

Command Syntax `fast-reroute keep-all-paths no fast-reroute keep-all-paths`

Parameters

None

Defaults

By default, fast rerouting is disabled.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf 200
                    (config-router)#fast-reroute keep-all-paths
```

fast-reroute tie-break

Use this command to set the tie-breaking policy for selecting a fast reroute repair path. You assign a priority to each type of repair path.

Use the `no` parameter with this command to set the tie-breaking policy for a specific type of repair path to its default priority. To set all types of repair paths to their default priorities, do not specify a repair path with the `no` form of this command.

Command Syntax

```
 fast-reroute tie-break (primary-path|interface-disjoint|node-protecting|broadcast-
interface-disjoint) index <1-4>

no fast-reroute tie-break (primary-path|interface-disjoint|node-
protecting|broadcast-interface-disjoint) index <1-4>

no fast-reroute tie-break
```

Parameters

`primary-path` When there are multiple loop-free alternate paths. The primary path is selected for an frr if it is node-protecting as well as link-protecting

`interface-disjoint`

Do not select point-to-point interfaces that have no alternate next hop for rerouting if the primary gateway fails, thus protecting the interface.

`node-protecting`

Bypass the `primary-path` gateway router which might not protect the router that is the next hop in the primary path.

`broadcast-interface-disjoint`

Do not use the interface if connected to a broadcast network. Repair paths protect links when a repair path and a protected primary path use *different* next-hop interfaces. However, on broadcast interfaces, if the repair path is computed via the same interface as the primary path, but their next-hop gateways are different, the router is protected but the link might not be.

`index` Tie break priority. A lower value has higher preference.

`<1-4>` Range of priority values.

Defaults

The default priority scheme is:

1. primary-path
2. interface-disjoint
3. node-protecting
4. broadcast-interface-disjoint

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf 200
                    (config-router)#fast-reroute tie-break interface-disjoint index 1
```

exit-address-family

Use this command to exit address-family mode and return to router mode.

Command Syntax `exit-address-family`

Parameters

None

Default

By default, exit address family is disabled

Command Mode

Router address-family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config) # router ipv6 ospf 10
(config-router) # router-id 10.10.10.10
(config-router) # address-family ipv4 unicast
(config-router-af) # area 1 range 10.0.0.0/8
(config-router-af) # exit-address-family
```

ipv6 ospf cost

Use this command to specify the link-cost described in LSAs.

The cost (or metric) of an interface in OSPF indicates the overhead required to send packets across a certain interface. The value is taken to describe Link State information, and used for route calculation.

Use the `no` parameter with this command to reset the cost to default.

Command Syntax `ipv6 ospf cost <1-65535> ipv6 ospf cost <1-65535> instance-id (<0-31>|<64-95>) no ipv6 ospf cost`

`no ipv6 ospf cost instance-id (<0-31>|<64-95>)`

Parameters `cost` Specify the link-state metric.

`<1-65535>` Specify the link-state metric.

`instance-id` Specify the instance.

`<0-31>` Interface instance ID for IPv6 unicast `<64-95>`

Interface instance ID for IPv4 unicast.

Default

By default, ipv6 cost value is 10.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 ospf cost 20 instance-id 1
```

ipv6 ospf dead-interval

Use this command to set the amount of time that the router waits to receive an OSPF hello packet from the neighbor before declaring the neighbor down.

The dead interval is advertised in hello packets. OSPF compares the dead interval in a received packet to the dead interval configured for the receiving interface. If the intervals do not match, the hello packet is discarded.

Use the `no` parameter with this command to reset the interval to default.

Command Syntax `ipv6 ospf dead-interval <1-65535> ipv6 ospf dead-interval <1-65535> instance-id (<0-31>|<64-95>) no ipv6 ospf dead-interval`

```
no ipv6 ospf dead-interval instance-id (<0-31>|<64-95>)
```

Parameters `dead-interval` Specify the interval.

`<1-65535>` Specify the interval in seconds.

`instance-id` Specify the instance.

`<0-31>` Interface instance ID for IPv6 unicast `<64-95>` Interface instance ID for IPv4 unicast.

Default

By default, dead interval is 40 seconds

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 ospf dead-interval 20
```

ipv6 ospf demand-circuit

Use this command to enable Hello Suppression and LSA Suppression sent on OSPFv3 interface

Note: Hello's and LSA's will be suppressed on Point-to-point and Point-to-multipoint links and only LSA's will be suppressed for Broadcast link

Use the `no` parameter with this command to disable Hello Suppression and LSA Suppression.

Command Syntax `ipv6 ospf demand-circuit (instance-id (<0-31>|<64-95>)) no ipv6 ospf demand-circuit (instance-id (<0-31>|<64-95>))`

Parameters `instance-id` Specify the instance.

`<0-31>` Interface instance ID for IPv6 unicast `<64-95>` Interface instance ID for IPv4 unicast.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#ipv6 ospf demand-circuit

(config-if)#no ipv6 ospf demand-circuit
```

ipv6 ospf display route single-line

Use this command to display the output of the show ipv6 ospf route command with each route entry in a single-line.

Use the `no` parameter with this command to display the output with each route entry in a multiple lines.

Command Syntax `ipv6 ospf display route single-line no ipv6 ospf display route single-line`

Parameters

None

Default

By default, show ipv6 ospf route displays routes in multiple lines

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ipv6 ospf display route single-line
```

ipv6 ospf hello-interval

Use this command to specify the interval between `hello` packets.

The hello interval is advertised in the hello packets. An OSPF router compares the hello interval in a received packet to the interval configured for the receiving interface. If this interval does not match, the hello packet is discarded. A shorter hello interval ensures faster detection of topological changes, but results in more routing traffic.

Use the `no` parameter with this command to reset the interval to default.

Command Syntax `ipv6 ospf hello-interval <1-65535> ipv6 ospf hello-interval <1-65535> instance-id (<0-31>|<64-95>) no ipv6 ospf hello-interval`

```
no ipv6 ospf hello-interval instance-id (<0-31>|<64-95>)
```

Parameters `hello-interval` Specify the interval.

`<1-65535>` Specify the interval in seconds.

`instance-id` Specify the instance.

`<0-31>` Interface instance ID for IPv6 unicast `<64-95>`

Interface instance ID for IPv4 unicast.

Default

By default, hello interval is 10 seconds

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 ospf hello-interval 5 instance-id 1
```

ipv6 ospf link-lsa-suppression

Use this command to enable or disable link LSA (type 8) suppression. A type 8 LSA gives information about link-local addresses and a list of IPv6 addresses on the link.

If enabled and the interface type is *not* broadcast or NBMA, the router does not send type 8 link LSAs. This implies that other routers on the link determine the router's next-hop address using a mechanism other than the type 8 link LSA. This feature is implicitly disabled if the interface type is broadcast or NBMA.

Command Syntax `ipv6 ospf link-lsa-suppression (enable|disable)`

`ipv6 ospf link-lsa-suppression (enable|disable) instance-id (<0-31>|<64-95>)`

Parameters

`enable`	Enable type 8 link LSA suppression
`disable`	Disable type 8 link LSA suppression (default).
`<0-31>`	Interface instance ID for IPv6 unicast
`<64-95>`	Interface instance ID for IPv4 unicast.

Default

By default, type 8 link LSA suppression is disabled

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 ospf link-lsa-suppression enable
```

ipv6 ospf mtu-ignore

Use this command to configure OSPF so that it does not check the MTU size during DD (Database Description) exchange.

Use the `no` form of this command to make OSPF check the MTU size during DD exchange.

Command syntax `ipv6 ospf mtu-ignore ipv6 ospf mtu-ignore instance-id (<0-31>|<64-95>) no ipv6 ospf mtu-ignore`

```
no ipv6 ospf mtu-ignore instance-id (<0-31>|<64-95>)
```

Parameters

`<0-31>`	Interface instance ID for IPv6 unicast
`<64-95>`	Interface instance ID for IPv4 unicast.

Default

By default, during the DD exchange process, OSPF checks the MTU size described in DD packets received from its neighbor. If the MTU size does not match the interface MTU, the neighbor adjacency is not established. Using this command makes OSPF ignore this check and allows establishing of adjacency regardless of MTU size in the DD packet.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#interface eth1
(config-if)#ipv6 ospf mtu-ignore
```

ipv6 ospf neighbor

Use this command to connect OSPFv3 routers to non-broadcast multi-access (NBMA) networks.

One neighbor entry must be included for each known NBMA neighbor. The neighbor address must be a link-local address.

Note: For point-to-multipoint interfaces, the `cost` parameter is the only applicable option.

Use the `no` parameter with this command to remove a configuration.

Command Syntax `ipv6 ospf neighbor X:X::X:X (instance-id (<0-31>|<64-95>)|) ipv6 ospf neighbor X:X::X:X {cost <1-65535>} (instance-id (<0-31>|<64-95>)|) ipv6 ospf neighbor X:X::X:X {poll-interval <0-4294967295>|priority <0-255>} (instance-id (<0-31>|<64-95>)|) no ipv6 ospf neighbor X:X::X:X ({cost <1-65535>}|{poll-interval <0-4294967295>|priority <0-255>}|) (instance-id (<0-31>|<64-95>)|)`

Parameters

`X:X::X:X` Specify a neighbor IP address.

`instance-id` Specify the instance.

`<0-255>` Specify the instance ID.

`cost` Cost of the interface. This parameter does not apply to NBMA networks.

`<1-65535>` Cost of the interface.

`poll-interval` Dead neighbor polling interval.

`<0-4294967295>`

Dead neighbor polling interval in seconds. It is recommended to set this value much higher than the hello interval.

`priority` Specify a priority. This parameter does not apply to point-to-multipoint interfaces.

`<0-31>` Interface instance ID for IPv6 unicast `<64-95>`

Interface instance ID for IPv4 unicast.

Default

Default cost is 10.

Default poll interval is 120 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
```

```
(config)#interface eth0
(config-if)#ipv6 ospf neighbor 2000:500::1 cost 2 instance-id 3
```


© Symanitron Proprietary

ipv6 ospf network

Use this command to set an OSPFv3 network type.

Use the `no` option with this command to return to the default value.

Command Syntax

```
ipv6 ospf network (broadcast|non-broadcast|point-to-multipoint (non-
  broadcast|)|point-to-point) (instance-id (<0-31>|<64-95>)|)

no ipv6 ospf network (broadcast|non-broadcast|point-to-multipoint (non-
  broadcast|)|point-to-point) (instance-id (<0-31>|<64-95>)|)
```

Parameters `broadcast` Sets the network type to broadcast. `non-broadcast` Sets the network type to NBMA. `point-to-multipoint`

Sets the network type to point-to-multipoint.

`non-broadcast`

Sets the network type to NBMA.

`point-to-point` Sets the network type to point-to-point. `instance-id` Specify the instance.

`<0-31>` Interface instance ID for IPv6 unicast `<64-95>` Interface instance ID for IPv4 unicast.

Default

By default, ipv6 ospf network is broadcast type

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows how to set the network to point-to-point type on the eth0 interface.

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 ospf network point-to-point
```

ipv6 ospf priority

Use this command to set the router priority for determining the designated router (DR) for the network.

A router with the higher router priority becomes the DR. If the priority is the same for two routers, the router with the higher router ID takes precedence.

Only routers with a nonzero priority value are eligible to become the designated or backup designated router. Configure router priority for broadcast or NBMA networks only and not for point-to-point networks.

Use the `no` parameter with this command to reset the value to default.

Command Syntax `ipv6 ospf priority <0-255> ipv6 ospf priority <0-255> instance-id (<0-31>|<64-95>) no ipv6 ospf priority instance-id (<0-31>|<64-95>)`

Parameters

`priority`	Specify the router priority of the interface.
`<0-255>`	Specify the router priority of the interface. The default is 1.
`instance-id`	Specify the instance.
`<0-31>`	Interface instance ID for IPv6 unicast
`<64-95>`	Interface instance ID for IPv4 unicast.

Default

By default, priority is 1

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 ospf priority 127
```

ipv6 ospf restart grace-period

Use this command to enable the graceful restart feature and set the grace period for restarting the router.

If graceful restart is enabled, NSM is notified about the grace period. If the OSPF daemon unexpectedly shuts down, NSM sends this value to the OSPF daemon when it comes up again which uses this value to end the graceful state.

Use the `no` parameter with this command to revert to the default grace period.

Command Syntax `ipv6 ospf restart grace-period <1-1800> no ipv6 ospf restart grace-period`

Parameters `grace-period` Specify the grace period.

`<1-1800>`	Specify the grace period in seconds.

Default

By default, grace period is 120 seconds

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ipv6 ospf restart grace-period 250
```

ipv6 ospf restart helper

Use this command to configure the helper behavior for graceful restart.

Use the `no` parameter with this command to revert to the default.

Command Syntax `ipv6 ospf restart helper {only-reload|only-upgrade|max-grace-period <1-1800>} ipv6 ospf restart helper never (router-id A.B.C.D|) no ipv6 ospf restart helper no ipv6 ospf restart helper never no ipv6 ospf restart helper {only-reload|only-upgrade|max-grace-period|never router-id (A.B.C.D|all)}`

Parameters `only-reload` Help only on software reloads.

`only-upgrade` Help only on software upgrades.

`max-grace-period`

Help only if received grace-period is less than this value. `<1-1800>` Help only if received grace-period is less than this value.

`never`	Prevent the neighbor from entering helper mode.
`router-id`	Router of neighbor to never to act as helper.
`A.B.C.D`	Router ID of neighbor to never to act as helper.

Default

By default, router behave as helper. To disable it as helper, `ospf restart helper never` command should be configured. `ospf restart helper max-grace-period` – Max-grace-period to function as helper. If not configured, value will be the grace-period in restarting node.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ipv6 ospf restart helper never router-id 1.1.1.1

#configure terminal
```

```
(config)#ipv6 ospf restart helper only-reload

#configure terminal
(config)#ipv6 ospf restart helper only-reload max-grace-period 200

#configure terminal
```

```
(config)#no ipv6 ospf restart helper never
```

ipv6 ospf retransmit-interval

Use this command to set the interval between retransmission of Link State Update packets. This interval is also used to retransmit DD packets and Link State Request packets.

After sending an LSA to a neighbor, the router keeps the LSA on the LS-retransmission list until it receives an acknowledgement. If the router does not receive an acknowledgment from the neighbor during the retransmit interval, it sends the LSA to the neighbor again.

Use the `no` parameter with this command to reset the interval to the default value.

Command Syntax `ipv6 ospf retransmit-interval <1-1800> ipv6 ospf retransmit-interval <1-1800> instance-id (<0-31>|<64-95>) no ipv6 ospf retransmit-interval`

`no ipv6 ospf retransmit-interval instance-id (<0-31>|<64-95>)`

Parameters `retransmit-interval`

	Specify the interval.
`<1-1800>`	Specify the interval in seconds.
`instance-id`	Specify the instance.
`<0-31>`	Interface instance ID for IPv6 unicast
`<64-95>`	Interface instance ID for IPv4 unicast.

Default

By default, ipv6 ospf retransmit interval is 5 seconds

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 ospf retransmit-interval 3
```

ipv6 ospf transmit-delay

Use this command to set the estimated time it takes to transmit a Link State Update packet over the interface. The transmit-delay value is added to the LS age of LSAs and is advertised through this interface whenever the LSAs are transmitted.

Use the `no` parameter with this command to reset the delay to the default value.

Command Syntax `ipv6 ospf transmit-delay <1-1800> ipv6 ospf transmit-delay <1-1800> instance-id (<0-31>|<64-95>) no ipv6 ospf transmit-delay`

`no ipv6 ospf transmit-delay instance-id (<0-31>|<64-95>)`

Parameters

`transmit-delay` Specify the time to transmit a link-state update.

`<1-1800>` Specify the time in seconds to transmit a link-state update.

`instance-id` Specify the instance.

`<0-31>` Interface instance ID for IPv6 unicast `<64-95>`

Interface instance ID for IPv4 unicast.

Default

By default, transmit delay is 1 second

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 ospf transmit-delay 2
```

ipv6 router ospf

Use this command to enable OSPFv3 routing on an interface.

Specify the process ID to configure multiple instances of OSPFv3. When running a single instance of OSPFv3, you do not need to specify a instance ID.

When OSPFv3 receives a packet, it checks if the instance ID in the packet matches the instance ID of the receiving interface.

Use the `no` parameter with this command to disable OSPFv3 routing on an interface.

Command Syntax `ipv6 router ospf area (A.B.C.D|<0-4294967295>) ipv6 router ospf area (A.B.C.D|<0-4294967295>) instance-id (<0-31>|<64-95>) ipv6 router ospf area (A.B.C.D|<0-4294967295>) tag WORD ipv6 router ospf area (A.B.C.D|<0-4294967295>) tag WORD instance-id (<0-31>|<64-95>) ipv6 router ospf tag WORD area (A.B.C.D|<0-4294967295>) ipv6 router ospf tag WORD area (A.B.C.D|<0-4294967295>) instance-id (<0-31>|<64-`

```
  95>) no ipv6 router ospf area (A.B.C.D|<0-4294967295>) no ipv6 router ospf
area (A.B.C.D|<0-4294967295>) instance-id (<0-31>|<64-95>) no ipv6 router
ospf area (A.B.C.D|<0-4294967295>) tag WORD no ipv6 router ospf area
(A.B.C.D|<0-4294967295>) tag WORD instance-id (<0-31>|<64-
  95>) no ipv6 router ospf tag WORD area (A.B.C.D|<0-4294967295>) no ipv6
router ospf tag WORD area (A.B.C.D|<0-4294967295>) instance-id (<0-31>|<6495>)
```

Parameters `area` OSPF Area ID in IPv4 address format.

`A.B.C.D` OSPF area ID in IP address format.

`<0-4294967295>`

OSPF area ID as a decimal value.

`instance-id` Specify the instance.

`<0-31>` Interface instance ID for IPv6 unicast `<64-95>`

Interface instance ID for IPv4 unicast.

`tag` Tag value to use as a “match” value for controlling redistribution via route maps.

`WORD` Set the tag value.

Default

By default, ipv6 router ospf is disabled

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
                (config-if)#ipv6 router ospf area 1 tag Tag1 instance-id 1
```

ipv6 te-metric

Use this command to set the traffic engineering metric for an interface.

The traffic engineering metric is used in OSPF-TE Link State Advertisements. If the traffic engineering metric is not set, the ipv6 ospf cost value for an interface is used in OSPF-TE Link State Advertisements.

Use the `no` parameter with this command to unset the traffic engineering metric for this interface.

Command Syntax `ipv6 te-metric <1-65535> ipv6 te-metric <1-65535> instance-id (<0-31>|<64-95>) no ipv6 te-metric instance-id (<0-31>|<64-95>)`

Parameters

`te-metric` Specify the TE metric.

`<1-65535>` Specify the TE metric value.

`instance-id` Specify the instance.

`<0-31>` Interface instance ID for IPv6 unicast `<64-95>` Interface instance ID for IPv4 unicast.

Default

By default, traffic engineering metric value is 0

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 te-metric 6
```

max-concurrent-dd

Use this command to limit the number of Database Descriptors (DD) that can be processed concurrently.

This command is useful when a router's performance is affected from simultaneously bringing up several OSPFv3 adjacencies. This command limits the maximum number of DD exchanges that can occur concurrently per OSPFv3 instance, thus allowing for all of the adjacencies to come up.

Use the `no` option with this command to remove the limit.

Command Syntax `max-concurrent-dd <1-65535> no max-concurrent-dd`

Parameters

`<1-65535>`	Specify the number of DD processes.

Default

By default, number of maximum concurrent DD processes is 5

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example set the `max-concurrent-dd` value to 4.

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#max-concurrent-dd 4
```

passive-interface

Use this command to suppress sending Hello packets on all interfaces, or on a specified interface.

This command configures OSPFv3 on simplex Ethernet interfaces. Since a simplex interface represents only one network segment between two devices, configure the transmitting interface as a passive interface. This ensures that OSPFv3 does not send hello packets for the transmitting interface. Both the devices can see each other via the hello packet generated for the receiving interface.

Use the `no` form with this command to resume sending `hello` packets on all interfaces, or on a specified interface.

Command Syntax `passive-interface (IFNAME |) no passive-interface (IFNAME |)`

Parameters

IFNAME	Specify an interface name

Default

By default, passive interface is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#passive-interface eth0
```

redistribute

Use this command to import routes from other routing protocols, or from another OSPF instance, into OSPFv3 ASexternal-LSAs.

OSPFv3 advertises routes learned from other routing protocols or from other OSPF instances, including static or connected routes. Each injected prefix is put into the AS-external-LSA with a specified metric and metric-type.

Use the `no` parameter with this command to stop redistribution.

Command Syntax

```
redistribute (kernel|connected|static|rip|bgp|isis|ospf (WORD|<1-65535>|)) {metric
<0-16777214>|metric-type (1|2)|?route-map WORD|tag <0-4294967295>} no
```

```
redistribute(kernel|connected|static|rip|bgp|isis|ospf (WORD|))
```

Parameters

kernel	Specify kernel routes.
connected	Specify connected routes.
static	Specify static routes.
rip	Specify RIP routes.
bgp	Specify BGP routes.
isis	Specify IS-IS routes.
ospf	Specify OSPF routes.
WORD	Specify an OSPFv3 Process Tag. If not specified, redistribute OSPF process with tag "null".
<1-65535>	Specify an OSPF process identifier. If not specified, redistribute OSPF instance with process ID 0.

`metric`	Specify the external metric.
`<0-16777214>`	Specify the external metric.
`metric-type`	Specify the external metric-type (see RFC 3101):
`1`	Set OSPF External Type 1 metric.
`2`	Set OSPF External Type 2 metric.
`route-map`	Specify a route map reference.
`WORD`	Specify name of the route-map.
`tag`	Tag value to use as a “match” value for controlling redistribution via route maps
`<0-4294967295>`	Specify the route tag.

Default

By default, redistribute is disabled

Command Mode

Router mode

Router address-family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows redistribution of BGP routes into the OSPFv3 routing table, with the metric as 10.

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#redistribute bgp metric 10 metric-type 1
```

The following example shows redistribution of static IPv4 routes into the OSPFv3 routing table.

```
#configure terminal
(config)#router ipv6 ospf (config-
router)#address-family ipv4 unicast
(config-router-af)#redistribute static
(config-router-af)#exit-address-family
```


© Symanitron Proprietary

restart ipv6 ospf graceful

Use this command to restart OSPFv3 gracefully.

After this command is executed, the router immediately shuts down. NSM is notified that OSPF has shut down gracefully. NSM preserves routes installed by OSPF until the grace period expires.

Command Syntax `restart ipv6 ospf graceful (grace-period <1-1800>|)`

Parameters `grace-period` Specify a grace period.

`<1-1800>` Specify a grace period in seconds.

Default

By default, restart ipv6 ospf graceful is disabled

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#restart ipv6 ospf graceful grace-period 200
```

router-id

Use this command to specify a router ID for the OSPFv3 process.

Configure each router with a unique router-id. In an OSPFv3 router process that has active neighbors, a new router-id is used at the next reload or when you start the OSPFv3 manually.

Use the `no` form of this command to force OSPFv3 to stop the routing functionality.

Command Syntax `router-id A.B.C.D`

`no router-id (A.B.C.D|)`

Parameters

`A.B.C.D` Specify the router ID in IPv4 address format.

Default

By default, router id is loop-back IP address of IP address with highest IP

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows a fixed router ID `43.3.3.3`

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#router-id 43.3.3.3
```

router ipv6 ospf

Use this command to initiate OSPFv3 routing process and enter Router mode to configure OSPFv3 routing process. For making the OSPFv3 routing process functional, you must specify OSPFv3 process tag in router mode and enable OSPFv3 on at least one interface. OSPFv3 is only enabled on interfaces where OSPFv3 process tag matches the tag specified using ipv6 router ospf area command in Interface mode. Use the `no` parameter with this command to remove OSPFv3 process.

Command Syntax `router ipv6 ospf`

```
router ipv6 ospf WORD router
ipv6 vrf ospf WORD no router
ipv6 ospf no router ipv6 ospf
WORD no router ipv6 vrf ospf
WORD
```

Parameters

`WORD`	Tag value to use as a “match” value for controlling redistribution via route maps.
`vrf`	Enable an IPv6 VRF routing process

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 ospf Tag1
(config-router)#
```

show debugging ipv6 ospf

Use this command to display the OSPFv3 debugging options.

Command Syntax `show debugging ipv6 ospf`

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show debugging ipv6 ospf

OSPFv3 debugging status:
 OSPFv3 all packet debugging is on
 OSPFv3 all NFSM debugging is on
#
```

show ipv6 ospf

Use this command to display global and area information about OSPFv3.

Command Syntax `show ipv6 ospf (WORD|)`

Parameters

`WORD`	Tag value to use as a “match” value for controlling redistribution via route maps.

Command Mode

Privileged Exec mode and Exec Mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ipv6 ospf
Routing Process "OSPFv3 0" with ID 1.2.3.4
SPF schedule delay 5 secs, Hold time between SPFs 10 secs Minimum LSA interval
5 secs,
Minimum LSA arrival 1 secs Number of external LSA 3. Checksum Sum
0x2CD6F Number of areas in this router is 1
Area BACKBONE(0)
Number of interfaces in this area is 1
SPF algorithm executed 3 times
Number of LSA 4. Checksum Sum 0x2A6AC
```

Table 2-137 explains the fields for each ospf entry.

Table 2-137: show ipv6 ospf output details

Field	Description
Area	Number of areas in device, area addresses, and so on.
Interface attached to this area	The device interfaces attached to the area.
SPF algorithm executed is N	The number of times (N) the OSPF Shortest Path First (SPF) algorithm is executed within the area.
Number of Area scoped LSAs is N	Number of LSAs (N) with a scope of the specified area.

SPF last updated	The interval in seconds that the SPF algorithm was last executed within the area.
Router	Number of router LSAs in the area.
Hold time	Minimum hold time between consecutive SPF calculations.
Checksum	LSA header checksum.

show ipv6 ospf database

Use this command to display information in the OSPFv3 Link State database.

Command Syntax `show ipv6 ospf database show ipv6 ospf database (self-originate|max-age|adv-router A.B.C.D|) show ipv6 ospf database (router|network|inter-prefix|inter-router|external|nssaexternal|link|intra-prefix|te|grace)`

`show ipv6 ospf database (router|network|inter-prefix|inter-router|external|nssaexternal|link|intra-prefix|te|grace) (self-originate|adv-router A.B.C.D|)`

`show ipv6 ospf database (router|network|inter-prefix|inter-router|external|nssa-external|link|intra-prefix|te|grace) A.B.C.D (self-originate|adv-router A.B.C.D|)`

`show ipv6 ospf WORD database show ipv6 ospf WORD database (router|network|inter-prefix|interrouter|external|nssa-external|link|intra-prefix|te|grace)`

`show ipv6 ospf WORD database (router|network|inter-prefix|inter-router|external|nssa-external|link|intra-prefix|te|grace) adv-router A.B.C.D`

Parameters

`self-originate`	Self-originated link states
`max-age`	LSAs in MaxAge list
`adv-router`	Advertising router for Type 8 Link LSAs (Link State Advertisements):
`A.B.C.D`	Router ID of the advertising router.
`router`	Router LSAs.
`network`	Network LSAs.
`inter-prefix`	Inter-Area-Prefix LSAs.
`inter-router`	Inter-Area-Router LSAs.
`external`	AS external LSAs.
`nssa-external`	NSSA LSAs.
`link`	Link LSAs.
`intra-prefix`	Intra-Area-Prefix LSAs (Type 9) with prefixes for stub and transit networks
`te`	Intra-area TE LSAs.
`grace`	Grace LSAs.
`A.B.C.D`	Link state ID as an IP address.

WORD	Tag value to use as a “match” value for controlling redistribution via route maps.

Command Mode

Privileged Exec mode and Exec Mode

Applicability

This command was introduced before SWMRE version 1.3.

Example: adv-router Parameter

This example shows using the `adv-router` parameter:

```
#show ipv6 ospf database link adv-router 10.70.0.58
            OSPFv3 Router with ID (10.70.0.58) (Process 100)
                Link-LSA (Interface eth1)
  LS age: 492
  LS Type: Link-LSA
  Link State ID: 0.0.0.3
  Advertising Router: 10.70.0.58
  LS Seq Number: 0x80000001
  Checksum: 0xC2D6
  Length: 68
  Priority: 1
  Options: 0x000013 (-|R|-|-|E|V6)
  Link-Local Address: fe80::204:75ff:feaa:fedb
  Number of Prefixes: 2
    Prefix: 5f00:1:2:10::/64
    Prefix Options: 0 (-|-|-|-)
```

Header

```
OSPFv3 Router with ID (10.70.0.58) (Process 100)
Link-LSA (Interface eth1)
```

The router ID and OSPFv3 process tag of the local router.

Interface name of the router associated with this Link-LSA.

OSPFv3 Database Fields

Table 2-138 explains the fields for each database entry.

Table 2-138: OSPFv3 database fields

Field	Description
LS age	The length of time in seconds since the LSA was originated.
LS Type	The type of LSA
Link State ID	Interface identifier of the originating router.
Advertising router	The Router ID of the router advertising this LSA. On a transit network, this is always the Designated Router ID.
LS Seq Number	Sequence number of an LSA.
Checksum	LSA header checksum (excluding the LS age field).

Length	The length in bytes of the LSA (including the 20-byte header).
Priority	The router priority of the interface attaching the originating router of the link.

Table 2-138: OSPFv3 database fields

Field	Description
Options	Bits in network LSAs that originate on the link: DC-bit: Whether the router supports OSPF over Demand Circuits. R-bit: Whether the router is active. If this bit is clear, routes which transit the advertising node cannot be computed. N-bit: How the router handles Type 7 LSAs. MC-bit: Whether IP multicast packets are forwarded. E-bit: Whether AS-External-LSAs are flooded. This bit is set in all AS External LSAs and in all LSAs. originated in the backbone and non-stub areas. V6-bit: Whether to include the router/link in routing calculations.
Link-Local Address	The originating router's link-local interface address.
Number of Prefixes	The number of IPv6 prefixes associated to the link: Prefix: The global IPv6 prefix associated to this link. Prefix Options: Each prefix is advertised along with an 8-bit capabilities field.They serve as input for routing calculations allowing, for example, some prefixes to be ignored or marked as not re-advertisable.
Referenced LS Type	Identifies the Router-LSA or Network-LSA with which the IPv6 prefixes are associated: Type 0x2001: prefixes associated with Router-LSA Type 0x2002: prefixes associated with Network-LSA
Referenced Link State ID	Referenced LS Type 0x2001: this field is 0 Referenced LS Type 0x2002: the interface ID of the link's Designated Router.
Referenced Advertising Router	Referenced LS Type 0x2001: ID of the originating router. Referenced LS Type 0x2002: ID of the Designated Router Prefix: Referenced LS Type 0x2001: global IPv6 prefix associated with the router Referenced LS Type 0x2002: global IPv6 prefix associated with the transit link Prefix Options: Bits in network LSAs that originate on the link: DC: How the router handles demand circuits R: Whether the router is active. If this bit is clear, routes which transit the advertising node cannot be computed. N: How the router handles Type 7 LSAs MC: Whether IP multicast packets are forwarded E: Whether AS-External-LSAs are flooded V6: Whether to include the router/link in routing calculations Metric: The cost of this prefix.

Example: intra-prefix and adv-router Parameters

This example shows using the `adv-router` and `intra-prefix` parameters.

Note: The same information for OSPFv2 can be viewed in type 1 router LSAs and type 2 network LSAs. However, in OSPFv3 all addressing information has been removed from router LSAs and network LSAs, leading to the introduction of the Intra-Area-Prefix LSA. In a transit network, the Intra-Area-Prefix-LSA serves the same purpose as a network LSA and on a point-to-point or point-to-multipoint network serves the same purpose as a router LSA.

```
#show ipv6 ospf database intra-prefix adv-router
10.70.0.58 OSPFv3 Router with ID (10.70.0.58) (Process
100) Intra-Area-Prefix-LSA (Area 0.0.0.0)
  LS age: 1435
  LS Type: Intra-Area-Prefix-LSA
  Link State ID: 0.0.0.2
  Advertising Router: 10.70.0.58
  LS Seq Number: 0x80000001
  Checksum: 0x1B4E
  Length: 56
  Number of Prefixes: 2
  Referenced LS Type: 0x2002
  Referenced Link State ID: 0.0.0.3
  Referenced Advertising Router: 10.70.0.58
    Prefix: 5f00:1:2:10::/64
    Prefix Options: 0 (-|-|-|-)
    Metric: 0
    Prefix: 6f00:1:2:10::/64
    Prefix Options: 0 (-|-|-|-)
    Metric: 0
```

Header

```
OSPFv3 Router with ID (10.70.0.58) (Process 100)
Intra-Area-Prefix-LSA (Area 0.0.0.0)
```

- The router ID and OSPFv3 process tag for the router.
- Intra-Area-Prefix-LSA has area flooding scope. This LSA belongs to Area 0.0.0.0.

show ipv6 ospf interface

Use this command to display OSPFv3 interface information.

Command Syntax `show ipv6 ospf interface`

```
show ipv6 ospf interface IFNAME
```

Parameters

`IFNAME`	The name of the interface.

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Usage

This is a sample output from the `show ipv6 ospf interface` command displaying the OSPFv3 interface information:

```
#show ipv6 ospf interface eth0 is
up, line protocol is up
  Interface ID 3, Instance ID 0, Area 0.0.0.0
  IPv6 Link-Local Address fe80::248:54ff:fec0:f32d/10
 Router ID 1.2.3.4, Network Type BROADCAST, Cost: 10
 Transmit Delay is 1 sec, State Backup, Priority 1
 Designated Router (ID) 5.6.7.8
Interface Address fe80::203:47ff:fe4c:776e
 Backup Designated Router (ID) 1.2.3.4
Interface Address fe80::248:54ff:fec0:f32d
 Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:01
 Neighbor Count is 1, Adjacent neighbor count is 1
```

If Hello Suppression is enabled

```
RTR_B#show ipv6 ospf interface eth1 is
up, line protocol is up
  Interface ID 3
  IPv6 Prefixes
    fe80::5054:ff:fef3:f166/64 (Link-Local Address)
    2001::2/64
  OSPFv3 Process (1), Area 0.0.0.0, Instance ID 66
    Router ID 2.2.2.2, Network Type P2MP-NBMA, Cost: 1, TE Metric:
    1 Reduce LSA Flooding
    Transmit Delay is 1 sec, State Point-To-Point, Priority 1
    Timer interval configured, Hello 30, Dead 120, Wait 120, Retransmit 5
```

```
  Hello due in 00:00:32
Neighbor Count is 1, Adjacent neighbor count is 1
Suppress hello for 1 neighbor(s)
Hello received 2 sent 3, DD received 4 sent 6
          LS-Req received 1 sent 1, LS-Upd received 7 sent 4
LS-Ack received 0 sent 3, Discarded 0
```

Table 2-139 explains the fields for each ospf interface entry.

Table 2-139: show ipv6 ospf interface output details

Field	Description
Interface Type and whether it is up or down.	Status of the interface type.
Line protocol	Status of the line protocol.
Interface ID	Interface for which information is displayed.
Instance ID	For running multiple instances of OSPFv3 on the router
Area	Area ID in A.B.C.D form
IPv6 Link-Local Address	link-local address is an IPv6 unicast address – cannot communicate to link-local addresses that are outside the directly connected network. In IPv6 (X:X::X:X/M) form.
Router ID	As stated – In A.B.C.D form.
Network Type	One of the following: •Ethernet is Broadcast •Serial p2p non-broadcast •NBMA – Non-Broadcast MultiAccess (NBMA) media
cost	The cost of sending packets over this interface – range is 1 to 65535.
Transmit Delay	The delay, in seconds, between link-state transmits. This value must be the same for all nodes on the network. The range is 1 to 65535. The default is 1.
Priority	OSPFv3 router priority for the interface. The range is 0 to 255. A router with priority 0 can never become the designated router, the default is 1.
Designated Router (ID)	The ID number of the Designated Router (DR).

Interface Address	The IPV6 address of this device.
Backup Designated Router	The ID number or the Backup Designated Router (BDR).
Interface Address	The IPv6 address of the Backup Designated Router.
Timer interval configured	The timer values of the following instances: Hello, Dead, Wait, Retransmit.
Hello due in	The countdown for receiving the next Hello packet.
Neighbor Count is	Number of neighbor count.
Adjacent neighbor count is	Number of adjacent neighbor count.

show ipv6 ospf neighbor

Use this command to display information about an OSPFv3 neighbor.

Command Syntax `show ipv6 ospf neighbor show ipv6 ospf WORD neighbor show ipv6 ospf neighbor INTERFACE show ipv6 ospf WORD neighbor INTERFACE show ipv6 ospf neighbor INTERFACE detail show ipv6 ospf WORD neighbor INTERFACE detail show ipv6 ospf neighbor detail show ipv6 ospf WORD neighbor detail show ipv6 ospf neighbor A.B.C.D show ipv6 ospf WORD neighbor A.B.C.D`

Parameters

`WORD`	Tag value to use as a “match” value for controlling redistribution via route maps.
`INTERFACE`	Display the name of the Interface
`A.B.C.D`	Neighbor IP address.
`detail`	Details of neighbors

Command Mode

Privileged Exec mode and Exec Mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

This is a sample output from the show ipv6 ospf neighbor command displaying information about the OSPFv3 neighbor.

```
#show ipv6 ospf neighbor
OSPFv3 Process (*null*)
Neighbor ID Pri State Dead Time Interface Instance ID
5.6.7.8 1 Full/DR 00:00:38 eth0 0
```

If Hello Suppression is enabled

```
RTR_B#
RTR_B#show ipv6 ospf neighbor
OSPFv3 Process (1)
Neighbor ID      Pri   State           Dead Time   Interface  Instance ID
1.1.1.1            1   Full/ -         inactive    eth1       0
4.4.4.4            1   Full/DR         00:00:40    eth2       0
4.4.4.4            1   Full/ -         inactive    VLINK1     0
RTR_B#
```

```
RTR_B#
RTR_B#show ipv6 ospf neighbor detail
 Neighbor 1.1.1.1, interface address fe80::5054:ff:feb3:d3bc
    In the area 0.0.0.0 via interface eth1
    Neighbor priority is 1, State is Full, 7 state changes
    Hello is suppressed
    DR is 0.0.0.0 BDR is 0.0.0.0
    Options is 0x000133 (AF|*|*|DC|R|-|-|E|V6)
    Dead timer due in inactive
    Database Summary List 0
    Link State Request List 0
```

Table 2-140 explains the fields for each ospf neighbor entry.

Table 2-140: show ipv6 ospf neighbor output details

Field	Description
Neighbor	Router ID of the neighbor router.
interface address	IPv6 address of the neighbor's interface.
In the area	The neighbor router's area ID.
via interface	Neighbor router's interface name.
Neighbor Priority is	OSPFv3 router priority for the interface. The range is 0 to 255. A router with priority 0 can never become the designated router, the default is 1.
State	The Link State Address (LSA) of the neighbor, and there has been 7 state changes, and sending Hello packets is suppressed.

DR	Designated Router (DR) ID
BDR	Backup Designated Router (BDR) ID
Options is	The hexadecimal representation of the seven bits in the Options Field of Hello packets (see RFC 5340): • AF-bit – Address Family bit. • V6-bit – If this bit is clear, the router/link should be excluded from IPv6 routing calculations. • E-bit – This bit describes the way AS-external-LSAs are flooded. • N-bit – This bit indicates whether or not the router is attached to an NSSA. • R-bit – This bit (the `Router' bit) indicates whether the originator is an active router. If the router bit is clear, then routes that transit the advertising node cannot be computed. Clearing the router bit is appropriate for a multi-homed host that wants to participate in routing, but does not want to forward non-locally addressed packets. • DC-bit – This bit describes the router's handling of demand circuits, as specified in [DEMAND]. • *-bit – These bits are reserved for migration of OSPFv2 protocol extensions.
Dead timer due in	The countdown timer for marking neighbor connections dead. In this example, the Deat Timer has been deactivated.

Table 2-140: show ipv6 ospf neighbor output details (Continued)

Field	Description
Database Summary List	Describes routes to IPv6 address prefixes that belong to other areas.
Link State Request List	Sent or received when Link-State Request packets finds that parts of the Link State Database are out of date.
Timer interval configured	The set values for the following packet types: Hello, Dead, Wait, Retransmit.
Neighbor Count	The number of known neighbors.
Adjacent neighbor count	The number of directly adjacent neighbors.

show ipv6 ospf route

Use this command to display the IPv6 routing table for OSPFv3.

The routes can be displayed in two ways:

- Each routing entry in a single-line
- Each routing entry in multiple lines

By default, the routing table is displayed in the multi-line format. For a single line display, give the ipv6 ospf display route single-line command.

Command Syntax `show ipv6 ospf`

`route show ipv6 ospf WORD`

`route`

Parameters

`WORD`	Tag value to use as a “match” value for controlling redistribution via route maps.

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following is sample output in single-line format:

```
#show ipv6 ospf route
Destination Metric Next-hop
3ffe:1:1::/48 10 directly connected, eth0
3ffe:2:1::/48 10 directly connected, eth0
3ffe:2:2::/48 10 directly connected, eth0
3ffe:3:1::/48 10 directly connected, eth0
3ffe:3:2::/48 10 directly connected, eth0
3ffe:3:3::/48 10 directly connected, eth0
E2 3ffe:100:1::1/128 10/20 via fe80::203:47ff:fe4c:776e, eth0
E2 3ffe:100:2::1/128 10/20 via fe80::203:47ff:fe4c:776e, eth0
E2 3ffe:100:3::1/128 10/20 via fe80::203:47ff:fe4c:776e, eth0
IA 3ffe:101:1::/48 20 via fe80::203:47ff:fe4c:776e, eth0
IA 3ffe:101:2::/48 20 via fe80::203:47ff:fe4c:776e, eth0
IA 3ffe:101:3::/48 20 via fe80::203:47ff:fe4c:776e, eth0
```

The following is sample output in multi-line format:

```
#show ipv6 ospf route
Destination Metric
Next-hop Interface
3ffe:1:1::/48 10
-- eth0
```

```
3ffe:2:1::/48 10
-- eth0
3ffe:2:2::/48 10
-- eth0
3ffe:3:1::/48 10
-- eth0
3ffe:3:2::/48 10
-- eth0
3ffe:3:3::/48 10
-- eth0
E2 3ffe:100:1::1/128 10/20 fe80::203:47ff:fe4c:776e eth0
```

Table 2-141 explains the fields for each ospf route entry.

Table 2-141: show ipv6 ospf route output details

Field	Description
IP address	IP address of the remote network.
Metric	For OSPF the metric is cost, which indicates the best quality path to use to forward packets.
Next hop router IP address	This route is available through the next hop router located at this IP address. This identifies exactly where packets go when they match this route.
Outgoing interface name	Interface used to get to the next-hop address for this route.

show ipv6 route fast-reroute

Use this command to display loop-free alternate routes with alternate next hops.

Command Syntax `show ipv6 route fast-reroute`

Parameters

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Usage

```
#show ipv6 route fast-reroute
```

show ipv6 ospfv3 topology

Use this command to display information about OSPFv3 topology for each area.

Command Syntax `show ipv6 ospfv3 topology show ipv6 ospfv3 WORD topology show ipv6 ospfv3 topology area (A.B.C.D|<0-4294967295>) show ipv6 ospfv3 WORD topology area (A.B.C.D|<0-4294967295>)`

Parameters

`WORD`	Tag value to use as a “match” value for controlling redistribution via route maps.
`area`	OSPFv3 area ID
`A.B.C.D`	OSPFv3 Area ID in IPv4 address format.
`<0-4294967295>`	OSPFv3 Area ID as a decimal value.

Command Mode

Privileged Exec mode and Exec Mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ipv6 ospfv3 topology
OSPFv3 paths to Area (0.0.0.0) routers
Router ID Bits Metric Next-Hop Interface
1.2.3.4 --
5.6.7.8 E 10 5.6.7.8 eth0
```

Example

```
#show ipv6 ospfv3 topology

OSPFv3 paths to Area (0.0.0.0) routers
Router ID        Bits  Metric     Next-Hop            Interface
1.2.3.4                                               --
5.6.7.8          E     10         5.6.7.8             eth0
```

Table 2-142 explains the fields for each ospfv3 topology entry.

Table 2-142: show ipv6 ospfv3 topology output details

Field	Description
OSPFv3 path to Area	Area ID in IPv4 format.
Router ID	ID in IPv4 format,

Table 2-142: show ipv6 ospfv3 topology output details

Field	Description
Bits	Bits appended to packets: •V-bit Indicates whether the advertising router is an endpoint of a virtual link. • E-bit Indicates whether the advertising router is an Autonomous System Border Router (ASBR). • B-bit Indicates whether the advertising router is an Area Border Router (ABR). • W-bit When set, the router is a wild-card multicast receiver.
Metric	The value of ospfv3 metric.
Next-Hop	The next-hop identifier.
Interface	The interface name through which the virtual link extends.

show ipv6 ospf virtual-links

Use this command to display information about OSPFv3 virtual-links.

Command Syntax `show ipv6 ospf virtual-links show ipv6 ospf WORD virtual-links`

Parameters

`WORD`	Tag value to use as a “match” value for controlling redistribution via route maps.

Command Mode

Privileged Exec mode and Exec Mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ipv6 ospf virtual-links
Virtual Link VLINK1 to router 5.6.7.8 is up
Transit area 0.0.0.1 via interface eth0, instance ID 0
Local address 3ffe:1234:1::1/128
Remote address 3ffe:5678:3::1/128
Transmit Delay is 1 sec, State Point-To-Point,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:01
Adjacency state Up
```

If Hello Suppression is enabled

```
RTR_B#show ipv6 ospf virtual-links
Virtual Link VLINK1 to router 4.4.4.4 is up
  Transit area 0.0.0.1 via interface eth2, instance ID 0
  Hello suppression Enabled
  DoNotAge LSA allowed
  Local address 2002::1/128
  Remote address 2002::2/128
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
    5 Hello due in inactive
    Adajcency state Full
RTR_B#
RTR_B#
```

Table 2-143 explains the fields for each ospf virtual-links entry.

Table 2-143: show ipv6 ospf virtual-links output details

Field	Description

Virtual Link	Virtual link name, the router ID to which it is connected, and the state of the link.
Transit area	Transit area ID, the interface it uses, and its instance ID – an Instance ID should default to 0. It is only necessary to assign a value other than 0 on those links that will contain multiple separate communities of OSPF routers.
Local address	The local IPV6 address and subnet mask.
Remote address	The remote IPv6 address and subnet mask.
Transmit Delay	The delay, in seconds, between link-state transmits. This value must be the same for all nodes on the network. The range is 1 to 65535. The default is 1. The state is pointto-point.
Timer intervals configured	The configured values in seconds of the following timers: Hello, Dead, Wait, Retransmit.
Hello due in	A countdown timer that indicates when the next Hello packet should arrive.
Adjacency State	Whether the adjacency state is either up or down.

show ipv6 vrf

Use this command to list information about VRFs.

Command Syntax `show ipv6 vrf (WORD|)`

Parameter

`WORD`	VPN Routing/Forwarding instance name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following is a sample output of the `show ipv6 vrf` command displaying VRF information:

```
#show ipv6 vrf
Name              Interfaces

qa                        eth0  you
eth1 myVRF             eth2
```

Table 2-144 explains the fields.

Table 2-144: show ipv6 vrf output details

Field	Description
Name	Name of the interface.
Interfaces	Type of an interface.

snmp restart ospf6

Use this command restart SNMP in OSPFv3

Command Syntax `snmp restart ospf6`

Parameter

None

Default

By default, SNMP restart is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#snmp restart ospf6
```

summary-address

Use this command to summarize or suppress external routes with the specified address range.

An address range is a pairing of a starting address and a mask that is almost the same as IP network number. For example:

- If the specified IPV6 address range is 2020:100:100:2000::/53, it matches 2020:100:100:2222::/64, 2020:100:100:2666::/64 and so on.
- If the specified IPV4 address range is 192.168.0.0/255.255.240.0, it matches 192.168.1.0/24, 192.168.4.0/22, 192.168.8.128/25 and so on.

Redistributing routes from other protocols into OSPF requires the router to advertise each route individually in an external LSA. Use this command to advertise one summary route for all redistributed routes covered by a specified network address and mask. This minimizes the size of the OSPF link state database.

Use the `no` form this command to remove summary addresses.

Command Syntax

```
summary-address X:X::X:X/M (not-advertise|(all-tag (<0-4294967295> ))| )
  (translate-tag (<0-4294967295>) | ) summary-address A.B.C.D/M
(not-advertise|tag <0-4294967295>|) no summary-address
A.B.C.D/M no summary-address X:X::X:X/M (not-advertise|tag (<0-
4294967295>|))
no summary-address X:X::X:X/M (not-advertise|(all-tag (<0-4294967295> )) |
  ) (translate-tag (<0-4294967295>)| ) no summary-address A.B.C.D/M
(not-advertise|tag (<0-4294967295>|))
```

Parameters

`X:X::X:X/M` The range of addresses given as IPv6 starting address and a mask. `A.B.C.D/M`

The range of addresses given as IPv4 starting address and a mask.

`not-advertise` Suppress routes that match the range.

`tag` Tag value to use as a “match” value for controlling redistribution via route maps.

`<0-4294967295>`

Set a tag value. The default is 0.

`all-tag` Set tag for all summarized type-5, translated type5 and type-7 LSA. `translate-tag` Set tag only for summarized translated type-5 LSA.

Default

By default, summary-address value is 0

Command Mode

Router mode

Router address-family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example uses the `summary-address` command to aggregate external LSAs that match the network 172.16.0.0/24 and assign a tag value of 3.

```
#configure terminal
(config)#router ipv6 ospf
(config-router)#summary-address 2020:100:100:2000::/53 all-tag 3
```

© Symanitron Proprietary

CHAPTER 3 OSPF VPN Commands

This chapter provides an alphabetized reference of the OSPF VPN commands. It includes the following commands:

- capability vrf-lite
- router ospf vrf

capability vrf-lite

Use this command to enable the `vrf-lite` capability for an OSPF instance.

Use the `no` parameter with this command to disable the same for an OSPF instance.

Command Syntax `capability vrf-lite no capability vrf-lite`

Parameters

None

Default

By default, VRF lite capability for an OSPF instance is disabled.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router ospf 100
(config-router)#capability vrf-lite
```

```
(config)#router ospf 100
(config-router)#no capability vrf-lite
```


router ospf vrf

Use this command to specify a VRF instance in OSPF. To use this command, you must first create a VRF Name in the NSM using the `ip vrf` command. Associate the same name with the OSPF instance using this command.

Command Syntax `router ospf <1-65535> WORD`

Parameters

`<1-65535>`	Routing process ID; should be unique for each routing process.
`WORD`	Name of the VRF to associate with this OSPF instance.

Default

By default, router ospf vrf is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100 myVRF
(config-router)#
```

OSPF VPN Commands

CHAPTER 4 CSPF-TE Commands

This chapter provides an alphabetized reference for each of the CSPF-TE commands. It includes the following commands:

- capability te
- cspf default-retry-interval
- cspf tie-break
- debug cspf
- show cspf ipv6 lsp
- show cspf lsp
- show debugging cspf
- show debugging ipv6 cspf
- show ip ospf te-database
- show ipv6 ospf te-database

capability te

Use this command to enable the traffic engineering feature for an OSPFv2 or OSPFv3 instance. SWMRE generates traffic engineering LSAs for each link for which it is configured.

Use the `no` parameter form of command to disable the traffic engineering feature.

Command Syntax

OSPFv2:

```
    capability (te|traffic-engineering) no
capability (te|traffic-engineering)
```

OSPFv3:

```
    capability   te   no
    capability te
```

Parameters

None

Default

Enabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
    #configure terminal
    (config)#router ospf 100
    (config-router)#capability te

    #configure terminal
    (config)#router ipv6 ospf
    (config-router)#no capability te
```

cspf default-retry-interval

Use this command to set the default route computation retry interval for an OSPFv2 or OSPFv3 instance. This value is used for route recomputation (in the case of computation failures) and no retry interval is specified for a given LSP.

Use the `no` parameter with this command to unset default route computation retry interval.

Command Syntax `cspf default-retry-interval`

```
    <1-3600> no cspf default-retry-interval
```

Parameter `default-retry-interval`

The retry interval.

`<1-3600>` The retry interval in seconds. The default is 10 seconds.

Default

Enabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#cspf default-retry-interval 720

#configure terminal
(config)#router ipv6 ospf
(config-router)#cspf default-retry-interval 720
```

cspf tie-break

Use this command to set the tie-break method for an OSPFv2 or OSPFv3 instance. This selects a link (during route computation) when more than one candidate link satisfies all the route constraints and the associated cost and hop limit link attributes are equal.

Use the `no` parameter with this command to unset tie-break method.

Command Syntax `cspf tie-break (random|least-fill|most-fill) no cspf tie-break`

Parameters

`random`	Pick any path at random. This method places an equal number of LSPs on each link without taking into account the available bandwidth ratio. This is the default tie-break method.
`least-fill`	Pick the path with the largest minimum available bandwidth ratio. This method equalizes the reservation on each link.
`most-fill`	Pick the path with the smallest minimum available bandwidth ratio. This method uses one link until it is completely full and then uses the next link.

Default

By default, the tie-break method is set to `random`.

Default

Enabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ospf 100
(config-router)#cspf tie-break least-fill

#configure terminal
(config)#router ipv6 ospf
(config-router)#no cspf tie-break
```

debug cspf

Use this command to enable the CSPF debugging options in OSPFv2.

Use the `no` parameter with this command to disable debugging.

Command Syntax `debug cspf events debug cspf hexdump`

`no debug cspf events`

`undebug cspf events no`

`debug cspf hexdump`

`undebug cspf hexdump`

Parameters

`events`	Debug CSPF event information.
`hexdump`	Debug CSPF message hex dumps.

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before SWMRE version 1.3.

Examples

Following is a sample output section from this command. Some of the lines in this sample display have wrapped, please note that in the actual output the lines may not wrap.

```
#debug cspf hexdump

#debug cspf events
```

```
#terminal monitor

#2002/03/19 15:17:29 OSPF: cspf_api_msg_delete_recv: Delete message received from
client 2
2002/03/19 15:17:29 OSPF: cspf_api_msg_delete_process: Client = 2, lspid =
0x8000
2002/03/19 15:17:29 OSPF: cspf_api_msg_request_recv: Route request message
received from client 2
2002/03/19 15:17:29 OSPF: cspf_api_msg_request_process: Client = 2, request
type = 1, ingress = 192.40.40.3, egress = 192.20.20.1, lspid = 0x8000
2002/03/19 15:17:29 OSPF: cspf_compute_route: lspid = 0x8000, setup priority = 7,
ingress = 192.40.40.3, egress = 192.20.20.1, hop limit constraint = 255,
bandwidth constraint = 125000.000000, include mask = 0x0, exclude mask = 0x0,
path constraint count = 0
....
2002/03/19 15:17:34 OSPF: cspf_process_network_lsa_vertex: Vertex id =
192.20.20.2, dest addr = 192.20.20.1
2002/03/19 15:17:34 OSPF: cspf_api_msg_established_recv: LSP Established message
received from client 2
2002/03/19 15:17:34 OSPF: cspf_api_msg_established_process: Client = 2, lspid =
0x8000, metric = 0
```

show cspf ipv6 lsp

Use this command to display information about all the LSPs stored in the CSPF database for all OSPFv3 instances.

Command Syntax `show cspf ipv6 lsp`

Command mode

Exec and Privileged Exec mode

Parameters

None

Applicability

This command was introduced before SWMRE version 1.3.

Example

Following is a sample output from the `show cspf ipv6 lsp` command.

```
#show cspf ipv6 lsp
   Lsp Id          : 0x650065
   Ingress         : 2001:5152::1
   Egress          : 2001:5154::1
   Ext Tunnel ID   : 2001:5152::1
   LSP Type        : 0
   Client ID       : 3
   State           : 2
   Setup Priority  : 7
   Hold Priority   : 0
   Hop Limit       : 255
   Include Mask    : 0x0
   Exclude Mask    : 0x0
LSP Metric      : 0
   Computed ERO    :
       3ffe:1::2
       3ffe:2::2
```

show cspf lsp

Use this command to display information about all the LSPs stored in CSPF for OSPFv2.

Command Syntax `show cspf lsp`

Parameters

None

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before SWMRE version 1.3.

Example

Following is a sample output from the `show cspf lsp` command.

```
#show cspf lsp
Lsp Id              : 0xbfe0
   Client ID        : 2
   State            : 2
   Ingress          : 192.40.40.3
   Egress           : 192.20.20.1
   Setup Priority   : 7
   Hold Priority    : 0
   Bandwidth        : 10.000 Kbits/s
   Hop Limit        : 255
   Retry Interval   : 5
   Retry Limit      : 3
   LSP Metric       : 20
   Computed ERO     :
       192.40.40.2
       192.20.20.1
```

show debugging cspf

Use this command to display the CSPF debugging options in OSPFv2.

Command Syntax `show debugging cspf`

Parameters

None

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before SWMRE version 1.3.

Example

Following is a sample output section from the `show debugging cspf` command. Some of the lines in this sample display have wrapped, please note that in the actual output the lines may not wrap.

```
#show debugging cspf
CSPF debugging status:
CSPF events debugging is on
```

```
#terminal monitor
#2002/03/27 17:09:21 OSPF: cspf_api_msg_delete_recv: Delete message received from
client 2
2002/03/27 17:09:21 OSPF: cspf_api_msg_delete_process: Client = 2, lspid =
0x8000
2002/03/27 17:09:21 OSPF: cspf_api_msg_request_recv: Route request message
received from client 2
...
2002/03/27 17:09:21 OSPF: cspf_process_network_lsa_vertex: Vertex id
= 192.10.10.9, dest addr = 192.20.20.1
2002/03/27 17:09:21 OSPF: cspf_process_network_lsa_vertex: Vertex id =
192.20.20.2, dest addr = 192.20.20.1
2002/03/27 17:09:21 OSPF: cspf_api_msg_established_recv: LSP Established message
received from client 2

2002/03/27 17:09:21 OSPF: cspf_api_msg_established_process: Client = 2, lspid
= 0x8000, metric = 0
```

show debugging ipv6 cspf

Use this command to display the CSPF debugging options in OSPFv3.

Command Syntax `show debugging ipv6 cspf`

Parameters

None

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show debugging ipv6 cspf

CSPF debugging status:
#
```

show ip ospf te-database

Use this command to display traffic engineering (TE) information in OSPFv2.

Command Syntax `show ip ospf (<0-65535>|) te-database`

Parameter

`<0-65535>`	Display the process ID number.

Command Mode

Exec and Privileged Exec modes

Applicability

This command was introduced before SWMRE version 1.3.

Example

Following is a sample output from the `show ip ospf te-database` command.

```
#show ip ospf te-database
LS Age                        : 2
Options                       : 0x2
LS Type                       : 10 (Area-Local Opaque-LSA)
Opaque  Type                  : 1
Instance                      : 0xffff
Advertising Router            : 192.10.10.1
LS Sequence Number            : 0x8000005a
LS Checksum                   : 0xfb4f
Length                        : 28
Router Address                : 192.10.10.1
---------------------------------------------------------------
LS Age                        : 2
Options                       : 0x2
LS Type                       : 10 (Area-Local Opaque-LSA)
Opaque  Type                  : 1
Instance                      : 0x3
Advertising Router            : 192.10.10.1
LS Sequence Number            : 0x8000002e
LS Checksum                   : 0x3ef
Length                        : 124
Link Type                     : Multiaccess
Link ID                       : 192.20.20.2
Local Interface Addresses     :          192.20.20.1
Remote Interface Addresses    :        192.20.20.2
Te Metric                     : 10
Max Bandwidth                 : 10000.000 Kbits/s Max Reservable
Bandwidth     : 1000.000 Kbits/s
Available Bandwidth           :
```

```
Priority 0                : 1000.000 Kbits/s
    Priority 1                : 1000.000 Kbits/s
    Priority 2                : 1000.000 Kbits/s
    Priority 3                : 1000.000 Kbits/s
Priority 4                : 1000.000 Kbits/s
Priority 5                : 1000.000 Kbits/s
```

show ipv6 ospf te-database

Use this command to display traffic engineering (TE) information in OSPFv3.

Command Syntax `show ipv6 ospf (WORD|) te-database`

Parameter

`WORD`	Tag value to use as a “match” value for controlling redistribution via route maps.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

Following is a sample output from the `show ipv6 ospf te-database` command.

```
#show ipv6 ospf te-database
LS Age                        : 12
LS Type                       : 10 (Intra-Area-Te-LSA)
Instance                      : 0x3
Advertising Router            : 4.4.4.4
LS Sequence Number            : 0x8000004d
LS Checksum                   : 0xf58a
Length                        : 164
Router Address                : 2001:5152::1
---------------------------------------------------------------
LS Age                        : 12
LS Type                       : 10 (Intra-Area-Te-LSA)
Instance                      : 0x3
Advertising Router            : 4.4.4.4
LS Sequence Number            : 0x8000004d
LS Checksum                   : 0xf58a
Length                        : 164
Link Type                     : Multiaccess
Neighbor Interface ID         : 135450284
Neighbor Router ID            : 4.4.4.4 Local
 Interface Addresses     : 3ffe:1::1
Remote Interface Addresses    :
              ::
Te Metric                     : 0
Max Bandwidth                 : 100000.000 Kbits/s
Max Reservable Bandwidth      : 100000.000 Kbits/s
Available Bandwidth           :
    Priority 0                : 100000.000 Kbits/s
```

```
     Priority 1                : 100000.000 Kbits/s
     Priority 2                : 100000.000 Kbits/s
     Priority 3                : 100000.000 Kbits/s
     Priority 4                : 100000.000 Kbits/s
     Priority 5                : 100000.000 Kbits/s
Priority 6                : 100000.000 Kbits/s
Priority 7                : 100000.000 Kbits/s
```

Intermediate System to Intermediate System Command Reference

Contents

This document contains these chapters:

- Chapter 1, *IS-IS Commands*
- Chapter 2, *IS-IS Show Commands*

CHAPTER 1 IS-IS Commands

This chapter describes the IS-IS commands:

- accept-lifetime
- adjacency-check
- area-password
- authentication key-chain • authentication mode
- authentication send-only
- bfd all-interfaces
- clear clns neighbors
- clear clns is-neighbors
- clear isis adjacency
- clear isis counter
- clear isis interface counter
- clear isis process
- clear ip isis route
- debug isis
- default-information originate
- distance (IPv6)
- domain-password
- ignore-lsp-errors
- ip router isis
- isis authentication key-chain
- isis authentication mode md5
- isis authentication send-only
- isis bfd
- isis circuit-type
- isis csnp-interval
- isis hello-interval
- isis hello-multiplier
- isis hello padding
- isis lsp-interval
- isis metric
- isis network
- isis password
- isis priority
- isis retransmit-interval

- ispf
- isis wait-timer
- is-type
- key chain
- key
- key-string
- lsp-gen-interval
- lsp-mtu
- lsp-refresh-interval
- max-area-address
- max-lsp-lifetime
- net
- prc-interval-exp
- redistribute
- redistribute isis
- router isis
- send-lifetime
- set-overload-bit
- snmp restart isis
- spf-interval-exp
- summary-address

accept-lifetime

Use this command to specify the time period during which the authentication on a key chain is received as valid.

Use the `no` parameter with this command to negate this command.

Command Syntax `accept-lifetime HH:MM:SS <1-31> MONTH <1993-2035> HH:MM:SS <1-31> MONTH <1993-2035> accept-lifetime HH:MM:SS <1-31> MONTH <1993-2035> HH:MM:SS MONTH <1-31> <1993-2035> accept-lifetime HH:MM:SS MONTH <1-31> <1993-2035> HH:MM:SS <1-31> MONTH <1993-2035> accept-lifetime HH:MM:SS MONTH <1-31> <1993-2035> HH:MM:SS MONTH <1-31> <1993-2035> accept-lifetime HH:MM:SS <1-31> MONTH <1993-2035> infinite accept-lifetime HH:MM:SS MONTH <1-31> <1993-2035> infinite accept-lifetime HH:MM:SS <1-31> MONTH <1993-2035> duration <1-2147483646> accept-lifetime HH:MM:SS MONTH <1-31> <1993-2035> duration <1-2147483646> no accept-lifetime`

Parameters

`HH:MM:SS`	Specify the start time of accept-lifetime in hours, minutes and seconds.
`<1-31>`	Specify the day of the month to start.

MONTH Specify the month of the year to start as the first three letters of the month, for example, Jan.

<1993-2035> Specify the year to start.

HH:MM:SS Specify the end time of accept-lifetime in hours, minutes and seconds.

<1-31> Specify the day of the month to end.

MONTH Specify the month of the year to end as the first three letters of the month, for example, Jan.

<1993-2035> Specify the year to end.

duration Indicate the duration parameter.

<1-2147483646>

Specify the actual end time duration of a key in seconds.

infinite Specify the end time to never expire.

Default

By default, accept-lifetime command is disabled

Command Mode

Keychain-key mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows the setting of accept-lifetime for key1 on the key chain named mychain.

```
#configure terminal
(config)#key chain mychain
(config-keychain)#key 1
     (config-keychain-key)#accept-lifetime 03:03:01 Dec 3 2004 04:04:02 Oct 6 2006
```

adjacency-check

Use this command to check ISIS neighbor protocol support.

Use the `no` parameter with this command to uncheck ISIS neighbor protocol support.

Command Syntax `adjacency-check no adjacency-check`

Parameters

None

Default

By default, adjacency-check command is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#router isis bb
(config-router)#adjacency-check

(config-router)#no adjacency-check
```

area-password

Use this command to set the authentication password for the Level-1 area and to set authentication on Level-1 sequence number PDUs. This command enables authentication when receiving and sending link-state and sequence number PDUs in Level-1 areas. The password must be the same for all the ISIS routers in the same area.

Use the `no` parameter with this command to clear the area password.

Command Syntax `area-password WORD area-password WORD`

```
authenticate snp (send-only|validate) no area-password
```

Parameters

`WORD`	Password string.
`authenticate`	Insert the password into Level-1 SNP PDUs.
`snp`	Sequence number PDUs.
`send-only`	Only insert the password into the Level-1 sequence number PDUs, but not check the password in sequence number PDUs that it receives. Use this keyword during a software upgrade to ease the transition.
`validate`	Insert the password into Level-1 sequence number PDUs and check the password in sequence number PDUs that it receives.

Default

By default, the area password is not configured

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#router isis bb
(config-router)#area-password mypasswd

(config)#router isis bb
(config-router)#area-password myPass authenticate snp send-only

(config)#router isis bb
(config-router)#no area-password
```

authentication key-chain

Use this command to set the key chain to be used for authentication at the instance level. Authentication mode must be set to `md5` to configure the key chain. If no key chain is configured with the key-chain command, no key-chain authentication is performed.

Only one authentication key-chain is applied to an ISIS interface at a time. That is, issuing a second `isis authentication key-chain` command overrides the first `isis authentication key-chain` command. If neither the `level-1` nor the `level-2` keyword is configured, the chain applies to both levels. Authentication can be specified for an individual ISIS interface using the `isis authentication key-chain` command.

Use the `no` parameter with this command to unset the key chain used for authentication.

Command Syntax `authentication key-chain WORD (level-1|level-2|) no authentication key-chain WORD (level-1|level-2|) no authentication key-chain (level-1|level-2|)`

Parameters

`WORD`	Specify the chain name (valid authentication keys).
`level-1`	Specify an authentication key-chain for level-1 PDUs.
`level-2`	Specify an authentication key-chain for level-2 PDUs.

Default

The key chain applies to the level(s) on which authentication mode is configured as MD5 if no level is specified.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router isis 1
(config-router)#authentication key-chain myKey level-1
```

authentication mode

Use this command to set the authentication mode at the instance level.

If clear-text authentication was configured using the `area-password` or `domain-password` commands, the `authentication mode` command overrides both of those commands (based on the level at which MD5 is configured). If the `authentication mode` command was used first, and subsequently an attempt is made to use the `area-password` or `domain-password` commands, the attempt fails. To configure clear-text authentication using the `area-password` or `domain-password` commands, first use the `no authentication mode` command.

The type of authentication and the level to which it applies can be specified for a single ISIS interface, rather than per ISIS instance, using the `isis authentication mode` command.

Use the `no` parameter with this command to unset the authentication mode.

Command Syntax `authentication mode {md5|text} (level-1|level-2|) no authentication mode {md5|text} (level-1|level-2|)`

Parameters

`md5`	Keyed message digest
`text`	Text mode

`level-1`	Specify an authentication key-chain for level-1 PDUs.
`level-2`	Specify an authentication key-chain for level-2 PDUs.

Default

The authentication mode is set to MD5 for both levels if no level is specified.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router isis 1
(config-router)#authentication mode md5 level-1

(config-router)#no authentication mode md5 level-1
```

authentication send-only

Use this command to set the send-only option at the instance level.

Use this command before configuring the authentication mode and authentication key-chain, so that the implementation of authentication goes smoothly. That is, the routers will have more time for the keys to be configured on each router if authentication is inserted only on the packets being sent, not checked on packets being received. After all routers that must communicate are configured with this command, enable the authentication mode and key chain on each router. Then, specify the `no authentication send-only` command to disable the send-only feature.

If neither the `level-1` nor `level-2` keyword is configured, the send-only feature applies to both levels.The send-only option applies to both levels if no level is specified.

Use the `no` parameter with this command to unset the send-only option.

Command Syntax `authentication send-only (level-1|level-2|)` `no authentication send-only (level-1|level-2|)`

Parameters

`level-1`	Specify an authentication key-chain for level-1 PDUs.
`level-2`	Specify an authentication key-chain for level-2 PDUs.

Default

By default, authentication send only is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router isis 1
(config-router)#authentication send-only level-1

(config-router)#no authentication send-only level-1
```

bfd all-interfaces

Use this command to enable the Bidirectional Forwarding Detection (BFD) feature on the interfaces enabled with this ISIS instance.

This command sets BFD fall-over check for all the neighbors under specified process. To disable BFD checking on particular interface use `isis bfd disable` command at interface mode.

Use the no parameter with this command to disable BFD functionality for an ISIS instance.

Command Syntax `bfd all-interfaces no bfd all-interfaces`

Parameters

None

Default

By default, the BFD feature is disabled.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#router isis
(config-router)#bfd all-interfaces

(config-router)#no bfd all-interfaces
```

clear clns neighbors

Use this command to clear CLNS neighbor adjacencies.

Command Syntax `clear clns neighbors`

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
>ena
#clear clns neighbors
```

clear clns is-neighbors

Use this command to clear IS neighbor adjacencies.

Command Syntax `clear clns is-neighbors System-ID`

Parameters

`System-ID`	Neighbor system ID in XXXX.XXXX.XXXX format.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
>enable
#clear clns is-neighbors 1111.1111.1111.1111
```

clear ip isis route

Use this command to clear IPv4 routes.

Command Syntax `clear ip isis (WORD|) route (redistribution|all)`

Parameters

`WORD` Name that identifies the IS-IS area. `redistribution` Clear IS-IS local redistribution routes. `all` Clear all of the IS-IS routing tables.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
>ena
#clear ip isis route redistribution
```

clear isis adjacency

This command is used to remove the entries from the IS-IS adjacency database. Clears all adjacencies for the specified routing instance or specified interface or particular system ID.

Command Syntax `clear isis adjacency (*|IFNAME|system-id XXXX.XXXX.XXXX|) (vrf VRFNAME|)`

Parameters

`*`	Clear all neighbors.
`IFNAME`	Interface name.
`XXXX.XXXX.XXXX`	Neighbor System-ID.
`VRFNAME`	VRF name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear isis adjacency *
```

clear isis counter

Use this command to clear system-wide IS-IS counters (IsisSystemCounterEntry in RFC 4444).

Command Syntax `clear isis counter`

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear isis counter
```

clear isis interface counter

Use this command to clear interface counters. If you do not specify a parameter, then counters for all interfaces are cleared.

Command Syntax `clear isis interface counter`

`(IFNAME|)`

Parameters

`IFNAME`	Interface name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear isis interface counter
```

clear isis process

Use this command to restart ISIS processes. If you do not specify a parameter, then all ISIS processes are restarted.

Command Syntax `clear isis (WORD|) process`

Parameters

`WORD`	Name that identifies the IS-IS area.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear isis process
```

debug isis

Use this command to turn on debugging for specified criteria. Debug commands enable to show some debugging information about specified criteria into file or terminal.

Use the `no` parameter to turn off debugging for specified criteria.

Command syntax `debug`

```
isis (all|)

debug isis (authentication|bfd|checksum|events|hello|mpls (interface IFNAME |
  System-ID|)|ifsm|local-updates|lsp|nfsm|nsm|pdu|protocol-errors|rib|spf)

no debug isis (all|) no debug all no debug all isis undebug all

undebug isis (all|) undebug all isis

 no debug isis (authentication|bfd|checksum|events|hello|mpls (interface IFNAME |
  System-ID|)|ifsm|local-updates|lsp|nfsm|nsm|pdu|protocol-errors|rib|spf) undebug
isis (authentication|bfd|checksum|events|hello|mpls (interface IFNAME |
System-ID|)|ifsm|local-updates|lsp|nfsm|nsm|pdu|protocol-errors|rib|spf)
```

Parameters

`all` Enables all debugging. `authentication`
Debugging for authentication.

`checksum`	Debugging for checksums.
`bfd`	Debugging for bidirectional forwarding detection.
`events`	Debugging for internal events.
`hello`	Debugging for hello processing.
`interface`	Interface.
`IFNAME`	Interface name.
`System-ID`	System identifier.
`ifsm`	Debugging for interface finite state machine.
`local-updates`	Debugging for local updates.
`lsp`	Debugging for link-state packet.
`nfsm`	Debugging for neighbor finite state machine.
`nsm`	Debugging for NSM messages.
`pdu`	Debugging for protocol data unit.
`protocol-errors`	Debugging for protocol errors.
`rib`	Debugging for RIB information.

`spf`	Debugging for shortest path first route calculation.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#debug isis pdu
```

```
#configure terminal
(config)#debug isis nsm
```

default-information originate

Use this command to originate reachability information to a default route into link-state packets.

There is no default information in a Level-2 domain by default, while a Level-1 router calculates a default to L1L2 route during SPF calculation. This command originates a default route into a Level-2 domain.

Use the `no` parameter with this command to withdraw reachability information to a default route from link-state packets.

Command Syntax `default-information originate (always|) (route-map WORD|) no default-information originate (always|) (route-map WORD|)`

Parameters

`originate`	Specify to distribute a default route
`always`	The default route is advertised even if there is no default route in the router's routing table.
`route-map`	Identifies the level into which the default route is to be announced and can specify other filtering options via a route map.

Default

There is no default information in Level-2 domain by default, while Level-1 router calculates default to L1L2 route during SPF calculation. This command enables to originate default route into Level-2 domain.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#default-information originate
(config-router)#exit
(config)#exit
```

distance (IPv6)

Use this command in router mode to set the administrative distance for all IPv6 routes. By default all options are turned off.

Use the `no` parameter with this command to remove an administrative distance.

Command Syntax `distance <1-255> (System-ID (WORD|)|) no distance`

Parameters

`<1-255>`	Distance range.

System-ID	Source ID in XXXX.XXXX.XXXX format.
WORD	Access-list name.

Default

By default, all options are turned off.

Command Mode

Address-family ipv6 mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows setting the administrative distance for all routes.

```
#configure terminal
(config)#router isis
(config-router)#distance 10
```

The following example shows setting the administrative distance for a specific route source.

```
#configure terminal
(config)#router isis
(config-router)#distance 40 0000.0000.0001
```

domain-password

Use this command to set the authentication password for the Level-2 domain, and optionally, the authentication password on Level-2 sequence number PDUs.

Configuring this command to enable authentication when receiving and sending link state and sequence number PDUs in Level-2 domain. The domain password must be the same in the Level-2 domain.

Use the no parameter with this command to clear the domain password.

Command Syntax `domain-password WORD domain-password WORD authenticate snp (send-only|validate) no domain-password`

Parameters

WORD	Password string.
authenticate	Inserts th password into Level-1 sequence number PDUs.
snp	sequence number PDUs.
send-only	Only inserts the password into the Level-1 sequence number PDUs, but does not check the password in sequence number PDUs that it receives. Use this keyword during a software upgrade to ease the transition.
validate	Inserts the password into the Level-1 sequence number PDUs and checks the password in sequence number PDUs received.

Default

By default, there is no domain password.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#domain-password mypasswd

(config)#router isis bb
(config-router)#domain-password myPass authenticate snp send-only

(config)#router isis bb
(config-router)#no domain-password
```

ignore-lsp-errors

Use this command to ignore link-state packets (LSPs) with checksum errors. By default, ISIS validates the checksum for LSP and if the checksum has an error, the LSP is dropped. Giving this command says to ignore the LSP checksum error and treat it as if checksum is passed. Use the `no` parameter to turn off this function.

Command Syntax `ignore-lsp-errors` `no ignore-lsp-errors`

Parameters

None

Default

By default, the LSP checksum is checked on receipt.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

In this sample, rtr1 does not drop LSP packets with bad checksum.

```
#configure terminal
(config)#router isis bb
(config-router)#ignore-lsp-errors
```

ip router isis

Use this command to enable ISIS IPv4 routing on the interface. This command is mandatory to ISIS configuration.

After giving this command, the router sends ISIS Hello with IP address TLV on this interface and IP reachability information TLV in link-state packets are updated.

Use the `no` parameter with this command to disable ISIS IPv4 routing on the interface. This action does not clear the ISIS database. To clear the database, unconfigure the ISIS routing instance.

Command Syntax `ip router isis`

```
(WORD|) no ip router isis
(WORD|)
```

Parameters

`WORD`	Name that identifies the IS-IS area. Specify an existing area name or a new area name.

Default

By default, IPv4 routing is disabled on the router.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ip router isis bb
```

isis authentication key-chain

Use this command to set the key chain to be used for authentication on the interface-related packets.

Authentication mode must be set to `md5` to configure the key chain. If no key chain is configured with the `key-chain` command, no key-chain authentication is performed. Only one authentication key-chain is applied to an ISIS interface at a time. That is, issuing a second `isis authentication key-chain` command overrides the first `isis authentication key-chain` command.

If neither the `level-1` nor `level-2` keyword is configured, the key chain applies to the level(s) on which the authentication mode is configured as `md5`. Authentication can be specified for an entire instance of ISIS, instead of at the interface level, by using the `authentication key-chain` command.

Use the `no` parameter with this command to unset the key chain used for authentication on the interface-related packets.

Command Syntax `isis authentication key-chain WORD (level-1|level-2|) no isis authentication key-chain (level-1|level-2|) no isis authentication key-chain WORD (level-1|level-2|)`

Parameters

WORD	Chain name - valid authentication keys.
level-1	Specify an authentication key-chain for level-1 PDUs.
level-2	Specify an authentication key-chain for level-2 PDUs.

Default

By default, this option is disabled. The key chain applies to the level(s) on which authentication mode is configured as MD5 if no level is specified.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#isis authentication key-chain myKey level-1
```

isis authentication mode md5

Use this command to set the MD5 authentication mode. If clear text authentication was configured using the `isis password` command, the `isis authentication mode` command overrides the `isis password` command. If the `isis authentication mode` command was used, then subsequently an attempt is made to use the `isis password` command, the attempt fails.

To configure clear text authentication using the `isis password` command, first use the `no isis authentication mode` command. The type of authentication and the level to which it applies can be specified for the entire ISIS instance, rather than per interface, using the `authentication mode` command.

Use the `no` parameter with this command to unset the MD5 authentication mode.

Command Syntax

```
isis authentication mode {md5|text} (level-1|level-2|)
no isis authentication mode {md5|text} (level-1|level-2|)
```

Parameters

md5	Keyed message digest
text	Text mode
level-1	Specify an authentication key-chain for level-1 PDUs.
level-2	Specify an authentication key-chain for level-2 PDUs.

Default

By default, this option is disabled. The authentication mode will be set to MD5 for both levels if no level is specified.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#isis authentication mode md5 level-1
```

isis authentication send-only

Use this command to set the send-only option to the interface-related packets.

Use this command before configuring the ISIS authentication mode and ISIS authentication key-chain, so that the implementation of authentication goes smoothly. That is, the routers will have more time for the keys to be configured on each router if authentication is inserted only on the packets being sent, not checked on packets being received. After all routers that must communicate are configured with this command, enable the authentication mode and key chain on each router.

Use the `no` parameter with this command to unset the send-only option to the interface-related packets.

Command Syntax `isis authentication send-only (level-1|level-2|)` `no isis authentication send-only (level-1|level-2|)`

Parameters

`level-1`	Specify an authentication key-chain for level-1 PDUs.
`level-2`	Specify an authentication key-chain for level-2 PDUs.

Default

By default, this option is disabled. The send-only option applies to both levels if no level is specified.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#isis authentication send-only level-1
```

isis bfd

Use this command to enable/disable the BFD check on interface.

The `isis bfd` command allows a user to enable BFD on an interface. The `isis bfd disable` command disables BFD checking on an interface. However, the `no isis bfd` and `no isis bfd disable` commands both remove the enable/disable configuration, but do not disable/enable BFD.

The `bfd all-interfaces` command enables BFD on all interfaces attached to an instance then configuring. This command disables BFD configuration on a particular interface.

Command Syntax `isis bfd`

`(disable|) no isis bfd`

`(disable|)`

Parameters `disable` Specify to disable BFD.

Default

By default, bfd feature enable/disable is not configured.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#isis bfd disable
```

isis circuit-type

Use this command to set the circuit type for the interface.

If level-1 or level-2-only is specified in this command, ISIS sends only the specified level of PDUs. On the point-to-point interface, there is only one type of Hello packet, so in this case ISIS Hello will be sent regardless of circuit-type. If istype is configured as level-1 or level-2 only, routing for this instance is performed for only the specified level. In this manner, only the particular level of PDU is sent on the interface.

Use the `no` parameter to reset circuit type to the default.

Command Syntax `isis circuit-type (level-1|level-1-2|level-2-only) no isis circuit-type`

Parameters `level-1` Specify that only Level-1 adjacencies are formed.

`level-1-2` Specify that Level-1-2 adjacencies are formed.

`level-2-only` Specify that only Level-2 adjacencies are formed.

Default

By default, the default circuit-type is level-1-2.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#isis circuit-type level-2-only
```

isis csnp-interval

Use this command to set CSNP (Complete sequence number PDU) interval in seconds.

Configuring this command changes the interval between two consecutive CSNP transmission. By default, CSNP is sent every 10 seconds only by LAN DIS. This parameter is only valid on broadcast interface, since periodic CSNP is only sent on broadcast interface, while CSNP on Point-to-Point interface is sent only when adjacency is initiated.

Use the `no` parameter with this command to reset CSNP interval to the default value.

Command Syntax `isis csnp-interval <1-65535> (level-1|level-2|) no isis csnp-interval (level-1|level-2|) no isis csnp-interval <1-65535> (level-1|level-2|)`

Parameters

`<1-65535>` Specify the CSNP interval in seconds.

`level-1` Specify Level-1 CSNP. `level-2` Specify Level-2 CSNP.

Default

By default, ISIS uses 10 seconds for the interval and the interval is applied to both level-1 and level-2.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#isis csnp-interval 20
```

isis hello-interval

Use this command to set the Hello interval in seconds. The Hello-interval is set with the hello-multiplier (see `isis hello-multiplier` command).

Configuring this command changes the time interval between two consecutive Hello transmissions. If a device receives its own LSP with a maximum sequence number, then it suspends ISIS for the hold interval. DIS sends Hello transmissions at three times the rate than non-DIS. If ISIS is elected as DIS on this interface, ISIS sends Hello every 3.3 seconds.

If `minimal` keyword is specified, Holding timer in Hello PDU is set to 1 second and Hello interval is calculated by dividing by the hello-multiplier. For example, if the hello-multiplier is configured as 4 and `hello-interval minimal` is the command used, an Hello PDU is sent every 250 milliseconds.

Use the `no` parameter to set the Hello interval to the default.

Command Syntax `isis hello-interval <1-65535> (level-1|level-2|) isis hello-interval minimal (level-1|level-2|) no isis hello-interval (level-1|level-2|) no isis hello-interval <1-65535> (level-1|level-2|) no isis hello-interval minimal (level-1|level-2|)`

Parameters

`<1-65535>`	Specify the hello interval in seconds.
`minimal`	Specify the holding-time as 1 second.
`level-1`	Specify Level-1 CSNP.
`level-2`	Specify Level-2 CSNP.

Default

By default, ISIS uses 10 seconds for the interval and the interval is applied to both level-1 and level-2.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#isis hello-interval 5 level-1

(config)#interface eth0
(config-if)#isis hello-interval minimal
```

isis hello-multiplier

Use this command to set multiplier for Hello holding time.

Changes Holding Timer in Hello PDU. Holding timer is calculated by “Hello-Interval” multiplied by this value. If `minimal` keyword is specified with the Hello-Interval, the holding timer is set to 1 second and the hello-interval is calculated by dividing 1 by this value.

Use the `no` parameter with this command to set multiplier to the default.

Command Syntax `isis hello-multiplier <2-100> (level-1|level-2|)` `no isis hello-multiplier (level-1|level-2|)`

`no isis hello-multiplier <2-100> (level-1|level-2|)`

Parameters

`<2-100>` Specify a hello multiplier value.

`level-1` Specify Level-1 hello. `level-2` Specify Level-2 hello.

Default

By default, ISIS uses 3 seconds for the multiplier value and the multiplier is applied to both level-1 and level-2.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#isis hello-multiplier 4
```

isis hello padding

Use this command to enable IS-IS hello padding at the interface level.

Intermediate System-to-Intermediate System (IS-IS) hellos are padded to the full maximum transmission unit (MTU) size. The benefit of padding IS-IS hellos to the full MTU is that it allows for early detection of errors that result from transmission problems with large frames or errors that result from mismatched MTUs on adjacent interfaces.

Use the `no` parameter with this command to disable IS-IS hello padding.

Command Syntax `isis hello padding` `no isis hello padding`

Parameters

None

Default

By default, ISIS hello padding is enabled

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#isis hello padding

(config-if)#no isis hello padding
```

isis lsp-interval

Use this command to set the link-state packet (LSP) transmission interval.

Giving this command changes the minimum interval between two consecutive LSP transmission. When flooding or some other event triggers LSP transmission, the LSP is put in the interface queue and scheduled to send according to this interval. Two consecutive LSP transmissions are scheduled to have at least this interval.

Use the `no` parameter with this command to set LSP transmission interval to the default.

Command Syntax `isis lsp-interval <1-4294967295> no isis lsp-interval`

Parameters

`<1-4294967295>` LSP transmission interval in milliseconds.

Default

By default, ISIS uses 33 milliseconds for the interval.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#isis lsp-interval 100

(config-if)#no isis lsp-interval
```

isis metric

Use this command to set the default metric for the interface. The interface default metric is put into IP reachability information TLVs and in IS reachability information TLVs in link-state packets. The value is used for SPF calculation, and is applied when the metric-style is configured as “narrow”.

Use the `no` parameter with this command to set default metric to the default.

Command Syntax `isis metric <1-63> (level-1|level-2|) no isis metric (level-1|level-2|) no isis metric <1-63> (level-1|level-2|)`

Parameters

`<1-63>`	Default metric.
`level-1`	Default metric for level-1 circuit.
`level-2`	Default metric for level-2 circuit.

Default

By default, ISIS uses 10 for the metric value and the value is applied to both level-1 and level-2.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#isis metric 20
```

isis network

Use this command to change a broadcast interface network type to a point-to-point network type.

Use the `no` parameter with this command to revert to the default setting of a broadcast interface network type.

Command Syntax `isis network (broadcast|point-to-point) no isis network (broadcast|point-to-point|)`

Parameters

`broadcast`	Specify ISIS a broadcast multi-access network.
`point-to-point`	Specify ISIS a point-to-point network.

Default

By default, the network is set to a broadcast multi-access network type.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
```

```
(config)#interface eth0
(config-if)#isis network point-to-point
```

isis password

Use this command to set the authentication password of Hello PDU on the interface.

Use the `no` parameter to clear the password.

Command Syntax `isis password WORD (level-1|level-2|) no isis password (level-1|level-2|) no isis password WORD (level-1|level-2|)`

Parameters

`WORD`	Specify a password string.
`level-1`	Specify a password for Level-1 hello PDUs.
`level-2`	Specify a password for Level-2 hello PDUs.

Default

By default, no password is configured; this applies to both level-1 and level-2.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#isis password mypassword level-1
```

isis priority

Use this command to set the priority for LAN DIS election. This command changes the priority value in LAN ISIS Hello PDUs. A lower priority value is less preferred in DIS election, and a higher priority value is more preferred.

Note:This command is not valid for Point-to-Point interface.

Use the `no` parameter to set priority to the default.

Command Syntax `isis priority <0-127> (level-1|level-2|) no isis priority (level-1|level-2|) no isis priority <0-127> (level-1|level-2|)`

Parameters

`<0-127>`	Priority value
`level-1`	Specify a password for Level-1 hello PDUs.
`level-2`	Specify a password for Level-2 hello PDUs.

Default

By default, ISIS uses 64 for the priority value, and the priority is applied to both level-1 and level-2.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#isis priority 127
```

isis retransmit-interval

Use this command to set the link-state packet (LSP) retransmission interval.

Use the `no` parameter to set the interval to the default.

Command Syntax `isis retransmit-interval <1-65535> no isis retransmit-interval`

Parameters

`<1-65535>`	Interval for retransmission of the same LSP in seconds.

Default

By default, ISIS uses an interval of 5 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#isis retransmit-interval 10 (config-if)#no isis retransmit-
interval
```

ispf

Use this command to enable incremental SPF for a routing process.

Use the `no` parameter to disable incremental SPF from a routing process.

Command Syntax `ispf ispf (level-1|level-1-2|level-2-only) no ispf`

Parameters `level-1` Act as level-1 only IS. `level-1-2` Act as level-1-2 IS. `level-2-only` Act as level-2 only IS.

Default

By default, all levels are turned off.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#ispf level-1

(config)#router isis bb
(config-router)#no ispf
```

isis wait-timer

Use the isis wait-timer seconds command to configure the number of seconds the router will wait for adjacency information

Use the `no` parameter to set the wait-timer to the default.

Command Syntax `isis wait-timer <1-65535> (level-1|level-1-2|level-2|) no isis wait-timer <1-65535> (level-1|level-1-2|level-2|)`

Parameters `level-1` Act as level-1 only IS. `level-1-2` Act as level-1-2 IS. `level-2-only`

Act as level-2 only IS.

Default

By default, wait-timer will be 20 seconds (2 times the hello timer).

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
```

```
(config-router)#isis wait-timer 30

(config)#router isis bb
(config-router)#no isis wait-timer
```

is-type

Use this command to set the IS to the specified level of routing.

Changing `is-type` brings down, then brings up a particular level of routing. There is a limitation: Only one ISIS instance can run Level-2 routing (either Level-2 only IS, or Level-1-2 IS).

Use the `no` parameter to set the IS to the default.

Command Syntax `is-type (level-1|level-1-2|level-2-only) no is-type`

Parameters `level-1` Act as level-1 only IS. `level-1-2` Act as level-1-2 IS. `level-2-only`

Act as level-2 only IS.

Default

By default, ISIS uses level-1-2 if there is no Level-2 instance nor a Level-1-2 instance. Otherwise, it uses level-1.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#is-type level-1

(config)#router isis bb
(config-router)#no is-type
```

key chain

Use this command to enter the key chain management mode and to configure a key chain with a key chain name. This command allows you to enter the keychain mode to specify keys on this key chain.

Command Syntax `key chain WORD no key chain WORD`

Parameters

`WORD`	Specify the name of the key chain to manage.

Default

By default, keychain mode is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows the creation of a key chain named `mychain` and the change to keychain mode:

```
#configure terminal
(config)#key chain mychain
(config-keychain)#
```

key

Use this command to manage, add or delete authentication keys in a key-chain. This command allows you to enter the keychain-key mode to set a password for the key.

Command Syntax `key <0-2147483647>` `no key <0-2147483647>`

Parameters

`<0-2147483647>` Specify a key identifier.

Default

By default, ISIS uses level-1-2 if there is no Level-2 instance nor a Level-1-2 instance. Otherwise, it uses level-1.

Command Mode

Keychain mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example configures a key number 1 and shows the change to keychain-key command mode.

```
#configure terminal
(config)#key chain mychain
(config-keychain)#key 1
(config-keychain-key)#
```

key-string

Use this command to define a password to be used by a key.

Use the `no` parameter with this command to disable this feature.

Command Syntax `key-string LINE`

`no key-string`

Parameters

`LINE`	Specify a string of characters to be used as a password by the key.

Default

By default, password is not configured.

Command Mode

Keychain mode and Keychain-key mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

In the following example, the password for `key 1` in the key chain named `mychain` is set to `prime`:

```
#configure terminal
(config)#key chain mychain
(config-keychain)#key 1
(config-keychain-key)#key-string prime

(config-keychain)#key 1
(config-keychain-key)#no key-string
```

lsp-gen-interval

Use this command to set the minimum interval before regenerating the same link-state packet (LSP). The smaller the interval, the faster the convergence. However, this setting might cause more frequent flooding.

Use the `no` parameter with this command to set the interval to the default.

Command Syntax `lsp-gen-interval <1-120> lsp-gen-interval (level-1|level-2) <1-120> no lsp-gen-interval`

Parameters

`<1-120>`	Minimum interval in seconds.
`level-1`	Interval for Level-1 IS.
`level-2`	Interval for Level-2 IS.

Default

By default, ISIS uses 30 seconds for the interval and the interval is applied to both level-1 and level-2.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router isis bb
(config-router)#lsp-gen-interval 5
```

lsp-mtu

Use this command to set maximum transfer unit for link-state packets (LSPs).

Use the `no` parameter with this command to set the interval to the default.

Command Syntax `lsp-mtu (level-1|level-2|) <512-1492> no lsp-mtu (level-1|level-2|)`

Parameters

`<512-1492>` MTU size `level-1` Size for Level-1 IS. `level-2` Size for Level-2 IS.

Default

By default, the MTU is 1492 bytes.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router isis bb
(config-router)#lsp-mtu 555
```

lsp-refresh-interval

Use this command to set the link-state packet (LSP) refresh interval.

Symanitron recommends making the `lsp-refresh-interval` smaller than the max-lsp-lifetime value.

Use the `no` parameter to set the interval to the default value.

Command Syntax `lsp-refresh-interval <1-65535> no lsp-refresh-interval`

Parameters

<1-65535>	Refresh interval in seconds.

Default

By default, the interval is 900 seconds.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#lsp-refresh-interval 600

(config)#router isis bb
(config-router)#no lsp-refresh-interval
```

max-area-address

Use this command to set the maximum number of ISIS areas that can be configured on this router with the `net` command. By default, ISIS permits a maximum of three areas that can be defined on a router. Use the `no` parameter with this command to set the maximum number of ISIS areas to its default (3).

Command Syntax `max-area-address`

```
<3-254> no max-area-address
```

Parameters

<3-254>	The maximum number of areas in the network.

Default

By default, the maximum number of areas is 3.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#router isis net2 (config-
router)#max-area-address 5 (config-router)#net
71.0001.0000.0000.0001.00 (config-router)#net
72.0001.0000.0000.0001.00
```

```
(config-router)#net 73.0001.0000.0000.0001.00
(config-router)#net 74.0001.0000.0000.0001.00
(config-router)#net 75.0001.0000.0000.0001.00
```

max-lsp-lifetime

Use this command to set the maximum link-state packet (LSP) lifetime. You must set `max-lsp-lifetime` greater than the lsp-refresh-interval interval.

Use the `no` parameter to set the lifetime to the default.

Command Syntax `max-lsp-lifetime <350-65535>` `no max-lsp-lifetime`

Parameters

`<350-65535>` Maximum LSP lifetime in seconds.

Default

By default, max-lsp-lifetime is set to 1200 seconds.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#max-lsp-lifetime 1500

(config)#router isis bb
(config-router)#no max-lsp-lifetime
```

net

Use this command to add a Network Entity Title (NET) for the instance.

On a router running ISIS, a NET can be 8 to 20 bytes in length. The last byte is always the n-selector, and must be zero. The n-selector indicates no transport entity, and means that the packet is for the routing software of the system. The six bytes directly preceding the n-selector are the system ID. The system ID length is a fixed size and cannot be changed. The system ID must be unique throughout each area (Level 1) and throughout the backbone (Level 2).

The bytes preceding the system ID are the area ID, which can be from 1 - 13 bytes in length. By default, a maximum of three NETs per router are allowed with a different area ID but the system ID should be the same for all NETs. You can increase the number of area IDs per system ID with the `max-area-address` command.

Use the `no` parameter to remove the NET.

Command Syntax

```
net NET no
net NET
```

Parameters

NET	Specify a network entity title (NET) in 1 to 13 octets (that is, XX.XXXX. ... .XXXX.XX).

Default

By default, ISIS does not configure a NET and routing is not enabled for the interface.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router isis bb
(config-router)#net 49.0000.0001.0002.0003.00
```

prc-interval-exp

Use this command to configure exponential back-off delay between PRC calculations.

Use the no parameter to disable any set exponential back-off delay between PRC calculations.

Command Syntax `prc-interval-exp prc-interval-exp <0-2147483647> <0-2147483647> no prc-interval-exp`

Parameters

<0-2147483647>	Set the minimum delay between receiving a change to PRC calculation in milliseconds.
<0-2147483647>	Set the maximum delay between receiving a change to PRC calculation in milliseconds.

Default

By default, minimum delay is 500 milliseconds and maximum delay is 50 seconds.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#router isis
```

```
(config-router)#prc-interval-exp 100 10000

(config)#router isis
(config-router)#no prc-interval-exp
```

redistribute

Use this command to redistribute routes from another protocol into the ISIS routing table.

Use the `no` parameter to disable this function.

Command Syntax

```
redistribute (kernel|connected|static|rip|ospf|bgp) {metric <0-4261412864>|
  metric-type (internal|external)|level-1|level-2|level-1-2|?route-map WORD}
no redistribute (kernel|connected|static|rip|ospf|bgp)
```

Parameters

`kernel`	Redistribute kernel routes.
`connected`	Redistribute connected routes.
`static`	Redistribute static routes.
`rip`	Redistribute RIP routes.
`ospf`	Redistribute OSPF routes.
`bgp`	Redistribute BGP routes.
`metric`	Specify the metric for redistributed routes.
`<0-4261412864>`	Specify the IS-IS default metric.
`metric-type`	Specify the IS-IS exterior metric type for redistributed routes:
`internal`	Set IS-IS internal metric type.
`external`	Set IS-IS external metric type.
`level-1`	IS-IS Level-1 routes.
`level-2`	IS-IS Level-2 routes.
`level-1-2`	IS-IS Level-1 and Level-2 routes.
`route-map`	Specify a Route map reference.
`WORD`	Specify name of the route-map.

Default

By default, redistribute command is disabled.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
>ena
#con term
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
(config)#router isis A
(config-router)#redistribute bgp metric 12
```

redistribute isis

Use this command to redistribute reachability information from one level to the other level. If an distribute-list name is given with this command for an access list that does not exist, the routes are still redistributed.

Use the `no` parameter with this command to stop redistribution.

Command Syntax `redistribute isis level-1 into level-2 redistribute isis level-2 into level-1 distribute-list WORD redistribute isis level-2 into level-1 distribute-list WORD no redistribute isis level-1 into level-2 no redistribute isis level-2 into level-1`

Parameters

`level-1`	Specify an inter-area route from level-1.
`level-2`	Specify an inter-area routes from level-2.
`into`	Specify a from level-n level into level-m.
`level-1`	Specify an inter-area route into level-1.
`level-2`	Specify an inter-area routes into level-2.
`distribute-list`	Indicate the distributed-list parameter.
`WORD`	Specify the actual selected route.

Default

By default, ISIS redistributes selected L1 routes into L2.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#redistribute isis level-2 into level-1

(config)#router isis bb
(config-router)#redistribute isis level-2 into level-1 distribute-list new

(config)#router isis bb
(config-router)#no redistribute isis level-2 into level-1
```

router isis

Use this command to initiate an ISIS routing instance. This command starts the ISIS routing instance and enters router configuration mode. Configure at least one NET to start routing. Also, enable a particular interface with the ip router isis command.

Use the `no` parameter with this command to remove an ISIS routing instance.

Command Syntax `router isis`

`(WORD|) no router isis`

`(WORD|)`

Parameters

`WORD`	Name that identifies the IS-IS area.

Default

By default, ISIS routing instance is not configured.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router isis New
(config-router)#
```

send-lifetime

Use this command to specify the time period during which the authentication key on a key chain can be sent.

Use the `no` parameter with this command to negate this command.

Command Syntax `send-lifetime HH:MM:SS <1-31> MONTH <1993-2035> HH:MM:SS <1-31> MONTH <1993-2035> send-lifetime HH:MM:SS <1-31> MONTH <1993-2035> HH:MM:SS MONTH <1-31> <1993-2035> send-lifetime HH:MM:SS MONTH <1-31> <1993-2035> HH:MM:SS <1-31> MONTH <1993-2035> send-lifetime HH:MM:SS MONTH <1-31> <1993-2035> HH:MM:SS MONTH <1-31> <1993-2035> send-lifetime HH:MM:SS <1-31> MONTH <1993-2035> infinite send-lifetime HH:MM:SS MONTH <1-31> <1993-2035> infinite send-lifetime HH:MM:SS <1-31> MONTH <1993-2035> duration <1-2147483646> send-lifetime HH:MM:SS MONTH <1-31> <1993-2035> duration <1-2147483646> no send-lifetime`

Parameters

HH:MM:SS	Specify the start time of accept-lifetime in hours, minutes and seconds.
<1-31>	Specify the day of the month to start.
MONTH	Specify the month of the year to start as the first three letters of the month, for example, Jan.
<1993-2035>	Specify the year to start.
HH:MM:SS	Specify the end time of accept-lifetime in hours, minutes and seconds.
<1-31>	Specify the day of the month to end.
MONTH	Specify the month of the year to end as the first three letters of the month, for example, Jan.
<1993-2035>	Specify the year to end.
duration	Indicate the duration parameter.
<1-2147483646>	Specify the actual end time duration of a key in seconds.
infinite	Specify the end time to never expire.

Applicability

No default value is specified

Command Mode

Keychain-key mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows the setting of `send-lifetime` for `key 1` on the key chain named `mychain`:

```
#configure terminal
(config)#key chain mychain
(config-keychain)#key 1
       (config-keychain-key)#send-lifetime 03:03:01 Jan 3 2004 04:04:02 Dec 6 2006
```

set-overload-bit

Use this command to set the overload-bit in self link-state packets (LSPs). If the overload-bit is set in an LSP, the router is not used as a transit router during SPF calculation. The router continues to receive LSPs when the overload bit is set.

Use the `no` parameter to clear the overload-bit from self-LSPs.

Command Syntax

```
set-overload-bit ({suppress (external|interlevel|external interlevel|interlevel
external)|on-startup (<5-86400>|wait-for-bgp)}|)
no set-overload-bit
```

Parameters

`suppress`	Suppress redistribution of specified types of reachability data during overload state.
`external`	Suppress redistribution of external reachability (prevents IP prefixes learned from other protocols from being advertised).
`interlevel`	Suppress redistribution of interlevel reachability.
`on-startup`	Set the overload bit only at startup, then clear the bit after the specified interval has elapsed.
`<5-86400>`	Specify the time in seconds to advertise one self as overloaded after reboot.
`wait-for-bgp`	Set the overload bit is set up at startup, then clear the bit after BGP signals it has finished converging or if the BGP does not signal it has finished converging in 10 minutes. If BGP is not running, clear the overload bit immediately.

Default

By default, the overload-bit is not set.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

This example sets overload bit at startup, does not unset the overload bit until BGP converges, suppresses redistribution between levels, and suppresses redistribution from external routing protocols while the overload bit is set.

```
(config)#router isis bb
(config-router)#set-overload-bit on-startup wait-for-bgp suppress
interlevel external
```

snmp restart isis

Use this command to restart SNMP in Intermediate System to Intermediate System (IS-IS)

Command Syntax `snmp restart isis`

Parameters

None

Default

By default, snmp restart is not configured.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#snmp restart isis
```

spf-interval-exp

Use this command to set the minimum and maximum hold intervals between Shortest Path First (SPF) calculations.

The `spf-interval-exp` command configures the minimum and maximum interval time between the receipt of a topology change and the calculation of the SPF.

Use the `no` parameter with this command to set the minimum and maximum hold intervals to the default.

Command Syntax `spf-interval-exp <0-2147483647> <0-2147483647> spf-interval-exp (level-1|level-2) <0-2147483647> <0-2147483647> no spf-interval-exp`

Parameters

`<0-2147483647>` Specify the minimum delay between receiving a change to the SPF calculation in milliseconds. The default SPF minimum hold-time interval value is 500 milliseconds.

`<0-2147483647>` Specify the maximum delay between receiving a change to the SPF calculation in milliseconds. The default SPF maximum hold-time interval value is 50 seconds.

`level-1` Specify an interval for Level-1 IS. `level-2`

Specify an interval for Level-2 IS.

Default

By default, ISIS uses 500 milliseconds and 50,000 milliseconds for the minimum and maximum hold intervals, respectively. The values are applied to both level-1 and level-2 if the `level` parameter is omitted.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#spf-interval-exp level-1 600 60000

(config)#router isis bb
(config-router)#no spf-interval-exp
```

summary-address

Use this command to configure Summary Address to summarize IPv4 reachability information.

Use the `no` parameter with this command to unconfigure the summary.

Command Syntax `summary-address A.B.C.D/M (level-1|level-1-2|level-2) metric (<1-63>) no summary-address A.B.C.D/M`

Parameters

`A.B.C.D/M`	Specify the IPv4 prefix to be announced.
`level-1`	Specify the reachability information only for Level-1.
`level-1-2`	Specify the reachability information for both Level-1 and Level-2.
`level-2`	Specify the reachability information only for Level-2.
`metric`	Specify the metric for the summarized address.
`<1-63>`	Specify the metric. The default is 0.

Default

By default, ISIS does not configure the summary-address. Summary-address is applied to Level-2 IS if level parameter is omitted.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router isis bb
(config-router)#summary-address 10.10.0.0/16 level-1-2 metric 3

(config)#router isis bb
(config-router)#no summary-address 10.10.0.0/16
```

CHAPTER 2 IS-IS Show Commands

This chapter provides describes the IS-IS show commands:

- show clns is-neighbors
- show clns neighbors
- show debugging isis
- show ip isis igp-shortcut-lsp
- show ip isis route
- show ip isis route igp-shortcut
- show ip protocols
- show isis counter
- show isis database
- show isis interface
- show isis tag database
- show isis topology
- show running-config interface isis
- show running-config router isis

show clns is-neighbors

Use this command to display IS neighbor adjacencies.

Command Syntax `show clns is-neighbors (detail|) show clns WORD is-neighbors (detail|) show clns is-neighbors IFNAME (detail|) show clns WORD is-neighbors IFNAME (detail|)`

Parameters

`detail`	Detailed information.
`WORD`	Information for a single IS-IS area.
`IFNAME`	Information for a single interface.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show clns is-neighbors detail
Tag abc: VRF : default
System Id      Interface   State  Type Priority  Circuit Id
0000.0000.0003 eth1        Up     L1   64        0000.0000.0003.01
L1 Adjacency ID: 1
L2 Adjacency ID: 2
Uptime: 00:12:31
Area Address(es): 52
IP Address(es): 11.11.11.2
Level-1 Protocols Supported: IPv4
Adjacency advertisement: Advertise
#
```

Table 2-145 explains the fields in the output.

Table 2-145: show clns is-neighbors output

Field	Description
Tag	Name that identifies the IS-IS area.
VRF	VRF name.
System Id	Uniquely identifies a system within an area.
Interface	Interface from which the system was learned.

Table 2-145: show clns is-neighbors output (Continued)

Field	Description
State	Adjacency state: Init: Router is an IS and is waiting for an IS-IS hello message. IS-IS regards the neighbor as not adjacent. Up: IS is considered reachable
Type	Type of adjacency: L1: Router adjacency for level 1 routing only L2: Router adjacency for level 2 only L1L2: Router adjacency for level 1 and level 2 routing
Priority	IS-IS priority that the respective neighbor is advertising. The highest priority neighbor is elected the designated ISIS router for the interface.
Circuit Id	Number that the router uses to uniquely identify its IS-IS interface. When the interface is attached to a broadcast network, the Circuit ID is concatenated with System ID of the designated router for the interface.
Adjacency ID	Adjacency identifier.
Uptime	How long the adjacency has existed.
Area Addresses	Area addresses associated with the intermediate-system adjacencies.
IPv4/IPv6 address(es)	IP addresses of the ES or IS.
Protocols Supported	IPv4 and/or IPv6.
Adjacency advertisement	Restart: Suppress or Advertise.

show clns neighbors

Use this command to display ES and IS neighbor adjacencies.

Command Syntax `show clns neighbors (detail|)`

`show clns WORD neighbors (detail|) show clns neighbors IFNAME (detail|) show clns WORD neighbors IFNAME (detail|)`

Parameters

`detail` Detailed information for all interfaces.

WORD	Information for a single IS-IS area.
IFNAME	Information for a single interface.

Command Mode

Exec mode, Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show clns neighbors detail

Tag abc: VRF : default
System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0000.0003 eth1        0800.277b.411d  Up     6         L1   IS-IS
L1 Adjacency ID:  1
L2 Adjacency ID:  2
Uptime: 00:15:58
Area Address(es): 52
IP Address(es): 11.11.11.2
Level-1 Protocols Supported: IPv4
Adjacency advertisement: Advertise
#
```

Table 2-146 explains the fields in the output.

Table 2-146: show clns neighbors output

Field	Description
Tag	Name that identifies the IS-IS area.
VRF	VRF name.
System Id	Uniquely identifies a system within an area.
Interface	Interface from which the system was learned.

Table 2-146: show clns neighbors output (Continued)

Field	Description
SNPA	SubNetwork Point of Attachment (SNPA): MAC address of the next-hop.
State	Adjacency state: Init: Router is an IS and is waiting for an IS-IS hello message. IS-IS regards the neighbor as not adjacent. Up: ES or IS is considered reachable

Holdtime	Number of seconds before this adjacency entry times out.
Type	Type of adjacency: L1: Router adjacency for level 1 routing only L2: Router adjacency for level 2 only L1L2: Router adjacency for level 1 and level 2 routing
Protocol	Protocol through which the adjacency was learned.
Adjacency ID	Adjacency identifier.
Uptime	How long the adjacency has existed.
Area Addresses	Area addresses associated with the intermediate-system adjacencies.
IPv4/IPv6 address(es)	IP addresses of the ES or IS.
Topology	IPv4 and/or IPv6.
Protocols Supported	IPv4 and/or IPv6.
Adjacency advertisement	Restart: Suppress or Advertise.

show debugging isis

Use this command to display the status of the debugging of the ISIS system.

Command Syntax `show debugging isis`

Parameters

None

Command Mode

Exec mode, Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show debugging isis
```

```
IS-IS debugging status:
IS-IS Interface FSM debugging is on
IS-IS Neighbor FSM debugging is on
IS-IS events debugging is on
IS-IS PDU debugging is on
IS-IS lsp debugging is on
IS-IS spf debugging is on
IS-IS NSM debugging is on
IS-IS Check-sum debugging is on
IS-IS Authentication debugging is on
IS-IS Protocol-error debugging is on
IS-IS Local Updates debugging is on
IS-IS Hello debugging is on
IS-IS BFD debugging is on
IS-IS MPLS debugging is on
IS-IS RIB debugging is on
#
```

show ip isis igp-shortcut-lsp

Use this command to display IS-IS shortcut MPLS label-switched paths (LSPs).

Command Syntax `show ip isis (WORD|) igp-shortcut-lsp`

Parameters

`WORD`	Information for a single IS-IS area.

Command Mode

Exec mode, Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip isis igp-shortcut-lsp
#
```

Table 2-147 explains the fields in the output.

Table 2-147: show ip isis igp-shortcut-lsp output

Field	Description
Tunnel-endpoint	Tunnel endpoint address.
Tunnel-id	Tunnel identifier.

Tunnel-metric	Tunnel metric.
active/inactive	Whether the tunnel is active or inactive.

show ip isis route

Use this command to display IS-IS routing table for IPv4.

Command Syntax `show ip isis (WORD|) route`

Parameters

`WORD` Information for a single IS-IS area.

Command Mode

Exec mode, Privileged exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip isis route
Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, D - discard, e - external metric
Tag xyz: VRF : default
          Destination         Metric      Next-Hop            Interface      Tag
L1        10.10.10.0/24       20          11.11.11.1          eth1           0 C
11.11.11.0/24        10          -                   eth1            0 #
```

Header

Each entry in this table has a code preceding it, indicating the source of the routing entry. Table 2-148 shows these codes.

Table 2-148: Route codes and modifiers

Code	Description
C	Routes directly connected to the local device that were not distributed via IGP. The device inherently knows of these networks, so there is no need to learn about these from another device. Connected routes are preferred over routes for the same network learned from other routing protocols.
E	External.
L1	IS-IS level-1.

L2	IS-IS level-2.
ia	IS-IS inter area (leaked).

Table 2-148: Route codes and modifiers (Continued)

Code	Description
D	Discard route. A device performing summarization installs a discard route in its routing table for the summarized network range to prevent routing loops where portions of the summarized network range do not have a more specific route in the RIB. External and internal discard route entries are installed by default. During route summarization, routing loops can happen if data sent to a nonexisting network appears to be a part of the summary, and the router doing the summarization has a less specific route that points back to the sending router for the network.
e	External metric. Routes can be redistributed into IS-IS with either internal or external metrics (internal is the default). The metric type determines the base metric value of the redistributed routes. The value of an internal metric is lower than 64. The value of an external metric is 64-128.

Route Entry Fields

Table 2-149 shows the route entry fields.

Table 2-149: Route entry fields

Field	Description
Code	As explained in Table 2-148.
Tag	Name that identifies the IS-IS area.
VRF	VRF name.
Destination	IP address of the remote network.
Metric	ISIS metric used for SPF calculation (1-63). When a route is imported into the IS-IS network without a specified metric, IS-IS uses 10 for the metric value and the value is applied to both level-1 and level-2.
Next-Hop	This route is available through the next hop router located at this IP address. This identifies exactly where packets go when they match this route.
Interface	Interface used to get to the next-hop address for this route.
Tag	Name that identifies the IS-IS area.

show ip isis route igp-shortcut

Use this command to display the IS-IS IGP shortcut routing table.

Command Syntax `show ip isis (WORD|) route igp-shortcut`

Parameters

`WORD`	Information for an IS-IS area.

Command Mode

Exec mode, Privileged exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip isis new_isis route igp-shortcut
Codes: C - connected, E - external, L1 - IS-IS level-1, L2 - IS-IS level-2 ia
- IS-IS inter area, D - discard, e - external metric

Tag aa: VRF : default
     Destination         Metric      Tunnel-ID         Tunnel-End-Point #
```

Header

Each entry in this table has a code preceding it, indicating the source of the routing entry. Table 2-150 shows these codes.

Table 2-150: Route codes and modifiers

Code	Description
C	Routes directly connected to the local device that were not distributed via IGP. The device inherently knows of these networks, so there is no need to learn about these from another device. Connected routes are preferred over routes for the same network learned from other routing protocols.
E	External.
L1	IS-IS level-1.
L2	IS-IS level-2.
ia	IS-IS inter area (leaked).

Table 2-150: Route codes and modifiers (Continued)

Code	Description
D	Discard route. A device performing summarization installs a discard route in its routing table for the summarized network range to prevent routing loops where portions of the summarized network range do not have a more specific route in the RIB. External and internal discard route entries are installed by default. During route summarization, routing loops can happen if data sent to a nonexisting network appears to be a part of the summary, and the router doing the summarization has a less specific route that points back to the sending router for the network.
e	External metric. Routes can be redistributed into IS-IS with either internal or external metrics (internal is the default). The metric type determines the base metric value of the redistributed routes. The value of an internal metric is lower than 64. The value of an external metric is 64-128.

Route Entry Fields

Table 2-151 shows the route entry fields.

Table 2-151: Route entry fields

Field	Description
Code	As explained in Table 2-148.
Tag	Name that identifies the IS-IS area.
VRF	VRF name.
Destination	IP address.
Metric	Tunnel metric.
Tunnel-ID	Tunnel identifier.
Tunnel-End-Point	Tunnel endpoint address.

show ip protocols

Use this command to display IP process parameters and statistics.

Command Syntax `show ip protocols show ip protocols isis`

Parameters

None

Command Mode

Exec mode, Privileged exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip protocols
Routing Protocol is "isis 1 "
Redistributing:
Area Address(es): 52
Distance : (default is 115)
#
```

Table 2-152 explains the output fields.

Table 2-152: show ip protocols output

Field	Description
Routing Protocol	“isis” and the name that identifies the IS-IS area.
Redistributing	Protocols being redistributed (such as RIP, OSPF, or BGP), including metric, metric type (internal or external), and route map.
redistribute isis	Whether redistributing IS-IS level-1 into level-2 and vice versa.
Area Address	Network address of the areas into which the routing process is injecting routes.
Distance: (default is 115)	Administrative distance.

show isis counter

Use this command to display the MIB variables used to construct routing tables for IP networks for IS-IS as defined in RFC 4444.

Command Syntax `show`

```
isis counter
```

Parameters

None

Command Mode

Exec mode, Privileged exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show isis counter
Tag abc: VRF : default
IS-IS Level-1 isisSystemCounterEntry:
isisSysStatCorrLSPs: 0
isisSysStatAuthTypeFails: 0
isisSysStatAuthFails: 0
isisSysStatLSPDbaseOloads: 0
isisSysStatManAddrDropFromAreas: 0
isisSysStatAttmptToExMaxSeqNums: 0
isisSysStatSeqNumSkips: 0
isisSysStatOwnLSPPurges: 0
isisSysStatIDFieldLenMismatches: 0
isisSysStatMaxAreaAddrMismatches: 0
isisSysStatPartChanges: 0
isisSysStatSPFRuns: 7
isisSysStatPRCRuns: 0

IS-IS Level-2 isisSystemCounterEntry:
isisSysStatCorrLSPs: 0
isisSysStatAuthTypeFails: 0
isisSysStatAuthFails: 0
isisSysStatLSPDbaseOloads: 0
isisSysStatManAddrDropFromAreas: 0
isisSysStatAttmptToExMaxSeqNums: 0
isisSysStatSeqNumSkips: 0
isisSysStatOwnLSPPurges: 0
isisSysStatIDFieldLenMismatches: 0
isisSysStatMaxAreaAddrMismatches: 0
isisSysStatPartChanges: 0
isisSysStatSPFRuns: 3
isisSysStatPRCRuns: 0
#
```

show isis database

Use this command to display link-state database (LSDB) database information. The LSDB is the core of IS-IS routing. All link-state information advertised by neighbors in the same area is stored in the LSDB.

Command Syntax `show isis database show isis database (detail|verbose) show isis database (detail|verbose) WORD show isis database (detail|verbose) WORD (l1|l2|level-1|level-2) show isis database (detail|verbose) (l1|l2|level-1|level-2) show isis database (detail|verbose) (l1|l2|level-1|level-2) WORD show isis database WORD show isis database WORD (l1|l2|level-1|level-2) show isis database WORD (l1|l2|level-1|level-2) (detail|verbose) show isis database WORD (detail|verbose) show isis database WORD`

```
(detail|verbose) (l1|l2|level-1|level-2) show isis database
(l1|l2|level-1|level-2) show isis database (l1|l2|level-1|level-
2) (detail|verbose) show isis database (l1|l2|level-1|level-2)
(detail|verbose) WORD show isis database (l1|l2|level-1|level-
2) WORD
show isis database (l1|l2|level-1|level-2) WORD (detail|verbose)
```

Parameters

detail	Detailed information.
verbose	Verbose information.
WORD	Link-state packet (LSP) identifier in the form of XXXX.XXXX.XXXX.XX-XX.
l1	IS-IS level-1.
l2	IS-IS level-2.
level-1	IS-IS level-1.
level-2	IS-IS level-2.

Command Mode

Exec mode, Privileged exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show isis database detail
Area bb:
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
000F.0000.0001.00-00* 0x00000007   0xE15E        1188              1/0/0
  Area Address: 49.000F
  NLPID:        0xCC
  IP Address:   10.10.12.97
  Metric: 10         IP 10.10.12.0 255.255.255.0
  Metric: 10         IS 000F.0000.0001.02
000F.0000.0001.02-00* 0x00000003   0x3C66        1026              1/0/0
  Metric:   0        IS 000F.0000.0001.00
  Metric:   0        IS 000F.0000.0002.00
000F.0000.0002.00-00  0x00000003   0x8C4B        1025              1/0/0
  Area Address: 49.000F
  NLPID:        0xCC
  Hostname:     isisd@redhat
  IP Address:   10.10.12.94
  Metric: 10         IP 10.10.12.0 255.255.255.0
  Metric: 10         IS 000F.0000.0001.02 #
```

Table 2-153 explains the output fields.

Table 2-153: show isis database output

Field	Description
Tag	Name that identifies the IS-IS area.
VRF	VRF name.
IS-IS Level-n Link State Database	Each IS-IS level has a section with Link-State Packet (LSP) information.
LSPID	Link-state packet identifier in the form of XXXX.XXXX.XXXX.XX-XX. The first six octets (“XXXX.XXXX.XXXX”) are the system identifier of the router that originated the LSP. The next octet is the pseudonode identifier: • When this octet is nonzero, the LSP describes links from a designated router (pseudonode) that creates and floods an LSP that describes all systems attached to the network. This mechanism is similar to a router link-state advertisement (LSA) in OSPF. • When this octet is zero, the LSP is from a nonpseudonode which describes the state of the originating router. The last octet is the LSP number. If the value is 0x00, the entire LSP was carried in one LSP. If there is more data than can fit in a single LSP, the LSP is divided into multiple LSP fragments and each fragment has a different LSP number. An asterisk (*) means the LSP originated on the system where the command was given.
LSP Seq Num	LSP sequence number.
LSP Checksum	LSP checksum.
LSP Holdtime	Amount of time the LSP remains valid (in seconds). An LSP hold time of zero means the LSP was purged and is being removed from the link-state database (LSDB) of all routers. The value indicates how long the purged LSP will stay in the LSDB before being completely removed.
ATT	Attached bit. A Level-2 IS indicates its attachment to other areas by setting its attached bit in its Level-1 LSP 0. In other words, this is only set for inter-area routes. Level 1-only routers and Level 1-2 routers that have lost connection to other Level 2 routers will use the attach bit to find the closest Level-2 router. They will point a default route to the closest Level-2 router.

Table 2-153: show isis database output

Field	Description
P	Partition repair. A Level-1 area can become partitioned; this bit means the partition can be repaired via use of Level-2 routes.
OL	Overload bit. Determines whether the IS is congested. When the overload-bit is set in an LSP, other routers will not use this router as a transit router during SPF calculation. Only packets for destinations directly connected to the overloaded router will be sent to this router.

This command also displays information about the IS-IS TLVs in Table 2-154 if present in an LSP. For more about the TLV information, search for “IS-IS TLV Codepoints” on the Interne, check ISO/IEC 10589:2002(E), or other standard mentioned in Table 2-154.

Table 2-154: IS-IS TLV Codepoints

IS-IS TLV Codepoint	Description	Standard
1	Area Addresses	ISO 10589
2	IIS Neighbors	ISO 10589
3	ES Neighbors	ISO 10589
10	Authentication	ISO 10589, RFC 6233
22	Extended IS reachability	RFC 5305
128	IP internal reachability	RFC 1195, RFC 5302
129	Protocols supported	RFC 1195
130	IP external reachability	RFC 1195, RFC 5302
132	IP interface address	RFC 1195
134	Traffic engineering router ID	RFC 5305
135	Extended IP reachability	RFC 5305

137	Host name	RFC 5301, RFC 6233
222	Multi IS reachability	RFC 5120
229	Multi topology	RFC 5120
232	IPv6 interface address	RFC 5308
235	Multi IPv4 reachability	RFC 5120
236	IPv6 reachability	RFC 5308
237	Multi IPv6 reachability	RFC 5120

show isis interface

Use this command to display detailed interface information.

Command Syntax `show isis interface show isis interface IFNAME show isis interface counter`

Parameters

`IFNAME`	Interface name.
`counter`	Interface counters.

Command Mode

Exec mode, Privileged exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
>show isis interface eth2 is up, line
protocol is up
Routing Protocol: IS-IS (abc)
Network Type: Broadcast
Circuit Type: level-2
Local circuit ID: 0x01
Extended Local circuit ID: 0x00000004 Local SNPA:
0800.2731.a9a0
IP interface address:
10.10.10.1/24 IPv6 interface address:
fe80::a00:27ff:fe31:a9a0/64
```

```
Level-2 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0001.01
Number of active level-2 adjacencies: 0
Level-2 LSP MTU: 1492
Next IS-IS LAN Level-2 Hello in 9 seconds eth1 is
up, line protocol is up
Routing Protocol: IS-IS (abc)
Network Type: Broadcast
Circuit Type: level-1
Local circuit ID: 0x02
Extended Local circuit ID: 0x00000003 Local SNPA:
0800.2714.e7f8
IP interface address:
11.11.11.1/24 IPv6 interface address:
fe80::a00:27ff:fe14:e7f8/64
Level-1 Metric: 10/10, Priority: 64, Circuit ID: 0000.0000.0003.01
Number of active level-1 adjacencies: 1
Level-1 LSP MTU: 1492
Next IS-IS LAN Level-1 Hello in 5 seconds

>show isis interface eth1 eth1 is up,
line protocol is up Routing Protocol:
IS-IS ((null))
Network Type: Broadcast
Circuit Type: level-1
Local circuit ID: 0x02
Extended Local circuit ID: 0x00000003 Local
SNPA: 0800.27e3.0e64
IP interface address:
30.0.0.1/24
IPv6 interface address: fe80::a00:27ff:fee3:e64/64
LDP-ISIS Sync Configured
Holddown timer = 100 seconds, Remaining time = 90 seconds
Level-1 Metric: 63/16777214, Priority: 64, Circuit ID: 0000.0000.0001.02
Number of active level-1 adjacencies: 1
Level-1 LSP MTU: 1492
Next IS-IS LAN Level-1 Hello in 1 seconds
```

Table 2-155 explains the output fields.

Table 2-155: show isis interface

Field	Description
IFNAME is up, line protocol is up/down	Whether the interface is up or down
Routing Protocol	“IS-IS” and the name that identifies the IS-IS instance.

Network Type	• Broadcast • Point-to-Point • Loopback
Circuit Type	Whether the interface is configured for: • Local routing: level-1 • Area routing: level 2 • Local and area routing: level-1-2
Local circuit ID	Local circuit identifier assigned when interface is created. Each IS-IS interface is assigned a circuit identifier to identify the interface within the link-state database. If the interface is attached to a multiaccess network, the circuit ID is concatenated with the system ID of the designated IS. This is called the pseudonode ID.
Extended Local circuit ID	Interface index.
Local SNPA	SubNetwork Point of Attachment: for broadcast networks, MAC address.
IP interface address	IPv4 addresses assigned to IS-IS interface.
IPv6 interface address	IPv6 addresses assigned to IS-IS interface.
LDP-ISIS Sync Configured	LDP IS-IS synchronization is enabled.

Table 2-155: show isis interface (Continued)

Field	Description
Holddown timer	Delay for notifications of LDP convergence to IS-IS
Remaining time	Remaining LDP convergence hold time in seconds.
Holddown timer not configured	The LDP convergence holddown timer has not been set.
Level-1 Metric	Interface metric value; used for SPF calculation.
Priority	Priority for designated IS election.
Circuit ID	Unique ID assigned to a circuit internally.

Number of active level-1 adjacencies	Number of adjacencies formed with a neighboring router.
Level-1 LSP MTU	Maximum transmission unit: maximum transmission size for a packet on this interface.
Level-2 Metric	Interface metric value; used for SPF calculation.
Priority	Priority for designated IS election.
Circuit ID	Unique ID assigned to a circuit internally.
Number of active level-2 adjacencies	Number of adjacencies formed with a neighboring router.
Level-2 LSP MTU	Maximum transmission unit: maximum transmission size for a packet on this interface.
Next IS-IS LAN Level-1 Hello	For broadcast networks, when the next IS hello will be sent on this interface.
Next IS-IS LAN Level-2 Hello	For broadcast networks, when the next IS hello will be sent on this interface.
Next IS-IS Hello in	For point-to-point networks, when the next IS hello will be sent on this interface.
Bandwidth	Traffic engineering: interface bandwidth.
Maximum reservable bandwidth	Traffic engineering: maximum reservable interface bandwidth.
Available bandwidth at priority	Traffic engineering: available interface bandwidth at priority.
Bidirectional Forwarding Detection is disabled/enabled/ configured	BFD state

show isis tag database

Use this command to display detailed link-state database information for an IS-IS routing area.

Command Syntax `show isis WORD database show isis WORD database (detail|verbose) show isis WORD database (detail|verbose) WORD show isis WORD database (detail|verbose) WORD (l1|l2|level-1|level-2) show isis WORD database (detail|verbose) (l1|l2|level-1|level-2) show isis WORD database (detail|verbose) (l1|l2|level-1|level-2) WORD show isis WORD database WORD show isis WORD database WORD (l1|l2|level-1|level-2) show isis WORD database WORD (l1|l2|level-1|level-2) (detail|verbose) show isis WORD database WORD (detail|verbose) show isis WORD database WORD (detail|verbose) (l1|l2|level-1|level-2) show isis WORD database (l1|l2|level-1|level-2) show isis WORD database (l1|l2|level-1|level-2) (detail|verbose) show isis WORD database (l1|l2|level-1|level-2) (detail|verbose) WORD show isis WORD database (l1|l2|level-1|level-2) WORD (detail|verbose) show isis WORD database (l1|l2|level-1|level-2) WORD`

Parameters

`WORD`	Name that identifies the IS-IS area.
`detail`	Detailed database information.
`verbose`	Verbose database information.
`WORD`	Link-state packet (LSP) identifier in the form of XXXX.XXXX.XXXX.XX-XX.
`l1`	IS-IS level-1 link state database.
`l2`	IS-IS level-2 link state database.
`level-1`	IS-IS level-1 link state database.
`level-2`	IS-IS level-2 link state database.

Command Mode

Exec mode, Privileged exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#sh isis abc database verbose
Tag abc: VRF : default
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00* 0x00000008   0xA076        1018              0/0/0
Area Address: 52
NLPID: 0xCC
IP Address: 11.11.11.1
Metric: 10 IS 0000.0000.0003.01
Metric: 10 IP 11.11.11.0 255.255.255.0
Metric: 10 IP 10.10.10.0 255.255.255.0
```

```
0000.0000.0003.00-00 0x00000007 0x1CB0 1029 0/0/0
Area Address: 52
NLPID: 0xCC
IP Address: 11.11.11.2
Metric: 10 IS 0000.0000.0003.01
Metric: 10 IP 11.11.11.0 255.255.255.0
0000.0000.0003.01-00 0x00000005 0x0ACB 1000 0/0/0
Metric: 0 IS 0000.0000.0003.00 Metric: 0 IS
0000.0000.0001.00

IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
0000.0000.0001.00-00* 0x00000007   0x7243        988               0/0/0
Area Address: 52
NLPID: 0xCC
IP Address: 11.11.11.1
Metric: 10 IP 11.11.11.0 255.255.255.0
Metric: 10 IP 10.10.10.0 255.255.255.0
```

See Table 2-153 and Table 2-154 for an explanation of the output of this command.

show isis topology

Use this command to display paths to Intermediate Systems.

Command Syntax `show isis topology (l1|l2|level-1|level-2|) show isis WORD topology (l1|l2|level-1|level-2|)`

Parameters

`WORD`	Display information for specified instance.
`l1`	Display the path to all level-1 routers in the area.
`l2`	Display the path to all level-2 routers in the domain.
`level-1`	Display the path to all level-1 routers in the area.
`level-2`	Display the path to all level-2 routers in the domain.

Command Mode

Exec mode, Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show isis topology

Tag abc: VRF : default
IS-IS paths to level-1 routers
System Id            Metric     Next-Hop            Interface   SNPA
000F.0000.0001       --
000F.0000.0002       10         000F.0000.0002      eth2        0006.5B0E.D27D

IS-IS paths to level-2 routers
System Id            Metric     Next-Hop            Interface   SNPA
0000.0000.0001       10         0000.0000.0001      eth2        0000.0CFA.F002
```

Table 2-156 explains the output fields.

Table 2-156: show isis topology output

Field	Description
Tag	Name that identifies the IS-IS area.
VRF	VRF name.
IS-IS paths to leveln routers	Each IS-IS level has a section with topology information.

System Id	Uniquely identifies a system within an area.
Metric	ISIS metric used for SPF calculation (1-63).

Table 2-156: show isis topology output

Field	Description
Next-Hop	This route is available through the next hop router located at this IP address.
Interface	Interface from which the system was learned.
SNPA	SubNetwork Point of Attachment (SNPA): MAC address of the device.

show running-config interface isis

Use this command to display the ISIS interface configuration.

Command Syntax `show running-config interface IFNAME isis`

Parameters

`IFNAME`	Interface name.

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
                                        #show running-config interface eth0 isis
    ! interface eth0 isis tag 500 level-1 !
```

show running-config router isis

Use this command to display the ISIS router configuration.

Command Syntax `show running-config router isis`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
                                    (config-router)#show running-config router isis
!
router isis !
```

© Symanitron Proprietary

Unicast Routing Information Base Command Reference

Contents

This document contains this chapter:

- Chapter 1, *Unicast RIB Commands*

CHAPTER 1 Unicast RIB Commands

This chapter describes the following unicast RIB commands:

- clear ip route kernel
- clear ip route
- clear ip route vrf NAME
- debug rib
- description
- fib retain
- ip route
- ip vrf
- maximum-paths
- max-fib-routes
- max-static-routes
- show debugging rib
- snmp restart rib

clear ip route kernel

Use this command to clear stale IPv4 routes from the RIB (Routing Information Base) and FIB (Forwarding Information Base).

Command Syntax `clear ip route kernel clear ip kernel route`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear ip route kernel
```

clear ip route

Use this command to clear an all IPv4 routes or any specific prefix routes.

Command Syntax `clear ip route (*|A.B.C.D/M)`

Parameters

`*`	Clears all routes
`A.B.C.D/M`	Prefix to be cleared

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear ip route *
#clear ip route 1.1.1.0/24
```

clear ip route vrf NAME

Use this command to clear all IPv4 VRF route or any specific prefix VRF route of any particular VRF name.

Command Syntax `clear ip route vrf NAME (*|A.B.C.D/M)`

Parameters

`NAME`	VPN Routing or Forwarding instance name
`*`	Clears all routes
`A.B.C.D/M`	Prefix to be cleared

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear ip route vrf myVRF *
```

debug rib

Use this command to debug the `ribd` process.

Use the `no` form of this command or the `undebug` command to stop debugging.

Command Syntax `debug rib (all|) debug rib events debug rib packet (recv|send|) (detail|) debug rib nsm debug rib bfd debug rib kernel debug rib monitor debug ip routing (add-route|delete-route|mod-route| no debug all no debug rib (all|) no debug all rib no debug rib events no debug rib packet (recv|send|) (detail|) no debug rib nsm no debug rib bfd no debug rib kernel no debug rib monitor no debug ip routing (add-route|delete-route|mod-route|) undebug all undebug rib (all|) undebug all rib undebug rib events`

`undebug rib packet (recv|send|) (detail|) undebug rib nsm undebug rib bfd undebug rib kernel`

Parameters

`all`	Alldebugging functions
`events`	Events
`packet`	Packet events
`recv`	Received packets
`send`	Sent packets
`detail`	Detailed information
`nsm`	NSM events
`kernel`	RIB kernel
`monitor`	Enable Monitor route netlink
`bfd`	BFD (Bidirectional Forwarding Detection) events
`ip routing`	IPv4 routing events
`add-route`	Add route events
`delete-route`	Delete route events
`mod-route`	Modify route events

Disabled

By default, debug command is disabled.

Command Mode

Privileged Exec mod

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#debug rib all
```

description

Use this command to assign a description to a Virtual Router instance.

Use the `no` parameter to remove a description.

Command Syntax `description LINE no description`

Parameters

`LINE`	Virtual Router description maximum 80 characters

Disabled

By default, description command is disabled

Command Mode

VR mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#virtual-router VR1
(config-vr)#description VR1 has been created for CLI testing (config-vr)#exit

(config)#virtual-router VR1
(config-vr)#no description
(config-vr)#exit
```

fib retain

Use this command to set the retention time for stale routes in the Forwarding Information Base (FIB) when `ribd` restarts. The `ribd` process reads the FIB and treats previously self-installed routes as stale.

You can display stale routes by running the `show route database` command. All routes preceded by the symbol `ip p` are stale routes. When protocol modules `ribd` overrides these stale routes with routes updated by the restart, protocol modules.

Table 1-157 show the behavior of routes when `ribd` stops.

Table 1-157: FIB retention

Command	Behavior
`fib retain`	Does not clear routes from the FIB and retains stale routes for 60 seconds when restarted.
`fib retain forever`	Does not clear routes and retains stale routes forever.
`fib retain time <1-65535>`	Does not clear routes and retains stale routes for the specified seconds.
`no fib retain` (default)	Cleans up routes in the FIB, but retains stale routes for 60 seconds when restarted.

You can remove stale routes at any time with the clear ip route kernel command.

Use the `no` form of this command to revert to default; that is, do not retain routes in the FIB when `ribd` stops.

Command Syntax `fib retain (forever|time <1-65535>|) no fib retain (forever|time <1-65535>|)`

Parameters `forever` Retain FIB forever `time` Retain FIB for a time after `ribd` restarts

`<1-65535>` Retention time in seconds; if you omit this value, the default is 60 seconds

Default

Routes are cleared from the FIB when `ribd` stops. However, when `ribd` restarts, stale routes are retained for 60 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#fib retain time 180
```

ip route

Use this command to create an IPv4 static route.

Use the `no` form of this command to delete a static route.

Command Syntax `ip route A.B.C.D/M (A.B.C.D|IFNAME) ip route A.B.C.D A.B.C.D (A.B.C.D|IFNAME) ip route A.B.C.D/M (A.B.C.D|IFNAME){<1-255>|tag <0-`

4294967295>|description WORD} ip route A.B.C.D A.B.C.D (A.B.C.D|IFNAME){<1-255>|tag <0-4294967295>|description

WORD} ip route vrf NAME A.B.C.D/M IFNAME ip route vrf NAME A.B.C.D/M A.B.C.D IFNAME ip route vrf NAME A.B.C.D/M A.B.C.D IFNAME global ip route vrf NAME A.B.C.D/M IFNAME {<1-255>|tag <0-4294967295>|description WORD} ip route vrf NAME A.B.C.D/M A.B.C.D IFNAME {<1-255>|tag <0-4294967295>|description

WORD} no ip route A.B.C.D/M (A.B.C.D|IFNAME|) no ip route A.B.C.D A.B.C.D (A.B.C.D|IFNAME) no ip route A.B.C.D/M (A.B.C.D|IFNAME){<1-255>|tag <0-4294967295>|description WORD} no ip route A.B.C.D A.B.C.D (A.B.C.D|IFNAME){<1-255>|tag <0-4294967295>|description

WORD} no ip route vrf NAME A.B.C.D/M IFNAME no ip route vrf NAME A.B.C.D/M A.B.C.D IFNAME no ip route vrf NAME A.B.C.D/M IFNAME {<1-225>|tag <0-4294967295>|description WORD} no ip route vrf NAME A.B.C.D/M A.B.C.D IFNAME {<1-255>|tag <0-

4294967295>|description WORD}

Parameters

A.B.C.D/M Subnet: IP destination prefix and a mask length

A.B.C.D A.B.C.D

Subnet: IP destination address and mask

A.B.C.D Gateway nexthop IPv4 address

global Global table lookup (to support inter-VRF static route leaking)

<1-255> Administrative distance IFNAME

Gateway nexthop interface name

description Description of the static route maximum 80 character tag Tag

used as a “match” value to control redistribution via route maps

<0-4294967295>

Tag value

vrf VRF (Virtual Routing and Forwarding) instance

NAME VRF name

Default

By default, no static IPv4 route configured

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3 and was updated in SWMRE version 1.3.4.

Examples

```
#configure terminal
(config)#ip route 192.168.3.0 255.255.255.0 2.2.2.2
128 (config)#ip route 1.1.1.0/24 eth0 32
(config)#ip route vrf new 1.1.1.1/1 1.1.1.1 eth1 description new tag 1
```

This example creates VRF static routes with the nexthops belonging to the default VRF. The nexthop gateway address can be the IFNAME network address or any other IP address reachable via IFNAME.

```
 #show ip route vrf
 Codes: K - kernel,  C - connected, S - static, R - RIP, B - BGP
        O -  OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
v - vrf leaked        * - candidate default

IP Route Table for VRF "default"
C     10.12.19.0/24 is directly connected, eth0, 4d23h06m
C11.1.1.0/24 is directly connected, eth4, 4d23h01m
C13.13.13.0/31 is directly connected, eth3, 4d23h06m
C50.5.5.0/24 is directly connected, eth3, 4d23h06m
C100.100.100.0/24 is directly connected, lo, 4d23h06m
O101.1.1.1/32 [110/11] via 11.1.1.2, eth4, 19:20:39
C 127.0.0.0/8 is directly connected, lo, 4d23h06m
Gateway of last resort is not set

(config)#ip route vrf vrf1 201.201.201.201/32 11.1.1.11 eth4
global (config)#ip route vrf vrf1 202.202.202.202/32 101.1.1.1
eth4 global
#show ip route vrf vrf1 static
IP Route Table for VRF "vrf1"
S    v201.201.201.201/32 [1/0] via 11.1.1.11, eth4, 00:00:44
S     v202.202.202.202/32 [1/0] via 101.1.1.1, eth4 (recursive via 11.1.1.2), 00:00:17
Gateway of last resort is not set
```

ip vrf

This command creates a VRF (Virtual Routing and Forwarding) RIB (Routing Information Base), assigns a VRF identifier, and switches to VRF mode.

Use the `no` parameter with command to remove a VRF RIB.

Command Syntax `ip  vrf`

```
WORD no ip vrf WORD
```

Parameter

`WORD`	VRF identifier

Default

By Default, ip vrf is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ip vrf myVRF
(config-vrf)#
```

maximum-paths

Use this command to set the maximum number of paths to install in the FIB (Forwarding Information Base) for the ECMP (Equal-Cost MultiPath) feature.

Use the `no` parameter with this command to revert to default.

Note: If you change the number of paths from the default (8), you must save the running configuration and perform a reboot.

Command Syntax `maximum-paths <1-64>` `no maximum-paths`

Parameter

`<1-64>`	Maximum number of paths to install in the FIB

Default

By default, the maximum number of paths is 8.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
```

```
(config)#maximum-paths 5
```

max-fib-routes

Use this command to set the maximum number of FIB (Forwarding Information Base) routes including kernel, connected, and static routes.

Use the `no` parameter to remove this configuration.

Command Syntax `max-fib-routes <1-16384> no max-fib-routes`

Parameters

`<1-16384>`	Maximum number of FIB routes, including kernel, connected, and static routes

Default

By default, no FIB routes configured.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#max-fib-routes 12345

(config)#no max-fib-routes
```

max-static-routes

Use this command to set the maximum number of static routes.

Use the `no` parameter to disable this command.

Command Syntax `max-static-routes <1-4294967294> no max-static-routes`

Parameters

`<1-4294967294>` Maximum number of static routes

Default

By default, max static routes value is 4294967294

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#max-static-routes 123

(config)#no max-static-routes
```

show debugging rib

Use this command to display debug settings.

Command Syntax `show debugging rib`

Parameters

None

Command Mode

Privileged Exec Mode and Exec Mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show debugging rib
```

snmp restart rib

Use this command to restart SNMP in Routing Information Base (RIB)

Command Syntax `snmp restart rib`

Parameters

None

Default

By default, snmp restart command is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#config terminal
(config)#snmp restart rib
```

Routing Information Protocol Command Reference

Contents

This document contains these chapters and appendix:

- Chapter 1, *Routing Information Protocol Commands*
- Chapter 2, *RIPng Commands*
- Chapter 3, *Routing Information Protocol VPN Commands*
- Appendix A, *Routing Information Protocol Authentication*

CHAPTER 1 Routing Information Protocol Commands

This chapter provides an alphabetized reference for each of the Routing Information Protocol (RIP) commands, which support IPv4. It includes the following commands:

- accept-lifetime
- cisco-metric-behavior
- clear ip rip route
- clear ip rip route vrf NAME
- clear ip rip statistics
- debug rip
- default-information originate
- default-metric
- distance
- distribute-list
- ip rip authentication key-chain
- ip rip authentication mode
- ip rip authentication string
- ip rip receive-packet
- ip rip receive version
- ip rip send-packet
- ip rip send version
- ip rip split-horizon
- key
- key chain
- key-string
- maximum-prefix
- neighbor
- network
- offset-list
- passive-interface
- recv-buffer-size
- redistribute
- route
- router rip
- send-lifetime
- show debugging rip
- show ip protocols rip

- show ip rip
- show ip rip interface
- show ip rip statistics
- snmp restart rip
- timers basic
- version

accept-lifetime

Use this command to specify the time period during which the authentication key on a key chain is received as valid.

Use the `no` option with this command to disable it.

See Appendix A, *Routing Information Protocol Authentication* for information on how this command is related to the other authentication commands.

Command Syntax `accept-lifetime HH:MM:SS <1-31> MONTH <1993-2035> HH:MM:SS <1-31> MONTH <1993-2035> accept-lifetime HH:MM:SS <1-31> MONTH <1993-2035> HH:MM:SS MONTH <1-31> <1993-2035> accept-lifetime HH:MM:SS MONTH <1-31> <1993-2035> HH:MM:SS <1-31> MONTH <1993-2035> accept-lifetime HH:MM:SS MONTH <1-31> <1993-2035> HH:MM:SS MONTH <1-31> <1993-2035> accept-lifetime HH:MM:SS <1-31> MONTH <1993-2035> infinite accept-lifetime HH:MM:SS MONTH <1-31> <1993-2035> infinite accept-lifetime HH:MM:SS <1-31> MONTH <1993-2035> duration <1-2147483646> accept-lifetime HH:MM:SS MONTH <1-31> <1993-2035> duration <1-2147483646> no accept-lifetime`

Parameters

`HH:MM:SS`	Specify the start time of accept-lifetime in hours, minutes and seconds.
`<1-31>`	Specify the day of the month to start.
`MONTH`	Specify the month of the year to start (the first three letters of the month, for example, `Jan.`).
`<1993-2035>`	Specify the year to start.
`HH:MM:SS`	Specify the time when accept-lifetime expires in hours, minutes and seconds.
`<1-31>`	Specify the day of the month to expire.
`MONTH`	Specify the month of the year to expire (the first three letters of the month, for example, `Jan.`).
`<1993-2035>`	Specify the year to expire.
`duration`	Specify the duration of the key in seconds <1-2147483646>.
`infinite`	Specify the end time to never expire.

Default

None

Command Mode

Keychain-key mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows the setting of accept-lifetime for `key1` on the key chain named `mychain`.

```
#configure terminal
(config)#key chain mychain
(config-keychain)#key 1
(config-keychain-key)#accept-lifetime 03:03:01 Dec 3 2004 04:04:02 Oct 6 2006

(config)#key chain mychain
(config-keychain)#key 1
(config-keychain-key)#no accept-lifetime
```

cisco-metric-behavior

Use this command to enable the metric update consistent with Cisco.

Use either the `no` or `disable` parameter with this command to disable this feature.

Command Syntax `cisco-metric-behavior`

`(enable|disable) no cisco-metric-behavior`

Parameters

`enable`	Enable updating the metric consistent with Cisco.
`disable`	Disable updating the metric consistent with Cisco.

Default

By default, the Cisco metric-behavior is disabled.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

This example shows how to enable the metric update behavior to be consistent with Cisco in the Router mode.

```
#configure terminal
(config)#router rip
 (config-router)#cisco-metric-behavior enable
```

clear ip rip route

Use this command to clear specific data from the RIP routing tables.

Using this command with the `all` parameter, clears the RIP table of all the routes. If you do not want that your RIP network to be deleted, use the `redistribute connected` command and make the RIP network a connected route. To delete the RIP routes learned from neighbor and also keep the RIP network intact, use the `rip` (`clear ip rip route rip`) parameter with this command.

Command Syntax `clear ip rip route (A.B.C.D/M|rip|kernel|connected|static|ospf|isis|bgp|all)` **Parameters**

`A.B.C.D/M`	Removes entries which exactly match this destination address from RIP routing table.
`bgp`	Removes only BGP routes from the RIP routing table.
`connected`	Removes entries for connected routes from the RIP routing table.
`isis`	Removes only IS-IS routes from the RIP routing table
`kernel`	Removes kernel entries from the RIP routing table.
`ospf`	Removes only OSPF routes from the RIP routing table.

rip	Removes only RIP routes from the RIP routing table.
static	Removes static entries from the RIP routing table.
all	Removes the entire RIP routing table.

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear ip rip route 10.0.0.0/8
#clear ip rip route ospf
```

clear ip rip route vrf NAME

Use this command to clear all IPv4 RIP VRF route or any specific prefix RIP VRF route of any particular VRF name.

Command Syntax `clear ip rip route vrf NAME (*|A.B.C.D/M)`

Parameters

A.B.C.D/M	Removes entries with the prefix specified.
*	Removes all routes
NAME	VPN Routing or Forwarding instance name

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear ip rip route vrf myVRF *
```

clear ip rip statistics

Use this command to clear an IPv4 RIP statistics.

Command Syntax `clear ip rip statistics (IFNAME |)`

Parameters

IFNAME	Removes entries from the interface.

Default

None

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear ip rip statistics
```

debug rip

Use this command to specify the options for the displayed debugging information for RIP events, RIP packets and RIP NSM.

Use the `no` parameter with this command to disable all debugging. The `undebug` alias command can also be used.

Command Syntax `debug rip (all|) debug rip bfd debug rip events debug rip nsm debug rip packet (recv|send|) (detail|) debug rip rib no debug rip (all|) no debug rip bfd no debug rip events no debug rip nsm no debug rip packet (recv|send|) (detail|) no debug rip rib undebug rip (all|) undebug rip bfd undebug rip events undebug rip nsm undebug rip packet (recv|send|) (detail|) undebug rip rib`

Parameters

`all`	Debug all RIP information.
`bfd`	Debug all RIP and BFD information.
`events`	Debug RIP events.
`nsm`	Debug RIP and NSM communications.
`packet`	Debug RIP packets, only
`recv`	Debug received packets.
`rib`	Debug RIP and RIB communications.
`send`	Debug sent packets.
`detail`	Display detailed information for the sent or received packet.

Default

Disabled

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example specifies the options for the displayed debugging information in `Configure` mode prompt.

```
#configure terminal
(config)#debug rip events
(config)#debug rip packet send detail
```

```
(config)#debug rip nsm
```

The following example shows to disable all debugging in `Privileged Exec` mode prompt.

```
#undebug rip events
#undebug rip packet send detail
#undebug rip nsm
```

default-information originate

Use this command to add default routes to the RIP updates.

Use the `no` parameter with this command to disable this feature.

Command Syntax `default-information originate (always|) (route-map WORD|) no default-information originate`

Parameters

`always`	Always advertise default route
`route map`	Route map reference
`WORD`	Pointer to route-map entries

Default

Disabled

Command Mode*

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router rip
                    (config-router)#default-information originate route-map pmap
```

default-metric

Use this command to specify the metrics to be assigned to redistributed routers.

This command is used in conjunction with the `redistribute` command to make the routing protocol use the specified metric value for all redistributed routes. A default metric is useful in redistributing routes with incompatible metrics. Every protocol has different metrics and can not be compared directly. Default metric provides the standard to compare. All routes that are redistributed will use the default metric.

Use the `no` parameter with this command to disable this feature.

Command Syntax `default-metric <1-15>`

`no default-metric`

Parameter

`<1-15>`	Specify the default metric.

Default

By default, the metric value is set to 1.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

This example assigns the cost of 10 to the OSPF routes which are redistributed into RIP.

```
#configure terminal
(config)#router rip
(config-router)#redistribute ospf
(config-router)#default-metric 10
```

distance

Use this command to set the administrative distance. The administrative distance is a feature used by the routers to select the path when there are two or more different routes to the same destination from two different routing protocols.
A smaller administrative distance indicating a more reliable protocol.

Use the `no` parameter with this command to disable this function.

Command Syntax `distance <1-255>`

`distance <1-255> A.B.C.D/M (WORD|)`

`no distance (<1-255>|)`

`no distance <1-255> A.B.C.D/M (WORD|)`

Parameters

<1-255>	Specify the administrative distance value.
A.B.C.D./M	Specify the network prefix and length WORD
	Specify the access list name.

Default

By default, the administrative distance is 120.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router rip
(config-router)#distance 8 10.0.0.0/8 mylist
```

distribute-list

Use this command to filter incoming or outgoing route updates using an access list or a prefix list. You can filter out incoming or outgoing route updates using an access list or a prefix list. If you do not specify the name of the interface, the filter will be applied to all the interfaces.

Use the no parameter with this command to disable this feature.

Command Syntax distribute-list WORD (in|out)
(IFNAME|) distribute-listprefix

(IFNAME|) no distribute-list WORD (in|out)

(IFNAME|) no distribute-list prefix WORD (in|out)

(IFNAME|)

Parameters

WORD	Specify the IPv4 access-list number or name to use.
prefix	Filter prefixes in routing updates.
WORD	Specify the name of the IPv4 prefix-list to use.
in	Filter incoming routing updates.
out	Filter outgoing routing updates.
IFNAME	Specify the name of the interface on which distribute-list applies.

Default

Disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router rip
(config-router)#distribute-list prefix myfilter in eth0
```

ip rip authentication key-chain

Use this command to enable RIPv2 authentication on an interface and specify the name of the key chain to be used. If you do not configure a key chain results in no authentication. Use the `no` parameter with this command to disable this function.

See Appendix A, *Routing Information Protocol Authentication* for information on how this command is related to the other authentication commands.

Command Syntax `ip rip authentication key-chain LINE` `no ip rip authentication key-chain (LINE|)`

Parameters

`LINE`	Specify the name of the key chain.

Default

If you do not configure a key chain, authentication is not used.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

In the following example, interface eth0 is configured key-chain authentication and the name is specified as `mykey`. This name is used to enter the key-chain mode to specify the password. See the `key` command.

```
#configure terminal
(config)#interface eth0
(config-if)#ip rip authentication key-chain mykey
```

ip rip authentication mode

Use this command to specify the type of authentication mode used for RIP v2 packets.

Use the `no` parameter with this command to restore clear text authentication.

See Appendix A, *Routing Information Protocol Authentication* for information on how this command is related to the other authentication commands.

Command Syntax `ip rip authentication mode md5 ip rip`

`authentication mode text no ip rip authentication mode`

Parameters

`md5`	Uses the keyed MD5 authentication algorithm.
`text`	Specify the clear text or simple password authentication.

Default

No authentication mode is enabled by default. But, when any authentication key (string or key-chain) is configured, text authentication mode is enabled by default.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows `md5` authentication configured on the `eth1` interface, ensuring authentication of RIP packets received.

```
#configure terminal
(config)#interface eth1
(config-if)#ip rip authentication mode md5
```

ip rip authentication string

Use this command to specify the authentication string or password used by a key.

You can configure authentication for a single key or multiple keys at different times. Use this command to specify password for a single key on an interface.

Use the `no` parameter with this command to disable this feature.

See Appendix A, *Routing Information Protocol Authentication* for how this command is related to the other authentication commands.

Command Syntax `ip rip authentication string LINE no ip rip authentication string`

Parameters

LINE	Specify the authentication string or password used by a key.

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

In the following example, the interface eth1 is configured to have an authentication string as guest, any receiving RIP packet in that interface should have the same string as password.

```
#configure terminal
(config)#interface eth1
(config-if)#ip rip authentication string guest
```

ip rip receive-packet

Use this command to configure the interface to enable the reception of RIP packets.

Use the no parameter with this command to disable this feature.

Command Syntax ip rip receive-packet no ip rip receive-packet

Parameters

None

Default

Receive-packet is enabled

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

This example shows packet receiving being turned on for interface eth0.

```
#configure terminal
(config)#interface eth0
(config-if)#ip rip receive-packet
```

ip rip receive version

Use this command to receive specified version of RIP packets on an interface basis using version control, and override the setting of the version command.

Use the `no` form of this command to use the setting established by the version command.

Command Syntax `ip rip receive version (1|2) ip rip receive version 1 2 ip rip receive version 2 1 no ip rip receive version`

Parameters

`1` Specify acceptance of RIP version 1 packets on the interface.

`2` Specify acceptance of RIP version 2 packets on the interface.

`1 2` Specify acceptance of RIP version 1 and version 2 packets on the interface. `2 1` Specify acceptance of RIP version 2 and version 1 packets on the interface.

Default

Version 2

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

In the following example, interface eth1 in configured to receive both RIP version 1 and 2 packets.

```
#configure terminal
(config)#interface eth1
(config-if)#ip rip receive version 1 2
```

ip rip send-packet

Use this command to enable sending RIP packets through the current interface.

Use the `no` parameter with this command to disable this feature.

Command Syntax `ip rip send-packet no ip rip send-packet`

Parameters

None

Default

Send packet is enabled.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

This example shows packet sending being turned on for interface `eth0`.

```
#configure terminal
(config)#interface eth0
(config-if)#ip rip send-packet
```

ip rip send version

Use this command to send RIP packets on an interface using version control. In addition to version 1 and version 2, compatible version packets can be specified. With the parameter 1-compatible, a version 2 RIP interface will broadcast the packets instead of multicasting them.

This command applies to a specific interface and overrides any the version specified by the `version` command.

Use the `no` parameter with this command to use the global RIP version control rules.

Command Syntax `ip rip send version (1|2|1-compatible) ip rip send version 1 2 ip rip send version 2 1 no ip rip send version`

Parameters

`1`	Specify sending RIP version 1 packets out of an interface.
`2`	Specify sending RIP version 2 packets out of an interface.
`1 2`	Specify acceptance of RIP version 1 and version 2 packets on the interface.
`2 1`	Specify acceptance of RIP version 2 and version 1 packets on the interface.
`1-compatible`	Specify sending RIP version 1 compatible packets from a version 2 RIP interface.

Default

Version 2

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

In the following example, interface eth1 is configured to send both RIP version 1 and 2 packets.

```
#configure terminal
(config)#interface eth1
(config-if)#ip rip send version 1 2
```

ip rip split-horizon

Use this command to perform the split-horizon action on the interface

This command helps avoid including routes in updates sent to the same gateway from which they were learned. Using the `split horizon` command omits routes learned from one neighbor, in updates sent to that neighbor. Using the `poisoned` parameter with this command includes such routes in updates, but sets their metrics to infinity. Thus, advertising that these routes are not reachable.

Use the `no` parameter with this command to disable this function.

Command Syntax `ip rip split-horizon ip rip split-horizon poisoned no ip rip split-horizon`

Parameter `poisoned` Performs split-horizon with poisoned reverse.

Default

Split horizon poisoned

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip rip split-horizon poisoned
```

key

Use this command to manage, add or delete authentication keys in a key-chain. This command allows you to enter the Keychain-key mode to set a password for the key.

Use the no option with this command to disable this feature.

See Appendix A, *Routing Information Protocol Authentication* for information on how this command is related to the other authentication commands.

Command Syntax `key <0-2147483647> no key <0-2147483647>`

Parameters

`<0-2147483647>` Specify a key identifier.

Default

By default, RIP uses level-1-2 if there is no Level-2 instance nor a Level-1-2 instance. Otherwise, it uses level-1.

Command Mode

Keychain mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

In the following example, the password for `key 1` in the key chain named `mychain` is set to `prime`:

```
#configure terminal
(config)#key chain mychain
(config-keychain)#key 1
(config-keychain-key)#key-string prime

(config-keychain)#key 1
(config-keychain-key)#no key-string
```

key chain

Use this command to enter the key chain management mode and to configure a key chain with a key chain name. This command allows you to enter the keychain mode to specify keys on this key chain.

Use the no option with this command to disable this feature.

See Appendix A, *Routing Information Protocol Authentication* for information on how this command is related to the other authentication commands.

Command Syntax `key chain WORD no key chain WORD`

Parameter

`WORD` Specify the name of the key chain to manage.

Default

None

Command Mode

Configure mode and Keychain mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows the creation of a key chain named `mychain` and the change into `keychain` mode prompt.

```
#configure terminal
(config)#key chain mychain
(config-keychain)#
```

The following example shows the creation of a key chain named `mykeychain3` in the Keychain mode and the addition of an authentication key `key10` in the same mode.

```
(config-keychain)#key chain mykeychain3
(config-keychain)#key 10
(config-keychain-key)#
```

key-string

Use this command to define a password to be used by a key.

Use the `no` parameter with this command to disable this feature.

See Appendix A, *Routing Information Protocol Authentication* for information on how this command is related to the other authentication commands.

Command Syntax `key-string LINE no key-string`

Parameters

`LINE`	Specify a string of characters to be used as a password by the key.

Default

Disabled

Command Mode

Keychain-key mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

In the following example, the password for `key 1` in the key chain named `mychain` is set to `prime`:

```
#configure terminal
(config)#key chain mychain
(config-keychain)#key 1
(config-keychain-key)#key-string prime

(config-keychain)#key 1
(config-keychain-key)#no key-string
```

maximum-prefix

Use this command to configure the maximum prefix.

Use the `no` parameter with this command to disable the limiting of the number of RIP routes in the routing table.

Command Syntax `maximum-prefix <1-65535>`

`(<1-100>|) no maximum-prefix`

Parameters

`<1-65535>`	The maximum number of RIP routes allowed.
`<1-100>`	Percentage of maximum routes to generate a warning. The default threshold is 75%.

Default

The default maximum-prefix threshold is 75%.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router rip
(config-router)#maximum-prefix 150
```

neighbor

Use this command to specify a neighbor router. It is used for each connected point-to-point link. This command to exchanges non-broadcast routing information. It can be used multiple times for additional neighbors.

`Passive-interface` command disables sending routing updates on an interface. Use the `neighbor` command in conjunction with the `passive-interface` command to send routing updates to specific neighbors.

Use the `no` parameter with this command to disable the specific router.

Command Syntax

```
neighbor A.B.C.D no
neighbor A.B.C.D
```

Parameter

A.B.C.D	An IP address of a neighboring router with which the routing information will be exchanged.

Default

Disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router rip
(config-router)#neighbor 10.7.1.12
```

network

Use this command to specify a network as one that runs RIP. This command specifies the networks to which routing updates will be sent and received. If a network is not specified, the interfaces in that network will not be advertised in any RIP update.

Use the `no` parameter with this command to remove the specified network as one that runs RIP.

Command Syntax `network`

```
A.B.C.D/M     network
IFNAME   no   network
A.B.C.D/M no network
IFNAME
```

Parameters

A.B.C.D/M	The IP address prefix and length of this IP network.
IFNAME	Alphanumeric string that defines the interface name.

Default

Disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router rip
(config-router)#network 10.0.0.0/8
(config-router)#network eth0
```

offset-list

Use this command to add an offset to in and out metrics to routes learned through RIP. This command specifies the offset value that is added to the routing metric. When the networks match the access list the offset is applied to the metrics. No change occurs if the offset value is zero.

Use the `no` parameter with this command to remove the offset list.

Command Syntax `offset-list WORD (in|out) <0-16>`

`(IFNAME|) no offset-list WORD (in|out) <0-16>`

`(IFNAME|)`

Parameters

`WORD`	Specify the access-list number or names to apply.
`in`	Indicates the access list will be used for metrics of incoming advertised routes.
`out`	Indicates the access list will be used for metrics of outgoing advertised routes.
`<0-16>`	Specify that the offset is used for metrics of networks matching the access list.
`IFNAME`	An alphanumeric string that specifies the interface to match.

Default

The default `offset value` is the interface metric value which is defined by the operating system.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

In this example the router examines the RIP updates being sent out from interface eth0 and adds 16 hops to the routes matching the ip addresses specified in the access list `accesslist1`.

```
#configure terminal
(config)#router rip
(config-router)#offset-list accesslist1 in 16 eth0
```

passive-interface

Use this command to block RIP broadcast on the interface.

Use the `no` parameter with this command to disable this function.

Command Syntax `passive-interface IFNAME no passive-interface IFNAME`

Parameters

`IFNAME`	Specify the interface name.

Default

Disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router rip
                    (config-router)#passive-interface eth0
```

recv-buffer-size

Use this command to run-time configure the RIP UDP receive-buffer size.

Use the `no` parameter with this command to return to the default value.

Command Syntax `recv-buffer-size <8192-2147483647> no recv-buffer-size`

Parameters

`<8192-2147483647>`	Specify the RIP UDP receive buffer size value.

Default

The default value of the RIP UDP receive-buffer size is 32768.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router rip
(config-router)#recv-buffer-size 150000
```

redistribute

Use this command to redistribute information from other routing protocols.

Use the `no` parameter with this command to disable this function.

Command Syntax `redistribute (kernel|connected|static|ospf|isis|bgp) redistribute (kernel|connected|static|ospf|isis|bgp) metric <0-16> redistribute (kernel|connected|static|ospf|isis|bgp) route-map WORD redistribute (kernel|connected|static|ospf|isis|bgp) metric <0-16> route-map WORD no redistribute (kernel|connected|static|ospf|isis|bgp) no redistribute (kernel|connected|static|ospf|isis|bgp) metric <0-16> no redistribute (kernel|connected|static|ospf|isis|bgp) route-map WORD`

`no redistribute (kernel|connected|static|ospf|isis|bgp) metric <0-16> route-map WORD`

Parameters

`bgp`	Redistribute from BGP routes
`connected`	Redistribute from connected routes
`isis`	Redistribute from ISO IS-IS routes
`kernel`	Redistribute from kernel routes
`ospf`	Redistribute from OSPFv3 routes
`static`	Redistribute from static routes
`metric`	Metric value
`<0-16>`	Specify a metric value
`route-map`	Route map reference
`WORD`	Specify name of the route-map

Default

Disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router rip
```

```
(config-router)#redistribute kernel
```

```
#configure terminal
(config)#router rip
(config-router)#redistribute kernel route-map myroutemap
```

route

Use this command to configure static RIP routes.

Use the `no` parameter with this command to disable this function.

Command Syntax

```
route
A.B.C.D/M    no
route
A.B.C.D/M
```

Parameter

`A.B.C.D/M`	Specify the IP address prefix and length.

Default

No route is added.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

Use this command to add a static RIP route. This command is used most often for debugging purposes and does not show up in the kernel routing table. After adding the RIP route, it can be checked in the RIP routing table.

```
#configure terminal
(config)#router rip
(config-router)#version 1
(config-router)#network 10.10.10.0/24
(config-router)#network 10.10.11.0/24
(config-router)#neighbor 10.10.10.10
(config-router)#route 10.10.10.0/24

(config-router)#version 1
(config-router)#network 10.10.10.0/24
(config-router)#network 10.10.11.0/24
(config-router)#no route 10.10.10.0/24
```

router rip

Use this global command to enable a RIP routing process.

Use the `no` parameter with this command to disable RIP routing.

Command Syntax `router rip no router rip`

Parameter

None

Default

Disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

This command is used to begin the RIP routing process.

```
#configure terminal
(config)#router rip
(config-router)#version 1
(config-router)#network 10.10.10.0/24
(config-router)#network 10.10.11.0/24
(config-router)#neighbor 10.10.10.10
```

send-lifetime

Use this command to specify the time period during which the authentication key on a key chain can be sent.

Use the `no` parameter with this command to negate this command.

Command Syntax `send-lifetime HH:MM:SS <1-31> MONTH <1993-2035> HH:MM:SS <1-31> MONTH <1993-2035> send-lifetime HH:MM:SS <1-31> MONTH <1993-2035> HH:MM:SS MONTH <1-31> <1993-2035> send-lifetime HH:MM:SS MONTH <1-31> <1993-2035> HH:MM:SS <1-31> MONTH <1993-2035> send-lifetime HH:MM:SS MONTH <1-31> <1993-2035> HH:MM:SS MONTH <1-31> <1993-2035> send-lifetime HH:MM:SS <1-31> MONTH <1993-2035> infinite send-lifetime HH:MM:SS MONTH <1-31> <1993-2035> infinite send-lifetime HH:MM:SS <1-31> MONTH <1993-2035> duration <1-2147483646> send-lifetime HH:MM:SS MONTH <1-31> <1993-2035> duration <1-2147483646> no send-lifetime`

Parameters

`HH:MM:SS`	Specify the start time of send-lifetime in hours, minutes and seconds.
`<1-31>`	Specify the day of the month to start.
`MONTH`	Specify the month of the year to start (the first three letters of the month, for example, `Jan.`).
`<1993-2035>`	Specify the year to start.
`HH:MM:SS`	Specify the time when send-lifetime expires in hours, minutes and seconds.

`<1-31>`	Specify the day of the month to expire.
`MONTH`	Specify the month of the year to expire (the first three letters of the month, for example, `Jan.`).
`<1993-2035>`	Specify the year to expire.
`duration`	Specify the duration of the key in seconds <1-2147483646>.
`infinite`	Specify the end time to never expire.

Default

Disabled

Command Mode

Keychain-key mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows the setting of `send-lifetime` for `key 1` on the key chain named `mychain`:

```
#configure terminal
(config)#key chain mychain
(config-keychain)#key 1
(config-keychain-key)#send-lifetime 03:03:01 Jan 3 2004 04:04:02 Dec 6 2006
```

show debugging rip

Use this command to display the RIP debugging status for these debugging options: nsm debugging, RIP event debugging, RIP packet debugging and RIP nsm debugging.

Command Syntax `show`

```
debugging rip
```

Parameters

None

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show debugging rip
RIP debugging status:
```

show ip protocols rip

Use this command to display RIP process parameters and statistics.

Command Syntax `show ip protocols`

```
show ip protocols rip
```

Parameters

None

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

This is an example of the output from the `show ip protocols rip` command:

```
#show ip protocols rip
Routing Protocol is "rip"
Sending updates every 30 seconds with +/-50%, next due in 12 seconds
Timeout after 180 seconds, garbage collect after 120 seconds
Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set
Default redistribution metric is 1
Redistributing: connected static
Default version control: send version 2, receive version 2
Interface        Send  Recv   Key-chain      eth0
2   2
Routing for Networks:
  10.10.0.0/24
Routing Information Sources:
  Gateway          BadPackets BadRoutes  Distance Last Update
Distance: (default is 120)
#
```

Figure 1-158 Explains the show command output details.

Table 1-158: Show ip protocols output details

Field	Description

Routing Protocol is "rip"	Specifies the routing protocol used.
Sending updates every 30 seconds	Specifies the time between sending updates.

Next due in 12 seconds	Precisely when the next update is due to be sent.
Timeout after 180 seconds	Specifies the value of the timeout parameter.
Redistributing	Lists the protocol that is being redistributed.
Routing for Networks	Specifies the networks for which the routing process is currently injecting routes.
Routing Information Sources	Lists all the routing sources the Symanitron Networks software is using to build its routing table.

© Symanitron Proprietary

show ip rip

Use this command to show RIP routes.

Command Syntax `show ip rip`

`(database|)`

Parameters `database` Specify to display information about the IP RIP database.

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following output displays the RIP routing table with the destination network, nexthop and metric to reach it.

```
#show ip rip
Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS,
B-BGP
Network Next Hop Metric From If Time
K 0.0.0.0/0 10.0.1.1 16 eth1 01:58
C 10.0.1.0/24 1 eth1
S 10.10.10.0/24 1 eth0
C 10.10.11.0/24 1 eth0
S 192.168.101.0/24 1 eth0 R
192.192.192.0/24 1 --
```

Table 1-159 shows the status codes displayed at the start of a route entry.

Table 1-159: Status codes

Status Code	Meaning	Description
R	RIP	RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination.
K	Kernel	Kernel is central component of operating system.
C	Connected	Redistribute from locally connected networks.

S	Static	Connections in a static network are fixed links, while connections in a dynamic network are established on the fly as needed.
O	OSPF	Open Shortest Path First (OSPF) is a routing protocol for Internet Protocol (IP) networks.

I	IS-IS	Intermediate System to Intermediate System (IS-IS) is a routing protocol designed to move information efficiently within a host network.
B	BGP	BGP makes routing decisions based on paths, rules or network policies configured by a network administrator.

© Symanitron Proprietary 2004

show ip rip interface

Use this command to display information about RIP interfaces. You can specify an interface name to display information about a specific interface.

Command Syntax `show ip rip interface (IFNAME|)`

Parameters

`IFNAME`	Name of the interface for which information is to be displayed.

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following output displays the RIP routing table with the destination network, nexthop and metric to reach it.

```
#show ip rip interface lo is up, line
protocol is up RIP is not enabled on
this interface eth0 is up, line protocol
is up RIP is not enabled on this
interface eth1 is down, line protocol is
down RIP is not enabled on this
interface eth2 is up, line protocol is
up
Routing Protocol: RIP
Receive RIP packets
Send RIPv1 Compatible
Passive interface: Disabled
Split horizon: Enabled with Poisoned Reversed
IP interface address:
10.10.1.1/24
10.10.2.1/24
```

Figure 1-160 Explains the show command output details.

Table 1-160: Show ip rip interface output details

Field	Description

Network	IP address of a network entity.
Nexthop	IP address of the next system that is used when forwarding a packet to the destination network.

Metric	If shown, the value of the inter-autonomous system metric.
Routing Protocol	Specifies the routing protocol used.
Passive Interface	Used in all routing protocols to disable sending updates out from a specific interface.
Split horizon	the routing switch does not advertise a route on the same interface as the one on which the routing switch learned the route.
IP Interface address	IP address of the RIP peer neighbor.

© Symanitron Proprietary 2006

show ip rip statistics

Use this command to display information about RIP statistics. You can specify an interface name to display information about a specific interface.

Command Syntax `show ip rip statistics (IFNAME|)`

Parameters

`IFNAME`	Name of the interface for which information is to be displayed.

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following output displays the RIP routing table with the destination network, nexthop and metric to reach it.

```
#show ip rip statistics eth1
Interface Name : eth1
  Sent Multicast Updates  : 3
  Sent Multicast Requests : 1
  Sent Unicast Updates    : 0
  Sent Unicast Requests   : 0
  Recv Multicast Updates  : 3
  Recv Multicast Requests : 0
  Recv Unicast Updates    : 1
  Recv Unicast Requests   : 0
  Recv Bad Packets        : 0
  Recv Bad Routes         : 0
```

Figure 1-161 Explains the show command output details.

Table 1-161: Show ip rip statistics output details

Field	Description
Network	IP address of a network entity.

Nexthop	IP address of the next system that is used when forwarding a packet to the destination network.
Metric	If shown, the value of the inter autonomous system metric.
Sent updates	Number of RIP routing updates that have been sent on Multicast/Unicast interface.

Sent Request	Number of RIP routing request that have been sent on Multicast/Unicast interface.
Recv updates	Number of RIP routing updates that have been received on Multicast/Unicast interface.
Recv Request	Number of RIP routing request that have been received on Multicast/Unicast interface.
Recv Bad Packets	Number of packets that were received on this interface and were not processed for any reason.
Recv Bad Routes	Number of route entries that were received on this interface and were not processed for any reason.

© Symanitron Proprietary 2008

snmp restart rip

Use this command to restart SNMP in Routing Information Protocol (RIP)

Command Syntax `snmp restart rip`

Parameters

None

Default

By default, snmp restart is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#snmp restart rip
```

timers basic

Use this command to adjust routing network timers.

This command adjusts the RIP timing parameters. Every 30 seconds, an update is sent out containing the complete routing table to every neighboring router. When the time specified by the timeout parameter expires, the route is no longer valid. However, it is retained in the routing table for a short time so that neighbors are notified that the route has been dropped. When the time specified by the garbage parameter expires, the route is finally removed from the routing table. Until the garbage time expires, the route is included in all updates sent by the router.

All routers in the network must have the same timers to allow RIP to execute a distributed and asynchronous routing algorithms. The timers should not be synchronized as it might lead to unnecessary collisions on the network.

Use the `no` parameter with this command to restore the default routing network timers.

Command Syntax `timers basic <5-2147483647> <5-2147483647> <5-2147483647> no timers basic`

Parameters

`<5-2147483647>`	Specify the routing table update timer in seconds. The default is 30 seconds.
`<5-2147483647>`	Specify the routing information timeout timer in seconds. The default is 180 seconds. After this interval has elapsed and no updates for a route are received, the route is declared invalid.
`<5-2147483647>`	Specify the routing garbage collection timer in seconds. The default is 120 seconds.

Default

The default routing table update time is 30 seconds.

The default routing information timeout time is 180 seconds.

The default routing garbage collection time is 120 seconds.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router rip
(config-router)#timers basic 30 180 120

(config)#router rip
(config-router)#no timers basic
```

version

Use this command to specify a RIP version used globally by the router. RIP can be run in version 1 as well as version 2 mode. Version 2 has more features than version 1 including authentication. Once the rip version is set, rip packets

of that version will be received and sent on all the rip-enabled interfaces. Use the `no` parameter with this command to restore the default version.

Note: The `ip rip receive version` command and the `ip rip send version` command override the value set by the `version` command.

Command Syntax

```
version  <1-
2> no version
```

Parameters

<1-2>	Specify the version of RIP processing.

Default

Version 2

Command Mode

Router mode and Address Family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router rip
(config-router)#version 1
(config-router)#network 10.10.10.0/24
(config-router)# network 10.10.11.0/24
```

```
#configure terminal
(config)#router rip
(config-router)#address-family ipv4 vrf myVRF
(config-router-af)#version 2
```

© Symanitron Proprietary

CHAPTER 2 RIPng Commands

This chapter provides an alphabetized reference for each of the Routing Information Protocol next generation (RIPng) commands, which support IPv6. It includes the following commands:

- aggregate-address
- cisco-metric-behavior
- clear ipv6 rip route
- debug ipv6 rip
- default-information originate
- default-metric
- distance
- distribute-list
- ipv6 rip metric-offset
- ipv6 rip split-horizon
- ipv6 router rip
- neighbor
- offset-list
- passive-interface
- recv-buffer-size
- redistribute
- route
- route-map
- router ipv6 rip
- show debugging ipv6 rip
- show ipv6 protocols rip
- show ipv6 rip
- show ipv6 rip interface
- timers basic

aggregate-address

Use this command to set an aggregate RIPng route announcement.

Use the `no` parameter with this command to disable this feature.

Command Syntax `aggregate-address X:X::X:X/M no aggregate-address X:X::X:X/M`

Parameter

`X:X::X:X/M`	Specify an aggregate network (IPv6 address prefix and length).

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 rip
(config-router)#aggregate-address 3ffe:8088::/32

(config)#router ipv6 rip
(config-router)#no aggregate-address 3ffe:8088::/32
```

cisco-metric-behavior

Use this command to enable or disable the metric update as Cisco.

Use the `no` parameter with this command to disable this feature.

Command Syntax `cisco-metric-behavior (enable|disable) no cisco-metric-behavior`

Parameters

`enable`	Enable updating the metric consistent with Cisco.
`disable`	Disable updating the metric consistent with Cisco.

Default

By default, the Cisco metric-behavior is disabled.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

This example shows how to enable the metric update behavior to be consistent with Cisco in the Router mode.

```
#configure terminal
```

```
(config)#router ipv6 rip (config-
router)#cisco-metric-behavior enable
```

clear ipv6 rip route

Use this command to clear specific data from the RIPng routing table.

Command Syntax `clear ipv6 rip route (X:X::X:X/M|rip|kernel|connected|static|ospf6|isis|bgp|all)` **Parameters**

`X:X::X:X/M`	Removes entries which exactly match this destination address from the RIPng routing table.
`bgp`	Removes only BGP routes from the RIP routing table.
`connected`	Removes entries for connected routes from the RIP routing table.
`isis`	Removes only IS-IS routes from the RIP routing table
`kernel`	Removes kernel entries from the RIP routing table.
`ospf`	Removes only OSPF routes from the RIP routing table.
`static`	Removes static entries from the RIP routing table.
`all`	Removes the entire RIP routing table.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear ipv6 rip route isis
#clear ipv6 rip route 3ffe:ffff::/16
```

debug ipv6 rip

Use this command to specify the options for the displayed debugging information for RIPng events, RIPng packets and RIPng NSM communications.

Use the `no` option with this command to turn off debugging options for RIPng. The `undebug` alias command can also be used.

Command Syntax `debug ipv6 rip (all|) debug ipv6 rip events debug ipv6 rip nsm debug ipv6 rip packet (recv|send|) (detail|) debug ipv6 rip rib no debug ipv6 rip (all|) no debug ipv6 rip events no debug ipv6 rip nsm no debug ipv6 rip packet (recv|send|) (detail|) no debug ipv6 rip rib undebug ipv6 rip (all|) undebug ipv6 rip events`

```
undebug ipv6 rip nsm undebug ipv6 rip packet
(recv|send|) (detail|) undebug ipv6 rip rib
```

Parameters

`all`	Debug all RIP information.
`events`	Debug RIP events.
`nsm`	Debug RIP and NSM communications.
`packet`	Debug RIP packets, only Routing Information Protocol
`recv`	Debug received packets.
`rib`	Debug RIP and RIB communications.
`send`	Debug sent packets.
`detail`	Display detailed information for the sent or received packet.

Default

Disabled

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example specifies the options for the displayed debugging information in `Configure` mode prompt.

```
#configure terminal
(config)#debug ipv6 rip events
(config)#debug ipv6 rip packet send detail
(config)#debug ipv6 rip nsm
```

The following example shows to disable all debugging in `Privileged Exec` mode prompt.

```
#undebug ipv6 rip events
#undebug ipv6 rip packet send detail
#undebug ipv6 rip nsm
```

© Symanitron Proprietary

default-information originate

Use this command to generate a default route into the RIPng.

Use the `no` parameter with this command to disable this feature.

Command Syntax `default-information originate no default-information originate`

Parameters

None

Default

Disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 rip
                                    (config-router)#default-information originate
```

default-metric

Use this command to specify the metrics to be assigned to redistributed routes.

Use the `no` parameter with this command to disable this feature.

For more details about this command, see the IPv4 version of this command (default-metric).

Command Syntax `default-metric <1-15> no default-metric`

Parameter

`<1-15>`	Specify the default metric.

Default

By default, the metric value is set to 1.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 rip
(config-router)#default-metric 8
```

distance

Use this command to set the administrative distance for RIP.

Use the no option with this command to disable this function.

For more details about this command, see the IPv4 version of this command (distance).

Command Syntax `distance <1-255> no distance (<1-255>|)`

Parameter

`<1-255>`	Specify the administrative distance value.

Default

By default, the administrative distance is 120.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router ipv6 rip
(config-router)#distance 100
```

distribute-list

Use this command to filter incoming or outgoing route updates using the access-list or the prefix-list. You can filter out incoming or outgoing route updates using access-list or prefix-list. If you do not specify the name of the interface, the filter will be applied to all the interfaces.

Use the `no` parameter with this command to disable this feature.

Command Syntax `distribute-list WORD (in|out) (IFNAME|)` `distribute-listprefix`

```
(IFNAME|)   no   distribute-list   WORD   (in|out)
(IFNAME|) no distribute-list prefix WORD (in|out)
(IFNAME|)
```

Parameters

`WORD`	Specify the IPv6 access-list number or name to use.
`prefix`	Filter prefixes in routing updates.
`WORD`	Specify the name of the IPv6 prefix-list to use.
`in`	Filter incoming routing updates.
`out`	Filter outgoing routing updates.
`IFNAME`	Specify the name of the interface on which distribute-list applies.

Default

Disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
```

```
(config)#router ipv6 rip
(config-router)#distribute-list prefix myfilter in eth0
```

ipv6 rip metric-offset

Use this command to set RIP metric offset.

Use the `no` parameter with this command to disable this function.

Command Syntax `ipv6 rip metric-offset <1-16> no ipv6 rip metric-offset <1-16>`

Parameter

`<1-16>`	Set a metric value

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 rip metric-offset 1

(config)#interface eth0
(config-if)#no ipv6 rip metric-offset 1
```

ipv6 rip split-horizon

Use this command to perform the split-horizon action on the interface.

Use the `no` parameter with this command to disable this function.

For more details about this command, see the IPv4 version of this command (ip rip split-horizon).

Command Syntax `ipv6 rip split-horizon ipv6 rip split-horizon poisoned no ipv6 rip split-horizon`

Parameter `poisoned` Performs split-horizon with poisoned reverse.

Default

By default, Split horizon poisoned is enabled.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#ipv6 rip split-horizon

(config)#interface eth1
(config-if)#no ipv6 rip split-horizon
```

ipv6 router rip

Use this command to enable RIPng routing on the interface.

Use the `no` parameter with this command to disable RIPng routing.

Command Syntax `ipv6 router rip no ipv6 router rip`

Parameters

None

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 router rip
```

neighbor

Use this command to specify a neighbor router.

Use the `no` parameter with this command to disable the specific router.

For more details about this command, see the IPv4 version of this command (neighbor).

Command Syntax `neighbor X:X::X:X IFNAME no neighbor X:X::X:X IFNAME`

Parameters

`X:X::X:X`	Specify a link-local IP address of a neighboring router with which the routing information is exchanged.
`IFNAME`	Specify the name of the interface.

Default

Disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router ipv6 rip
(config-router)#neighbor 80::1 eth0
```

offset-list

Use this command to add an offset to in and out metrics to routes learned through RIPng.

Use the `no` parameter with this command to remove this function.

For more details about this command, see the IPv4 version of this command (offset-list).

Command Syntax `offset-list WORD (in|out) <0-16> (IFNAME|) no offset-list (WORD) in|out <0-16> (IFNAME|)`

Parameters

`WORD`	Specify the access-list number or names to apply.
`in`	Indicates the access list will be used for metrics of incoming advertised routes.
`out`	Indicates the access list will be used for metrics of outgoing advertised routes.
`<0-16>`	Specify that the offset is used for metrics of networks matching the access list.
`IFNAME`	An alphanumeric string that specifies the interface to match.

Default

The default offset value is the metric value of the interface which is defined by the operating system.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

In this example the router examines the RIP updates being sent out from interface eth0 and adds 16 hops to the routes matching the ip addresses specified in the access list `accesslist1`.

```
#configure terminal
(config)#router ipv6 rip
(config-router)#offset-list accesslist1 in 16 eth0
```

passive-interface

Use this command to suppress routing updates on an interface.

Use the `no` parameter with this command to disable this function.

Command Syntax `passive-interface IFNAME no passive-interface IFNAME`

Parameters

`IFNAME`	Specify the interface name.

Default

Disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 rip
                    (config-router)#passive-interface eth0
```

recv-buffer-size

Use this command to run-time configure the RIPng UDP receive-buffer size.

Use the `no` parameter with this command to return to the default value.

Command Syntax `recv-buffer-size <8192-2147483647> no recv-buffer-size`

Parameters

`<8192-2147483647>`

Specify the RIP UDP receive buffer size value.

Default

The default value of the RIP UDP receive-buffer size is 8192.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 rip
(config-router)#recv-buffer-size 150000
```

redistribute

Use this command to redistribute information from other routing protocols.

Use the `no` parameter with this command to disable this function.

Command Syntax `redistribute (kernel|connected|static|ospf|isis|bgp)` `redistribute (kernel|connected|static|ospf|isis|bgp) metric <0-16>` `redistribute (kernel|connected|static|ospf|isis|bgp) route-map WORD` `redistribute (kernel|connected|static|ospf|isis|bgp) metric <0-16> route-map WORD` `no redistribute (kernel|connected|static|ospf|isis|bgp)` `no redistribute (kernel|connected|static|ospf|isis|bgp) metric <0-16>` `no redistribute (kernel|connected|static|ospf|isis|bgp) route-map WORD` `no redistribute (kernel|connected|static|ospf|isis|bgp) metric <0-16> route-map WORD`

Parameters

`bgp`	Redistribute from BGP routes
`connected`	Redistribute from connected routes
`isis`	Redistribute from ISO IS-IS routes
`kernel`	Redistribute from kernel routes

ospf	Redistribute from OSPF routes (version 3)
static	Redistribute from static routes
metric	Metric value
<0-16>	Specify a metric value
route-map	Route map reference
WORD	Specify name of the route-map

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 rip
(config-router)#redistribute kernel route-map mymap
(config-router)#redistribute kernel metric 8
```

route

Use this command to debug the specified route advertisement. Use this command to configure static RIPng routes.

Use the no parameter with this command to disable this function.

Command Syntax route

X:X::X:X/M

no route

X:X::X:X/M

Parameter

X:X::X:X/M	Specify the IPv6 address prefix and length.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 rip
(config-router)#route 3ffe:1234:5678::1/64
```

route-map

Use this command to set a route map for input or output filtering on a specified interface.

Use the `no` parameter with this command to disable this function.

Command Syntax `route-map WORD (in|out) IFNAME no route-map WORD (in|out) IFNAME`

Parameters

`WORD`	Specify a route map name
`in`	Specify to set the route map for input filtering
`out`	Specify to set the route map for output filtering
`IFNAME`	Specify an interface name to which to associate the route map

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 rip
(config-router)#route-map myRM in eth1
```

router ipv6 rip

Use this global command to enable a RIPng routing process.

Use the `no` parameter with this command to disable the RIPng routing process.

Command Syntax `router ipv6 rip no router ipv6 rip`

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
```

```
(config)#router ipv6 rip
(config-router)#
```

© Symanitron Proprietary

show debugging ipv6 rip

Use this command to display the RIPng debugging status for RIPng NSM, RIPng events, and RIPng packets.

Command Syntax `show debugging ipv6 rip`

Parameters

None

Command Mode

Exec Mode and Privileged Exec Mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show debugging ipv6 rip
 RIPng packet debugging is on
```

show ipv6 protocols rip

Use this command to display RIPng process parameters and statistics.

Command Syntax `show ipv6 protocols rip`

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following is a sample output from the `show ipv6 protocols rip` command.

```
#show ipv6 protocols rip
Routing Protocol is "ripng"
  Sending updates every 30 seconds with +/-50%, next due in 10 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribute metric is 1   Redistributing:
connected
  Routing for Networks:
    3ffe:1::/64
#
```

show ipv6 rip

Use this command to show RIP routes.

Command Syntax `show ipv6 rip (database|)`

Parameters `database` Specify to display information about the IPv6 RIP database.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following is a sample output from the show ipv6 rip database command.

```
#show ipv6 rip database
Codes: R - RIP, K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS,
B - BGP, a - aggregate, s - suppressed Network Next Hop If Met Tag Time

R 3ffe:1234:5678::/64 fe80::3 eth1 3 0 02:28
C 3ffe:ffff:1::/64 :: eth0 1 0
Ra 3ffe:ffff:2::/48 -- 1 0
Rs 3ffe:ffff:2::/48 fe80::3 eth1 3 0 02:32
Cs 3ffe:ffff:2::/64 :: eth1 1 0
R 3ffe:ffff:ffff:ffff::/64 fe80::3 eth1 3 0 02:28
```

show ipv6 rip interface

Use this command to display information about the RIPng interfaces. You can specify an interface name to display information about a specific interface.

Command Syntax `show ipv6 rip interface`

```
(IFNAME|)
```

Parameters

`IFNAME`	Name of the interface for which information is to be displayed.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following is a sample output from the `show ipv6 rip interface` command.

```
#show ipv6 rip interface lo is
up, line protocol is up
RIPng is not enabled on this interface
eth0 is up, line protocol is up RIPng is
not enabled on this interface eth1 is
down, line protocol is down RIPng is not
enabled on this interface eth2 is up,
line protocol is up Routing Protocol:
RIPng
```

```
Passive interface: Disabled
Split horizon: Enabled with Poisoned Reversed
IP interface address:
3ffe:ffff::1/64
3ffe:fffe::1/64
```

timers basic

Use this command to adjust routing network timers.

Use the `no` parameter with this command to restore the defaults.

For more details about this command, see the IPv4 version of this command (timers basic).

Command Syntax `timers basic <5-2147483647> <5-2147483647> <5-2147483647> no timers basic`

Parameters

`<5-2147483647>`	Specify the routing table update timer in seconds. The default is 30 seconds.
`<5-2147483647>`	Specify the routing information timeout timer in seconds. The default is 180 seconds. After this interval has elapsed and no updates for a route are received, the route is declared invalid.
`<5-2147483647>`	Specify the routing garbage collection timer in seconds. The default is 120 seconds.

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#router ipv6 rip
(config-router)#timers basic 30 180 120

(config)#router ipv6 rip
(config-router)#no timers basic
```

CHAPTER 3 Routing Information Protocol VPN Commands

This chapter provides information about RIP VPN commands. These commands are available when the RIP Provider Edge (PE) and Customer Edge (CE) feature is supported. Using these commands, VPN you can use RIP to receive information which the CE-router places into the connected Virtual Routing and Forwarding (VRF) from the receiving interface. The information is then advertised across the MPLS/VPN backbone between PE-routers.

To provide a VPN service, the PE-router needs to be configured so that any routing information learned from a VPN customer interface can be associated with a particular VRF. This is achieved using any standard routing protocol process (RIP, OSPF, BGP or static routes etc).

To enable the RIP PE-CE feature, an Address Family sub-mode is used. Most of the RIP commands that are available in Router and Interface mode are also available in Address Family mode. Additionally, all RIP debug commands display additional VRF information when the RIP PE-CE feature is supported.

This chapter contains the following commands:

- address-family ipv4 vrf
- exit-address-family
- show ip rip interface vrf
- show ip rip vrf
- show ip vrf

address-family ipv4 vrf

Use this command to enable the exchanging of VRF routing information and to enter the Address Family mode. This command configures the routing exchange between PE and CE devices. Configure a RIP address family for each VRF configured on the PE router.

To use this command, you must first create a VRF-Name in the NSM using the `ip vrf` command. Associate the same name with the RIP process using this command. Use the `no` parameter with this command to disable it.

Command Syntax `address-family ipv4`

`vrf NAME no address-family ipv4`

`vrf NAME`

Parameters

`NAME`	Specify the name for the VRF instance

Default

None

Command Mode

Router mode

SWMRE version 1.3

This command was introduced before SWMRE version 1.3.

Examples

The following example places the router in Address Family mode and specifies VRF1 as the name of the VRF instance to associate with subsequent IP Version 4 Address Family mode commands:

```
#configure terminal
(config)#router rip
(config-router)#address-family ipv4 vrf VRF1
(config-router-af)#
```

exit-address-family

Use this command to exit the Address Family mode. This command is supported in RIP (IPv4).

Command Syntax `exit-address-family`

Parameters

None

Default

None

Command Mode

Address Family mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following examples show the change in prompt after using the `exit-address-family` command to exit the `Address Family` mode.

```
(config)#router rip
(config-router)#address-family ipv4 vrf myVRF
(config-router-af)#exit-address-family
(config-router)#
```

show ip rip interface vrf

Command Syntax `show ip rip interface vrf WORD (IFNAME|)`

Parameters

`WORD`	Specify the name for the VRF instance.
`IFNAME`	Specify name for the interface.

Default

None

Command Mode

Exec mode and Privileged Exec mode

Field	Description
Routing Protocol	Specifies the routing protocol used.
VPN Routing/Forwarding	Specifies the name of the virtual routing and forwarding (VRF) instance.
Receive RIP packets	Number of RIP packets that were received on this interface.
Send RIP packets	Number of RIP packets that were send on this interface.

Passive Interface	Used in all routing protocols to disable sending updates out from a specific interface.

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip rip interface vrf myVRF

eth1 is up, line protocol is up   Routing Protocol:
RIP
    VPN Routing/Forwarding: myVRF
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:       1.1.1.92/24
eth3 is up, line protocol is up
  RIP is not enabled on this interface
```

Figure 3-162 Explains the show command output details.

Table 3-162: Show ip rip interface vrf output details

Split horizon	the routing switch does not advertise a route on the same interface as the one on which the routing switch learned the route.
IP Interface address	IP address of the RIP peer neighbor.

show ip rip vrf

Command Syntax `show ip rip (database) vrf WORD`

Parameters `database` Specify to display information about the IP RIP database.

`WORD` Specify the name for the VRF instance.

Default

None

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show ip rip database vrf myVRF
Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP

   Network            Next Hop         Metric From            If      Time
Rc 1.1.1.0/24                              1                  eth1
S  72.72.75.0/24      98.98.8.2            1                  eth3
```

Table 3-163 shows the status codes displayed at the start of a route entry.

Table 3-163: Status codes

Status Code	Meaning	Description
R	RIP	RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination.
Rc	RIP Connected	Redistribute from locally RIP connected networks.
Rs	RIP Static	Connections in a RIP static network are fixed links, while connections in a dynamic network are established on the fly as needed.

K	Kernel	Kernel is central component of operating system.
C	Connected	Redistribute from locally connected networks.
Rs	RIP Static	Connections in a RIP static network are fixed links, while connections in a dynamic network are established on the fly as needed.
O	OSPF	Open Shortest Path First (OSPF) is a routing protocol for Internet Protocol (IP) networks.
I	IS-IS	Intermediate System to Intermediate System (IS-IS) is a routing protocol designed to move information efficiently within a host network.
B	BGP	BGP makes routing decisions based on paths, rules or network policies configured by a network administrator.
	Network	IP address of a network entity.
	Nexthop	IP address of the next system that is used when forwarding a packet to the destination network.
	Metric	If shown, the value of the inter-autonomous system metric.

Figure 3-164 Explains the show command output details.

Table 3-164: Show ip rip vrf output details

Field	Description
Network	IP address of a network entity.
Nexthop	IP address of the next system that is used when forwarding a packet to the destination network.
Metric From	If shown, the value of the inter-autonomous system metric.
If	Ethernet interface.
Time	Specifies the time between forwarding packets.

show ip vrf

Command Syntax `show ip vrf show ip vrf WORD`

Parameters

`WORD` Specify the name for the VRF instance.

Default

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip vrf myVRF

VRF myVRF, FIB ID 1 Router ID: 1.1.1.2 (config)
Interfaces:   eth1   eth3
VRF myVRF; (id=1); RIP enabled Interfaces:   eth1
```

Appendix A Routing Information Protocol Authentication

To support RIPv2 message authentication, you can choose plain text or MD5 authentication, with the option for a single key or multiple keys in different modes and stages.

Single Key Authentication

Use the following steps to configure route to enable RIPv2 authentication using a single key or password:

1. Define the authentication string or password

   In the Interface mode, specify the authentication string or password used by the key using the following command: `ip rip authentication string LINE`

   where `LINE` is the authentication string or password

2. Specify mode of authentication for the interface

   In the Interface mode, specify either text or MD5 authentication using the following command: `ip rip authentication mode md5|text`

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ip rip authentication string mykey
(config-if)#ip rip authentication mode md5
```

Multiple Keys Authentication

Use the following steps to configure route to enable RIPv2 authentication using multiple keys at different times:

1. Define a key chain

   In the Configure mode, identify a key chain with a key chain name using the following command:

   `key chain KEYNAME` where `KEYNAME` is the name of the chain to manage.

2. Define the key(s)

   In the Keychain mode, specify a key on this key chain using the following command: `key KEYID`

   where `KEYID` = `<0-2147483647>` Key Identifier number

3. Define the authentication string or password

   In the Keychain-key mode, define the password used by a key, using the following command:

   `key-string LINE` where `LINE` is a string of characters to be used as a password by the key.

4. Set key management options

   This step can be performed at this stage or later when multiple keys are used. The options are configured in the `keychain-key` command mode.

- Set the time period during which the authentication key on a key chain is received as valid, using the following command:

  `accept-lifetime START END` where `START` and `END` are the beginning and end of the time period.

- Set the time period during which the authentication key on a key chain can be sent using the following command:

  `send-lifetime START END` where `START` and `END` are the beginning and end of the time period.

5. Enable authentication on an interface

   In the Interface mode, enable authentication on an interface and specify the key chain to be used, using the following command:

   ```
   ip rip authentication key-chain CHAINNAME
   ```

   where `CHAINNAME` is a set of valid authentication keys

6. Specify mode of authentication for the interface

   In the Interface mode, specify either text or MD5 authentication using the following command: `ip rip authentication mode md5|text`

Example

In the following example, a password `toyota` is set for a `key 1` in a key chain `cars`. On Interface `eth0` authentication is enabled and the authentication mode is set as `MD5`.

```
#configure terminal
(config)#key chain cars (config-keychain)#key 1
(config-keychain-key)#key-string toyota
(config-keychain-key)#accept-lifetime 10:00:00 Oct 08 2002 duration 43200
(config-keychain-key)#send-lifetime 10:00:00 Oct 8 2002 duration 43200
(config-keychain-key)#exit
(config-keychain)#exit
(config)#interface eth0
(config-if)#ip rip authentication key-chain cars
(config-if)#ip rip authentication mode md5
(config-if)#exit
```

SECTION 7 Multicast

Multicast Configuration Guide

Contents

This document contains these chapters and appendices:

- Chapter 1, *IGMP Configuration*
- Chapter 2, *IGMP Proxy Configuration*
- Chapter 3, *PIM Sparse Mode Configuration*
- Chapter 4, *PIM Dense Mode Configuration*
- Chapter 5, *IGMP Snooping Configuration*
- Chapter 6, *Multicast Virtual Routing Configuration*
- Chapter 7, *PIM-ECMP Redirect Configuration*
- Chapter 8, *MSDP Configuration*
- Chapter 9, *PIM Sparse-Dense Mode Configuration*
- Appendix A, *Tunnel Interface*

CHAPTER 1 IGMP Configuration

This chapter describes how to configure Internet Group Management Protocol (IGMP).

The Internet Group Management Protocol (IGMP) is used by IP hosts to report their multicast group memberships to any immediately-neighboring multicast routers.

Using the information obtained through IGMP, the router maintains a list of multicast group on a per-interface basis. The routers that receive these IGMP packets send multicast data that they receive for requested groups out the network segment of the known receivers.

By default, when PIM is enabled on an interface, IGMP version 3 is enabled. IGMP can be enabled on an interface explicitly.

IGMP Versions

SWMRE supports IGMPv2 and IGMPv3, as well as IGMPv1 report reception. By default, SWMRE enables IGMPv3 when PIM is enabled on an interface.

IGMPv3 includes the following key changes from IGMPv2:

- Support for Source-Specific Multicast (SSM), which builds shortest path trees from each receiver to the source, through the following feature:
- Host messages that can specify both the group and the source.
- The multicast state that is maintained for groups and sources, not just for groups as in IGMPv2.
- Hosts no longer perform report suppression, which means that hosts always send IGMP membership reports when an IGMP query message is received.

IGMP Operation

IGMP works on the premise of three major packets exchange between IGMP enabled routers and hosts, interested in joining a particular group.

IGMP Query Operation

Once IGMP is enabled or pim is enabled (which enables igmpv3), on any interface it starts sending Query message, which is called general query to the all-hosts multicast group at 224.0.0.1 periodically to discover whether any hosts want to receive multicast data.

SWMRE elects a router as the IGMP querier on a subnet if it has the lowest IP address. As long as a router continues to receive query messages from a router with a lower IP address, it resets a timer that is based on its querier timeout value. If the querier timer of a router expires, it becomes the designated querier. If that router later receives a host query message from a router with a lower IP address, it drops its role as the designated querier and sets its querier timer again.

In the figure below Router-1 eth2 sends query every query-interval. Since Router1-eth2 IP address is less than Router2 eth2, Router-1 eth2 becomes querier on the LAN.

IGMP Membership Report Operation

When a host receives a query from the local router it sends a Host Membership Report for all the multicast groups for which it wants to receive multicast traffic. This is called solicited membership report.

When a host joins a new group, the host immediately sends a Membership Report to inform a local router that it wants to receive multicast traffic for the group it has just joined without waiting to receive a Query. This is called unsolicited membership report.

In the figure below Host-1 and Host-2 sends membership reports to Router-1 eth2 for all the multicast groups for which they want to receive multicast traffic. Upon reception of membership report Router-1 maintains an IGMP group table containing multicast group-address, interface name on which it receives the report.

IGMP Leave Operation

When a multicast host leaves a group, a host that runs IGMPv2 or later sends an IGMP leave message. To check if this host is the last host to leave the group, the router sends an IGMP query (Called as Group-specific-query) message and starts a timer that you can configure called the last member query response interval. If no reports are received before the timer expires, the software removes the group state. The router continues to send multicast traffic for a group until its state is removed.

In the figure below Host-1 and Host-2 sends leave message to Router-1 eth2 for all the multicast groups for which they don't want to receive multicast traffic. In response to leave message Router-1 eth2 sends an group-specific-query message before removing the multicast group address from the IGMP table.

Topology

The procedures in this section use the topology in Figure 1-112

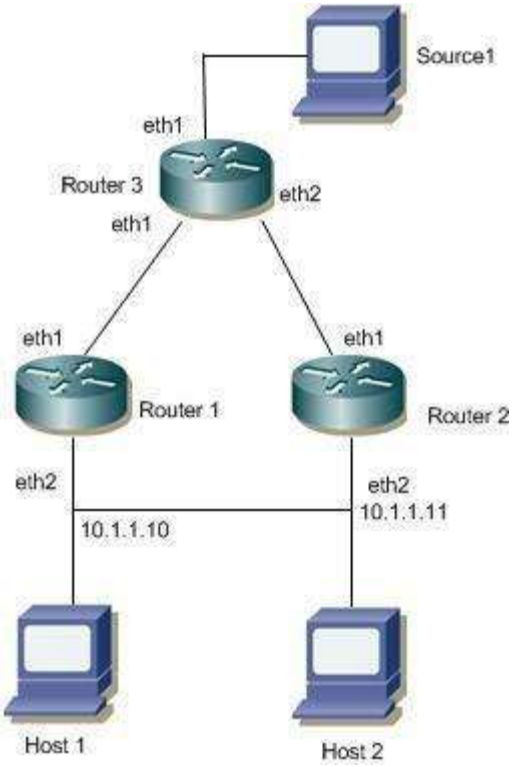


Figure 1-112: IGMP Topology

IGMP Configuration

The following example shows IGMP configuration on Router1.

Configuring IGMP Version

The configuration that follows shows how IGMP version can be configured.

`#configure terminal`	Enter Configure mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 10.1.1.10/24`	Assign IP address to an interface
`(config-if)#ip igmp version 2`	Enable IGMP version as v2.
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit Configure mode.

Validation

Enter the commands listed in this section to confirm the previous configurations.

```
#show  running-config
!
no service password-encryption
!
hostname rtr1
!
ip multicast-routing
! ! interface eth2 ip address 10.1.1.10/24
no shutdown ip igmp version 2
```

Configuring IGMP Parameters

The configuration that follows shows how IGMP parameters can be configured.

`#configure terminal`	Enter Configure mode.
`(config)#interface eth2`	Enter Interface mode
`(config-if)#ip igmp access-group 1`	Configures a access-list policy to control the multicast groups that hosts on the subnet serviced by an interface can join.
`(config-if)#ip igmp immediate-leave group-list 1`	Enables the device to remove the group entry from the multicast routing table immediately upon receiving a leave message for the group.
`(config-if#ip igmp  join-group 224.1.1.1`	Statically binds a multicast group to the outgoing interface
`(config-if)# ip igmp  last-member-querycount 7`	Sets the query count used when the software starts up.
`(config-if)# ip igmp  last-member-queryinterval 25500`	Sets the query interval used when the software starts up.
`(config-if)#ip igmp limit 100`	Configure Max Allowed State on this interface

(config-if)#ip igmp querier-timeout 300	Sets the querier timeout that the router uses when deciding to take over as the querier.
(config-if)#ip igmp query-interval 200	Sets the frequency at which the router sends IGMP host query messages.
(config-if)#ip igmp query-max-response-time 150	Sets the response time advertised in IGMP queries.
(config-if)#ip igmp ra-option	Enable ra-option.
(config-if)#ip igmp robustness-variable 4	Sets the robustness variable.
(config-if)#ip igmp startup-query-count 4	Sets the query count used when the router starts up.
(config-if)# ip igmp startup-query-interval 50	Sets the query interval used when the router starts up.
(config-if)# ip igmp static-group 225.1.1.1	Statically binds a multicast group to the outgoing interface.
(config-if)#exit	Exit Interface mode.
(config)#exit	Exit Configure mode.

Validation

Enter the commands listed in this section to confirm the previous configurations.

```
Rtr1#show  running-config
!
no service password-encryption
!
hostname rtr1
! !
ip multicast-routing
! !
interface eth2 ip address 10.1.1.10/24 no shutdown ip igmp access-
group 1 ip igmp immediate-leave group-list 1 ip igmp last-member-
query-count 7 ip igmp limit 100 ip igmp join-group 224.1.1.1 ip igmp
static-group 225.1.1.1 ip igmp last-member-query-interval 25500 ip
igmp querier-timeout 300 ip igmp query-interval 200 ip igmp query-
max-response-time 150 ip igmp startup-query-interval 50 ip igmp
startup-query-count 4 ip igmp robustness-variable 4 ip igmp ra-option
ip igmp version 2 !!
Rtr1#show  ip igmp   interface  eth2
Interface eth2 (Index 4)
 IGMP Enabled, Active, Querier, Configured for version 2
Internet address is 10.1.1.10
IGMP interface limit is 100
IGMP interface has 2 group-record states
IGMP Interface statistics: v1-reports: 0 v2-
reports: 0, v2-leaves: 0 v3-reports: 0 IGMP
query interval is 200 seconds
IGMP Startup query interval is 50 seconds
IGMP Startup query count is 4
IGMP querier timeout is 300 seconds
```

```
IGMP max query response time is 150 seconds
Group Membership interval is 950 seconds
IGMP Last member query count is 7
Last member query response interval is 25500 milliseconds
```

Here is the sample configuration on Router-1 with all the IGMP related commands configured.

```
Rtr1#show  running-config
!
no service password-encryption
!
hostname rtr1
! !
ip domain-lookup
!
ip multicast-routing
! ip pim register-rp-reachability ip pim crp-
cisco-prefix
! interface lo  ip address 127.0.0.1/8  ip address
1.1.1.57/32 secondary ipv6 address ::1/128 no
shutdown
! interface eth0  ip address 10.12.48.179/24
no shutdown
! interface eth1 ip address 192.168.1.27/24
no shutdown ip igmp version 2
 !
interface eth2 ip address 10.1.1.10/24 no shutdown ip
igmp access-group 1 ip igmp immediate-leave group-list
1 ip igmp last-member-query-count 7 ip igmp limit 100
ip igmp join-group 224.1.1.1
 ip igmp static-group 225.1.1.1 ip igmp
last-member-query-interval 25500 ip igmp
querier-timeout 300 ip igmp query-interval
200 ip igmp query-max-response-time 150 ip
igmp startup-query-interval 50 ip igmp
startup-query-count 4 ip igmp robustness-
variable 4 ip igmp ra-option ip igmp
version 2
 ! line con 0 login
line vty 0 16 exec-
timeout 0 0 login
line vty 17 39 login
!
End
```

IGMP Group Table after IGMPV2 Membership Report is received

IGMP group table is populated at router by virtue of either static join is configured on interface or dynamic report is being received on the interface.

The `show ip igmp group` command displays the IGMP group table. In this table, the following fields are defined.

Table 1-165: IGMP group table after IGMPV2 membership report

Group address	Displays the Multicast Group for which report is received.
Interface	Interface name on which Membership report is received.
Uptime	Duration since the report is received.
Expiry	Time frame in which the multicast group is going to expire.
Last Reporter	Host address from where the report is generated.

```
Rtr1#show   ip igmp groups
IGMP Connected Group Membership
Group Address    Interface      Uptime     Expires       Last Reporter
224.0.1.3             eth2        00:10:06    00:03:43      10.1.1.52 224.1.1.1
eth2        01:54:53   static         0.0.0.0
225.1.1.1             eth2      00:17:22   static          0.0.0.0

Rtr1#show ip igmp groups detail
IGMP Connected Group Membership Details

Flags: (M - SSM Mapping, R - Remote, L - Local,
        SG - Static Group, SS - Static Source)
Interface:      eth2
Group:          224.0.1.3
Flags:          R
Uptime:         00:10:06
Group mode:     Exclude (Expires: 00:03:43)
State: Active
Last reporter:  10.1.1.52
Source list is empty

Flags: (M - SSM Mapping, R - Remote, L - Local,
        SG - Static Group, SS - Static Source)
Interface:      eth2
Group:          224.1.1.1
Flags:          L
Uptime:         01:54:59
Group mode:     Exclude (Static)
State: Active
Last reporter:  0.0.0.0
Source list is empty

Flags: (M - SSM Mapping, R - Remote, L - Local,
        SG - Static Group, SS - Static Source)
Interface:      eth2
Group:          225.1.1.1
```

```
Flags:          SG
Uptime:         00:17:28
Group mode:     Exclude (Static)
State: Active
Last reporter:  0.0.0.0
Source list is empty
```

IGMP Group Table after IGMPV3 Membership report is received

IGMP group table is populated at router by virtue of either static join is configured on interface or dynamic report is being received on the interface. Here IGMPV3 should be configured on the interface (by default IGMPv3 will be enabled if pim is configured on the interface).

The `show ip igmp group` command displays the IGMP group table. In this table, the following fields are defined.

Table 1-166: IGMP group table after IGMPV3 membership

Group address	Displays the Multicast Group for which report is received.
Interface	Interface name on which Membership report is received.
Uptime	Duration since the report is received.
Expiry	Time frame in which the multicast group is going to expire.
Last Reporter	Host address from where the report is generated.

```
rtr6#show    ip  igmp    groups   IGMP
Connected   Group  Membership    Group
Address    Interface           Uptime
Expires    Last   Reporter  224.0.1.3
eth2                00:08:50 00:02:10
192.168.10.52  rtr6#show    ip   igmp
groups  detail  IGMP  Connected  Group
Membership Details

Flags: (M - SSM Mapping, R - Remote, L - Local,
        SG - Static Group, SS - Static Source)
Interface:      eth2
Group:          224.0.1.3
Flags:          R
Uptime:         00:08:50
Group mode:     Exclude (Expires: 00:04:57)
Last reporter:  192.168.10.52
Group source list: (R - Remote, M - SSM Mapping, S - Static, L - Local)

Exclude Source List :
  Source Address  Uptime    v3 Exp    Fwd  Flags
  1.2.3.4         00:08:50  stopped   No   R
```

For IGMPV3 report source list specifies which source to be included or exclude based on the membership report sent by the hosts.

In the above show command, Source address 1.2.3.4 is excluded to send Multicast data for group 224.0.1.3

CHAPTER 2 IGMP Proxy Configuration

In some simple tree topologies, it is not necessary to configure complex multicast routing protocols, such as PIM, on the boundary devices. It is sufficient to learn and proxy the group membership information and simply forward multicast packets based upon that information. Using IGMP forwarding (RFC 4605) to replicate multicast traffic on devices such as the edge boxes can greatly simplify the design and implementation of those devices. By not supporting more complicated multicast routing protocol such as Protocol Independent Multicast (PIM), it reduces not only the cost of the devices but also the operational overhead. Another advantage is that it makes the proxy devices independent of the multicast routing protocol used by the core network routers.

IGMP proxy can be used in such topologies instead of PIM. With IGMP proxy configured, the device serves as a proxy for the downstream hosts to send IGMP messages, maintain group memberships, and implement multicast forwarding based on the memberships. In this case, each boundary device configured with IGMP proxying is a host but no longer a PIM neighbor to the upstream device.

A device with IGMP proxy configured maintains a group membership database, which stores the group memberships on all the downstream interfaces. Each entry comprises the multicast address, filter mode, and source list. Such an entry is a collection of members in the same multicast group on each downstream interface.

A proxy device performs host functions on the upstream interface based on the database. It responds to queries according to the information in the database or sends join/leave messages when the database changes. On the other hand, the proxy device performs router functions on the downstream interfaces by participating in the querier election, sending queries, and maintaining memberships based on the reports.

Terminology

Following is a brief description of terms and concepts used to describe the IGMP Proxy:

Upstream interface

Also referred to as the proxy interface. A proxy interface is an interface on which IGMP proxy service is configured. It is in the direction toward the root of the multicast forwarding tree. An upstream interface acts as a host running IGMP; therefore, it is also called host interface.

Downstream interface

An interface that is running IGMP and in the direction contrary to the root of the multicast forwarding tree.
A downstream interface acts as a router running IGMP; therefore, it is also called router interface.

Member State

State of the associated group address and interface.

- Idle - Interface has not yet responded to a group membership query or general query for this group.
- Delay - Interface has responded to the latest group membership query or general query for this group.

IGMP-Proxy Configuration Steps

This section provides the configuration steps for configuring IGMP Proxy and example for a relevant scenario.

- Enable IP multicast on each router (see Enabling IP Multicast Routing)
- Enable IGMP Proxy service on the upstream interface.
- Enable IGMP mrouter configuration on the downstream interface.
- Enable IGMP proxy unsolicited report interval on the proxy interface. The proxy group membership reports are forwarded to the upstream router in this unsolicited report interval time. This is an optional parameter in which the default value of 1 sec is considered for forwarding proxy groups to upstream router.

Note:Configure IP addresses on all the interfaces used in the topology.

Unicast routing protocol should be configured in the PIM domain.

Topology

In this network topology, Router 1 acts as a proxying router to the upstream router Router 2 in which PIM domain is present. Also the source address is 172.31.1.52 and the group address is set to 224.0.1.3.

Note:Any PIM mode (PIM-SM,PIM-DM,PIM-SMDM) should be enabled on all the interfaces in the PIM domain.

Here in this example default value for unsolicited report interval is considered.

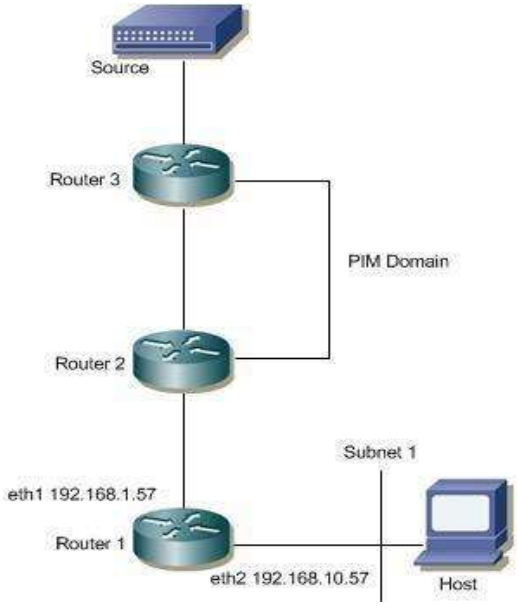


Figure 2-113: IGMP Proxy Topology

In this example, Routers 2 and 3 are running PIM and Router1 is the IGMP Proxying router.

- Host ends an IGMP membership report to Subnet 1.
- Downstream interface on Router1 received IGMP reports from host and updates the proxy interface.
- IGMP Proxying router (Router1) maintains the group membership information and forwards the received report to the upstream router (Router2).
- Source then sends a data packet for group.
- When the data packet reaches Router1, it forwards via the interface, eth2, because it has an IGMP join requested for Multicast traffic.

Enabling IP Multicast Routing

Enable IP multicast routing on all of the PIM routers inside the PIM domain:

#configure terminal	Enter Configure mode.
(config)# ip multicast-routing	Enable IP multicast routing.
(config)#exit	Exit Configure mode.

Enabling Proxy upstream interface

Enable IGMP proxy service on the interface in which the interface is in the direction toward the root of the multicast forwarding tree. In this example eth1 is the upstream interface which acts as an IGMP host.

#configure terminal	Enter Configure mode.
(config)#interface eth1	Enter interface mode.
(config-if)#ip address 192.168.1.57/24	Assign IP address to an interface
(config-if)#ip igmp proxy-service	Enable IGMP proxy service on the upstream interface.
(config-if)#exit	Exit interface mode.
(config)#exit	Exit Configure mode.

Enabling Proxy downstream interface

Enable IGMP mrouter proxy on the interface in which the interface is in the direction contrary to the root of the multicast forwarding tree. In this example eth2 is the downstream interface which is connected to receiver.

#configure terminal	Enter Configure mode.
(config)#interface eth2	Enter Interface mode
(config-if)#ip address 192.168.10.57/24	Assign IP address to an interface
(config-if)#ip igmp mrouter-proxy eth1	Enable IGMP mrouter proxy on the downstream interface and specify the upstream proxy interface name.
(config-if)#exit	Exit Interface mode.
(config)#exit	Exit Configure mode.

Validation

Here is the same configuration for IGMP Proxying router.

```
hostname Router1
!
interface lo
!!
ip multicast-routing
!
interface eth0
!
interface eth1 ip address 192.168.1.57/24 no
shutdown ip igmp proxy-service
!
```

```
interface eth2 ip address 192.168.10.57/24 no
shutdown ip igmp mrouter-proxy eth1 !
```

IGMP proxy interface

The following output displays the IGMP Proxy interface information.

```
Router1#show ip igmp interface

Interface eth1 (Index 3)
 IGMP Enabled, Active, Version 3 (default), proxy-service
 IGMP host version 3
 Internet address is 192.168.1.57
 Unsolicited Report Interval is 1000 milliseconds


Interface eth2 (Index 4)
 IGMP Enabled, Active, Querier, Version 3 (default)
 IGMP mroute-proxy interface is eth1
 Internet address is 192.168.10.57 IGMP interface has 1
group-record states
IGMP Interface statistics: v1-reports: 0 v2-
reports: 1, v2-leaves: 0 v3-reports: 0
IGMP query interval is 125 seconds
 IGMP Startup query interval is 31 seconds
 IGMP Startup query count is 2
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Group Membership interval is 260 seconds
 IGMP Last member query count is 2
 Last member query response interval is 1000 milliseconds
```

IGMP proxy

The following output displays the IGMP proxy information.

```
Router1#show ip igmp proxy

Interface eth2 (Index 4)
Administrative status: enabled
Operational status: up
Upstream interface is eth1
Number of multicast groups: 1
```

IGMP proxy groups

The following output displays the IGMP proxy group membership information.

```
Router1#show ip igmp proxy groups

IGMP Connected Proxy Group Membership
Group Address    Interface            State     Member state
224.0.1.3        eth1                 Active    Delay
```

IP Multicast Routing Table

The `show ip mroute` command displays the IP multicast routing table. `Router1#show ip mroute`

```
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
       B - BIDIR
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(172.31.1.52, 224.0.1.3), uptime 00:00:05
Owner IGMP-Proxy-Service, Flags: F
  Incoming interface: eth1
Outgoing interface list:
eth2 (1)
```

Enabling Unsolicited report interval

Enable IGMP proxy unsolicited report interval on the upstream interface. The proxy group membership reports are forwarded to the upstream router in this unsolicited report interval time.

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Enter Interface mode
`(config-if)#ip igmp proxy unsolicitedreport-interval 20000`	Enable IGMP proxy unsolicited report interval value on the upstream interface.
`(config-if)#exit`	Exit Interface mode.
`(config)#exit`	Exit Configure mode.

Validation

Here is the same configuration for IGMP Proxying router. `hostname Router1`

```
!
interface eth0
!
interface  eth1  ip  address
192.168.1.57/24   ip   igmp
proxy-service
ip igmp proxy unsolicited-report-interval 20000
!
interface  eth2  ip  address
192.168.10.57/24  ip  igmp
mrouter-proxy eth1
!
interface lo
!
!
```

```
ip multicast-routing
!
```

IGMP proxy Unsolicited report interval

The following output displays the IGMP proxy unsolicited report interval information.

```
Router1#show ip igmp interface eth1

Interface eth1 (Index 3)
 IGMP Enabled, Active, Version 3 (default), proxy-service
 IGMP host version 3
 Internet address is 192.168.1.57
 Unsolicited Report Interval is 20000 milliseconds
```

IGMP proxy group with unsolicited report interval

The following output displays the IGMP proxy group membership information when the proxy unsolicited report interval is configured to specific value.

```
Router1#show ip igmp proxy groups

IGMP Connected Proxy Group Membership
Group Address    Interface            State     Member state
224.0.1.3        eth1                 Active    Idle
```

IP Multicast Routing Table

The `show ip mroute` command displays the IP multicast routing table.

```
Router1#show ip mroute

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
       B - BIDIR
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(172.31.1.52, 224.0.1.3), uptime 00:00:05
Owner IGMP-Proxy-Service, Flags: F
  Incoming interface: eth1
Outgoing interface list:
eth2 (1)
```

CHAPTER 3 PIM Sparse Mode Configuration

The Protocol Independent Multicasting-Sparse Mode (PIM-SM) is a multicast routing protocol designed to operate efficiently across Wide Area Networks (WANs) with sparsely distributed groups. It helps geographically dispersed network nodes to conserve bandwidth and reduce traffic by simultaneously delivering a single stream of information to multiple locations. PIM-SM uses the IP multicast model of receiver-initiated membership, supporting both shared and shortest-path trees, and uses soft-state mechanisms to adapt to changing network conditions. It relies on a topologygathering protocol to populate a multicast routing table with routes.

This chapter provides the following topics:

- Terminology
- Data Flow from Source to Receivers in PIM-SM Network Domain
- PIM-SM Configuration
- Anycast-RP Configuration
- Override RP cnt: 0

Terminology

Following is a brief description of terms and concepts used to describe the PIM-SM protocol:

Rendezvous Point

A Rendezvous Point (RP) router is configured as the root of a non-source-specific distribution tree for a multicast group. Join messages from receivers for a group are sent towards the RP. Data from senders is sent to the RP so that receivers can discover who the senders are, and receive traffic destined for the group.

Multicast Routing Information Base

The Multicast Routing Information Base (MRIB) is a multicast topology table derived from the unicast routing table. In PIM-SM, the MRIB decides where to send Join/Prune messages. It also provides routing metrics for destination addresses. These metrics are used when sending and processing Assert messages.

Reverse Path Forwarding

Reverse Path Forwarding (RPF) is an optimized form of flooding, in which the router accepts a packet from `SourceA` through Interface `IF1`, only if `IF1` is the interface the router uses to reach `SourceA`. To determine if the interface is correct, it consults its unicast routing tables. The packet that arrives through interface `IF1` is forwarded because the routing table lists this interface as the shortest path. The router's unicast routing table determines the shortest path for the multicast packets. Because a router accepts a packet from only one neighbor, it floods the packet only once, meaning that (assuming point-to-point links) each packet is transmitted over each link, once in each direction.

Tree Information Base

The Tree Information Base (TIB) is a collection of states at a PIM router storing the state of all multicast distribution trees at that router. The TIB is created by receiving Join/Prune messages, Assert messages, and IGMP information from local hosts.

Upstream

Upstream indicates that traffic is going towards the root of the tree. The root of the tree might be either the Source or the RP.

Downstream

Downstream indicates that traffic is going away from the root of the tree. The root of tree might be either the Source or the RP.

Source-Based Trees

In Source-Based Trees, the forwarding paths are based on the shortest unicast path to the source. If the unicast routing metric used is `hop counts`, the branches of the multicast Source-Based Trees are minimum hop. If the metric used is `delay`, the branches are minimum delay. A corresponding multicast tree directly connects the source to all receivers for every multicast source. All traffic to the members of an associated group passes along the tree made for their source. Source-Based Trees have two entries with a list of outgoing interfaces -- the source address and the multicast group.

Shared Trees

Shared trees, or RP trees (RPT), rely on a central router called the Rendezvous Point (RP) that receives all traffic from the sources, and forwards that traffic to the receivers. There is a single tree for each multicast group, regardless of the number of sources. Only the routers on the tree know about the group, and information is sent only to interested receivers. With an RP, receivers have a place to join, even if no source exists. The shared tree is unidirectional, and information flows only from the RP to the receivers. If a host other than the RP has to send data on the tree, the data must first be tunneled to the RP, then multicast to the members. This means that even if a receiver is also a source, it can only use the tree to receive packets from the RP, and not to send packets to the RP (unless the source is located between the RP and the receivers).

Note:Not all hosts are receivers.

Bootstrap Router

When a new multicast sender starts sending data packets, or a new receiver starts sending Join messages towards the RP for that multicast group, the sender needs to know the next-hop router towards the RP. The bootstrap router (BSR) provides group-to-RP mapping information to all the PIM routers in a domain, allowing them to map to the correct RP address.

Data Flow from Source to Receivers in PIM-SM Network Domain

1. Sending out Hello Messages

PIM routers periodically send Hello messages to discover neighboring PIM routers. Hello messages are multicast using the address, 224.0.0.13 (`ALL-PIM-ROUTERS` group). Routers do not send any acknowledgement that a Hello message was received. A `holdtime` value determines the length of time for which the information is valid. In PIM-SM, a downstream receiver must join a group before traffic is forwarded on the interface.

2. Electing a Designated Router

In a multi-access network with multiple routers connected, one of the routers is selected to act as a designated router (DR) for a given period. The DR is responsible for sending Join/Prune messages to the RP for local members.

3. Determining the Rendezvous Point

PIM-SM uses a BSR to originate bootstrap messages, and to disseminate RP information. The messages are multicast to the group on each link. If the BSR is not apparent, the routers flood the domain with advertisements. The router with the highest priority (if priorities are same, the higher IP address applies) is selected to be the RP. Routers receive and store bootstrap messages originated by the BSR. When a DR gets a membership indication from IGMP for (or a data packet from) a directly connected host, for a group for which it has no entry, the designated router (DR) maps the group address to one of the candidate RPs that can service that group. The DR then sends a Join/Prune message towards that RP. In a small domain, the RP can also be configured statically.

4. Joining the Shared Tree

To join a multicast group, a host sends an IGMP message to its upstream router, after which the router can accept multicast traffic for that group. The router sends a Join message to its upstream PIM neighbor in the direction of the RP. When a router receives a Join message from a downstream router, it checks to see if a state exists for the group in its multicast routing table. If a state already exists, the Join message has reached the shared tree, and the interface from which the message was received is entered in the Outgoing Interface list. If no state exists, an entry is created, the interface is entered in the Outgoing Interface list, and the Join message is again sent towards the RP.

5. Registering with the RP

A DR can begin receiving traffic from a source without having a Source or a Group state for that source. In this case, the DR has no information on how to get multicast traffic to the RP through a tree. When the source DR receives the initial multicast packet, it encapsulates it in a Register message, and unicasts it to the RP for that group. The RP deencapsulates each Register message, and forwards the extracted data packet to downstream members on the RPT. Once the path is established from the source to the RP, the DR begins sending traffic to the RP as standard IP multicast packets, as well as encapsulated within Register messages. The RP temporarily receives packets twice. When the RP detects the normal multicast packets, it sends a Register-Stop message to the source DR, meaning it should stop sending register packets.

6. Sending Register-Stop Messages

When the RP begins receiving traffic from the source, both as Register messages and as unencapsulated IP packets, it sends a Register-Stop message to the DR. This notifies the DR that the traffic is now being received as standard IP multicast packets on the SPT. When the DR receives this message, it stops encapsulating traffic in Register messages.

7. Pruning the Interface

Routers attached to receivers send Prune messages to the RP to disassociate the source from the RP. When an RP receives a Prune message, it no longer forwards traffic from the source indicated in the Prune message. If all members of a multicast group are pruned, the IGMP state of the DR is deleted, and the interface is removed from the Source and Group lists of the group.

8. Forwarding Multicast Packets

PIM-SM routers forward multicast traffic onto all interfaces that lead to receivers that have explicitly joined a multicast group. Messages are sent to a group address in the local subnetwork, and have a Time to Live (TTL) of 1. The router

performs an RPF check, and forwards the packet. If a downstream router has sent a join to this router or is a member of this group, then traffic that arrives on the correct interface is sent to all outgoing interfaces that lead to downstream receivers.

PIM-SM Configuration

PIM-SM is a soft-state protocol. The required steps to configure PIM-SM are the following:

- Enable IP multicast on each PIM router (see Enabling IP Multicast Routing)
- Enable PIM-SM on the desired interfaces (see Enable PIM-SM on an Interface)
- Configure the RP statically (see Configuring Rendezvous Point Statically or dynamically (see Configure Rendezvous Point Dynamically Using Bootstrap Router Method) depending on which method you use)

All multicast group states are dynamically maintained as the result of IGMP `Report/Leave` and PIM `Join/Prune` messages.

This section provides the steps to configure the PIM-SM feature. Configuration steps and examples are used for two relevant scenarios.

Topology

The following figure displays the network topology used in these examples.

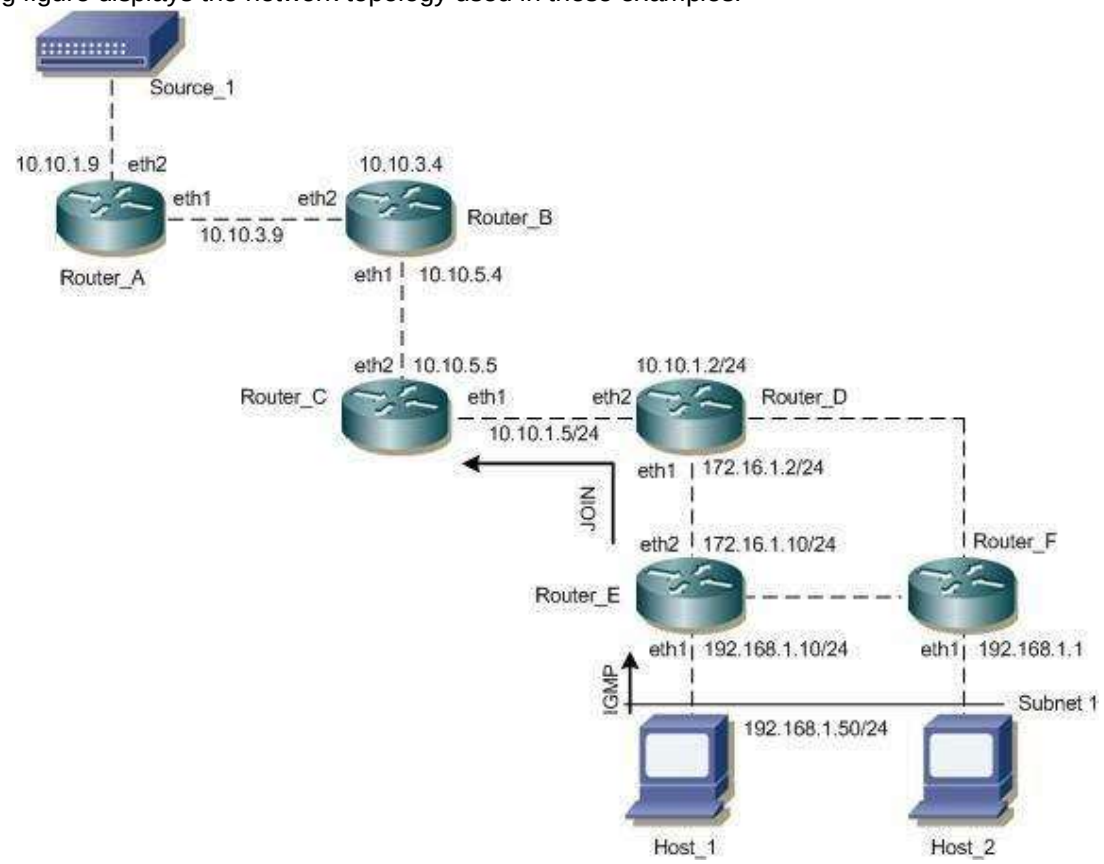


Figure 3-114: PIM-SM Topology

Enabling IP Multicast Routing

Enable IP multicast routing on all of the PIM routers inside the PIM domain:

Enable IP Multicast Routing

`#configure terminal`	Enter Configure mode.
`(config)#ip multicast-`	Enable IP multicast routing.
`routing (config)#exit`	Exit Configure mode.

Enable PIM-SM on an Interface

Enable PIM-SM on all participating interfaces within each of routers inside the PIM domain on which you want to run PIM. In the following sample configuration, both eth1 and eth2 are enabled for PIM-SM on the router.

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to be configured and enter the Interface mode.
`(config-if)#ip address 10.10.12.11/24`	Configure the IP address for `eth1`.
`(config-if)#ip pim sparse-mode`	Enable PIM sparse mode on the interface.
`(config-if)#exit`	Exit Interface mode.
`(config)#interface eth2`	Specify the interface (`eth2`) to be configured and enter the Interface mode.
`(config-if)#ip address 10.10.13.11/24`	Configure the IP address for `eth2`.
`(config-if)#ip pim sparse-mode`	Enable PIM sparse mode on the interface.
`(config-if)#exit`	Exit Interface mode.

Configuring Rendezvous Point Statically

Every PIM multicast group needs to be associated with the IP address of a Rendezvous Point (RP), which is a router that resides in a multicast network domain. The address of the RP is used as the root of a group-specific distribution tree. All nodes in the domain that want to receive traffic sent to the group are aware of the address of the RP. For all senders to reach all receivers within a group, all routers in the domain must be able to map to the RP address configured for the group. There can be several RPs configured in a network deploying PIM-SM, each serving a different group.

You can statically configure a RP by specifying the RP address with in every router in the PIM domain. The use of statically configured RPs is ideal for small network environments or ones that do not require many RPs and/or require changing the assignment of the RPs often. Changing the assignment of an RP requires the re-configuration of the RP address in all of the routers in the PIM domain.

In static RP configurations, RP failover is not available.

When configuring the RP statically, do the following:

- On every router, include the `ip pim rp-address A.B.C.D` statement even if a router does not have any source or group member attached to it
- Assign only one RP address for a multicast group in the PIM domain

Using the topology depicted in Figure 3-114, `Router_C` is the RP, and all routers are statically configured with RP information. Host_1 and Host_2 join group 224.0.1.3 for all the sources. They send the IGMP membership report to

Subnet 1. Two routers are attached to Subnet 1, `Router_E` and `Router_F`; both have default DR priority on `eth1`. Since `Router_E` has a higher IP address on interface `eth1`, it becomes the Designated Router, and is responsible for sending Join messages to the RP (`Router_C`).

Configure Static RP

`#configure terminal`	Enter Configure mode.
`(config)#ip pim rp-address 10.10.1.5`	Statically configure an RP address for multicast groups.
`(config)#exit`	Exit Configure mode.

Here is the sample configuration for `Router D`:

```
hostname  Router_D
!
interface eth0 !
interface eth1  ip
pim sparse-mode !
interface eth2  ip
pim sparse-mode !
interface lo ! ! ip
multicast-routing

ip pim rp-address 10.10.1.5
!
```

Validation

Enter the commands listed in this section to confirm the previous configurations.

RP Details

At Router_D, the `show ip pim rp mapping` command shows that `10.10.1.5` is the RP for all multicast groups `224.0.0.0/4`, and is statically configured. All other routers will have a similar output:

```
#show ip pim rp mapping
 PIM Group-to-RP Mappings
 This system is the Bootstrap Router (v2)
 Group(s): 224.0.0.0/4
 RP: 1.1.1.1
 Info source: 1.1.1.1, via bootstrap, priority 0
 Uptime: 00:34:46, expires: 00:01:49
 RP: 1.1.1.6
 Info source: 1.1.1.6, via bootstrap, priority 2
 Uptime: 00:51:49, expires: 00:01:48
```

Override RP cnt: 0At Router_D, use the `show ip pim rp-hash` command to display the selected RP for a specified group (224.0.1.3):

```
 Router_D#show  ip  pim  rp-hash  224.0.1.3
RP: 10.10.1.5
```

Interface Details

The `show ip pim interface` command displays the interface details for `Router_E`, and shows that `Router_E` is the Designated Router on `Subnet 1`.

```
Router_E#show ip pim interface
Address           Interface VIFindex Ver/   Nbr       DR    DR
                                     Mode   Count     Prior
192.168.1.10      eth1       0       v2/S   1           1    192.168.1.10
172.16.1.10       eth2       2       v2/S   1           1    172.16.1.10
```

IP Multicast Routing Table

Note: The multicast routing table displays for an RP router are different from other routers.

The `show ip pim mroute` command displays the IP multicast routing table. In this table, the following fields are defined:

`RPF nbr` Displays the unicast next-hop to reach RP.

and mask length.

`RPF idx` Displays the incoming interface for this (*, G) state.

`RP` Displays the IP address for the RP router

`B` Displays the bidirectional pim mode

`The leading dots ....`

Stand for VIF index

```
Router_E#show ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G)   Entries:   1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
(*, 224.0.1.3)
RP: 10.10.1.5
RPF nbr: 172.16.1.2
RPF idx: eth2
Upstream State: JOINED
 Local     ...............................
 Joined    j...............................
 Asserted  ...............................
 Outgoing  o...............................
```

At `Router_E`, `eth2` is the incoming interface of the (*, G) entry, and `eth1` is on the outgoing interface list of the (*, G) entry. This means that there is a group member through `eth1`, and the RP is reachable through `eth2`.

The 0 position on this 32-bit index is for `eth1` (as illustrated in the interface display above). The `j` on the 0 index indicates that the `Join` has come from `eth1`.

Since `Router_C` is the RP, and the root of this multicast tree, the `show ip pim mroute` command on `Router_C` shows `RPF nbr` as 0.0.0.0 and `RPF idx` as none.

```
Router_C#show ip pim mroute
IP Multicast Routing Table
```

```
(*,*,RP) Entries: 0
(*,G)   Entries:   1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
(*, 224.0.1.3)
RP: 10.10.1.5
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
 Local     ...............................
 Joined    j...............................
 Asserted  ...............................
 Outgoing  o...............................
```

Configure Rendezvous Point Dynamically Using Bootstrap Router Method

A static RP configuration works for a small, stable PIM network domain; however, it is not practical for a large and/or complex one. In such a network, if the RP fails or you have to change the assignment of the RP, you are required to reconfigure the static configurations on all PIM routers. Also, if you have several multicast groups mapped to several RPs, there are many repetitive configurations you are required to perform, which can be time consuming and laborious. Thus when it comes configuring RP in large and/or complex networking environments, configuring it dynamically is the best and most scalable method to use. Bootstrap router (BSR) configuration is one method of configuring the RP dynamically.

The BSR mechanism in a PIM domain uses the concept of a RP as a way for receivers to discover the sources that send to a particular multicast group. The BSR mechanism gives a way for a multicast router to learn the set of group-toRP mappings required in order to function. The BSR's function is to broadcast the RP set to all routers in the domain.

Some of the PIM routers within a PIM domain are configured as Candidate-RPs (C-RPs). A subset of the C-RPs is eventually used as the actual RPs for the domain. An RP configured with a lower value in the priority field has a higher priority.

Some of the PIM routers in the domain are configured to be Candidate-BSRs (C-BSR). One C-BSR is selected to be the BSR for the domain, and all PIM routers in the domain learn the result of this election through Bootstrap messages (BSM). The C-BSR with highest value in the priority field is elected to be the BSR. The C-RPs then report their candidacies to the elected BSR, which chooses a subset of the C-RPs, and distributes corresponding group-to-RP mappings to all the routers in the domain using Bootstrap messages.

This section provides 2 examples to illustrate the BSR configuration for configuring RP dynamically.

Example 1

For this example, refer to Figure 1 for the topology.

To dynamically configure the RP, `Router_C` on `eth1` and `Router_D` on `eth1` are configured as a Candidate RP using the `ip pim rp-candidate` command. `Router_D` on `eth1` is also configured as the Candidate BSR. Since no other router has been configured as the candidate BSR, `Router_D` becomes the BSR router and is responsible for sending group-to-RP-mapping information to all other routers in this PIM domain.

The highest priority router (configured with lowest priority value) is chosen as the RP. If two or more routers have the same priority, a hash function in the BSR mechanism is used to choose the RP to ensure that all routers in the PIMdomain have the same RP for the same group.

To change the default priority of any candidate RP, use the `ip pim rp-candidate IFNAME PRIORITY` command. At `Router_D`, the `show ip pim rp mapping` command shows that `Router_C` is chosen as the RP for a specified group.

Configure RP Dynamically for Router C

`#configure terminal`	Enter Configure mode.
`(config)#ip pim rp-candidate eth1 priority 2`	Give this router the candidate RP status using the IP address of the specified interface.

Configure RP Dynamically for Router D

`#configure terminal`	Enter Configure mode.
`(config)#ip pim bsr-candidate eth1`	Give this router the candidate BSR status using the name of the interface.
`(config)#ip pim rp-candidate eth1 priority 2`	Give this router the candidate RP status using the IP address of the specified interface.

The following output displays the complete configuration at `Router_C` and `Router_D`:

```
Router_D#show running-config
!
interface eth0 !
interface eth1  ip
pim sparse-mode !
interface eth2  ip
pim sparse-mode !
interface lo ! ip multicast-
routing ip pim bsr-candidate eth1
ip pim rp-candidate eth1 priority
2 !

Router_C#show running-
config interface eth0 !
interface eth1  ip
pim sparse-mode !
interface eth2  ip
pim sparse-mode !
interface lo ! ! ip
multicast-routing ip
pim rp-candidate eth1
```

Validation

This section provides the steps to verify the RP configuration.

PIM Group-to-RP Mappings

The `show ip pim rp mapping` command displays the group-to-RP mapping details and displays information about RP candidates. There are two RP candidates for the group range, 224.0.0.0/4. RP Candidate 10.10.1.5 has a default priority of 192, whereas, RP Candidate 172.16.1.2 has been configured to have a priority of 2. Since RP candidate 172.16.1.2 has a higher priority, it is selected as RP for the multicast group, 224.0.0.0/4.

```
Router_D#show ip pim rp mapping
```

```
This system is the Bootstrap Router (v2)
Group(s): 224.0.0.0/4
 RP: 10.10.1.5
    Info source: 172.16.1.2, via bootstrap, priority 192
         Uptime: 00:00:13, expires: 00:02:29
 RP: 172.16.1.2
    Info source: 172.16.1.2, via bootstrap, priority 2
Uptime: 00:34:42, expires: 00:01:49
```

RP Details

To display information about the RP router for a particular group, use the following command. This output displays that 172.16.1.2 has been chosen as the RP for the multicast group 224.0.1.3.

```
Router_D#show ip pim rp-hash 224.0.1.3
Group(s): 224.0.0.0/4
    RP: 172.16.1.2
    Info source: 172.16.1.2, via bootstrap
```

After RP information reaches all PIM routers in the domain, various state machines maintain all routing states, as a result of Join/Prune from group membership. To display information on interface details and the multicast routing table, refer to the *Configuring Rendezvous Point Statically* section.

Example 2

To dynamically configure the RP, `Router_2` on `eth1` is configured as a Candidate RP using the `ip pim rpcandidate` command. Since no other router is configured as C-RP, `Router_2` becomes the RP. `Router_1` on `eth1` and `Router_2` on `eth1` are configured as the Candidate BSRs. Since `Router_1` has a higher priority value than `Router_2`, `Router_1` becomes the BSR router and is responsible for sending group-to-RP-mapping information to all other routers in this PIM domain.

Topology

For this example, refer to Figure 3-115 for the topology.

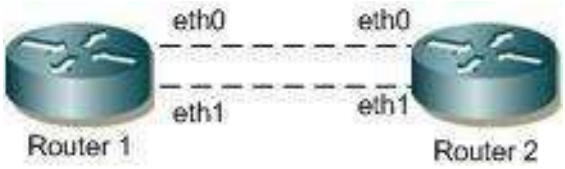


Figure 3-115: Boostrap Router Topology

Configuration

Router 1

`#configure terminal`	Enter Configure mode for `eth1`.
`(config)#ip pim bsr-candidate eth1`	Configure `eth1` of Router 1 as C-BSR. The default priority is 64, so it is not necessary to designate a priority.
`(config)#exit`	Exit Configure mode.

Router 2

`#configure terminal`	Enter the Configure mode.
`(config)#ip pim bsr-candidate eth1 10 25`	Configure `eth1` of Router 2 as C-BSR with a hash mask length of 10, and a priority of 25.
`(config)#ip pim rp-candidate eth1 priority 0`	Configure interface `eth1` as C-RP with a priority of 0.
`(config)#exit`	Exit Configure mode.

Router 2 Unicast BSM

When the `ip pim unicast-bsm` command is configured on an interface that is a DR for a network, then that interface unicasts the stored copy of BSM to the new or rebooting router.

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Enter the Interface mode for `eth1`.
`(config-if)#ip pim dr-priority 10`	Configure `eth1` as DR
`(config-if)#ip pim unicast-bsm`	Enable sending and receiving of Unicast BSM for backward compatibility.
`(config-if)#exit`	Exit Interface mode.

Validation

1. Verify the C-BSR state on Router 1.

```
#show ip pim bsr-router
      PIMv2 Bootstrap information
      This system is the Bootstrap Router
        (BSR) BSR address: 20.0.1.21
        Uptime:      00:37:12, BSR Priority: 64, Hash mask length: 10
        Next bootstrap message in 00:00:04
        Role: Candidate BSR
        State: Elected BSR
        Candidate RP: 20.0.1.21(eth1)
        Advertisement   interval   60   seconds
Next C-RP advertisement in 00:00:27
```

2. Verify the C-BSR state on Router 2.
   The initial state of C-BSR is P-BSR before transitioning to C-BSR. The two states are illustrated in the sample outputs from the `show ip pim bsr-router` command below.

```
 #show ip pim bsr-router
 PIMv2 Bootstrap information
   BSR address: 20.0.1.21
  Uptime:      00:02:39, BSR Priority: 64, Hash mask length: 10
  Expires:     00:00:03
  Role:   Candidate   BSR
State: Pending BSR

#show ip pim bsr-router
PIMv2 Bootstrap information
 BSR address: 20.0.1.21
 Uptime:      00:40:20, BSR Priority: 64, Hash mask length: 10
```

```
 Expires:     00:02:07
 Role: Candidate BSR
 State: Candidate BSR
```

3. Verify RP-set information on E-BSR.

```
#show ip pim rp mapping
PIM Group-to-RP Mappings
This system is the Bootstrap Router
(v2) Group(s): 224.0.0.0/4
 RP: 20.0.1.11
 Info source: 20.0.1.11, via bootstrap, priority 0
Uptime: 00:00:30, expires: 00:02:04
```

4. Verify RP-set information on C-BSR.

```
#show ip pim rp mapping
 PIM Group-to-RP Mappings
 Group(s): 224.0.0.0/4
 RP: 1.1.1.1
 Info source: 1.1.1.6, via bootstrap, priority 0
 Uptime: 00:36:19, expires: 00:02:18
 RP: 1.1.1.6
 Info source: 1.1.1.6, via bootstrap, priority 2
 Uptime: 00:36:32, expires: 00:02:18
 Override RP cnt: 0
```

Anycast-RP Configuration

The Anycast-RP feature provides load balancing among active RPs and redundancy in a PIM-SM network domain. In a PM-SM configuration, only a single active RP for each multicast group within a domain is permitted. However, in an Anycast-RP configuration, this restriction is removed with the support of multiple active RPs for each group in a domain.

SWMRE supports Anycast-RP using the PIM implementation. In PIM Anycast-RP, Multicast Source Discovery Protocol (MSDP) is not employed to share information about active sources. Instead the Register mechanism in PIM is extended to provide this same function.

The following describes Anycast-RP in PIM-SM:

- A Unicast IP address is used as the RP address. The address is statically configured, and associated with all PIM routers throughout the domain.
- A set of routers in the domain is chosen to act as RPs for this RP address. These routers are called the AnycastRP set.
- Each router in the Anycast-RP set is configured with a loopback address. The loopback address is configured on all RPs for the loopback interface, then configured as the RP address (static RP), and injected into OSPF using redistribute connected. The PIM-SM implementation uses only the first non-loopback address configured on the loopback interface. Therefore, it is important to be sure that the Anycast-RP address is configured with the first non-loopback address.
- Each router in the Anycast-RP set also needs a separate IP address, which is used for communication between the RPs.
- The RP address, or a prefix that includes the RP address, is injected into the unicast routing system inside the domain.

- Each router in the Anycast-RP set is configured with the addresses of all other routers in the Anycast-RP set. This must be consistently configured in all RPs in the set.

Topology

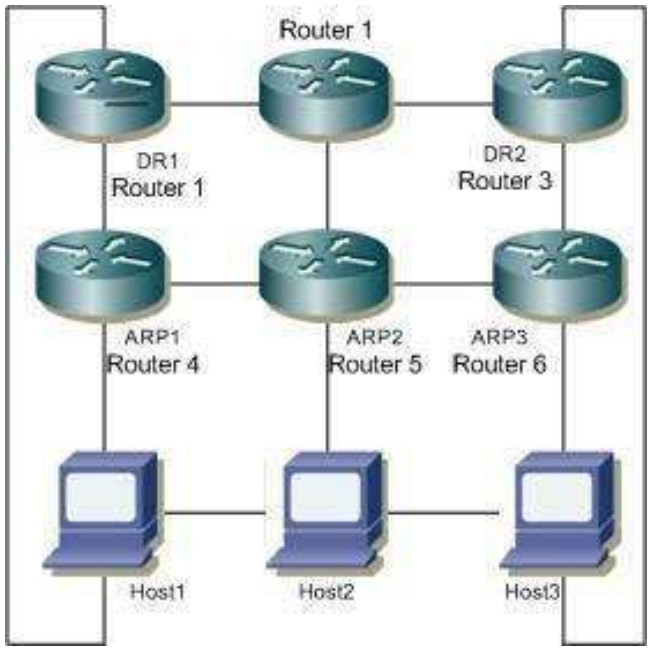


Figure 3-116: Anycast RP Topology

Host1 and Host3 act as hosts and sources for sending join and multicast data packets; Host2 acts as a host.

ARP1, ARP2 and ARP3

`#configure terminal`	Enter the Configure mode.
`(config)#interface lo`	Enter the loopback interface.
`(config)#ip address 1.1.1.152/32`	Configure the IP address for loopback
`(config)#exit`	Exit the Configure mode.
`(config)#ip pim rp-address 1.1.1.152`	Configure the static RP with the address of the loopback.
`(config)#ip pim anycast-rp 1.1.1.152 4.4.4.5`	Configure the member RP address. In this example, `4.4.4.5` is the member RP in ARP2. It is the address used for communication between all RPs.
`(config)#ip pim anycast-rp 1.1.1.152 7.7.7.1`	Configure the member RP address. In this example, `7.7.7.1` is the member RP in ARP3. It is the address used for communication between all RPs.
`(config)#ip pim anycast-rp 1.1.1.152 23.23.23.1`	Configure the member RP address. In this example, `23.23.23.1` is the member RP in ARP1. It is the address used for communication between all RPs.
`(config)#exit`	Exit the Configure mode.

Disable Anycast-RP

`#configure terminal`	Enter Configure mode.
`(config)#no ip pim anycast-rp 1.1.1.152`	Disable Anycast-RP.

(config)#no ip pim rp-address	Disable static RP.
1.1.1.152 (config)#exit	Exit Configure mode.

Validation

1. Verify RP-mapping in ARP1.

```
#show ip pim rp mapping
       PIM Group-to-RP Mappings
       Override RP cnt: 0
       Anycast-RP 1.1.1.152 members:23.23.23.1
       Group(s): 224.0.0.0/4, Static
       RP: 1.1.1.152
         Uptime: 00:00:13s
```

2. Verify RP-mapping in ARP1 after disabling anycast-RP and RP-address.

```
#show ip pim rp mapping
       PIM Group-to-RP Mappings
       Override RP cnt: 0
```

CHAPTER 4 PIM Dense Mode Configuration

Protocol Independent Multicast - Dense Mode (PIM-DM) is a data-driven multicast routing protocol that builds sourcebased multicast distribution trees that operate on the flood-and-prune principle. PIM-DM requires unicast-reachability information, but it does not depend on a specific unicast routing protocol.

Terminology

Following is a brief description of terms and concepts used to describe the PIM-DM protocol:

Reverse Path Forwarding

Reverse Path Forwarding (RPF) is an optimized form of flooding, in which the router accepts a packet from `SourceA` through Interface `IF1`, only when `IF1` is the interface the router would use in order to reach `SourceA`. It determines whether the interface is correct by consulting its unicast routing tables. The packet that arrives through interface `IF1` is forwarded because the routing table lists this interface as the shortest path to the network. The router's unicast routing table determines the shortest path for the multicast packets. Because a router accepts a packet from only one neighbor, it floods the packet only once, meaning that (assuming point-to-point links) each packet is transmitted over each link once in each direction.

Forwarding Multicast Packets

PIM-DM routers forward multicast traffic to all interfaces that lead to receivers that have explicitly joined a multicast group. Messages are sent to a group address in the local subnetwork. The router performs an RPF check, and forwards the packet. Traffic that arrives on the correct interface is sent to all outgoing interfaces that lead to downstream receivers, if the downstream router is a member of this group.

Upstream

Upstream traffic is traffic that is going towards the source.

Downstream

Downstream traffic is anything other than the upstream interface for that group.

Nexthop

PIM-DM does periodic lookups for prefixes to check router reachability. The nexthop lookup mechanism avoids periodic lookup. During start-up, PIM-DM notifies NSM (Network Services Manager) about the prefixes that pertain to them. NSM notifies the protocols if a better nexthop is available, or if a nexthop becomes unavailable. In this way, PIMDM does not expend resources to do periodic lookups, because NSM is proactive in their maintenance.

Configuration

Configuring PIM-DM requires the following steps:

- Enable IP multicast on each PIM router (see Enabling IP Multicast

Routing) PIM Dense Mode Configuration

- Enable PIM-DM on the desired interfaces (see Enabling PIM-DM)

This section provides the configuration steps for configuring PIM-DM and examples for a relevant scenario.

Topology

In this network topology, the Source_1 address is 10.10.1.52 and the group address is set to 224.0.1.3.

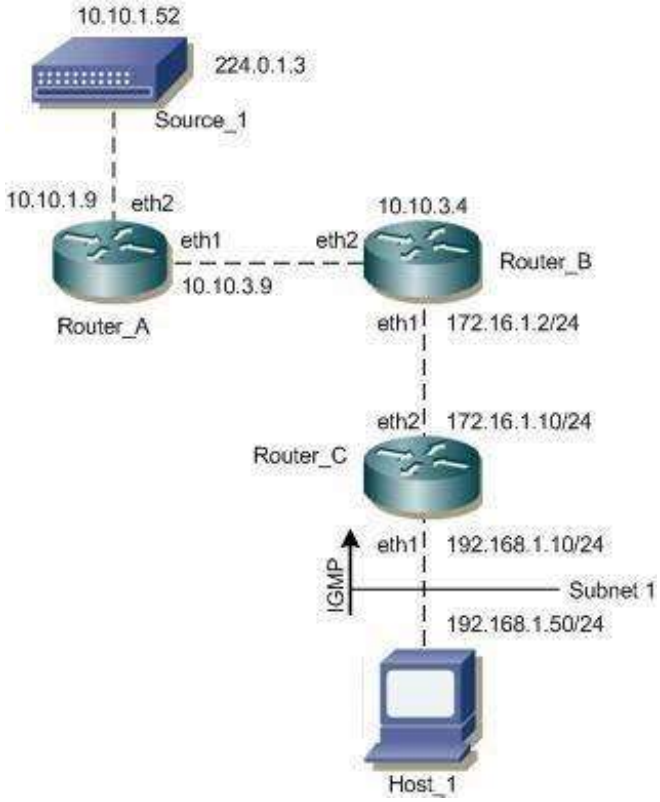


Figure 4-117: PIM-DM Configuration Topology

In this example, all routers are running PIM-DM.

1. Host_1 sends an IGMP membership report to Subnet 1.
2. After Router_C receives this report, it associates its receiving interface, `eth1`, with the group reported in the IGMP message, for example, group1.
3. Source_1 then sends a data packet for group1.
4. Every router creates an (S,G) entry in the multicast routing table.

5. When the data packet reaches `Router_C`, it forwards via the interface, `eth1`, because there is a local member on this interface for this group. `Router_C` has a downstream receiver, so it does not send a prune message to its upstream neighbor router, `Router_B`.

Enabling IP Multicast Routing

Enable IP multicast routing on all of the PIM routers inside the PIM domain:

PIM Dense Mode Configuration

`#configure terminal`	Enter Configure mode.
`(config)#ip multicast-`	Enable IP multicast routing.
`routing (config)#exit`	Exit Configure mode.

Enabling PIM-DM

Enable PIM-DM on all participating interfaces within each of routers inside the PIM domain on which you want to run PIM.

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 10.10.15.12/24`	Configure the IP address for `eth1`.
`(config-if)#ip pim dense-mode`	Enable PIM dense mode on the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 10.10.14.12/24`	Configure the IP address for `eth1`.
`(config-if)#ip pim dense-mode`	Enable PIM dense mode on the interface.
`(config-if)#exit`	Exit interface mode.

The following is a sample configuration for `Router_C`:

```
hostname  Router_C
!
interface eth0 !
interface eth1
ip pim dense-mode
! interface eth2
ip pim dense-mode
!
interface
lo ! !
ip  multicast-routing
!
```

Validation

The `show ip pim interface` command displays the interface details for `Router_C`.

```
Router_C#show ip pim interface
Address           Interface VIFindex Ver/   Nbr      DR
                                     Mode   Count    prior
192.168.1.10      eth1       0       v2/D   0          1
172.16.1.10       eth2       2       v2/D   1          1
```

PIM Dense Mode Configuration

The `show ip mroute` command displays the IP multicast routing table.

```
Router_C#show ip mroute
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(10.10.1.52, 224.0.1.3), uptime 00:00:15
Owner PIM-DM, Flags: F
 Incoming interface: eth2  Outgoing
interface list:     eth1 (1)
```

The `show ip pim mroute` displays the IP PIM-DM multicast routing table.

```
Router_C#show ip pim mroute
PIM-DM Multicast Routing Table
(10.10.1.52, 224.0.1.3)
 RPF Neighbor: 172.16.1.2, Nexthop: 172.16.1.2, eth2
 Upstream IF: eth2
    Upstream  State:  Forwarding     Assert  State:
NoInfo
 Downstream IF List:     eth1, in 'olist':
Downstream State: NoInfo
      Assert State: NoInfo
```

CHAPTER 5 IGMP Snooping Configuration

This chapter describes how to configure Internet Group Management Protocol (IGMP) Snooping.

Note: Run the `switchport` command on each port to change to Layer-2 mode.

Without IGMP, Layer-2 switches handle IP multicast traffic in the same manner as broadcast traffic and forwards frames received on one interface to all other interfaces. This creates excessive traffic on the network, and affects network performance. IGMP Snooping allows switches to monitor network traffic, and determine hosts to receive multicast traffic. Only one membership report is relayed from a group, instead of a report from each host in the group. To achieve this, IGMP Snooping is enabled on the switches.

Topology

This example describes the configuration on switch S1. The eth1 interface is configured as a multicast router port.

Because IGMP Snooping is used in bridged LAN environments, router R1 does not require running IGMP Snooping, and can run any multicast protocol (such as PIM-SM). Thus, the configuration on R1 is not included in this example.

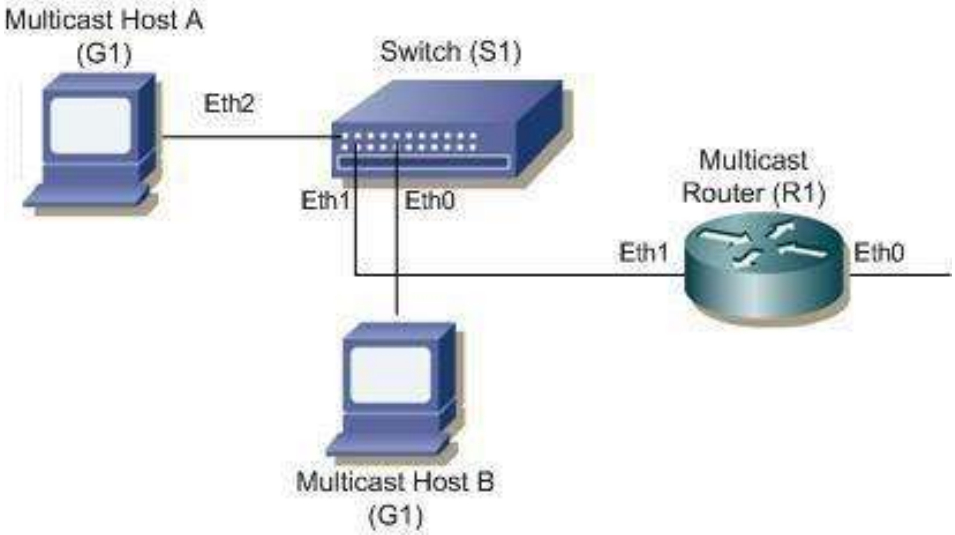


Figure 5-118: IGMP Snooping Topology

As a result of this configuration:

- The switch itself replies with membership report messages in response to queries received on interface eth1. However, if you do not enable report suppression on the switch, when it receives an IGMP Query message on eth1, it forwards it to both Host A and Host B. As a result, both hosts reply with a Membership report (as Layer-2 IGMP is running on the hosts).
- Because Host A and Host B are members of the same multicast group, the router is not notified when A leaves the group, because the group still has another member. When Host B leaves the group, the switch will send a Leave message to the Router with the destination address as 224.0.0.2 (All Router Destination Address).

Configuration

To enable IGMP Snooping on an interface:

1. Add a bridge to the spanning-tree table

IGMP Snooping Configuration

2. Specify the interface to be configured
3. Associate the interface with bridge group
4. IGMP snooping will be enabled by default
5. Configure ports that are connected to routers as multicast router ports
6. By default, IGMP report suppression is enabled on the switch

S1

`#configure terminal`	Enter the `Configure` mode.
`(config)#bridge 1 protocol ieee vlan-bridge`	Add bridge `1` to the spanning-tree table.
`(config)#interface eth0`	Specify the interface `eth0` to be configured, and enter the `Interface` mode.
`(config-if)#shutdown`	Shut down the interface.
`(config-if)#switchport`	Configure the interface as a switch port.
`(config-if)#bridge-group 1`	Associate the interface `eth1` with bridge-group `1`.
`(config-if)#switchport mode access`	Configure the port as an access port.
`(config-if)#no shutdown`	Bring up the interface.
`(config-if)#exit`	Exit the `Interface` mode.
`(config)#interface eth1`	Specify interface `eth1` to be configured.
`(config-if)#shutdown`	Shut down the interface.
`(config-if)#switchport`	Configure the interface as a switch port.
`(config-if)#bridge-group 1`	Associate interface `eth1` with bridge-group `1`.
`(config-if)#switchport mode access`	Configure the port as an access port.
`(config-if)#no shutdown`	Bring up the interface.
`(config-if)#exit`	Exit the `Interface` mode.
`(config)#interface eth2`	Specify interface `eth2` to be configured.
`(config-if)#shutdown`	Shut down the interface.
`(config-if)#switchport`	Configure the interface as a switch port.
`(config-if)#bridge-group 1`	Associate interface `eth2` with bridge-group `1`.
`(config-if)#switchport mode access`	Configure the port as an access port.
`(config-if)#no shutdown`	Bring up the interface.

(config-if)#exit	Exit the Interface mode.
(config)#interface vlan1.1	Specify interface vlan1.1 to be configured.
(config-if)# igmp snooping mrouter interface eth1	Configure this port as a multicast router port
(config-if)#exit	Exit the Interface mode

Validation

```
#show running-config interface eth0
!
interface eth0
```

IGMP Snooping Configuration

```
switchport bridge-group 1
switchport mode access
!
#show running-config interface eth1
! interface eth1
switchport bridge-group 1
switchport mode access !

#show running-config interface eth2
! interface eth2
switchport bridge-group 1
switchport mode access
!
#show igmp snooping groups IGMP
Snooping Group Membership
Group source list: (R - Remote, S - Static)
Vlan Group/Source Address Interface Flags Uptime Expires Last Reporter Version
1 224.1.1.1 eth0 R 00:00:03 00:04:17 0.0.0.0 V3
1 224.1.1.1 eth2 R 00:00:03 00:04:17 0.0.0.0
V3 #show igmp snooping interface vlan1.1
IGMP Snooping information for
vlan1.1 IGMP Snooping enabled
Snooping Querier none
IGMP Snooping other querier timeout is 255
seconds Group Membership interval is 260 seconds
IGMPv2 fast-leave is disabled IGMPv1/v2
Report suppression enabled IGMPv3
Report suppression enabled Router port
detection using IGMP Queries Number of
router-ports: 1
Number of Groups: 1
Number of v1-reports: 0
Number of v2-reports: 0
```

```
Number of v2-leaves: 0 Number of
v3-reports: 2
Active Ports:
eth0 eth1
eth2
```

IGMP Snooping Configuration

CHAPTER 6 Multicast Virtual Routing Configuration

This chapter contains Multicast Virtual Routing configuration examples.

Configuration Steps

The basic VR configuration can be divided into the following steps:

1. Log on as a Global Administrator
2. Create a VR and Assign a User
3. Bind an Interface to the VR
4. Configure the VR
5. Log in as VR Administrator
6. Save VR Configuration
7. Proceed to one of the following:
   - Enable PIM on a VR
   - Enable PIM-SMv6 on a VR

Log on as a Global Administrator

1. Launch the SWMRE daemons: (`nsm`, `ospfd`, `bgpd`, `imi`).
2. Start IMISH.
3. Use the `enable` command to enter Privileged Exec mode.

Create a VR and Assign a User

`#configure terminal`	Enter Configure mode.
`(config)#virtual-router VR1`	Enter the VR mode.
`(config-vr)#description VR1 for customer A`	Enter a description for the VR.
`(config-vr)#username user-A password abc12`	Add a user name for the VR.
`(config-vr)#configuration file VR-A.conf`	(Optional) Set the VR configuration file.
`(config-vr)#exit`	Exit VR mode.

Validation

```
#show virtual-router
Virtual Router vr1
 Description: vr1 for customer-A
```

```
Loaded Protocols:
VR-ID: 1
Router-ID: Unset  Interfaces:
```

Bind an Interface to the VR

`#configure terminal`	Enter Configure mode.
`(config)#interface eth0`	Specify the interface (`eth2`) to be configured and enter the Interface mode.
`(config-if)#virtual-router forwarding VR1`	Bind an interface to the VR, `VR1`.This command binds an interface, and informs all SWMRE clients about it.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to be configured and enter the Interface mode.
`(config-if)#virtual-router forwarding VR1`	Bind an interface to the VR, `VR1`.

Validation

Use the `show interface` command to validate the configuration.

Configure the VR

`#login virtual-router VR1`	From the Global Management Authority (GMA), enter the VR Management Authority (MA)
`#configure terminal`	Enter Configure mode.
`(config)#router ospf`	Enter router mode.
`(config-router)#neighbor 10.10.10.48`	Define the interface on which OSPF runs,
`(config-router)#network 172.16.1.0/24 area 5`	Associate the area ID (5) with the interface. Area ID 0 is the backbone.

Validation

Use the `how ip ospf` command to verify the OSPF configuration.

```
#show ip ospf
  Routing Process "ospf 1" with ID
  10.10.11.49 Process bound to VRF default
Process uptime is 0 minute
  ...
        SPF algorithm executed 0 times
        Number of LSA 0. Checksum Sum 0x000000
```

Log in as VR Administrator

Log in as a VR administrator using one of the following two methods:

- From the GMA, run the following command:
  ```
  login virtual-router VR1
  #
  ```
- From the UNIX shell, type the following: `imish -v VR1`
  ```
  #
  ```

Save VR Configuration

By default, GMA configuration statements are stored in the SWMRE configuration file in the `/usr/local/etc` directory.

By default, VR configuration statements are stored in the SWMRE configuration file in the `/usr/local/etc/<VRName>` directory. In this location, `<VR-Name>` is the name of the specific VR configured. A directory for each VR is created automatically whenever a new VR is initiated.

To store a configuration in a different file, enter the file name using the `configuration file` command, which creates a new file in the directory related to the VR. No other directory can be specified for storing configuration. `configuration file First.conf` where `First.conf` is the name of the file to store the configuration statements.

To display the current running configuration for each VR, execute the following command in the VR context:

```
show running-config
```

To save the running configuration to startup configuration, execute the following command in the VR context:

```
write file
```

or

```
write memory
```

The configuration is saved to the file specified using the `configuration file` command (`First.conf` in the example above) or in the default configuration file.

Enable PIM on a VR

The configuration that follows shows how PIM-SM can be configured on an IPv4 VR.

Topology

In this example:

- R3 is capable of Virtual Routing, and has two VRs:
- VR1 has interfaces Eth1 and Eth2
- VR2 has interfaces Eth3 and Eth4
- VR1 and VR2 are both configured to run PIM-SM
- VR1 and VR2 have different neighbors
- Eth4 of VR2 is the Rendezvous Point (RP).
- R1 is the multicast receiver • R2 is the source

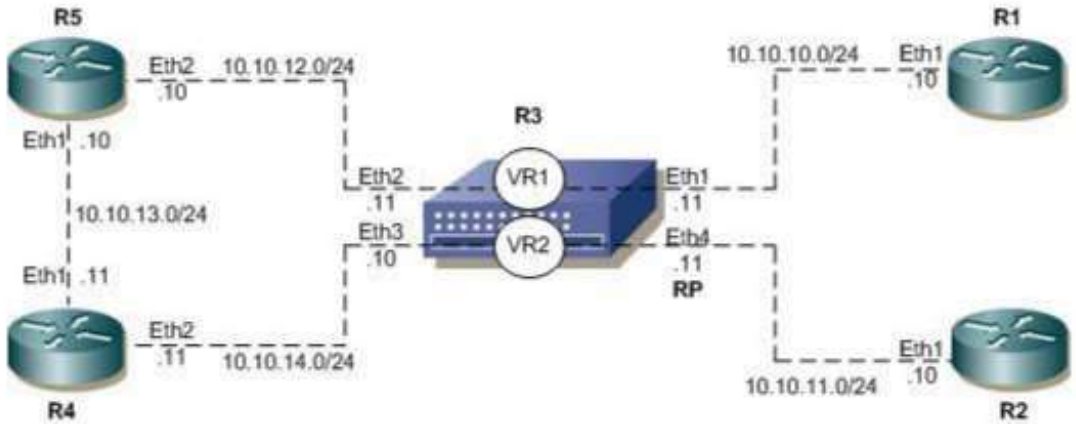


Figure 6-119: Configuration Topology

Create VR1 and VR2

`#configure terminal`	Enter Configure mode.
`(config)#virtual-router VR1`	Create a VR on R3, and specify the VR name `VR1`.
`(config-vr)#load pim`	Load the PIM-SM protocol module on this VR.
`(config-vr)#exit`	Exit the VR Management Authority (MA).
`(config)#virtual-router VR2`	Create a VR on R3, and specify the VR name `VR2`.
`(config-vr)#load pim`	Load the PIM-SM protocol module on this VR.
`(config-vr)#end`	Exit the virtual router mode.

Bind Interfaces to VR1 and VR2

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Enter the Interface mode for `eth1`.
`(config-if)#virtual-router forwarding VR1`	Bind interface `eth1` to `VR1`.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface eth2`	Enter the Interface mode for `eth2`.
`(config-if)#virtual-router forwarding VR1`	Bind interface `eth2` to `VR1`.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface eth3`	Enter the Interface mode for `eth3`.
`(config-if)#virtual-router forwarding VR2`	Bind interface `eth3` to `VR2`.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface eth4`	Enter the Interface mode for `eth4`.
`(config-if)#virtual-router forwarding VR2`	Bind interface `eth4` to `VR2`.
`(config-if)#end`	Exit the Interface mode and return to Configure mode.

Enable PIM-SM on VR1

`#login virtual-router VR1`	In Global Configuration mode, execute this command to jump to Configure mode for `VR1`.
`#configure terminal`	Enter Configure mode.
`(config)#ip multicast-routing`	Enable multicast routing.
`(config)#interface eth1`	Enter the Interface mode for `eth1`.
`(config-if)#ip address 10.10.10.11/24`	Configure the IP address for `eth1`.
`(config-if)#ip pim sparse-mode`	Enable PIM-SM on the interface.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface eth2`	Enter the Interface mode for `eth2`.
`(config-if)#ip address 10.10.12.11/24`	Configure the IP address for `eth2`.
`(config-if)#ip pim sparse-mode`	Enable PIM-SM on the interface.
`(config-if)#end`	Exit the Interface mode and return to Configure mode.

Enable PIM-SM on VR2

`#login virtual-router VR2`	In Global Configuration mode, run this command to jump to Configure mode on `VR2`.
`#configure terminal`	Enter Configure mode.
`(config)#ip multicast-routing`	Enable multicast routing.
`(config)#interface eth3`	Enter the Interface mode for `eth3`.
`(config-if)#ip address 10.10.14.10/24`	Configure the IP address for `eth3`.
`(config-if)#ip pim sparse-mode`	Enable PIM-SM on the interface.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface eth4`	Enter the Interface mode for `eth4`.
`(config-if)#ip address 10.10.11.11/24`	Configure the IP address for `eth4`.
`(config-if)#ip pim sparse-mode`	Enable PIM-SM on the interface.
`(config-if)#end`	Exit the Interface mode and return to Configure mode.

Configure RP on VR1

`#login virtual-router VR1`	From Global Configuration mode, run this command to jump to Configure mode on `VR1`.
`#configure terminal`	Enter Configure mode.
`(config)#ip pim rp-address 10.10.11.11`	Configure the RP address.
`(config)#end`	Exit the Configure mode.

Configure RP on VR2

`#login virtual-router VR2`	From Global Configuration mode, run this command to jump to Configure mode on `VR2`.

#configure terminal	Enter the Configure mode.
(config)#ip pim rp-address 10.10.11.11	Configure the RP address.
(config)#end	Exit the Configure mode.

Validation

Use the following commands to validate the configuration.

Display the global running configuration on the router:

```
#show running-config !
no service password-encryption ! no service dhcp hostname SWMRE !
ip domain-lookup ! virtual-router VR1  load ospf  load pim !
virtual-router VR2  load ospf  load pim !
mpls propagate-ttl !
spanning-tree mode provider-rstp !
vrrp vmac enable !
interface lo  ipv6 address::1/128 !
interface eth0  ip address 10.11.3.50/16 !
interface svlan0.1 !
interface eth1  virtual-router forwarding VR1 !
interface eth2  virtual-router forwarding VR1 !
interface lo1  virtual-router forwarding VR1 !
interface eth3  virtual-router forwarding VR2 !
interface eth4  virtual-router forwarding VR2 !
interface lo2  virtual-router forwarding VR2 ! line con 0  login line vty 0 4  login
! end
```

Display the running configuration at VR1:

```
#show running-config !
no service password-encryption !
no service dhcp hostname VR1 !
ip domain-lookup !
mpls propagate-ttl !
ip multicast-routing !
vrrp vmac enable !
ip pim rp-address 10.10.11.11 !
interface eth1  ip address 10.10.10.11/24  ip pim sparse-mode
!
interface eth2  ip address 10.10.12.11/24  ip pim sparse-mode !
interface lo1  ip address 127.0.0.1/8  ipv6 address ::1/128 !
router ospf 1  redistribute connected  network 10.10.10.0/24 area 0  network
10.10.12.0/24 area 0 ! line con 0  login line vty 0 4  login ! end
```

Display the running configuration at VR2:

```
#show running-config !
no service password-encryption !
no service dhcp hostname VR2 !
ip domain-lookup !
mpls propagate-ttl !
```

```
ip multicast-routing !
vrrp vmac enable !
ip pim rp-address 10.10.11.11 !
interface eth3 ip address 10.10.14.10/24 ip pim sparse-mode !
interface eth4 ip address 10.10.11.11/24 ip pim sparse-mode !
interface lo2 ip address 127.0.0.1/8 ipv6 address ::1/128 shutdown
! router ospf 1 redistribute connected
network 10.10.11.0/24 area 0 network
10.10.14.0/24 area 0 ! line con 0
login line vty 0 4 login ! end
```

Display PIM-SM interface information:

```
#show ip pim interface
Address          Interface  VIFindex Ver/   Nbr    DR    DR
                                     Mode   Count  Prior
10.10.10.11      eth1       0        v2/S   1      1     10.10.10.11
10.10.12.11      eth2       2        v2/S   1      1     10.10.12.11
```

Display PIM-SM RP information:

```
#show ip pim rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4, Static
    RP: 10.10.11.11
         Uptime: 00:04:57
```

Display PIM-SM neighbor information:

```
#show ip pim neighbor
Neighbor          Interface          Uptime/Expires    Ver   DR
Address                                                    Priority/Mode
10.10.10.10       eth1               00:17:33/00:01:30 v2    1  /
10.10.12.10       eth2               00:17:23/00:01:44 v2    1  /
```

Display the IP multicast routing table summary:

```
#show ip mroute

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(10.10.11.10, 224.0.1.3), uptime 00:00:07, stat expires
00:03:23 Owner PIM-SM, Flags: TF
  Incoming interface: eth2   Outgoing
interface list:     eth1 (1)
```

Display the IP multicast routing table details:

```
#show ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
```

```
(*,G) Entries: 1 (S,G) Entries:
0
(S,G,rpt) Entries: 0
FCR Entries: 1

(*, 224.0.1.3)
RP: 10.10.11.11
RPF nbr: 10.10.12.10
RPF idx: eth2
Upstream State: JOINED
 Local     i.............................
 Joined    .............................
 Asserted  .............................
FCR:
Source: 10.10.11.10
 Outgoing  o.............................
 KAT timer running, 196 seconds remaining
 Packet count 1
```

Display PIM-SM interface information:

```
#show ip pim interface
Address          Interface   VIFindex Ver/   Nbr    DR    DR
                                      Mode   Count  Prior
10.10.14.10      eth3        0        v2/S   1      1     10.10.14.11
10.10.11.11      eth4        2        v2/S   0      1     10.10.11.11
```

Display PIM-SM neighbor information:

```
#show ip pim neighbor
Neighbor          Interface          Uptime/Expires    Ver   DR
Address                                                    Priority/Mode
10.10.14.11       eth3               00:14:30/00:01:45 v2    1/DR
```

Display the IP multicast routing table:

```
#show ip mroute

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(10.10.11.10, 224.0.1.3), uptime 00:02:05, stat expires
00:02:06 Owner PIM-SM, Flags: TF
  Incoming  interface:  eth4       Outgoing
interface list:
    eth3 (1)
```

Display the IP multicast routing table details:

```
#show ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
```

```
(*,G) Entries: 1 (S,G) Entries: 1
(S,G,rpt) Entries: 1
FCR Entries: 0

(*, 224.0.1.3)
RP: 10.10.11.11
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
 Local     ..............................
 Joined    j..............................
 Asserted  ..............................
FCR:

(10.10.11.10, 224.0.1.3)
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: 1
Upstream State: JOINED
 Local     ..............................
 Joined    ..............................
 Asserted  ..............................
 Outgoing  o.............................

(10.10.11.10, 224.0.1.3, rpt)
RP: 10.10.11.11
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: NOT PRUNED
 Local     ..............................
 Pruned    ..............................
 Outgoing  o.............................
```

Enable PIM-SMv6 on a VR

This configuration shows how PIM-SMv6 (IPv6) can be configured on an IPv6 Virtual Router (VR).

Topology

In this example:

- R3 is capable of Virtual Routing and has two VRs:
- VR1 has interfaces eth1 and eth2
- VR2 has interfaces eth3 and eth4
- Both VR1 and VR2 run PIM-SMv6 •eth4 of VR2 is the Rendezvous Point (RP)
- VR1 and VR2 have different neighbors.
- R1 is the multicast receiver • R2 is the source

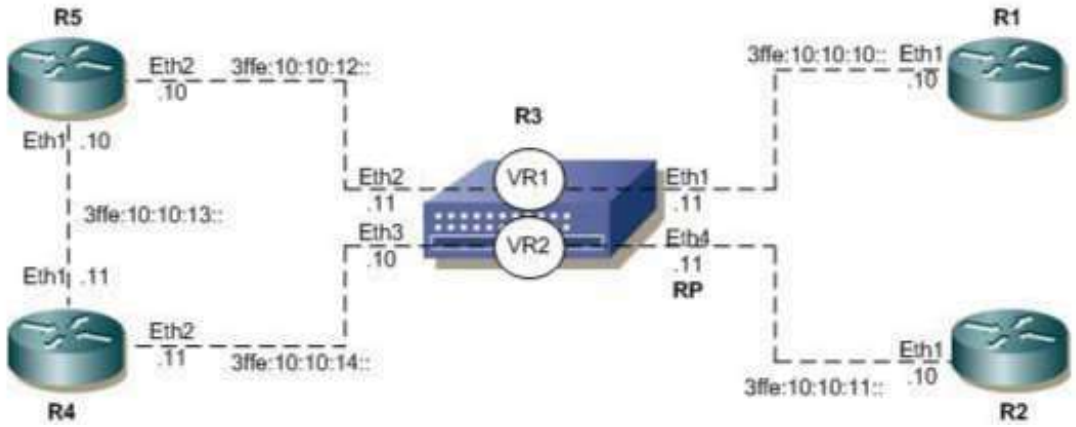


Figure 6-120: Configuration Topology

Create VR1 and VR2

`#configure terminal`	Enter Configure mode.
`(config)#virtual-router VR1`	Create a VR on R3, and specify the VR name (VR1).
`(config-vr)#load pim`	Load the PIM-SM protocol module on this VR.
`(config-vr)#exit`	Exit the Virtual Router Management Authority (MA).
`(config)#virtual-router VR2`	Create a VR on R3, and specify the VR name (VR2).
`(config-vr)#load pim`	Load the PIM-SM protocol module on this VR.
`(config-vr)#end`	Exit the virtual router mode.

Bind interfaces to VR1 and VR2

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to be configured.
`(config-if)#virtual-router forwarding VR1`	Bind interface `eth1` to `VR1`.
`(config-if)#exit`	Exit Interface mode.
`(config)#interface eth2`	Specify the interface (`eth2`) to be configured.
`(config-if)#virtual-router forwarding VR1`	Bind interface `eth2` to `VR1`.
`(config-if)#exit`	Exit Interface mode.
`(config)#interface eth3`	Specify the interface (`eth3`) to be configured.
`(config-if)#virtual-router forwarding VR2`	Bind interface `eth3` to `VR2`.
`(config-if)#exit`	Exit Interface mode.
`(config)#interface eth4`	Specify the interface (`eth4`) to be configured.
`(config-if)#virtual-router forwarding VR2`	Bind interface `eth4` to `VR2`.
`(config-if)#end`	Exit the Interface mode.

Enable PIM-SMv6 on VR1

`#login virtual-router VR1`	From Global Configuration mode, run this command to jump to Configure mode on `VR1`.
`#configure terminal`	Enter Configure mode.
`(config)#ipv6 multicast-routing`	Enable multicast routing.
`(config)#interface eth1`	Specify the interface (`eth1`) to be configured.
`(config-if)#ipv6 address 3ffe:10:10:10::11/64`	Configure the IPv6 address for the interface (`eth1`).
`(config-if)#ipv6 address fe80::70/64`	Configure the link local address for the interface (`eth1`).
`(config-if)#ipv6 pim sparse-mode`	Enable PIM-SMv6 on the interface.
`(config-if)#exit`	Exit Interface mode.
`(config)#interface eth2`	Specify the interface (`eth2`) to be configured.
`(config-if)#ipv6 address 3ffe:10:10:12::11/64`	Configure the IPv6 address for the interface (`eth2`).
`(config-if)#ipv6 address fe80::50/64`	Configure the link local address for the interface (`eth2`).
`(config-if)#ipv6 pim sparse-mode`	Enable PIM-SMv6 on the interface.
`(config-if)#end`	Exit the Interface mode.

Enable PIM-SMv6 on VR2

`#login virtual-router VR2`	From Global Configuration mode, run this command to jump to Configure mode on `VR2`.
`#configure terminal`	Enter Configure mode.
`(config)#ipv6 multicast-routing`	Enable multicast routing.
`(config)#interface eth3`	Specify the interface (`eth3`) to be configured.
`(config-if)#ipv6 address 3ffe:10:10:14::10/64`	Configure the IPv6 address for the interface (`eth3`).
`(config-if)#ipv6 address fe80::20/64`	Configure the link local address for the interface (`eth3`).
`(config-if)#ipv6 pim sparse-mode`	Enable PIM-SMv6 on the interface.
`(config-if)#exit`	Exit Interface mode.
`(config)#interface eth4`	Specify the interface (`eth4`) to be configured.
`(config-if)#ipv6 address 3ffe:10:10:11::11/64`	Configure the IPv6 address for the interface (`eth4`).
`(config-if)#ipv6 address fe80::30/64`	Configure the link local address for the interface (`eth4`).
`(config-if)#ipv6 pim sparse-mode`	Enable PIM-SMv6 on the interface.
`(config-if)#end`	Exit the Interface mode.

Configure RP on VR1

`#login virtual-router VR1`	From Global Configuration mode, run this command to jump to Configure mode on `VR1`.
`#configure terminal`	Enter Configure mode.
`(config)#ipv6 pim rp-address 3ffe:10:10:11::11`	Configure the RP address.

(config)#end	Exit the Configure mode.

Configure RP on VR2

#login virtual-router VR2	From Global Configuration mode, run this command to jump to Configure mode on VR2.
#configure terminal	Enter Configure mode.
(config)#ipv6 pim rp-address 3ffe:10:10:11::11	Configure the RP address.
(config)#end	Exit the Configure mode.

Verify Configurations

Use the following validation commands to verify the configurations.

Display the global running configuration at the router:

```
#show running-config
```

Display the running configuration at VR1:

```
#show running-config
```

Display the running configuration at VR2:

```
#show running-config
```

Display PIM-SMv6 interface information:

```
#show ipv6 pim interface
```

Display PIM-SM RP information:

```
#show ipv6 pim rp mapping
```

Display PIM-SMv6 neighbor information:

```
#show ipv6 pim neighbor
```

Display the IPv6 multicast routing table summary:

#show ipv6 mroute

Display the IPv6 multicast routing table details:

```
#show ipv6 pim mroute
```

Display PIM-SMv6 interface information:

```
#show ipv6 pim interface
```

Display PIM-SMv6 neighbor information:

```
#show ipv6 pim neighbor
```

Display the IPv6 multicast routing table:

#show ipv6 mroute

Display the IPv6 multicast routing table details:

```
#show ipv6 pim mroute
```

CHAPTER 7 PIM-ECMP Redirect Configuration

A Protocol Independent Multicast (PIM) router uses Reverse Path Forwarding (RPF) procedure to select an upstream interface and router in order to build forwarding state. When there are equal-cost multipaths (ECMPs), existing implementations often use hash algorithms to select a path. Such algorithms do not allow the spread of traffic among the ECMPs according to administrative metrics. This usually leads to inefficient or ineffective use of network resources. PIM ECMP Redirect (RFC 6754) provides a mechanism to improve the RPF procedure over ECMPs. It allows ECMP selection to be based on administratively selected metrics, such as data transmission delays, path preferences, and routing metric. An interface identifier option is used in PIM hello messages as a tiebreaker during ECMP path selection.

Note: PIM ECMP Redirect is not supported for Bidirectional PIM, PIM-DM and PIM-SMDM.

Note: PIM-ECMP feature is not supported for SWMRE

Terminology

Following is a brief description of terms and concepts used to describe the PIM-ECMP Redirect protocol:

Equal Cost Multipath (ECMP)

ECMP refers to parallel, single-hop, equal-cost links between adjacent nodes.

ECMP Bundle

An ECMP bundle is a set of PIM-enabled interfaces on a router, where all interfaces belonging to the same bundle share the same routing metric. The next hops for the ECMP are all one hop away. There can be one or more ECMP bundles on any router, while one individual interface can only belong to a single bundle. ECMP bundles are created on a router via configuration.

Reverse Path Forwarding

Reverse Path Forwarding (RPF) is an optimized form of flooding, in which the router accepts a packet from `SourceA` through Interface `IF1`, only if `IF1` is the interface the router uses to reach `SourceA`. To determine if the interface is correct, it consults its unicast routing tables. The packet that arrives through interface `IF1` is forwarded because the routing table lists this interface as the shortest path. The router's unicast routing table determines the shortest path for the multicast packets. Because a router accepts a packet from only one neighbor, it floods the packet only once, meaning that (assuming point-to-point links) each packet is transmitted over each link, once in each direction.

Upstream

Towards the root of the multicast forwarding tree. An upstream router refers to a router that is forwarding, or potentially capable of forwarding, data packets onto interfaces in an ECMP bundle. When there are multiple routers forwarding packets onto interfaces in the ECMP bundle, all these routers are called upstream routers.

Downstream

Away from the root of the multicast forwarding tree. A downstream router is a router that uses an interface in the ECMP bundle as an RPF interface for a multicast forwarding entry

When a PIM router downstream of the ECMP interfaces creates a new (*,G) or (S,G) entry, it will populate the RPF interface and RPF neighbor information according to the rules specified by [RFC4601]. This router will send its initial PIM Joins to that RPF neighbor. When the RPF neighbor router receives the Join message and finds that the

receiving interface is one of the ECMP interfaces, it will check if the same flow is already being forwarded out of another ECMP interface. If so, this RPF neighbor router will send a PIM ECMPRedirect message onto the interface the Join was received on. The PIM ECMP Redirect message contains the address of the desired RPF neighbor, an Interface ID [RFC6395], and the other parameters used as tiebreakers. In essence, a PIM ECMP Redirect message is sent by an upstream router to notify downstream routers to redirect PIM Joins to the new RPF neighbor via a different interface. When the downstream routers receive this message, they SHOULD trigger PIM Joins toward the new RPF neighbor specified in the packet.

This PIM ECMP Redirect message has similar functions as the existing PIM Assert message:

- It is sent by an upstream router.
- It is used to influence the RPF selection by downstream routers.
- A tiebreaker metric is used

However, the existing Assert message is used to select an upstream router within the same multi-access network (such as a LAN), while the Redirect message is used to select both a network and an upstream router.

Sending ECMP Redirect

ECMP Redirects are sent by an upstream router under either of the following conditions:

- It detects a PIM Join on a non-desired outgoing interface.
- It detects multicast traffic on a non-desired outgoing interface.

In both cases, an ECMP Redirect is sent to the non-desired interface. An outgoing interface is considered non-desired when:

- The upstream router is already forwarding the same flow out of another interface belonging to the same ECMP bundle.
- The upstream router is not yet forwarding the flow out any interfaces of the ECMP bundle, but there is another interface with more desired attributes.

Receiving ECMP Redirect

When a downstream router receives an ECMP Redirect, and detects that the desired RPF path from its upstream router's point of view is different from its current one, it should choose to join the newly suggested path and prune from the current path.

If a downstream router receives multiple ECMP Redirects sent by different upstream routers, it SHOULD use the Preference, Metric, or other fields as specified below as the tiebreakers to choose the most preferred RPF interface and neighbor. The tie-break procedure is the same as that used in PIM Assert processing described by [RFC4601].

If an upstream router receives an ECMP Redirect, it SHOULD NOT change its forwarding behavior even if the ECMP Redirect makes it a less preferred RPF neighbor on the receiving interface.

PIM-ECMP Configuration

This section provides the configuration steps for configuring PIM ECMP Redirect and examples for a relevant scenario.

Note:Configure PIM SM on the routers. For steps to configure PIM-SM refer to Chapter 3, *PIM Sparse Mode Configuration*

Topology

In this network topology, the source address is 172.31.1.52 and the group address is set to 224.0.1.3.

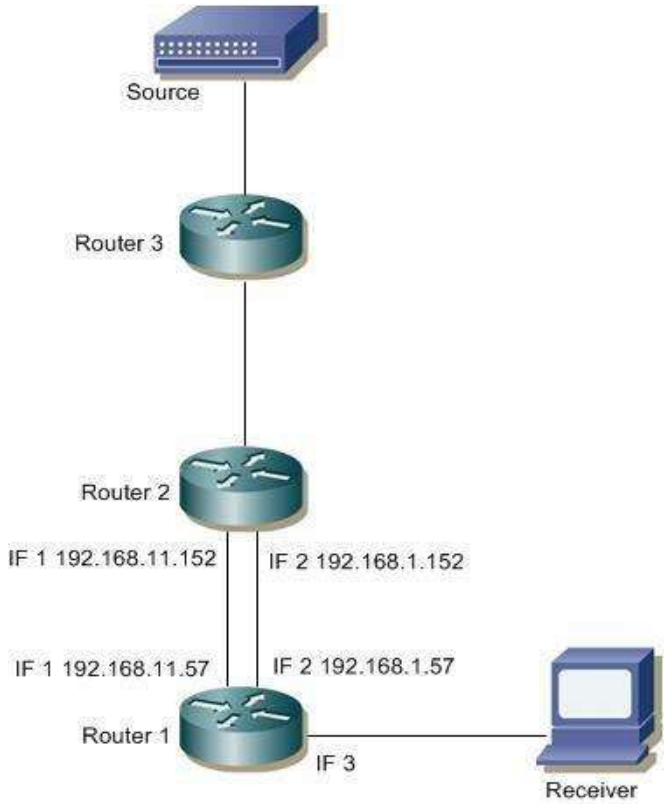


Figure 7-121: PIM ECMP Redirect Topology

Configure PIM Router-ID

Configure PIM router-id on all of the PIM routers inside the PIM domain:

`# configure terminal`	Enter Configure mode.
`(config)# ip pim router-id 1.1.1.1`	Configure PIM router-id
`(config)#exit`	Exit Configure mode.

Validation

```
#show running-config !
ip multicast-routing ! ip pim router-id 1.1.1.1
```

Configure PIM ECMP Bundle

Configure PIM ECMP Bundle on all of the PIM routers inside the PIM domain:

# configure terminal	Enter Configure mode.
(config)# ip pim ecmp-bundle <bundle-name>	Configure PIM ECMP Bundle
(config)#exit	Exit Configure mode.

Validation

```
#show running-config !
ip multicast-routing !
```

Bind PIM ECMP Bundle

Bind an ECMP Bundle to an interface on the PIM routers inside the PIM domain:

# configure terminal	Enter Configure mode.
(config)# interface eth1	Enter Interface mode
(config-if)# ip pim bind ecmp-bundle ecmpbundle	Bind PIM ECMP Bundle to an interface
(config-if)#exit	Exit Interface mode.

Validation

Validation 1

Enter the commands listed in this section to confirm the previous configurations. `router_1#show running-config interface eth2 interface eth2 ip address 192.168.1.57/24 no shutdown ip ospf cost 10`
`ip pim bind ecmp-bundle ecmpbundle ip pim sparse-mode`
`lldp-agent no dcbx enable exit`

Validation 2

The following output displays the bundle information: `router_1#show ip pim ecmp-bundle Name : ecmpbundle1 Interface : <ECMP REDIRECT status> eth2 : allowed eth3 : allowed`

```
router_1#show ip pim ecmp-bundle ecmpbundle1
Name       : ecmpbundle1
Interface   : <ECMP REDIRECT status>
eth2 : allowed       eth3 : allowed
exit
```

Validation 3

The following output displays the interface details:

```
router_1#show ip pim interface detail
eth1 (vif 0):
  Address 192.168.10.57, Mode: Sparse
  DR 192.168.10.57, DR's priority: 1
  Hello period 30 seconds, Next Hello in 22 seconds
```

```
    Triggered Hello period 5 seconds
    PIM GenID sent in Hellos: 56e71c93
    Propagation delay is 1000 milli-seconds
  Interface ID: Router-ID:1.1.1.1 Local-ID 3
    Neighbors:
     192.168.10.52
    PIM neighbor count: 1
    PIM neighbor holdtime: 105
    PIM configured DR priority: 1
    PIM border interface: no
    PIM Neighbor policy: not configured

    eth2 (vif 2):
    Address 192.168.1.57, Mode: Sparse
    DR 192.168.1.152, DR's priority: 1
    Hello period 30 seconds, Next Hello in 23 seconds
    Triggered Hello period 5 seconds
    PIM GenID sent in Hellos: 5f2ebb37
    Propagation delay is 1000 milli-seconds
    Interface ID: Router-ID:1.1.1.1 Local-ID 4
    ECMP REDIRECT, bundle : ecmpbundle1, status :  allowed
    Neighbors:
     192.168.1.149
     192.168.1.150
     192.168.1.152
    PIM neighbor count: 3
    PIM neighbor holdtime: 105
    PIM configured DR priority: 1
    PIM border interface: no
    PIM Neighbor policy: not configured
```

IP Multicast Routing Table for ECMP Redirect

Note: The multicast routing table displays for an RP router are different from other routers.

Validation 1:

Initially router_1 sends the (*, G) to Router_2 IF-2, as Router_2 IF-2 is RIB indicated RPF neighbor.The RIB indicated RPF neighbor can be checked using command `show ip rpf`

```
router_1#show ip rpf 172.31.5.153
RPF information for 172.31.5.153
  RPF interface: eth3
  RPF neighbor: 192.168.11.152
  RPF route: 172.31.5.0/24
  RPF type: unicast (ospf)
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
  Distance:        110
Metric: 30
```

Validation 2:

The `show ip pim mroute` command displays the IP multicast routing table. In this table, the following fields are defined:

`RPF nbr`	Displays the unicast next-hop to reach RP. and mask length.
`RPF idx`	Displays the incoming interface for this (*, G) state.
`RP`	Displays the IP address for the RP router
`B`	Displays the bidirectional pim mode
`The leading dots....`	Stand for VIF index

Router-2 upon receiving (*, G) on IF-2, which is rib indicated RPF, sends an ECMP redirect message to Router-1 IF-2 to intimate that, subsequent joins should be sent to IF-1 being the desired path with a (*,G). Since, Router-2 IF-1 already has a (*, G), the `show ip pim mroute` command output suggests 192.168.1.152 as the RPF neighbor, which is ECMP redirected RPF neighbor.

```
router_1#show ip pim mroute IP
Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1 (S,G)
Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0

(*, 224.1.1.1)
RP: 172.31.5.153
RPF nbr: 192.168.1.152
RPF idx: eth2
Upstream State: JOINED
 Local     i.............................
 Joined    .............................
 Asserted  .............................
FCR:
0
```

The below output displays (*,G) at router_2 IF-1 using the command `show ip pim mroute detail`:

```
router_2#show ip pim mroute detail IP
Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0

(*, 224.1.1.1) Uptime: 00:30:45
RP: 172.31.5.153, RPF nbr: 172.31.12.153, RPF idx: eth1
  Upstream:
   State: JOINED, SPT Switch: Disabled, JT Expiry: 15 secs Macro state: Join
Desired,
  Downstream:    eth1:
```

```
     State: JOINED, ET Expiry: 176 secs, PPT: off
     Assert State: NO INFO, AT: off
      Winner:  0.0.0.0,  Metric:  4294967295,  Pref:  4294967295,  RPT  bit:  on  Macro
state: Could Assert, Assert Track
  Local Olist:
   eth1   Join Olist:
   eth1
```

CHAPTER 8 MSDP Configuration

Multicast Source Discovery Protocol (MSDP) is used to exchange multicast source information between BGP-enabled PIM-SM domains. Using MSDP, routers in a PIM-SM domain can rely on their own RP to reach a source in a different PIM-SM domain.

Overview

MSDP routers in a PIM-SM domain have a MSDP peering relationship with MSDP peers in another domain using a TCP connection. MSDP peering is the first step towards exchanging inter-domain multicast source information using MSDP SA (Source-Active) messages.

When an RP in a PIM-SM domain first learns of a new sender (via PIM register messages), it constructs an SA message and sends it to its MSDP peers.

All RPs which intend to originate or receive SA messages must establish MSDP peering with other RPs, either directly or via an intermediate MSDP peer. An SA message contains these fields:

- Source address of the data source
- Group address the data source sends to
- IP address of the RP

Each SA message received from a MSDP peer goes through an RPF check. The peer-RPF check compares the RP address carried in the SA message with the MSDP peer from which the message was received:

- If the MSDP peer receives an SA from a non-RPF peer towards the originating RP, it drops the message.
- Otherwise, it forwards the message to all its MSDP peers (except the one from which it received the SA message).

When an RP receives a new SA message from a peer in another domain, it checks if there are any receivers interested in the traffic. An RP checks for a (*, G) entry with a non-empty outgoing list. If the outgoing list is non-empty, the RP sends a (S,G) join towards the source.

Caching SA state

If a member joins a group soon after a SA message is received by the local RP, that member needs to wait until the next SA message to learn about the source. MSDP SA caching is done at MSDP peers to reduce join latency for new receivers. The SA cache is populated as soon an MSDP peer receives a SA message from its peer.

MSDP Mesh Group

MSDP Mesh groups are used inside a PIM-SM domain to ease RPF checking and SA forwarding within the domain. Any SA messages received from a peer in a mesh group are not forwarded to other peers in the same mesh group. This reduces SA message flooding and simplifies peer-RPF flooding.

MSDP Default Peer

An MSDP default peer is used when MSDP peers are not BGP peers. SA messages coming from a default peer do not go through an RPF check and are always accepted.

Configure PIM-SM

For the MSDP topology in Figure 8-122, you must enable PIM-SM on all the routers in both PIM domains and make RTR-1 a rendezvous point (RP) in Domain-1 and RTR-2 an RP in Domain-2. For the steps to configure PIM-SM and RPs, see Chapter 3, *PIM Sparse Mode Configuration*.

Configure MSDP

In the topology in Figure 8-122, an MSDP session is established between RTR-1 and RTR-2 in both domains. The following sample configuration on RTR-1 shows how to enable MSDP peering between RTR-1 and RTR-2.

Topology

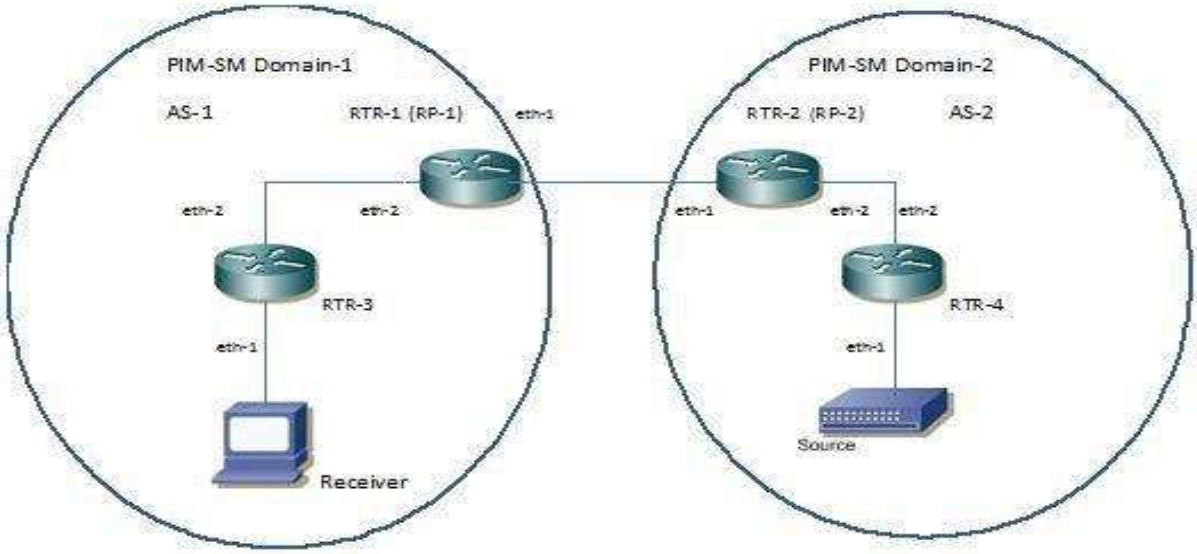


Figure 8-122: MSDP topology

IP addresses:

RTR-1 eth1: 11.1.1.11

RTR-1 eth2: 10.1.1.11 RTR-

2 eth1: 11.1.1.12

RTR-2 eth2: 12.1.1.12

RTR-4 eth1: 12.1.1.14

RTR-4 eth2: 20.1.1.14

RTR-3 eth1: 13.1.1.13

RTR-3 eth2: 10.1.1.13

Source: 20.1.1.10

Multicast group: 224.1.1.1

RTR-1

`#configure terminal`	Enter configure mode.

`(config)#ip msdp peer 11.1.1.12`
--or--
`(config)#ip msdp peer 11.1.1.12 connect source eth1`
	Configure a MSDP peer.
	
	Use the connect-source option to specify the primary IP address of the interface to use as the source IP address of the MSDP TCP connection.

`(config)#ip msdp password myPass peer 11.1.1.12`	Configure an MSDP password for the peer. You must specify the same command at RTR-2. The password must match at both the routers.
`(config)#ip msdp default-peer 11.1.1.12`	Configure MSDP default peer.
`(config)#ip msdp mesh-group mesh1 11.1.1.12`	Configure MSDP mesh group.
`(config)#ip msdp originator-id eth2`	Configure MSDP originator identifier.
`(config)#exit`	Exit configure mode.

Validation

RTR-1 `#show running-config`

```
ip msdp peer 11.1.1.12 ip msdp default-peer 11.1.1.12 ip msdp mesh-group mesh1
11.1.1.12 ip msdp password myPass peer 11.1.1.12 ip msdp originator-id eth2 ip
multicast-routing ! ip pim register-rp-reachability ip pim bsr-candidate eth2 ip
pim rp-candidate eth2 ip pim vrf management register-rp-reachability !
interface lo  ip address 127.0.0.1/8  ipv6 address ::1/128  no
shutdown ! interface eth0  ip address 10.12.48.175/24  no shutdown !
interface eth1  ip
address 11.1.1.11/24 no
shutdown  ip pim sparse-
mode ip pim bsr-border !
interface eth2  ip
address 10.1.1.11/24  no
shutdown ip pim sparse-
mode ! interface eth3
no shutdown ! interface
pimreg  no multicast  no
shutdown ! router ospf
100
 network 10.1.1.0/24 area 0.0.0.0
cspf disable-better-protection !
router bgp 1
```

```
neighbor 11.1.1.12 remote-as 2
! line con 0 login line vty 0
39 login !
```

This command shows the MSDP peer information at RTR-1:

```
#show ip msdp peer
MSDP Peer 11.1.1.12
 Connection status
  State: Up (Established)
  Keepalive sent: 1
  Keepalive received: 1
  Number of connect retries: 0
```

In the MSDP topology in Figure 8-122, when a source sends multicast traffic for group 224.1.1.1, RTR-4 (the DR) sends a register packet towards RTR-2 which is the RP in the domain. RTR-2 receives the register packet and sends an MSDP SA message to its MSDP peer (RTR-1). RTR-1 receives the SA message and creates an entry in the SA cache containing the source, group, and RP information.

This command at RTR-1 shows the SA information with source address, group address, and RP address:

```
#show ip msdp sa-cache MSDP
Source-Active Cache:
(20.1.1.11, 224.1.1.1), RP 10.1.1.11, RPF-Peer 11.1.1.12 Uptime  00:00:02 Exptime
00:03:28P
```

RTR-3 receives an IGMP join for group 224.1.1.1 and joins the shared tree path toward the RP (RTR-1). When RTR-1 receives an SA message from RTR-2, because it has a receiver, it sends an (S,G) join towards the source. Now traffic from the source is received at RTR-1 via the shortest path tree formed between RTR-1 and the source. RTR-1 distributes traffic downstream towards the receiver.

This command shows the PIM state at RTR-1 upon receiving an SA message and joining towards the source:

```
#show ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G)  Entries:  1  (S,G)
Entries: 1
(S,G,rpt) Entries: 1
FCR Entries: 0

(*, 224.1.1.1)
RP: 10.1.1.11
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
 Local     ..i.............................
 Joined    ................................
 Asserted  ................................ FCR:

(20.1.1.10, 224.1.1.1)
RPF nbr: 11.1.1.12
RPF idx: eth1
SPT bit: 0
```

```
Upstream State: JOINED
 Local     ..............................
 Joined    ..............................
 Asserted  ..............................
 Outgoing  ..o...........................

(20.1.1.10, 224.0.1.3, rpt)
RP: 10.1.1.11
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: NOT PRUNED
 Local     ..............................
 Pruned    ..............................
 Outgoing  ..o...........................
```

RTR-2

This command shows the MSDP peer information at RTR-2.

```
#show  ip msdp  peer
MSDP Peer 11.1.1.11
Connection status
 State: Up (Established)
 Keepalive sent: 2
 Keepalive received: 2
```

CHAPTER 9 PIM Sparse-Dense Mode Configuration

PIM-SMDM is an integrated protocol which handles both sparse groups and dense groups at the same time. In sparsedense mode, if the group is in dense mode, the interface will be treated as dense mode. If the group is in sparse mode, the interface will be treated in sparse mode. The group is sparse if the router knows about an RP for that group.

Note: PIM-SMDM is not supported for SWMRE releases.

Configuration Steps

The required steps to configure PIM-SMDM are the following:

- Enable IP multicast on each PIM router (see Enabling IP Multicast Routing)
- Enable PIM-SMDM on the desired interfaces (see Enabling PIM-SMDM)
- Example for the group operating in sparse-mode having Static RP (see Configuring Rendezvous Point Statically for PIM-SMDM
- Example for the group operating in dense-mode having no RP

All multicast group states are dynamically maintained as the result of IGMP Report/Leave and PIM Join/Prune messages.

This section provides the steps to configure the PIM-SMDM feature. Configuration steps and examples are used for two relevant scenarios. The following figure displays the network topology used in these examples:

Enabling IP Multicast Routing

Enable IP multicast routing on all of the PIM routers inside the PIM domain:

`#configure terminal`	Enter Configure mode.
`(config)#ip multicast-routing`	Enable IP multicast routing.
`(config)#exit`	Exit Configure mode.

Enabling PIM-SMDM

Enable PIM-SMDM on all participating interfaces within each of routers inside the PIM domain on which you want to run PIM. In the following sample configuration, both eth1 and eth2 are enabled for PIM-SMDM on the router.

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to be configured and enter the Interface mode.
`(config-if)#ip pim sparse-dense-mode`	Enable PIM sparse-dense mode on the interface.
`(config-if)#exit`	Exit Interface mode.

(config)#interface eth2	Specify the interface (eth2) to be configured and enter the Interface mode.
(config-if)# ip pim sparse-dense-	Enable PIM sparse -dense mode on the interface.
mode (config-if)#exit	Exit Interface mode.

Validation

Here is the sample configuration for Router_C:

```
hostname  Router_C
!
interface eth0 !
interface eth1  ip pim
sparse-dense-mode !
interface eth2  ip pim
sparse-dense-mode !
interface lo ! ! ip
multicast-routing
```

The show ip pim interface command displays the interface details for Router_C.

```
Router_C#show ip pim interface

Address             Interface           VIFindex Ver/  Nbr
                                                Mode  Count
192.168.1.10         eth1                0      v2/SD 0 172.16.1.10
eth2                 2      v2/SD   1
```

Sparse Mode Operation versus Dense Mode Operation

The following examples differentiates the group operating in sparse mode versus dense mode:

- Sparse mode operation when the RP is present for the group
- Dense mode operation when there is no RP for the group

Sparse Mode Operation

Configuring Rendezvous Point Statically for PIM-SMDM

Every PIM multicast group needs to be associated with the IP address of a Rendezvous Point (RP), which is a router that resides in a multicast network domain. The address of the RP is used as the root of a group-specific distribution tree. All nodes in the domain that want to receive traffic sent to the group are aware of the address of the RP. For all senders to reach all receivers within a group, all routers in the domain must be able to map to the RP address configured for the group. There can be several RPs configured in a network deploying PIM-SM, each serving a different group.

You can statically configure a RP by specifying the RP address in every router in the PIM domain. The use of statically configured RPs is ideal for small network environments or ones that do not require many RPs and/or require changing the assignment of the RPs often. Changing the assignment of an RP requires the re-configuration of the RP address in all of the routers in the PIM domain.

In static RP configurations, RP failover is not available.

When configuring the RP statically, do the following:

- On every router, include the `ip pim rp-address A.B.C.D` statement even if a router does not have any source or group member attached to it
- Assign only one RP address for a multicast group in the PIM domain

Using the topology depicted in Figure 9-123, `Router_C` is the RP, and all routers are statically configured with RP information. Host_1 and Host_2 join group 224.0.1.3 for all the sources. They send the IGMP membership report to Subnet 1. Two routers are attached to Subnet 1, `Router_E` and `Router_F`; both have default DR priority on `eth1`. Since `Router_E` has a higher IP address on interface `eth1`, it becomes the Designated Router, and is responsible for sending Join messages to the RP (`Router_C`).

Topology

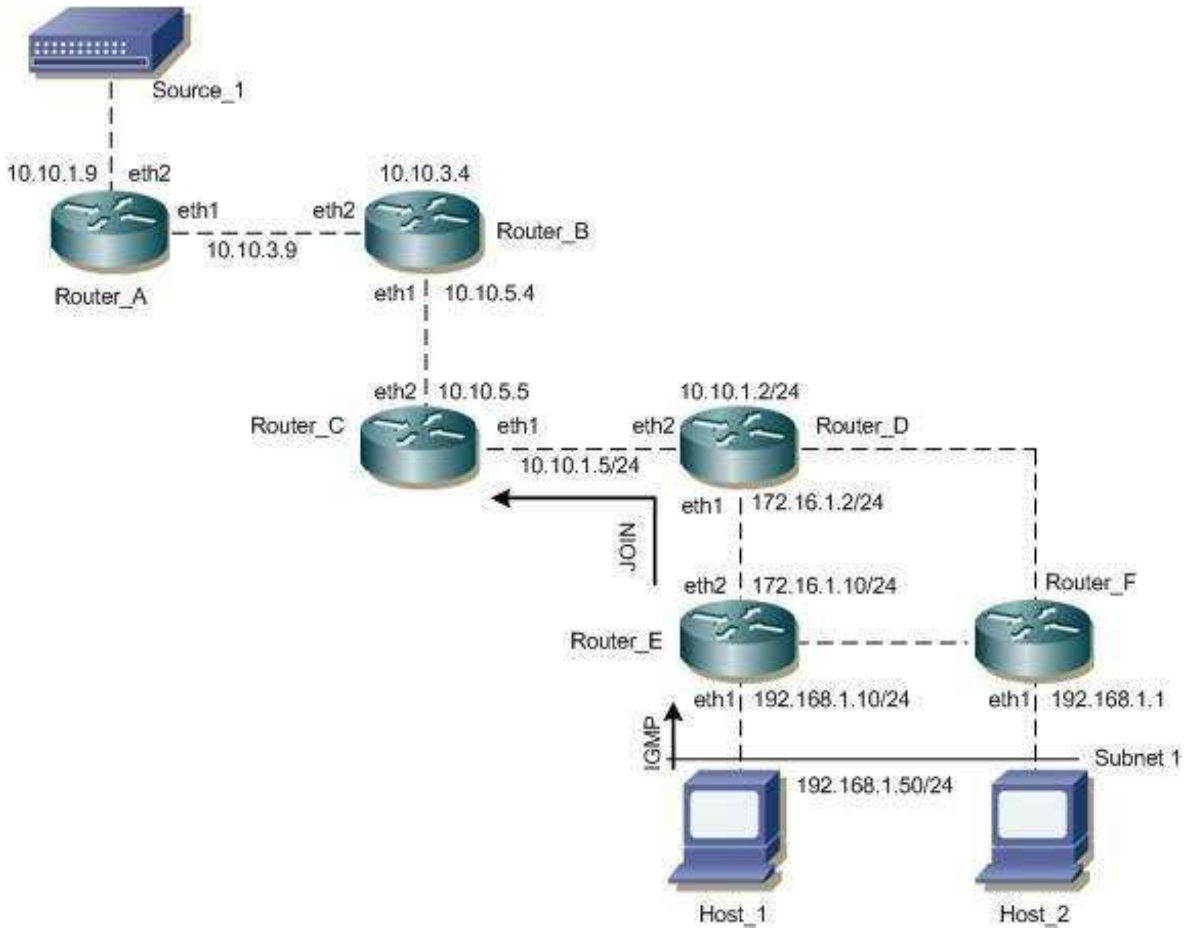


Figure 9-123: PIM-SMDM Configuration Topology (a)

Configure Static RP

`#configure terminal`	Enter Configure mode.
`(config)#ip pim rp-address 10.10.1.5`	Statically configure an RP address for multicast groups.
`(config)#exit`	Exit Configure mode.

Validation

Here is the sample configuration for `Router_D`:

```
hostname  Router_D
!
interface eth0 !
interface eth1  ip pim
sparse-dense-mode !
interface eth2  ip pim
sparse-dense-mode !
interface
lo ! !
ip multicast-routing ip
pim rp-address 10.10.1.5 !
```

RP Details

At Router_D, the `show ip pim rp mapping` command shows that `10.10.1.5` is the RP for all multicast groups `224.0.0.0/4`, and is statically configured. All other routers will have a similar output:

```
Router_D#sh ip pim rp mapping
PIM Group-to-RP Mappings
Override RP cnt: 0
Group(s): 224.0.0.0/4, Static
    RP: 10.10.1.5
         Uptime: 00:01:45
```

At Router_D, use the `show ip pim rp-hash` command to display the selected RP for a specified group (224.0.1.3):

```
Router_D#show  ip  pim  rp-hash  224.0.1.3
RP: 10.10.5.37
```

Interface Details

The `show ip pim interface` command displays the interface details for `Router_E`, and shows that `Router_E` is the Designated Router on `Subnet 1.`

```
Router_E#show ip pim interface
Address          Interface VIFindex Ver/    Nbr       DR    DR
                                    Mode    Count    Prior
192.168.1.10      eth1       0      v2/SD    1          1    192.168.1.10
172.16.1.10       eth2       2      v2/SD    1          1    172.16.1.10
```

IP Multicast Routing Table

Note:The multicast routing table displays for an RP router are different from other routers.

The `show ip pim mroute` command displays the IP multicast routing table. In this table, the following fields are defined:

`RPF nbr` Displays the unicast next-hop to reach RP.

and mask length.

`RPF idx` Displays the incoming interface for this (*, G) state.

`RP` Displays the IP address for the RP router

`B` Displays the bidirectional pim mode

`The leading dots ....`

Stand for VIF index

```
Router_E#show ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G)    Entries:    1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
(*, 224.0.1.3)
RP: 10.10.1.5
RPF nbr: 172.16.1.2
RPF idx: eth2
Upstream State: JOINED
 Local     ..............................
 Joined    j.............................
 Asserted  ..............................
 Outgoing  o.............................
```

At `Router_E`, `eth2` is the incoming interface of the (*, G) entry, and `eth1` is on the outgoing interface list of the (*, G) entry. This means that there is a group member through `eth1`, and the RP is reachable through `eth2`.

The 0 position on this 32-bit index is for `eth1` (as illustrated in the interface display above). The `j` on the 0 index indicates that the `Join` has come from `eth1`.

Since `Router_C` is the RP, and the root of this multicast tree, the `show ip pim mroute` command on `Router_C` shows `RPF nbr` as 0.0.0.0 and `RPF idx` as none.

```
Router_C#show ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G)    Entries:    1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
(*, 224.0.1.3)
RP: 10.10.1.5
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
 Local     ..............................
 Joined    j.............................
 Asserted  ..............................
 Outgoing  o.............................
```

For configuring Rendezvous point dynamically refer Configure Rendezvous Point Dynamically Using Bootstrap Router Method and Configuring Rendezvous Point Statically

Dense-mode Operation

Topology

In this network topology, the Source_1 address is 10.10.1.52 and the group address is set to 224.0.1.3.

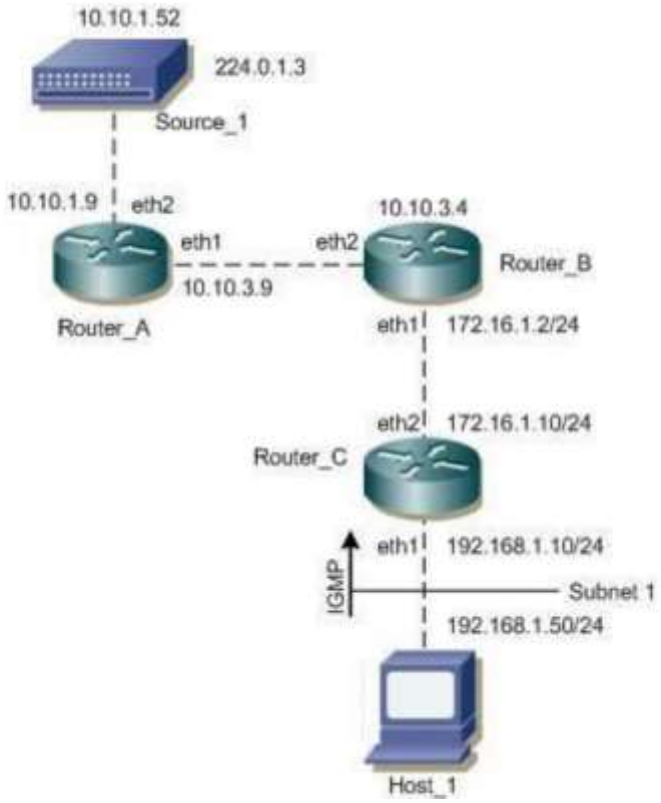


Figure 9-124: PIM-SMDM Configuration Topology (b)

In this network topology, the Source_1 address is 10.10.1.52 and the group address is set to 224.0.1.3

In this example all routers are running PIM-SMDM

1. Host_1 sends an IGMP membership report to Subnet 1
2. After Router_C receives this report, it associates its receiving interface, eth1, with the group reported in the IGMP message, for example, group1.
3. Source_1 then sends a data packet for group1.
4. Every router creates an (S,G) entry in the multicast routing table.
5. When the data packet reaches Router_C, it forwards via the interface, eth1, because there is a local member on this interface for this group. Router_C has a downstream receiver, so it does not send a prune message to its upstream neighbor router, Router_E.

Validation

Enter the commands listed in this section to confirm the previous configurations.

IP Multicast Routing Table

The `show ip pim mroute` command displays the IP multicast routing table.

```
Router_C#show ip mroute
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry Interface State:
```

```
Interface (TTL) (10.10.1.52, 224.0.1.3), uptime 00:00:15
Owner PIM-DM, Flags: F
Incoming interface: eth2 Outgoing
interface list: eth1 (1)
```

IP PIM-SMDM Multicast Routing Table

The `show ip pim dense-mode mroute` command displays the IP PIM-DM multicast routing table

```
Router_C#show ip pim mroute
PIM-DM Multicast Routing Table (10.10.1.52, 224.0.1.3)
RPF Neighbor: 172.16.1.2, Nexthop: 172.16.1.2, eth2
Upstream IF: eth2
Upstream State: Forwarding Assert State:
NoInfo
Downstream IF List: eth1, in 'olist': Downstream State: NoInfo Assert State:
NoInfo
```

Appendix A Tunnel Interface

To tunnel multicast traffic through intermediate routers which do not support multicast routing, a multicast tunnel can be created between two multicast routers (PIM-SM, PIM-DM) in IP-in-IP (IPIP) or Generic Routing Encapsulation (GRE) tunnel encapsulation mode. The following provides examples to create this tunnel.

Note: Tunnel interfaces are supported only on Linux.

Configuring Interface Tunnel between Two PIM-SM Routers

The following shows the commands to create an interface tunnel between two PIM-SM routers in IPIP mode.

`#configure terminal`	Enter Configure mode.
`(config)#interface tunnel 2`	Create a new tunnel interface and enter the Interface mode.
`(config-if)#tunnel source 10.10.1.52`	Specify the tunnel source address.
`(config-if)#tunnel destination 10.10.3.35`	Specify the tunnel destination address.
`(config-if)#tunnel ttl 23`	Set the time-to-live for the tunnel to 23.
`(config-if)#tunnel mode ipip`	Configure the tunnel mode.
`(config-if)#ip pim sparse-mode`	Enable PIM sparse mode on the interface.

PIM-DM

The following shows commands to create an interface tunnel between two PIM-DM routers in GRE mode.

`#configure terminal`	Enter Configure mode.
`(config)#interface tunnel 2`	Create a new tunnel interface and enter the Interface mode.
`(config-if)#tunnel source 10.10.1.52`	Specify the tunnel source address.
`(config-if)#tunnel destination 10.10.3.35`	Specify the tunnel destination address.
`(config-if)#tunnel ttl 23`	Set the time-to-live for the tunnel to 23.
`(config-if)#tunnel mode gre`	Configure the tunnel in Generic Routing Encapsulation (GRE) mode. Configure a Generic Routing Encapsulation (GRE) tunnel mode.
`(config-if)#ip pim dense-mode`	Enable PIM dense mode on the interface.

© Symanitron Proprietary

Multicast Routing Information Base Command Reference

Contents

This document contains these chapters:

- Chapter 1, *Multicast Commands*
- Chapter 2, *L3 IGMP Multicast Commands*
- Chapter 3, *MLD Multicast Commands*
- Chapter 4, *L2 IGMP Snooping Multicast Commands*
- Appendix 5, *L2 MLD Snooping Commands*

CHAPTER 1 Multicast Commands

SWMRE multicast protocol modules work with the Multicast Routing Information Base (MRIB).

- clear ip mroute
- debug ip mrib
- ip multicast route-limit
- ip multicast ttl-threshold
- ip multicast-routing
- show debugging ip mrib
- show ip mroute
- show ip mvif
- snmp restart mribd

clear ip mroute

Use this command to delete entries from the IP multicast routing table. This command clears the multicast route entries in the multicast route table and removes the entries from the multicast forwarder. MRIB sends a clear message to the multicast protocols. Each multicast protocol has its own clear multicast route command. The protocol-specific clear command clears multicast routes from the protocol and clears the routes from the MRIB.

Command Syntax `clear ip mroute * clear ip mroute A.B.C.D clear ip mroute A.B.C.D A.B.C.D clear ip mroute statistics * clear ip mroute statistics A.B.C.D clear ip mroute statistics A.B.C.D A.B.C.D clear ip mroute A.B.C.D pim sparse-mode clear ip mroute A.B.C.D A.B.C.D pim (dense mode| sparse-mode) clear ip mroute (vrf NAME|) * clear ip mroute (vrf NAME|) A.B.C.D clear ip mroute (vrf NAME|) A.B.C.D A.B.C.D clear ip mroute (vrf NAME|) statistics * clear ip mroute (vrf NAME|) statistics A.B.C.D clear ip mroute (vrf NAME|) statistics A.B.C.D A.B.C.D clear ip mroute (vrf Name|) A.B.C.D pim sparse-mode clear ip mroute (vrf Name|) A.B.C.D A.B.C.D pim (dense-mode | sparse-mode)`

Parameters

`*`	All multicast routes.
`A.B.C.D`	Group IP address.
`A.B.C.D`	Source IP address.
`vrf`	VRF name.
`statistics`	Multicast route statistics.
`dense-mode`	Dense Mode (PIM-DM).
`sparse-mode`	sparse Mode (PIM-SM)

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear ip mroute vrf VRF_A 225.1.1.1 3.3.3.3
```

debug ip mrib

Use this command to set debug options for IPv4 multicast.

Use the `no` parameter with this command to disable debugging IPv4 multicast.

Command Syntax

```
debug ip mrib (all|event|vif|mrt|stats|fib-msg|register-msg|nsm-
  msg|mribmsg|mtrace|mtrace-detail)
```

```
debug ip mrib (vrf NAME|)(all|event|vif|mrt|stats|fib-msg|register-
  msg|nsmmsg|mrib-msg|mtrace|mtrace-detail)

no debug ip mrib (all|event|vif|mrt|stats|fib-msg|register-msg|nsm-msg|mrib-
  msg|mtrace|mtrace-detail)

no debug ip mrib (vrf NAME|) ((all|event|vif|mrt|stats|fib-msg|register-msg|nsm-
  msg|mrib-msg|mtrace|mtrace-detail)
```

Parameters

`all`	Enable all IPv4 multicast debugging.
`event`	Enable debugging of multicast events.
`fib-msg`	Enable debugging of multicast FIB messages
`mrib-msg`	Enable debugging of multicast MRIB messages
`mrt`	Enable debugging of multicast route
`mtrace`	Enable debugging of multicast traceroute
`mtrace-detail`	Enable detailed debugging of multicast traceroute messages
`nsm-msg`	Enable debugging of multicast NSM messages
`register-msg`	Enable debugging of multicast PIM Register messages
`stats`	Enable debugging of multicast statistics.
`vif`	Enable debugging of multicast interface
`vrf`	Specify the VRF name

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#debug ip mrib all
```

ip multicast route-limit

Use this command to limit the number of multicast routes that can be added to a multicast routing table. It generates an error message when the limit is exceeded. If the threshold parameter is set, a threshold warning message is generated when this threshold is exceeded and the message continues to occur until the number of mroutes reaches the limit set by the limit argument.

Note:The mroute warning threshold must not exceed the mroute limit.

Use the `no` parameter with this command to disable this configuration.

Command Syntax `ip multicast route-limit <1-2147483647> ip multicast route-limit <1-2147483647> <1-2147483647> ip multicast (vrf NAME|) route-limit <1-2147483647> ip multicast (vrf NAME|) route-limit <1-2147483647> <1-2147483647> no ip multicast route-limit no ip multicast (vrf NAME|) route-limit`

Parameters

`vrf` VRF name

`<1-2147483647>` Number of routes `<1-2147483647>` Threshold at which to generate a warning message

Default

The default limit and threshold value is 2147483647.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ip multicast route-limit 34 24
```

ip multicast ttl-threshold

Use this command to configure the time-to-live (TTL) threshold of packets being forwarded out of an interface. Only multicast packets with a TTL value greater than the threshold are forwarded out of the interface.

Use the no parameter with this command to return to the default TTL threshold.

Command Syntax `ip multicast ttl-threshold <1-255> no ip multicast ttl-threshold`

Parameters

`<1-255>` The time-to-live threshold.

Default

The default TTL value is 1.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip multicast ttl-threshold 34
```

ip multicast-routing

Use this command to turn on/off multicast routing on the router; when turned off, the multicast protocol daemon remains present, but does not perform multicast functions. When multicast routing is enabled, the MRIB re-creates tunnels, and starts processing any VIF addition/deletion requests, MRT addition/deletion requests, and any multicast forwarding events.

Use the `no` parameter with this command to disable this function. When the `no` parameter is used, the MRIB releases all VIFs and tunnels, cleans up MRTs, stops IGMPv2 operation and stops relaying multicast forwarder events to multicast protocols.

Command Syntax `ip multicast-routing`

```
ip multicast-routing (vrf NAME|)
no ip multicast-routing no ip
multicast-routing (vrf NAME|)
```

Parameter

`vrf`	Specify the VRF name.

Default

By default, multicast routing is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ip multicast-routing
```

show debugging ip mrib

Use this command to display IPv4 multicast debugging information.

Command Syntax `show debugging ip mrib show debugging ip mrib`

```
(vrf NAME|)
```

Parameters `vrf` Display routes from a VPN Routing/Forwarding instance.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following is a sample output of the `show debugging ip mrib` command.

```
#show debugging ip mrib
Debugging status:
  MRIBv4 event debugging is on
  MRIBv4 VIF debugging is on
  MRIBv4 route debugging is on
  MRIBv4 route statistics debugging is on
  MRIBv4 FIB message debugging is on
  MRIBv4 PIM Register message debugging is on
  MRIBv4 NSM IPC message debugging is on
  MRIBv4 MRIB IPC message debugging is on
  MRIBv4 traceroute debugging is on
  MRIBv4 traceroute detailed debugging is on #
```

show ip mroute

Use this command to display the IP multicast routing (mroute) table. The routing table is based on the pairing of Source Addresses with their respective Destination Multicast Group Address (S, G).

Command Syntax `show ip mroute (dense|sparse|) (count|summary|) show ip mroute A.B.C.D (dense|sparse|)(count|summary|) show ip mroute A.B.C.D A.B.C.D (dense|sparse|) (count|summary|) show ip mroute (vrf NAME|) (dense|sparse|) (count|summary|) show ip mroute (vrf NAME|) A.B.C.D (dense|sparse|) (count|summary|) show ip mroute (vrf NAME|) A.B.C.D A.B.C.D (dense|sparse|) (count|summary|)` **Parameters**

`A.B.C.D`	Source or Group IP address.
`count`	Route and packet count data.
`summary`	Provide abbreviated display.
`dense`	Show dense multicast routes.
`sparse`	Show sparse multicast routes.
`vrf`	Specify the VRF name.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following is a sample output of this command displaying the IP multicast routing table, with and without specifying the group and source IP address: `rtr6#show ip mroute`

```
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
       B - BIDIR
Timers: Uptime/Stat Expiry
```

```
Interface State: Interface (TTL)

(172.31.1.52, 224.0.0.13), uptime 00:09:39
Owner PIM, Flags: F
  Incoming interface: eth1
Outgoing interface list:
eth2 (1)
```

The following is a sample output of this command displaying the packet count from the IP multicast routing table:

```
#show ip mroute count

IP Multicast Statistics
Total 1 routes using 132 bytes memory
Route limit/Route threshold: 2147483647/2147483647
Total NOCACHE/WRONGVIF/WHOLEPKT recv from fwd: 1/0/0
Total NOCACHE/WRONGVIF/WHOLEPKT sent to clients: 1/0/0
Immediate/Timed stat updates sent to clients: 0/0
Reg ACK recv/Reg NACK recv/Reg pkt sent: 0/0/0
Next stats poll: 00:01:10

Forwarding Counts: Pkt count/Byte count, Other Counts: Wrong If pkts
Fwd msg counts: WRONGVIF/WHOLEPKT recv
Client msg counts: WRONGVIF/WHOLEPKT/Imm Stat/Timed Stat sent
Reg pkt counts: Reg ACK recv/Reg NACK recv/Reg pkt sent
(10.10.1.52, 224.0.1.3), Forwarding: 2/19456, Other: 0
 Fwd msg: 0/0, Client msg: 0/0/0/0,  Reg: 0/0/0
```

The following is a sample output for this command displaying the IP multicast routing table in an abbreviated form:

```
#show ip mroute summary

IP Multicast Routing Table
```

Entry	Description
(a.d.c.d, 224.x.x.x)	Source Address paired with its Destination Multicast Group Address

uptime	As stated.

```
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(10.10.1.52, 224.0.0.13), 00:01:32/00:03:20, PIM-SM, Flags: TF
```

Table 1-167: Mroute pointers

Pointers	Description
I	Immediate statistics
T	Timed statistics
F	Forwarder installed
B	Bidirectional
Timers	• Uptime – route uptime. • Statistics Expiry –The time the routing table waits before updating statistics.
Interface State	Interface Time to Live (TTL)

Table 1-168: Show ip mroute output

Table 1-168: Show ip mroute output

Entry	Description
Owner	The owner is derived from the multicast group notable address (IANA). In the example above, the owner is specified as PIM because it is using the IANA address: 224.0.0.13. Other owners can be OSPF (224.0.0.5), IS-IS (224.0.0.19–21), and so on.
Flags	The flags associated with this mroute table entry.
Incoming interface	The name of the in coming interface (eth1, xe5/2, etc.).
Outgoing interface list	A numbered list of the outgoing interfaces

Table 1-169: Show ip mroute statistics received and sent

Entry	Description
NOCACHE	Number of No Cache messages received.
WRONGVIF	The Virtual Host Interface (VIF) enables the router to send and receive IP multicast packets on several different interfaces at once. This is the count of wrong VIFs received.
WHOLEPKT	When a source is multicasting a large volume data and the PIM router does not know about the particular Rendezvous Point (RP(G)), the PIM process will constantly receive WHOLEPKT notification from the kernel – this shows the count of such notifications.

show ip mvif

Use this command to display the MRIB VIF table entries.

The Virtual Host Interface (VIF) used in Pragmatic General Multicast (PGM) or “Reliable Multicast.” The VIF enables the router to send and receive IP multicast packets on several different interfaces at once, as dictated by the multicast routing tables on the router.

Command Syntax `show ip mvif show ip mvif IFNAME show ip mvif (vrf NAME|) show ip mvif (vrf NAME|) IFNAME`

Parameters

`IFNAME` Specify the interface name. `vrf`

Specify the VRF name.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following are sample outputs of this command displaying the contents for the MRIB VIF table, both with and without the interface parameter specified:

```
#show ip mvif
Interface     Vif   Owner    TTL  Local             Remote            Uptime
Idx   Module        Address          Address
  wm0           0    PIM-SM     1    192.168.1.53     0.0.0.0          00:04:26
Register      1              1    192.168.1.53      0.0.0.0         00:04:26 wm1
         2    PIM-SM   1    192.168.10.53     0.0.0.0          00:04:25
#show ip mvif wm0
Interface    Vif   Owner    TTL  Local             Remote           Uptime
Idx   Module        Address          Address wm0          0     PIM-SM   1
192.168.1.53      0.0.0.0          00:05:17
```

Table 1-170: Show ip mvif output

Entries	Description
Interface	The name of the interface.

Vif Idx	The VIF Index – the numbering of the entries in the MRIB table.
Owner	What multicast protocol is being used for an entry. For example, PIM-SM (PIM Sparce Mode).

Table 1-170: Show ip mvif output (Continued)

	Description
	Time to Live for the entry.
	AS stated.
	As stated.
	How long the multicast interface has been operating.

snmp restart mribd

Use this command to restart SNMP in Multicast Routing Information Base (MRIB)

Command Syntax `snmp restart mribd`

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#snmp restart mribd
```

CHAPTER 2 L3 IGMP Multicast Commands

This chapter describes the commands for Internet Group Management Protocol (IGMP) including the IGMP proxy service.

For IGMP multicast snooping commands, see Chapter 4, *L2 IGMP Snooping Multicast Commands*.

- clear ip igmp
- debug ip igmp
- ip igmp
- ip igmp access-group
- ip igmp immediate-leave
- ip igmp join-group
- ip igmp last-member-query-count
- ip igmp last-member-query-interval
- ip igmp limit
- ip igmp mroute-proxy
- ip igmp offlink
- ip igmp proxy-service
- ip igmp proxy unsolicited-report-interval
- ip igmp querier-timeout
- ip igmp query-interval
- ip igmp query-max-response-time
- ip igmp ra-option
- ip igmp robustness-variable
- ip igmp ssm-map enable
- ip igmp ssm-map static
- ip igmp static-group
- ip igmp startup-query-count
- ip igmp startup-query-interval
- ip igmp version
- show debugging ip igmp
- show ip igmp groups
- show ip igmp interface
- show ip igmp proxy
- show ip igmp ssm-map

clear ip igmp

Use this command to clear all IGMP local-memberships on all interfaces. This command applies to interfaces configured for IGMP Layer-3 multicast protocols, or IGMP Proxy.

Command Syntax `clear ip igmp clear ip igmp group * clear ip igmp group A.B.C.D clear ip igmp group A.B.C.D IFNAME clear ip igmp interface IFNAME clear ip igmp (vrf NAME|) clear ip igmp (vrf NAME|) group * clear ip igmp (vrf NAME|) group A.B.C.D clear ip igmp (vrf NAME|) group A.B.C.D IFNAME clear ip igmp (vrf NAME|) interface IFNAME`

Parameters

`*`	Clears all groups on all interfaces.
`A.B.C.D`	Specify the group address's local-membership to be cleared from all interfaces.
`interface`	Specify an interface. All groups learned from this interface are deleted.
`IFNAME`	Specify name of the interface.
`vrf`	Specify the VRF name.
`group`	Deletes IGMP group cache entries.
`interface`	Specify name of the interface; all groups learned from this interface are deleted.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear ip igmp
#clear ip igmp group *
#clear ip igmp group 224.1.1.1
#clear ip igmp interface eth1
#clear ip igmp vrf VRF_A
#clear ip igmp vrf new group *
#clear ip igmp vrf new interface eth1
```

debug ip igmp

Use this command to enable debugging of all IGMP, or a specific component of IGMP. This command applies to interfaces configured for IGMP Layer-3 multicast protocols.

Use the `no` parameter with this command to disable all IGMP debugging, or select a specific IGMP component.

Command Syntax `debug ip igmp all debug ip igmp decode debug ip igmp encode debug ip igmp`

```
events debug ip igmp fsm debug ip igmp tib
```

```
debug ip igmp (vrf NAME|) all debug ip igmp
(vrf NAME|) decode debug ip igmp (vrf
NAME|) encode debug ip igmp (vrf NAME|)
events debug ip igmp (vrf NAME|) fsm debug
ip igmp (vrf NAME|) tib no debug ip igmp
all no debug ip igmp decode no debug ip
igmp encode no debug ip igmp events no
debug ip igmp fsm no debug ip igmp tib no
debug ip igmp (vrf NAME|) all no debug ip
igmp (vrf NAME|) decode no debug ip igmp
(vrf NAME|) encode no debug ip igmp (vrf
NAME|) events no debug ip igmp (vrf NAME|)
fsm no debug ip igmp (vrf NAME|) tib
```

Parameters

`all`	Debug all IGMP.
`decode`	Debug IGMP decoding.
`encode`	Debug IGMP encoding.
`events`	Debug IGMP events.
`fsm`	Debug IGMP Finite State Machine (FSM).
`tib`	Debug IGMP Tree Information Base (TIB).
`vrf`	Debug VPN Routing/Forwarding instance.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#debug ip igmp all
```

ip igmp

Use this command to enable the IGMP operation on an interface. This command enables IGMP operation in standalone mode, and can be used to learn local-membership information prior to enabling a multicast routing protocol on the interface. This command will has no effect on interfaces configured for IGMP proxy.

Use the `no` parameter with this command to return all IGMP related configuration to the default (including IGMP proxy service).

Command Syntax `ip`

```
igmp   no   ip
igmp
```

Parameters

None

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp
```

ip igmp access-group

Use this command to control the multicast local-membership groups learned on an interface. This command applies to interfaces configured for IGMP Layer-3 multicast protocols, IGMP proxy.

Use the `no` parameter with this command to disable this access control.

Command Syntax `ip igmp access-group WORD no ip igmp access-group WORD`

Parameters

`WORD`	Standard IP access-list name.

Default

No access list configured

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

In the following example, hosts serviced by Ethernet interface 0 can only join the group 225.2.2.2:

```
#configure terminal
(config)#access-list 1 permit 225.2.2.2 0.0.0.0
(config)#interface eth1
(config-if)#ip igmp access-group xyz
(config-if)#exit
```

ip igmp immediate-leave

In IGMP version 2, use this command to minimize the leave latency of IGMP memberships. This command is used when only one receiver host is connected to each interface. This command applies to interfaces configured for IGMP Layer-3 multicast protocols, IGMP Proxy.

To disable this feature, use the `no` parameter with this command.

Command Syntax `ip igmp immediate-leave group-list WORD no ip igmp immediate-leave`

Parameters

group-list	Standard access-list name or number that defines multicast groups in which the immediate leave feature is enabled.
WORD	Standard IP access-list name.

Default

Disabled

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows how to enable the immediate-leave feature on an interface for a specific range of multicast groups. In this example, the router assumes that the group access-list consists of groups that have only one host membership at a time per interface:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp immediate-leave group-list xyz
(config-if)#exit
(config)#access-list 34 permit 225.192.20.0 0.0.0.255
```

ip igmp join-group

Use this command to configure a join multicast group.

Use the no parameter with this command to delete group membership entry.

Command Syntax ip igmp join-group A.B.C.D {(source (A.B.C.D)|)} no ip igmp join-group A.B.C.D {(source (A.B.C.D)|)}

Parameters

A.B.C.D	Standard IP multicast group address to be configured as a group member.
source	Static source to be joined.
A.B.C.D	Standard IP source address to be configured as a source from where multicast packets originate.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp join-group 225.1.1.1 source 1.1.1.2

(config-if)#no ip igmp join-group 225.1.1.1 source 1.1.1.2
```

ip igmp last-member-query-count

Use this command to set the last-member query-count value. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

Use the `no` parameter with this command to return to the default value on an interface.

Command Syntax `ip igmp last-member-query-count <2-7> no ip igmp last-member-query-count`

Parameter

`<2-7>`	Specify the last member query count value.

Default

The default last member query count value is 2.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp last-member-query-count 3
```

ip igmp last-member-query-interval

Use this command to configure the frequency at which the router sends IGMP group-specific host query messages. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

Use the `no` parameter with this command to set this frequency to the default value.

Command Syntax `ip igmp last-member-query-interval <1000-25500> no ip igmp last-member-query-interval`

Parameter

<1000-25500>	Frequency (in milliseconds) at which IGMP group-specific host query messages are sent.

Default

1000 milliseconds

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following example changes the IGMP group-specific host query message interval to 2 seconds:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp last-member-query-interval 2000
```

ip igmp limit

Use this command to set the maximum number of group membership states, at either the router level or at the interface level. Once the specified number of group memberships is reached, all further local-memberships are ignored. Optionally, an exception access-list can be configured to specify the group-address(es) to be excluded from being subject to the limit.

This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy. The limit applies, individually, to each of its constituent interfaces.

Use the `no` parameter with this command to unset the limit and any specified exception access-list.

Command Syntax `ip igmp limit (<1-2097152> (except WORD |)`

`ip igmp (vrf NAME) limit(<1-2097152> (except WORD |)`

`no ip igmp limit no ip igmp (vrf NAME|) limit`

Parameters

vrf	Specify the VRF name.
<1-2097152>	Maximum number of group membership states.
except	Number or name that defines multicast groups that are exempted from being subject to configured limit.
WORD	Standard IP access-list name.

Command Mode

Configure mode and Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example configures an IGMP limit of 100 group-membership states across all interfaces on which IGMP is enabled, and excludes group 224.1.1.1 from this limitation:

```
#configure terminal
(config)#access-list 1 permit 224.1.1.1 0.0.0.0
(config)#ip igmp limit 100 except xyz
```

The following example configures an IGMP limit of 100 group-membership states on eth1:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp limit 100
```

ip igmp mroute-proxy

Use this command to specify the IGMP Proxy service (upstream host-side) interface with which to be associated. IGMP router-side protocol operation is enabled only when the specified upstream proxy-service interface is functional.

Note: This command should not be used when configuring interfaces enabled for IGMP in association with a multicast routing protocol, otherwise the behavior will be undefined.

Use the `no` parameter with this command to remove the association with the proxy-service interface.

Command Syntax `ip igmp mroute-proxy IFNAME no ip igmp mroute-proxy`

Parameter

`IFNAME`	Specify an interface name.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following example configures the eth1 interface as the upstream proxy-service interface for the downstream router-side interface, eth1.

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp mroute-proxy eth1
```

ip igmp offlink

Use this command to configure off-link for IGMP.

Use the `no` parameter with this command to remove this configuration.

Command Syntax `ip igmp offlink no ip igmp offlink`

Parameter

None

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp offlink

(config-if)#no ip igmp offlink
```

ip igmp proxy-service

Use this command to designate an interface to be the IGMP proxy-service (upstream host-side) interface, thus enabling IGMP host-side protocol operation on this interface. All associated downstream router-side interfaces will have their memberships consolidated on this interface, according to IGMP host-side functionality.

Note: This command should not be used when configuring interfaces enabled for IGMP in association with a multicast-routing protocol, otherwise the behavior will be undefined.

Use the `no` parameter with this command to remove the designation of the interface as an upstream proxy-service interface.

Command Syntax `ip igmp proxy-service no ip igmp proxy-service`

Parameter

None

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following example designates the eth1 interface as the upstream proxy-service interface.

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp proxy-service
```

ip igmp proxy unsolicited-report-interval

Use this command to set an unsolicited report interval for an interface designated as an IGMP proxy (upstream hostside).

Use the `no` parameter with this command to remove the unsolicited report interval from the interface.

Command Syntax `ip igmp proxy unsolicited-report-interval <1000-25500>` `no ip igmp proxy unsolicited-report-interval`

Parameter

`<1000-25500>`	Specify an unsolicited report interval value in milliseconds.

Default

1000 milliseconds

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp proxy unsolicited-report-interval 1234

(config-if)#no ip igmp proxy unsolicited-report-interval
```

ip igmp querier-timeout

Use this command to set the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

To restore the default value, use the `no` parameter with this command.

Command Syntax `ip igmp querier-timeout <60-300>` `no ip igmp querier-timeout`

Parameter

<60-300>	Number of seconds that the router waits after the previous querier has stopped querying before it takes over as the querier.

Default

255 seconds

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following example configures the router to wait 120 seconds from the time it received the last query before it takes over as the querier for the interface:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp querier-timeout 120
```

ip igmp query-interval

Use this command to set the frequency of sending IGMP host query messages. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

To return to the default frequency, use the `no` parameter with this command.

Note: Querier timeout changes by changing query interval.

Command Syntax `ip igmp query-interval <1-18000>` `no ip igmp query-interval`

Parameter

<1-18000>	Frequency (in seconds) at which IGMP host query messages are sent.

Default

Default query interval is 125 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following example changes the frequency of sending IGMP host-query messages to 2 minutes:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp query-interval 120
```

ip igmp query-max-response-time

Use this command to set the maximum response time advertised in IGMP queries. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy. Use the `no` parameter with this command to restore the default value.

Command Syntax `ip igmp query-max-response-time <1-240> no ip igmp query-max-response-time`

Parameter

`<1-240>`	Maximum response time (in seconds) advertised in IGMP queries.

Default

10 seconds

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following example configures a maximum response time of 8 seconds:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp query-max-response-time 8
```

ip igmp ra-option

Use this command to configure strict RA (Router Advertisement) validation for IGMP.

Use the `no` parameter with this command to restore the default value.

Command Syntax `ip igmp ra-option no ip igmp ra-option`

Parameter

None

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following example configures a maximum response time of 8 seconds:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp ra-option

(config-if)#no ip igmp ra-option
```

ip igmp robustness-variable

Use this command to set the robustness variable value on an interface. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

To return to the default value on an interface, use the `no` parameter with this command.

Command Syntax `ip igmp robustness-variable <2-7> no ip igmp robustness-variable`

Parameter

`<2-7>`	Specify the robustness variable value.

Default

Default robustness variable value is 2.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface 0
(config-if)#ip igmp robustness-variable 3
```

ip igmp ssm-map enable

Use this command to enable SSM mapping on the router. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

Use the `no` parameter with this command to disable SSM mapping.

Command Syntax `ip igmp ssm-map enable ip igmp (vrf NAME|) ssm-map enable no ip igmp ssm-map enable no ip igmp (vrf NAME|) ssm-map enable`

Parameter

`vrf`	Specify the VRF name.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

This example shows how to configure SSM mapping on the router.

```
#configure terminal
(config)#ip igmp ssm-map enable
```

ip igmp ssm-map static

Use this command to specify the static mode of defining SSM mapping. SSM mapping statically assigns sources to IGMPv1 and IGMPv2 groups to translate such (*,G) groups' memberships to (S,G) memberships for use with PIMSSM. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy.

Use the `no` parameter with this command to remove the SSM map association.

Command Syntax `ip igmp ssm-map static WORD A.B.C.D ip igmp (vrf NAME|) ssm-map static WORD A.B.C.D no ip igmp (vrf NAME|) ssm-map static WORD A.B.C.D no ip igmp ssm-map static WORD A.B.C.D`

Parameters

`vrf`	Specify the VRF name.
`WORD`	Standard IP access-list name.
`A.B.C.D`	Source address to use for static map group.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

This example shows how to configure an SSM static mapping for group-address 224.1.1.1 Note:

`access-list` can only be a `permit` type `access-list`

```
#configure terminal
(config)# ip igmp ssm-map static xyz 1.2.3.4
(config)# access-list 1 permit 224.1.1.1 0.0.0.255
```

ip igmp static-group

Use this command to statically configure group membership entries on an interface. To statically add only a group membership, do not specify any parameters. This command applies to IGMP operation on a specific interface to statically add group and/or source records; on a VLAN interface to statically add group and/or source records.

Use the `no` parameter with this command to delete static group membership entries.

Command Syntax `ip igmp static-group A.B.C.D (source (A.B.C.D|ssm-map)|) no ip igmp static-group A.B.C.D (source (A.B.C.D|ssm-map)|)`

Parameters

`A.B.C.D`	Standard IP Multicast group address to be configured as a static group member.
`source`	Static source to be joined.
`A.B.C.D`	Standard IP source address to be configured as a static source from where multicast packets originate.
`ssm-map`	Mode of defining SSM mapping. SSM mapping statically assigns sources to IGMPv1 and IGMPv2 groups to translate these (*, G) groups' memberships to (S, G) memberships for use with PIM-SSM.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following examples show how to statically add group and/or source records for IGMP:

```
#configure terminal
(config)#interface eth1
(config-if)#ip igmp static-group 226.1.2.3

#configure terminal
(config)#interface eth1
(config-if)#ip igmp static-group 226.1.2.4 source 1.2.3.4

#configure terminal
(config)#interface eth1
(config-if)#ip igmp static-group 226.1.2.5 source ssm-map
```

ip igmp startup-query-count

Use this command to set a startup query count for IGMP.

Use the `no` parameter with this command to return to the default version.

Command Syntax `ip igmp startup-query-count <2-10> no ip igmp startup-query-count`

Parameters

`<2-10>`	Specify a startup query count value.

Default

The default value 2.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface 0
(config-if)#ip igmp startup-query-count 2

                (config-if)#no ip igmp startup-query-count
```

ip igmp startup-query-interval

Use this command to set a query interval value for IGMP.

Use the `no` parameter with this command to return to the default version.

Command Syntax `ip igmp startup-query-interval <1-18000> no ip igmp startup-query-interval`

Parameters

<1-18000>	Specify a startup query interval value in seconds.

Default

The default value 31 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface 0
(config-if)#ip igmp startup-query-interval 1

(config-if)#no ip igmp startup-query-interval
```

ip igmp version

Use this command to set the current IGMP protocol version on an interface. This command applies to interfaces configured for IGMP Layer-3 multicast protocols and IGMP Proxy. Use the `no` parameter with this command to return to the default version.

Command Syntax `ip igmp version <1-3> no ip igmp version`

Parameters

<1-3>	Specify IGMP protocol version number.

Default

The default IGMP protocol version number is 3.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
```

```
(config)#interface 0
(config-if)#ip igmp version 2
```

show debugging ip igmp

Use this command to display the status of the debugging of the IGMP system, or a specific VRF in the IGMP system.

Command Syntax `show debugging ip igmp`

`show debugging ip igmp (vrf NAME|)`

Parameters

`vrf`	Specify the VRF name.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show debugging ip igmp
 IGMP Debugging status:
 IGMP Decoder debugging is on
 IGMP Encoder debugging is on
 IGMP Events debugging is on
 IGMP FSM debugging is on
 IGMP Tree-Info-Base (TIB) debugging is on
```

show ip igmp groups

Use this command to display the multicast groups with receivers connected to the router and learned through IGMP.

Command Syntax `show ip igmp groups (detail|) show ip igmp groups A.B.C.D (detail|) show ip igmp groups IFNAME (detail|) show ip igmp groups IFNAME A.B.C.D (detail|) show ip igmp (vrf NAME|) groups (detail|) show ip igmp (vrf NAME|) groups A.B.C.D (detail|) show ip igmp (vrf NAME|) groups IFNAME (detail|) show ip igmp (vrf NAME|) groups IFNAME A.B.C.D (detail|)`

Parameters

`vrf`	Specify the VRF name.
`A.B.C.D`	Address of multicast group.
`IFNAME`	Name of the interface.

`detail`	IGMPv3 source information.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following command displays local-membership information for all interfaces:

```
rtr1#show ip igmp groups detail IGMP Connected Group
Membership Details

Flags: (M - SSM Mapping, R - Remote, L - Local,
SG - Static Group, SS - Static Source)
Interface:      eth1
Group:          224.1.1.1
Flags:          L
Uptime:         00:00:04
Group mode:     Exclude (Expires: 00:04:15, Static)
Last reporter:   3.3.3.3
Group source list: (R - Remote, M - SSM Mapping, S - Static, L - Local)
Include Source List :
 Source Address Uptime    v3 Exp    Fwd Flags
 2.2.2.2         00:00:04 stopped   Yes L
```

Table 2-171: Flags

Flag	Meaning
M	Source Specific Multicast
R	Remote multicast
L	Local multicast
SG	Static Group
SS	Static Source

Table 2-172: Show ip igmp groups output

Entry	Description
Interface	The interface on which multicast is operating.
Group	The Multicast group, identified by a multicast IP address.
Flags	Flag on this interface – in this case, the flag indicates that the multicast is Local. See Table 2-171.
Uptime	The amount of time that the multicast connection has been up.
Group mode	The group mode is determined by interactions between IGMP router database entries, which is beyond the scope of this document. For a detailed description of these interactions, see RFC 3376.
Last reporter	The IPv4 address of the last host to send multicast information.
Group source list	A list of flags that indicate the state of the multicast connections. See Table 2-171.
Include Source List	A table containing parameters about the multicast session: •Source Address – The IP address of the Source(s) connected to the multicast hosts. •Uptime – The multicast session's uptime. •v3 Exp – Tells whether IGMPv3 Explicit Tracking is running or not. •Fwd – Whether IGMP information is being forwarded by this device. •Flags – See Table 2-171.

show ip igmp interface

Use this command to display the state of IGMP, IGMP Proxy service for a specified interface, or all interfaces.

Command Syntax `show ip igmp interface (IFNAME|)`

`show ip igmp (vrf NAME|) interface (IFNAME|)`

Parameters

`vrf`	Specify the VRF name.
`interface`	Specify the interface parameter.
`IFNAME`	Specify the name of the interface.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following command displays the IGMP interface status on all interfaces enabled for IGMP.

```
#show ip igmp interface
Interface vlan1.1 (Index 4294967295)
IGMP Active, Non-Querier, Version 3 (default)
IGMP querying router is 0.0.0.0
IGMP query interval is 125 seconds
IGMP querier timeout is 255 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1000 milliseconds
Group Membership interval is 260 seconds| #
```

Table 2-173: Show ip igmp interface

Entry	Description
Interface	Interface type and number
IGMP Active	IGMP status – whether Active or Inactive; whether this interface is a querier; IGMP version (v1, v2, or v3).
IGMP querying router	IP address of the designated router for this LAN segment.
IGMP query interval	Interval at which the Cisco IOS software sends Protocol Independent Multicast (PIM) router query messages.
IGMP querier timeout	An interval of time that the software uses when deciding to take over as the querier.

IGMP max query response time	An interval of time that is advertised as the maximum response time that is advertised in IGMP queries.

Table 2-173: Show ip igmp interface (Continued)

Entry	Description
Last member query response interval	This interval is the maximum amount of time between query messages that the querier will wait before sending messages that indicate that the multicast session has ended.
Group Membership interval	A group membership interval timer is maintained for each dynamic multicast group added to a downstream interface in the table. The timer is refreshed when a membership report for a multicast group is received. If the timer expires, the multicast group is removed from the table.

show ip igmp proxy

Use this command to display the state of IGMP Proxy services for a specified interface or for all interfaces.

Command Syntax `show ip igmp proxy groups (detail|) show ip igmp proxy groups A.B.C.D (detail|) show ip igmp proxy groups IFNAME (detail|) show ip igmp proxy groups IFNAME A.B.C.D (detail|) show ip igmp (vrf NAME|) proxy groups (detail|) show ip igmp (vrf NAME|) proxy groups A.B.C.D (detail|) show ip igmp (vrf NAME|) proxy groups IFNAME (detail|) show ip igmp (vrf NAME|) proxy groups IFNAME A.B.C.D (detail|)`

Parameters

`vrf`	Specify the VRF name.
`groups`	IGMP proxy group membership information.
`A.B.C.D`	Address of multicast group.
`IFNAME`	The name of the VLAN interface.
`detail`	IGMPv3 source information

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip igmp proxy

Interface eth2 (Index 4)
Administrative status: enabled
Operational status: up
Upstream interface is eth1
Number of multicast groups: 1

#show ip igmp proxy groups

IGMP Connected Proxy Group Membership
Group Address    Interface            State     Member state
224.0.1.3        eth1                 Active    Delay
```

Table 2-174: Show ip igmp proxy output

Entry	Description
Interface	Interface and Index of the interface.
Administrative status	Depends on the interface states – Enabled only if both host and downstream interfaces are up. Otherwise, Disabled if only one interface is up.

Operational status	Depends on Administrative status – either Up or Down depending on Administrative status of corresponding interfaces.
Upstream interface	As stated.
Number of multicast groups	The number of multicast groups supported by this proxy.

Table 2-175: show ip igmp proxy groups output

Entry	Description
Group Address	Multicast address associated with each group.
Interface	Interface name, such as eth1, xe3/1, etc..
State	The state of the proxy group – can be either Active or Inactive.
Member state	The state of the proxy group member – can be either Idle or Delay, Idle is the default state.

show ip igmp ssm-map

Use this command to display IGMP SSM-map data.

Command Syntax `show ip igmp ssm-map show ip igmp ssm-map A.B.C.D show ip igmp (vrf NAME|) ssm-map show ip igmp (vrf NAME|) ssm-map A.B.C.D`

Parameters

`vrf` Specify the VRF name.

`A.B.C.D` Address of multicast group.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#sh ip igmp ssm-map
SSM Mapping : Enabled
                                        Database    : Static mappings configured
```

CHAPTER 3 MLD Multicast Commands

This chapter describes the commands for Multicast Listener Discovery (MLD) which includes the MLD proxy service.

- clear ipv6 mld
- debug ipv6 mld
- ipv6 mld
- ipv6 mld access-group
- ipv6 mld immediate-leave
- ipv6 mld last-member-query-count
- ipv6 mld last-member-query-interval
- ipv6 mld limit
- ipv6 mld mroute-proxy
- ipv6 mld proxy-service
- ipv6 mld querier-timeout
- ipv6 mld query-interval
- ipv6 mld query-max-response-time
- ipv6 mld robustness-variable
- ipv6 mld ssm-map enable
- ipv6 mld ssm-map static
- ipv6 mld static-group
- ipv6 mld version
- show debugging ipv6 mld
- show ipv6 mld groups
- show ipv6 mld interface
- show ipv6 mld ssm-map

clear ipv6 mld

Use this command to clear MLD local memberships in an interface or group. This command applies to entities configured for MLD layer-3 multicast protocols, or MLD proxy.

Command Syntax `clear ipv6 mld clear ipv6 mld group * clear ipv6 mld group X:X::X:X clear ipv6 mld group X:X::X:X IFNAME clear ipv6 mld group [*|X:X::X:X (IFNAME)] clear ipv6 mld interface IFNAME clear ipv6 mld (vrf NAME|) clear ipv6 mld (vrf NAME|) group * clear ipv6 mld (vrf NAME|) group X:X::X:X clear ipv6 mld (vrf NAME|) group X:X::X:X IFNAME clear ipv6 mld (vrf NAME|) interface IFNAME`

Parameter

vrf	Specify the VRF name.
groups	Clears groups from an interface.
*	Clears all groups from an interface.
X:X::X:X	Specify an IPv6 interface.
interface	Specify the interface parameter.
IFNAME	Specify the interface name.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear ipv6 mld group *
#clear ipv6 mld group 224.1.1.1
#clear ipv6 mld vrf VRF_A
```

debug ipv6 mld

Use this command to enable debugging of all MLD, or a specific component of MLD. This command applies to interfaces configured for MLD Layer-3 multicast protocols.

Use the no parameter with this command to disable all MLD debugging or debugging of a specific component of MLD.

Command Syntax debug ipv6 mld all debug ipv6 mld decode debug ipv6 mld encode debug ipv6 mld events debug ipv6 mld fsm debug ipv6 mld tib debug ipv6 mld (vrf NAME|) all debug ipv6 mld (vrf NAME|) decode debug ipv6 mld (vrf NAME|) encode debug ipv6 mld (vrf NAME|) events debug ipv6 mld (vrf NAME|) fsm debug ipv6 mld (vrf NAME|) tib no debug ipv6 mld all no debug ipv6 mld decode no debug ipv6 mld encode no debug ipv6 mld events no debug ipv6 mld fsm no debug ipv6 mld tib no debug ipv6 mld (vrf NAME|) all no debug ipv6 mld (vrf NAME|) decode no debug ipv6 mld (vrf NAME|) encode no debug ipv6 mld (vrf NAME|) events no debug

```
ipv6 mld (vrf NAME|) fsm no debug ipv6
mld (vrf NAME|) tib
```

Parameters

`all`	Debug all MLD.
`decode`	Debug MLD decoding.
`encode`	Debug MLD encoding.
`events`	Debug MLD events.
`fsm`	Debug MLD finite state machine (FSM).
`tib`	Debug MLD tree information base (TIB).

`vrf`	Debug VPN Routing/Forwarding instance.

Command Mode

Privileged Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#debug mld all
```


© Symanitron Proprietary

ipv6 mld

Use this command to enable the MLD protocol operation on an interface. This command enables MLD protocol operation in stand-alone mode, and can be used to learn local-membership information prior to enabling a multicast routing protocol on the interface. This command will has no effect on interfaces configured for MLD Proxy.

Note: This command can only be issued on VLAN interfaces.

Use the `no` parameter with this command to return all MLD related configuration to the default or MLD Proxy service.

Command Syntax

```
ipv6 mld no
ipv6 mld
```

Parameters

None

Default

Disabled

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ipv6 mld
```

ipv6 mld access-group

Use this command to control the multicast local-membership groups learnt on an interface. This command applies to interfaces configured for MLD layer-3 multicast protocols, or MLD proxy.

Note: This command can only be issued on VLAN interfaces.

Use the `no` parameter with this command to disable this access control.

Command Syntax

```
ipv6 mld access-group WORD no ipv6 mld access-group
```

Parameter

`WORD`	Standard IPv6 access-list name.

Default

No access list configured.

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced before SWMRE version 1.3.

Examples

In the following example, hosts serviced by Ethernet interface 0 can join the group `ff0e::1/128` only:

```
#configure terminal
(config)#ipv6 access-list Group1 permit ff0e::1/128
(config)#interface fxp0
(config-if)#ipv6 mld access-group Group1
```

ipv6 mld immediate-leave

Use this command to minimize the leave latency of MLD memberships. This command applies to interfaces configured for MLD Layer-3 multicast protocols, or MLD Proxy. Use this command when only one receiver host is connected to each interface.

Use the `no` parameter with this command to disable this feature.

Command Syntax `ipv6 mld immediate-leave group-list WORD no ipv6 mld immediate-leave`

Parameter `group-list` Standard IPv6 access-list name that defines multicast groups in which the immediate leave feature is enabled.

Default

Disabled

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows how to enable the immediate-leave feature on an interface for a specific range of multicast groups. In this example, the router assumes that the group access-list consists of groups that have only one node membership at a time per interface:

```
#configure terminal
(config)#interface eth0
```

```
(config-if)#ipv6 mld immediate-leave v6grp
(config-if)#exit
```

ipv6 mld last-member-query-count

Use this command to set the last-member query-count value. This command applies to interfaces configured for MLD Layer-3 multicast protocols, or MLD Proxy.

Use the `no` parameter with this command to return to the default value on an interface.

Command Syntax `ipv6 mld last-member-query-count <2-7> no ipv6 mld last-member-query-count`

Parameters

`<2-7>`	Specify a last-member query-count value.

Default

The default last-member query-count value is 2.

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface 0
(config-if)#ipv6 mld last-member-query-count 3
```

ipv6 mld last-member-query-interval

Use this command to set the frequency at which the router sends MLD group-specific host query messages. This command applies to interfaces configured for MLD Layer-3 multicast protocols, or MLD Proxy.

Use the `no` parameter with this command to set this frequency to the default value.

Command Syntax `ipv6 mld last-member-query-interval <1000-25500> no ipv6 mld last-member-query-interval`

Parameter

`<1000-25500>`	Specify a last member query interval value in milliseconds.

Default

The default last-member query-count value is 1000 milliseconds.

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following example changes the MLD group-specific host query message interval to 2 seconds:

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 mld last-member-query-interval 2000
```

ipv6 mld limit

Use this command to set the limit on the maximum number of group membership states at either the router level, or for the specified interface. Once the specified number of group memberships is reached, all further local-memberships will be ignored. Optionally, an exception access-list can be configured to specify the group-address(es) to be excluded from being subject to the limit.

This command applies to interfaces configured for MLD Layer-3 multicast protocols, or MLD Proxy.

Use the `no` parameter with this command to unset the limit and any specified exception access-list.

Command Syntax `ipv6 mld limit <1-2097152> (except WORD |)`

```
ipv6 mld (vrf NAME|) limit <1-2097152> (except WORD |)
no ipv6 mld limit
```

Parameters

`vrf`	Specify the VRF name.
`<1-2097152>`	Maximum number of group membership states.
`except`	Standard IPv6 access-list name that defines multicast groups which are exempted from being subject to the configured limit.
`WORD`	Specify the standard IPv6 access-list name.

Default

The default value is 0 (zero).

Command Mode

Configure mode and Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example configures an MLD limit of 100 group-membership states across all interfaces on which MLD is enabled, and excludes group 224.1.1.1 from this limitation:

```
#configure terminal
```

```
(config)#ipv6 mld limit 100 except v6grp
```

The following example configures an MLD limit of 100 group-membership states on eth0:

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 mld limit 100
```

ipv6 mld mroute-proxy

Use this command to specify the MLD Proxy service (upstream host-side) interface with which to be associated. MLD router-side protocol operation is enabled only when the specified upstream proxy-service interface is functional. This command should not be configured on interfaces enabled for MLD in association with a multicast routing protocol; otherwise, the behavior will be undefined.

Use the `no` parameter with this command to remove the association with the proxy-service interface.

Command Syntax `ipv6 mld mroute-proxy IFNAME no ipv6 mld mroute-proxy`

Parameters

`IFNAME`	Specify the interface name.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following example configures the eth0 interface as the upstream proxy-service interface for the downstream router-side interface, eth1.

```
#configure terminal
(config)#interface eth1
(config-if)#ipv6 mld mroute-proxy eth0
```

ipv6 mld proxy-service

Use this command to designate an interface to be the MLD proxy-service (upstream host-side) interface, thus enabling MLD host-side protocol operation on this interface. All associated downstream router-side interfaces will have their memberships consolidated on this interface, according to MLD host-side functionality.

This command should not be used when configuring interfaces enabled for MLD in association with a multicast-routing protocol, otherwise the behavior will be undefined.

Use the `no` parameter with this command to remove the designation of the interface as an upstream proxy-service interface.

Command Syntax `ipv6 mld proxy-service no ipv6 mld proxy-service`

Parameters

None

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following example designates the eth0 interface as the upstream proxy-service interface.

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 mld proxy-service
```

ipv6 mld querier-timeout

Use this command to configure the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying. This command applies to interfaces configured for MLD Layer-3 multicast protocols, or MLD Proxy.

Use the `no` parameter with this command to restore the default value.

Command Syntax `ipv6 mld querier-timeout <60-300> no ipv6 mld querier-timeout`

Parameter

`<60-300>`	Number of seconds that the router waits after the previous querier has stopped querying before it takes over as the querier.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following example configures the router to wait 120 seconds from the time it received the last query before it takes over as the querier for the interface:

```
#configure terminal
```

```
(config)#interface eth0
(config-if)#ipv6 mld querier-timeout 120
```

ipv6 mld query-interval

Use this command to set the frequency of sending MLD host query messages. This command applies to interfaces configured for MLD Layer-3 multicast protocols, or MLD Proxy.

Use the `no` parameter with this command to return to the default frequency.

Command Syntax `ipv6 mld query-interval <1-18000>  no  ipv6  mld  query-interval`

Parameter

`<1-18000>`	Frequency (in seconds) at which MLD host query messages are sent.

Default

125 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following example changes the frequency of sending MLD host-query messages to 2 minutes:

```
#configure terminal
(config)#interface fxp0
(config-if)#ipv6 mld query-interval 120
```

ipv6 mld query-max-response-time

Use this command to set the maximum response time advertised in MLD queries. This command applies to interfaces configured for MLD Layer-3 multicast protocols, or MLD Proxy. Use the `no` parameter with this command to restore the default value.

Command Syntax `ipv6 mld query-max-response-time <1-240>  no  ipv6  mld  query-max-response-time`

Parameter

`<1-240>`	Maximum response time (in seconds) advertised in MLD queries.

Default

10 seconds

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following example configures a maximum response time of 8 seconds:

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 mld query-max-response-time 8
```

ipv6 mld robustness-variable

Use this command to set the robustness variable value on an interface. This command applies to interfaces configured for MLD Layer-3 multicast protocols, or MLD Proxy.

Use the `no` parameter with this command to return to the default value on an interface.

Command Syntax `ipv6 mld robustness-variable <2-7> no ipv6 mld robustness-variable`

Parameter

`<2-7>`	Specify a robustness variable value in seconds.

Default

Default robustness value is 2 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface 0
(config-if)#ipv6 mld robustness-variable 3
```

ipv6 mld ssm-map enable

Use this command to enable SSM mapping on the router. This command applies to interfaces configured for MLD Layer-3 multicast protocols, or MLD Proxy.

Use the `no` parameter with this command to disable SSM mapping.

Command Syntax `ipv6 mld ssm-map enable ipv6`

`mld (vrf NAME|) ssm-map enable no ipv6`

`mld ssm-map enable no ipv6 mld (vrf NAME|)`

`ssm-map enable`

Parameter

`vrf`	Specify the VRF name.

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced before SWMRE version 1.3.

Example

This example shows how to enable MLD SSM mapping on the router.

```
#configure terminal
(config)#ipv6 mld ssm-map enable
```

ipv6 mld ssm-map static

Use this command to specify the static mode of defining SSM mapping. SSM mapping statically assigns sources to MLDv1 groups to translate such (*,G) groups' memberships to (S,G) memberships for use with PIM-SSM. This command applies to interfaces configured for MLD Layer-3 multicast protocols, or MLD Proxy.

Use the `no` parameter with this command to remove the SSM map association.

Command Syntax `ipv6 mld ssm-map static WORD X:X::X:X ipv6`

`mld (vrf NAME|) ssm-map static WORD X:X::X:X no ipv6 mld`

`ssm-map static WORD X:X::X:X no ipv6 mld (vrf NAME|)`

`ssm-map static WORD X:X::X:X`

Parameters

`vrf`	Specify the VRF name.
`WORD`	Specify IPv6 named standard access-list.
`X:X::X:X`	Specify IPv6 address.

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced before SWMRE version 1.3.

Example

This example shows how to configure an SSM static mapping for group-address ff0e::1/128.

```
#configure terminal
(config)#ipv6 mld ssm-map static v6grp 2006::3
(config)#ipv6 access-list v6grp permit ff0e::1/128
```

ipv6 mld static-group

Use this command to statically configure IPv6 group membership entries on an interface. To statically add only a group membership, do not specify any parameters. This command applies to MLD operation on a specific interface to statically add group and/or source records.

Use the `no` parameter with this command to delete static group membership entries.

Command Syntax `ipv6 mld static-group X:X::X:X {(source (X:X::X:X|ssm-map)|) (interface IFNAME|)} no ipv6 mld static-group X:X::X:X {(source (X:X::X:X|ssm-map)|) (interface IFNAME|)}`

Parameters

`X:X::X:X`	Standard IPv6 Multicast group address to be configured as a static group member.
`interface`	Physical interface. If used, static configuration is applied to the physical interface. If not used, static configuration is applied on all VLAN constituent interfaces.
`IFNAME`	Physical interface name.
`source`	Static source to be joined.
`X:X::X:X`	Standard IPv6 source address to be configured as a static source from where multicast packets originate.
`ssm-map`	Mode of defining SSM mapping. SSM mapping statically assigns sources to MLDv1 groups to translate these (*,G) groups' memberships to (S,G) memberships for use with PIM-SSM.

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following examples shows how to statically add group and/or source records:

```
#configure terminal
(config)#interface vlan1.1
(config-if)#ipv6 mld static-group ff1e::10

(config)#interface vlan1.1
(config-if)#ipv6 mld static-group ff1e::10 source fe80::2fd:6cff:fe1c:b

(config)#interface vlan1.1
(config-if)#ipv6 mld static-group ff1e::10 source ssm-map
(config)#interface vlan1.1
```

```
(config-if)#ipv6 mld static-group ff1e::10 interface eth0
```

ipv6 mld version

Use this command to set the current MLD protocol version on an interface. This command applies to interfaces configured for MLD Layer-3 multicast protocols, or MLD Proxy.

Use the `no` parameter with this command to return to the default version on an interface.

Command Syntax `ipv6 mld version <1-2> no ipv6 mld version`

Parameter

`<1-2>` Specify a MLD protocol version number.

Default

Default MLD protocol version number is 2.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface 0
(config-if)#ipv6 mld version 1
```

show debugging ipv6 mld

Use this command to display debugging information for MLD.

Command Syntax `show debugging ipv6 mld show debugging ipv6 mld (vrf NAME|)`

Parameters `vrf` Indicates the `vrf` keyword.

`NAME` Displays the VRF name.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following is a sample output of the `show debugging mld` command:

```
#show debugging ipv6 mld
MLD Debugging status:
  MLD Decoder debugging is off
  MLD Encoder debugging is off
  MLD Events debugging is off
  MLD FSM debugging is off
  MLD Tree-Info-Base (TIB) debugging is off
#
```

show ipv6 mld groups

Use this command to display the multicast groups with receivers directly connected to the router, and learned through MLD.

Command Syntax `show ipv6 mld groups (detail|) show ipv6 mld groups IFNAME (detail|) show ipv6 mld groups IFNAME X:X::X:X (detail|) show ipv6 mld groups X:X::X:X (detail|) show ipv6 mld (vrf NAME|) groups (detail|) show ipv6 mld (vrf NAME|) groups IFNAME (detail|) show ipv6 mld (vrf NAME|) groups IFNAME X:X::X:X (detail|) show ipv6 mld (vrf NAME|) groups X:X::X:X (detail|)`

Parameters

`vrf`	Indicates the `vrf` keyword.
`NAME`	Displays the VRF name.
`X:X::X:X`	Displays the multicast group address.
`IFNAME`	Interface name for which to display local information.
`detail`	MLDv2 source information.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following command displays local-membership information for all interfaces:

```
#show ipv6 mld groups
MLD Connected Group Membership
Group Address    Interface     Uptime      Expires    Last Reporter ff1e::10
ge10          00:03:16    00:01:09   fe80::202:b3ff:fef0:79d8
```

Table 3-176: Show ipv6 mld groups

Entry	Description
Group Address	As stated.
Interface	A directly connected interface to the router
Uptime	Up time for multicast group

Table 3-176: Show ipv6 mld groups (Continued)

Entry	Description
Expires	Time before multicast group needs to send another uptime message to the directly connected router.
Last Reporter	IPv6 IP address of last reporte node in the group.

show ipv6 mld interface

Use this command to display the state of MLD, MLD Proxy service, and for a specified interface, or all interfaces.

Command Syntax `show ipv6 mld interface (IFNAME|)`

`show ipv6 mld (vrf NAME|) interface (IFNAME|)`

Parameters `vrf` Indicates the `vrf` keyword.

`NAME` Displays the VRF name..

`IFNAME` Interface name for which to display local information.

Command Mode

Exec mode and Privileged Exec mode

Entry	Description
Interface	The type and name of the interface. (eth1, xe3/1, ge3, etc.).
MLD Enabled	Whether MLD is enabled on the interface.
Internet address	IPv6 internet address.
MLD interface	Number of group-record states.
MLD activity	MLD activity of the interface. In the example above, there is no activity.

MLD query interval	The amount of time between MLD queries.

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following displays MLD interface status on all interfaces enabled for MLD.

```
#show ipv6 mld interface
Interface eth1 (Index 2)
 MLD Enabled, Active, Querier, Version 2 (default)
 Internet address is fe80::2fd:6cff:fe1c:b
 MLD interface has 0 group-record states
 MLD activity: 0 joins, 0 leaves
 MLD query interval is 125 seconds
 MLD querier timeout is 255 seconds
 MLD max query response time is 10 seconds
 Last member query response interval is 1000 milliseconds
 Group Membership interval is 260 seconds
#
```

Table 3-177: Show ipv6 mld interface output

Table 3-177: Show ipv6 mld interface output (Continued)

Entry	Description
MLD query timeout	The amount of time before the interface resends an MLD query.
MLD max query response time	The amount of time before the interface is considered no longer a multicast listener and is removed from the multicast.
Last member query response interval	The time in which if no query requests are received by the router, it assumes the multicast is over.
Group membership interval	The amount of time the router will wait for a group query before the group is considered gone.

show ipv6 mld ssm-map

Use this command to display MLD SSM (source-specific-multicast) mapping.

Command Syntax `show ipv6 mld ssm-map show ipv6 mld ssm-map X:X::X:X show ipv6 mld (vrf NAME|) ssm-map X:X::X:X`

Parameters

`vrf`	Indicates the `vrf` keyword.
`NAME`	Displays the VRF name.
`X:X::X:X`	Displays the multicast group address.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following is an example of this command:

```
#show ipv6 mld ssm-map
SSM Mapping : Enabled
Database    : None configured

#
```

CHAPTER 4 L2 IGMP Snooping Multicast Commands

This chapter describes commands for Internet Group Management Protocol (IGMP) multicast snooping.

- igmp snooping
- igmp snooping fast-leave
- igmp snooping mrouter
- igmp snooping querier
- igmp snooping report-suppression
- igmp snooping static-group
- show igmp snooping interface
- show igmp snooping groups
- show igmp snooping mrouter
- show igmp snooping statistics

igmp snooping

Use this command to enable IGMP Snooping. When this command is given in the Configure mode, IGMP snooping is enabled at switch level on all the vlans in switch. When this command is given at the VLAN interface level, IGMP Snooping is enabled for that VLAN.

Note:IGMP Snooping can be only enabled/disabled on VLAN interfaces.

Use the `no` parameter with this command to globally disable IGMP Snooping, or for the specified interface.

Command Syntax `igmp`

```
snooping no igmp
snooping
```

Parameter

None

Default

IGMP Snooping is enabled.

Command Mode

Interface mode for VLAN interface

Configuration mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#igmp snooping
(config)#interface vlan1.1
(config-if)#igmp snooping
```

igmp snooping fast-leave

Use this command to enable IGMP Snooping fast-leave processing. Fast-leave processing is analogous to immediateleave processing; the IGMP group-membership is removed as soon as an IGMP leave group message is received without sending out a group-specific query.

Use the `no` parameter with this command to disable fast-leave processing.

Command Syntax `igmp snooping`

```
fast-leave no igmp snooping
fast-leave
```

Parameters

None

Default

IGMP Snooping fast-leave processing is disabled.

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced before SWMRE version 1.3.

Example

This example shows how to enable fast-leave processing on a VLAN.

```
#configure terminal
(config)#interface vlan1.1
(config-if)#igmp snooping fast-leave
```

igmp snooping mrouter

Use this command to statically configure the specified VLAN constituent interface as a multicast router interface for IGMP Snooping in that VLAN.

Use the `no` parameter with this command to remove the static configuration of the interface as a multicast router interface.

Command Syntax `igmp snooping mrouter interface`

```
IFNAME  no  igmp  snooping  mrouter  interface
IFNAME
```

Parameter

`IFNAME`	Specify the name of the interface.

Default

IGMP Snooping mrouter processing is disabled.

Command Mode

Interface mode for VLAN interface.

Applicability

This command was introduced before SWMRE version 1.3.

Example

This example shows interface fe8 statically configured to be a multicast router interface.

```
#configure terminal
(config)#interface vlan1.1
(config-if)#igmp snooping mrouter interface fe8
```

igmp snooping querier

Use this command to enable IGMP snooping querier functionality on a VLAN when IGMP is not enabled on the particular VLAN. When enabled, the IGMP Snooping querier sends out periodic IGMP queries for all interfaces on that VLAN.

The IGMP Snooping querier uses the 0.0.0.0 source IP address, because it only masquerades as a proxy IGMP querier for faster network convergence. It does not start, or automatically cease, the IGMP Querier operation if it detects query message(s) from a multicast router. It restarts as the IGMP Snooping querier if no queries are seen within the other querier interval.

Use the `no` parameter with this command to disable IGMP querier configuration.

Command Syntax `igmp snooping querier no igmp snooping querier`

Default

By default, Querier is disabled

Parameters

None

Command Mode

Interface mode for VLAN interface.

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface vlan1.1
(config-if)#igmp snooping querier
```

igmp snooping report-suppression

Use this command to enable report suppression for IGMP version 1, 2 and 3 reports. By default report suppression is enabled.

Use the `no` parameter with this command to disable report suppression.

Command Syntax `igmp snooping report-suppression no igmp snooping report-suppression`

Default

By default, report suppression is enabled.

Parameters

None

Command Mode

Interface mode for VLAN interface.

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface vlan1.1
(config-if)#igmp snooping report-suppression
```

igmp snooping static-group

Use this command to statically configure group membership entries on an interface
Use the `no` parameter with this command to disable report suppression.

Command Syntax `igmp snooping static-group A.B.C.D interface IFNAME no igmp snooping static-group A.B.C.D interface IFNAME igmp snooping static-group A.B.C.D source A.B.C.D interface IFNAME no igmp snooping static-group A.B.C.D source A.B.C.D interface IFNAME`

Parameters

`IFNAME`	Specify the name of the interface.
`A.B.C.D`	Specify the IP address In case of static-group, Multicast Address to be Joined. In case of source, Source Address to be Joined.

Command Mode

Interface mode for VLAN interface.

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#conf t
(config)#interface vlan1.1
(config-if)#igmp snooping static-group 230.0.0.1 interface xe2
(config-if)#igmp snooping static-group 230.0.0.1 source 10.10.10.10 interface
xe1
(config-if)#exit
(config)#exit
```

show igmp snooping interface

Use this command to know querier, fast-leave, report-suppression is enabled/disabled on that particular interface.

Command Syntax `show igmp snooping interface IFNAME`

Parameters

`IFNAME`	Specify the name of the interface.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following command displays the multicast router interfaces in VLAN 1.1.

```
#sh igmp snooping interface
Global IGMP Snooping information
IGMP Snooping Enabled
IGMPv1/v2 Report suppression Enabled IGMPv3
Report suppression Enabled

IGMP Snooping information for vlan1.1
IGMP Snooping enabled
Snooping Querier none
IGMP Snooping other querier timeout is 255 seconds
Group Membership interval is 260 seconds
IGMPv2 fast-leave is disabled
IGMPv1/v2 Report suppression enabled
IGMPv3 Report suppression enabled
Router port detection using IGMP Queries
Number of router-ports: 0
Number of Groups: 0
Number of v1-reports: 0
Number of v2-reports: 0
Number of v2-leaves: 0 Number of
v3-reports: 0
Active Ports:   xe5/1

IGMP Snooping information for vlan1.2
IGMP Snooping enabled Snooping Querier enabled,
address 0.0.0.0, Version 3
Querier interval: 125 seconds
Querier Last member query interval: 1000 milliseconds
```

```
IGMP Snooping maximum query response time is 10 seconds
IGMP Snooping Startup query interval is 31 seconds
Querier robustness: 2
IGMP Snooping other querier timeout is 255 seconds
Group Membership interval is 260 seconds
IGMPv2 fast-leave is disabled
IGMPv1/v2 Report suppression enabled
IGMPv3 Report suppression enabled
Router port detection using IGMP Queries
Number of router-ports: 0
Number of Groups: 0
Number of v1-reports: 0
Number of v2-reports: 0
Number of v2-leaves: 0 Number of v3-reports: 0
Active Ports:
  xe5/1
```

show igmp snooping groups

Use this command to display the multicast groups learnt through snooping or statically configured.

Command Syntax `show igmp snooping groups show igmp snooping groups details show igmp snooping groups A.B.C.D show igmp snooping groups A.B.C.D detail show igmp snooping groups IFNAME show igmp snooping groups IFNAME A.B.C.D show igmp snooping groups IFNAME A.B.C.D detail show igmp snooping groups IFNAME detail`

Parameters

`A.B.C.D`	Specify multicast group address.
`IFNAME`	Specify the name of the interface.
`detail`	IGMPv3 source information.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show igmp snooping groups
IGMP Snooping Group Membership
Group source list: (R - Remote, S - Static)
Vlan   Group/Source Address    Interface      Flags   Uptime     Expires  Last
Reporter   Version
200    230.0.0.1               xe1            S      00:02:07   static   0.0.0.0
V3
#show igmp snooping groups detail
IGMP Snooping Group Membership Details
Flags: (R - Remote, S - Static)

Interface:      xe1
Group:          230.0.0.1
Flags:          S
Uptime:         00:02:08
Group mode:     Exclude (Static)
Last reporter:  0.0.0.0
Source list is empty

#show igmp snooping groups 230.0.0.1
IGMP Snooping Group Membership
Group source list: (R - Remote, S - Static)
Vlan   Group/Source Address    Interface      Flags   Uptime     Expires  Last
Reporter   Version
```

```
      200    230.0.0.1               xe1            S      00:02:35   static   0.0.0.0
V3
      #show igmp snooping groups 230.0.0.1 detail
      IGMP Snooping Group Membership Details
      Flags: (R - Remote, S - Static)

      Interface:      xe1
      Group:          230.0.0.1
      Flags:          S
      Uptime:         00:02:37
      Group mode:     Exclude (Static)
      Last reporter:  0.0.0.0
      Source list is empty

      #show igmp snooping groups vlan1.200
      IGMP Snooping Group Membership
      Group source list: (R - Remote, S - Static)
      Vlan   Group/Source Address    Interface      Flags   Uptime     Expires  Last
Reporter   Version
      200    230.0.0.1               xe1            S      00:02:47   static   0.0.0.0
V3
      #show igmp snooping groups vlan1.200 detail
      IGMP Snooping Group Membership Details
      Flags: (R - Remote, S - Static)

      Interface:      xe1
      Group:          230.0.0.1
      Flags:          S
      Uptime:         00:02:50
      Group mode:     Exclude (Static)
      Last reporter:  0.0.0.0
      Source list is empty
```

Table 4-178: Show igmp snooping groups

Entries	Description
Interface	The interface (port) on the multicast router that is marked as taking place in the multicast.
Group	The multicast group identified by an IPv4 address.
Flags	S - Member is statically configured, R - Member is learned from the network.
Uptime	How long the member has been a part of the group.

Group mode	As stated.

Table 4-178: Show igmp snooping groups (Continued)

Entries	Description
Last reporter	In IGMPv3, a host can send a membership report that includes a list of source addresses. When the host sends a membership report in INCLUDE mode, the host is interested in group multicast traffic only from those sources in the source address list. If host sends a membership report in EXCLUDE mode, the host is interested in group multicast traffic from any source except the sources in the source address list. A host can also send an EXCLUDE report in which the source-list parameter is empty, which is known as an EXCLUDE NULL report. An EXCLUDE NULL report indicates that the host wants to join the multicast group and receive packets from all sources.
Vlan	VLAN number ID.
Group/Source Address	Multicast group and source addresses.
Interface	The interface (port) on the multicast router that is marked as taking place in the multicast.
Flags	S - Member is statically configured, R - Member is learned from the network.
Uptime	How long the member has been a part of the group.

© Symanitron Proprietary

Expires	Either by a timeout (IGMPv1) or by checking whether the member is still a part of the multicast (IGMPv2 or v3). Can also be statically configured.
Last Reporter	Indicates that the host wants to join a particular multicast group.
Version	IGMP version (v1, v2, or v3).

show igmp snooping mrouter

Use this command to display the multicast router interfaces, both configured and learned, in a VLAN.

Command Syntax `show igmp snooping mrouter IFNAME`

Parameters

`IFNAME` Specify the name of the interface.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following command displays the multicast router interfaces in VLAN 1.1.

```
#show igmp snooping mrouter vlan1.1
VLAN    Interface             IP-address    Expires
1         xe1(static)
```

show igmp snooping statistics

Use this command to display IGMP Snooping statistics data.

Command Syntax `show igmp snooping statistics interface IFNAME`

Parameters

`IFNAME`	Specify the name of the interface.

Command Mode

Exec and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show igmp snooping statistics interface vlan1.1
IGMP Snooping statistics for vlan1.1
Group Count             :  1
IGMPv1 reports received  :   0
IGMPv2 reports received    : 0
IGMPv2 leaves received   :   0
IGMPv3 reports received    : 0
IGMPv1 query warnings   :  0
IGMPv2 query warnings   :  0
IGMPv3 query warnings   :  0
```

CHAPTER 5 L2 MLD Snooping Commands

This chapter describes commands for Multicast Listener Discovery (MLD) snooping.

- mld snooping
- mld snooping fast-leave
- mld snooping mrouter
- mld snooping querier
- mld snooping report-suppression
- show debugging mld
- show mld snooping mrouter
- show mld snooping statistics

mld snooping

Use this command to enable MLD Snooping. When this command is given in the Configure mode, MLD Snooping is enabled at the switch level. When this command is given at the VLAN interface level, MLD Snooping is enabled for that VLAN.

Use the `no` parameter with this command to globally disable MLD Snooping, or for the specified interface.

Command Syntax `mld snooping`

```
mld (vrf NAME|) snooping no
mld snooping no mld (vrf
NAME|) snooping
```

Parameter

`vrf`	Specify the VRF name.

Default

MLD Snooping is enabled.

Command Mode

Configure mode and Interface mode for VLAN interface

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#mld snooping
(config)#interface vlan1.1
(config-if)#mld snooping
```

mld snooping fast-leave

Use this command to enable MLD Snooping fast-leave processing. Fast-leave processing is analogous to immediateleave processing; the MLD group-membership is removed, as soon as an MLD leave group message is received without sending out a group-specific query.

Use the `no` parameter with this command to disable fast-leave processing.

Command Syntax `mld snooping`

```
fast-leave no mld snooping
fast-leave
```

Parameters

None

Default

MLD Snooping fast-leave processing is disabled.

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced before SWMRE version 1.3.

Example

This example shows how to enable fast-leave processing on a VLAN.

```
#configure terminal
(config)#interface vlan1.1
(config-if)#mld snooping fast-leave
```

mld snooping mrouter

Use this command to statically configure the specified VLAN constituent interface as a multicast router interface for MLD Snooping in that VLAN.

Use the `no` parameter with this command to remove the static configuration of the interface as a multicast router interface.

Command Syntax `mld snooping mrouter interface`

```
IFNAME  no  mld  snooping  mrouter  interface
IFNAME
```

Parameters

```
IFNAME      Specify the name of the interface.
```

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced before SWMRE version 1.3.

Example

This example shows how to specify the next-hop interface to the multicast router.

```
#configure terminal
(config)#interface vlan1.1
(config-if)#mld snooping mrouter interface fe8
```

mld snooping querier

Use this command to enable MLD querier operation on a subnet (VLAN) when no multicast routing protocol is configured in the subnet (VLAN). When enabled, the MLD Snooping querier sends out periodic MLD queries for all interfaces on that VLAN.

The MLD Snooping querier uses the 0.0.0.0 source IP address, because it masquerades as a proxy

MLD querier for faster network convergence. It does not start or automatically cease the MLD querier operation if it detects a query message from a multicast router. It restarts as MLD snooping querier if no queries are seen within another querier interval.

Note: This command can only be configured on VLAN interfaces.

Use the `no` parameter with this command to disable MLD querier configuration.

Command Syntax `mld snooping`

`querier no mld snooping`

`querier`

Default

By default MLD snooping querier is disabled

Parameters

None

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface vlan1.1
(config-if)#mld snooping querier
```

mld snooping report-suppression

Use this command to enable report suppression for MLD version 1.

Note:MLD Snooping command can only be configured on VLAN interfaces.

Use the `no` parameter to disable report suppression.

Command Syntax `mld snooping report-suppression no mld snooping report-suppression`

Default

By default, mld snooping report suppression is enabled

Parameters

None

Default

Report suppression does not apply to MLDv2, so it is turned off by default for MLDv1 reports.

Command Mode

Interface mode for VLAN interface

Applicability

This command was introduced before SWMRE version 1.3.

Example

This example shows how to enable report suppression for MLDv1 reports.

```
#configure terminal
(config)#interface vlan1.1
(config-if)#mld version 1
(config-if)#mld snooping report-suppression
```

show debugging mld

Use this command to display debugging information for MLD.

Command Syntax `show debugging mld show debugging mld (vrf NAME|)`

Parameters `vrf` Indicates the `vrf` keyword.

`NAME` Displays the VRF name.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following is a sample output of the `show debugging mld` command:

```
#show debugging nsm show debugging mld
MLD Debugging status:
  MLD Decoder debugging is off
  MLD Encoder debugging is off
  MLD Events debugging is off
  MLD FSM debugging is off
  MLD Tree-Info-Base (TIB) debugging is off
#
```

show mld snooping mrouter

Use this command to display the multicast router interfaces, both configured and learned, in a VLAN.

Command Syntax `show mld snooping mrouter IFNAME show mld (vrf NAME|) snooping mrouter IFNAME`

Parameters `vrf` Indicates the `vrf` keyword.

`NAME` Displays the VRF name..

`IFNAME` The name of the VLAN interface

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following displays the multicast router interfaces in VLAN 1.1

```
#show mld snooping mrouter vlan1.1
VLAN    Interface
1       ge9
1       ge11
```

show mld snooping statistics

Use this command to display MLD Snooping statistics data.

Command Syntax `show mld snooping statistics interface IFNAME show mld (vrf NAME|)`

`snooping statistics interface IFNAME`

Parameters

`vrf`	Indicates the `vrf` keyword.
`NAME`	Displays the VRF name.
`IFNAME`	The name of the VLAN interface

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following displays MLDv2 statistical information for the ge10 interface.

```
#show mld snooping statistics ge10
Interface:      ge10
Group:          ff1e::10
Uptime:         00:00:13
Group mode:     Include
Last reporter:  fe80::202:b3ff:fef0:79d8
Group source list: (R - Remote, M - SSM Mapping)
  Source Address        Uptime    v2 Exp    Fwd  Flags
  7ffe::4               00:00:13  00:04:06  Yes  R #
```

© Symanitron Proprietary

Protocol Independent Multicasting Command Reference

Contents

This document contains these chapters:

- Chapter 1, *PIMv4 Commands*
- Chapter 2, *PIMv6 Commands*

CHAPTER 1 PIMv4 Commands

The chapter includes the commands that support the Protocol-Independent Multicast (PIM).

- clear ip mroute
- clear ip msdp peer
- clear ip msdp sa-cache
- clear ip pim sparse-mode
- debug ip pim
- debug ip pim packet
- debug pim all
- debug ip pim timer assert
- debug ip pim timer bsr
- debug ip pim timer hello
- debug ip pim timer joinprune
- debug ip pim timer register
- ip msdp default-peer
- ip msdp mesh-group
- ip msdp originator-id
- ip msdp password
- ip msdp peer
- ip pim accept-register
- ip pim anycast-rp
- ip pim bsr-border
- ip pim bsr-border
- ip pim bsr-candidate
- ip pim cisco-register-checksum
- ip pim
- ip pim passive
- ip pim dr-priority
- ip pim exclude-genid
- ip pim exclude-genid
- ip pim hello-holdtime
- ip pim hello-interval
- ip pim ignore-rp-set-priority
- ip pim jp-timer
- ip pim neighbor-filter

- ip pim propagation-delay
- ip pim register-rate-limit
- ip pim register-rp-reachability
- ip pim register-source
- ip pim register-suppression
- ip pim router-id
- ip pim rp-address
- ip pim rp-candidate
- ip pim rp-register-kat
- ip pim spt-threshold
- ip pim ssm
- ip pim state-refresh origination-interval
- ip pim unicast-bsm
- show debugging ip pim
- show debugging pim
- show ip msdp peer
- show ip msdp sa-cache
- show ip pim interface • show ip pim mroute
- show ip pim neighbor
- show ip pim nexthop
- show ip pim bsr-router
- show ip pim local-members
- show ip pim rp-hash
- show ip pim rp mapping
- snmp restart pim
- undebug all ip pim

clear ip mroute

Use this command to delete all multicast route table entries and all multicast routes at the PIM protocol level.

Command Syntax `clear ip mroute * clear ip mroute * pim (dense-mode|sparse-mode) clear ip mroute A.B.C.D clear ip mroute A.B.C.D A.B.C.D clear ip mroute A.B.C.D A.B.C.D pim (dense-mode|sparse-mode) clear ip mroute A.B.C.D pim sparse-mode clear ip mroute statistics * clear ip mroute statistics A.B.C.D clear ip mroute statistics A.B.C.D A.B.C.D clear ip mroute (vrf NAME|) * clear ip mroute (vrf NAME|) * pim (dense-mode|sparse-mode) clear ip mroute (vrf NAME|) A.B.C.D clear ip mroute (vrf NAME|) A.B.C.D A.B.C.D clear ip mroute (vrf NAME|) A.B.C.D A.B.C.D pim (dense-mode|sparse-mode) clear ip mroute (vrf NAME|) A.B.C.D pim sparse-mode`

clear ip mroute (vrf NAME|) statistics * clear ip mroute (vrf NAME|) statistics A.B.C.D clear ip mroute (vrf NAME|) statistics A.B.C.D A.B.C.D

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
*	Delete all multicast routes
pim	Protocol Independent Multicast (PIM)
A.B.C.D	Clears group IP address
A.B.C.D	Clears source IP address
dense-mode	Clears multicast rout table for PIM dense-mode
sparse-mode	Clears multicast route table for PIM sparse mode
statistics	Clears multicast route statistics

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear ip mroute * pim sparse-mode
#clear ip mroute 224.2.2.2 4.4.4.4 pim sparse-mode
```

clear ip msdp peer

Use this command to clear the TCP connection to a Multicast Source Discovery Protocol (MSDP) peer.

This command closes the TCP connection to the peer, resets all the MSDP peer statistics, and clears the input and output queues to and from the MSDP peer.

Command Syntax `clear ip msdp peer (A.B.C.D|)`

```
clear ip msdp (vrf NAME|) peer (A.B.C.D|)
```

Parameters

`A.B.C.D`	IPv4 address of peer
`NAME`	Name of the VPN routing/forwarding instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear ip msdp peer 192.168.1.26
```

clear ip msdp sa-cache

Use this command to clear Multicast Source Discovery Protocol (MSDP) Source-Active (SA) cache entries.

Command Syntax `clear ip msdp sa-cache (A.B.C.D |) clear ip msdp (vrf NAME|) sa-cache (A.B.C.D |)`

Parameters

`A.B.C.D`	Multicast group address; if not specified, all SA cache entries are cleared
`NAME`	Name of the VPN routing/forwarding instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear ip msdp sa-cache 225.25.25.1
```

clear ip pim sparse-mode

Use this command to clear all rendezvous point (RP) sets learned through the PIMv2 Bootstrap Router (BSR).

Command Syntax `clear ip pim sparse-mode bsr rp-set *`

```
clear ip pim (vrf NAME|) sparse-mode bsr rp-set *
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`rp-set`	PIMv2 bootstrap router RP set
`bsr`	PIMv2 Bootstrap Router
`*`	Clear all RP sets

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear ip pim sparse-mode bsr rp-set *
```

debug ip pim

Use this command to enable debugging for PIM.

Use the `no` option with this command to deactivate debugging for PIM.

Command Syntax `debug ip pim`

```
(all|events|mfc|mib|mtrace|msdp|nexthop|nsm|packet|state|timer) debug ip
pim (vrf
  NAME|)(all|events|mfc|mib|mtrace|msdp|nexthop|nsm|packet|state|timer) no
debug ip pim (all|events|mfc|mib|mtrace|msdp|nexthop|nsm|packet|state|timer)
no debug ip pim (vrf NAME|)
(all|events|mfc|mib|mtrace|msdp|nexthop|nsm|packet |state|timer)
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`all`	Enable debugging for all PIM events
`events`	Enable debugging for general configuration, Virtual Routing (VR), and VRF context
`mfc`	Enable debugging for MFC updates
`mib`	Enable debugging for MIB entries
`mtrace`	Enable debugging for MTRACE messages
`msdp`	Enable debugging for MSDP

nexthop	Enable debugging for Reverse Path Forwarding (RPF) neighbor nexthop cache handling
nsm	Enable debugging for NSM
packet	Enable debugging for PIM packets
state	Enable debugging for PIM states
timer	Enable debugging for PIM timers

Default

By default, all debug options are disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#debug ip pim all
```

debug ip pim packet

Use this command to activate debugging of incoming or outgoing PIM packets.

Use the `no` option with this command to deactivate debugging of incoming or outgoing PIM packets.

Command Syntax `debug ip pim packet debug ip pim packet in debug ip pim packet out debug ip pim (vrf NAME|) packet debug ip pim (vrf NAME|) packet in debug ip pim (vrf NAME|) packet out no debug ip pim packet no debug ip pim packet in no debug ip pim packet out no debug ip pim (vrf NAME|) packet no debug ip pim (vrf NAME|) packet in no debug ip pim (vrf NAME|) packet out`

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
in	Debug incoming packets
out	Debug outgoing packets

Default

By default, all debug options are disabled.

Command Mode

Configure and Exec modes

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#debug ip pim packet in
```

debug pim all

Use this command to enable debugging of all PIM events.

Use the `no` option with this command to disable debugging for PIM.

Command Syntax `debug pim all debug pim (vrf NAME|) all no debug pim all no debug pim (vrf NAME|) all`

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance

Default

By default, all debug options are disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#debug pim all
```

debug ip pim timer assert

Use this command to enable debugging of the PIM assert timers.

Use the `no` option with this command to disable debugging for PIM assert timers.

Command Syntax `debug ip pim timer assert debug ip pim timer assert at debug ip pim (vrf NAME|) timer assert debug ip pim (vrf NAME|) timer assert at no debug ip pim timer assert no debug ip pim timer assert at no debug ip pim (vrf NAME|) timer assert no debug ip pim (vrf NAME|) timer assert at`

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`at`	Use this option to turn on or off debugging of the PIM Assert Timer

Default

By default, all debug options are disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#debug ip pim timer assert at
```

debug ip pim timer bsr

Use this command to enable debugging of PIM BSR time.

Use the `no` option with this command to disable debugging of the PIM BSR timer.

Command Syntax `debug ip pim timer bsr debug ip pim timer bsr bst debug ip pim timer bsr crp debug ip pim (vrf NAME|) timer bsr debug ip pim (vrf NAME|) timer bsr bst debug ip pim (vrf NAME|) timer bsr crp no debug ip pim timer bsr no debug ip pim timer bsr bst no debug ip pim timer bsr crp no debug ip pim (vrf NAME|) timer bsr no debug ip pim (vrf NAME|) timer bsr bst no debug ip pim (vrf NAME|) timer bsr crp`

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`bst`	Turn on or turn off the bootstrap debugging timer
`crp`	Turn on or turn off the Candidate-RP debugging timer

Default

By default, all debug options are disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#debug ip pim timer bsr bst
```

debug ip pim timer hello

Use this command to enable debugging of various PIM Hello timers.

Use the `no` option with this command to disable debugging of the PIM Hello timers.

Command Syntax `debug ip pim timer hello debug ip pim timer hello ht debug ip pim timer hello nlt debug ip pim timer hello tht debug ip pim (vrf NAME|) timer hello debug ip pim (vrf NAME|) timer hello ht debug ip pim (vrf NAME|) timer hello nlt debug ip pim (vrf NAME|) timer hello tht no debug ip pim timer hello no debug ip pim timer hello ht no debug ip pim timer hello nlt no debug ip pim timer hello tht no debug ip pim (vrf NAME|) timer hello no debug ip pim (vrf NAME|) timer hello ht no debug ip pim (vrf NAME|) timer hello nlt no debug ip pim (vrf NAME|) timer hello tht`

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`ht`	Turn on or turn off the PIM Hello debugging timer (ht)
`nlt`	Turn on or turn off the PIM Neighbor Liveliness debugging timer (nlt)
`tht`	Turn on or turn off the Triggered Hello Timer (tht)

Default

By default, all debug options are disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
```

```
(config)#debug ip pim timer hello ht
```

debug ip pim timer joinprune

Use this command to enable debugging of various PIM JoinPrune timers.

Use the no option with this command to disable the debugging of the PIM JoinPrune timers.

Command Syntax `debug ip pim timer joinprune debug ip pim timer joinprune et debug ip pim timer joinprune kat debug ip pim timer joinprune jt debug ip pim timer joinprune ot debug ip pim timer joinprune ppt debug ip pim (vrf NAME|) timer joinprune debug ip pim (vrf NAME|) timer joinprune et debug ip pim (vrf NAME|) timer joinprune kat debug ip pim (vrf NAME|) timer joinprune jt debug ip pim (vrf NAME|) timer joinprune ot debug ip pim (vrf NAME|) timer joinprune ppt no debug ip pim timer joinprune no debug ip pim timer joinprune et no debug ip pim timer joinprune kat no debug ip pim timer joinprune jt no debug ip pim timer joinprune ot no debug ip pim timer joinprune ppt no debug ip pim (vrf NAME|) timer joinprune no debug ip pim (vrf NAME|) timer joinprune et no debug ip pim (vrf NAME|) timer joinprune kat no debug ip pim (vrf NAME|) timer joinprune jt no debug ip pim (vrf NAME|) timer joinprune ot no debug ip pim (vrf NAME|) timer joinprune ppt`

Parameters

Default

By default, all debug options are disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`et`	Turn on or turn off the PIM JoinPrune expiry timer (et)
`jt`	Turn on or turn off the PIM JoinPrune upstream Join Timer (jt)
`kat`	Turn on or turn off the PIM JoinPrune Keep Alive timer (kat)
`ot`	Turn on or turn off the PIM JoinPrune Upstream Override Timer (ot)
`ppt`	Turn on or turn off the PIM JoinPrune PrunePending Timer ((ppt)

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#debug ip pim timer joinprune et
```

debug ip pim timer register

Use this command to enable the PIM register timer's debugging.

Use the no option with this command to disable the PIM register timer's debugging.

Command Syntax `debug ip pim timer register debug ip pim timer register rst debug ip pim (vrf NAME|) timer register debug ip pim (vrf NAME|) timer register rst no debug ip pim timer register no debug ip pim timer register rst no debug ip pim (vrf NAME|) timer register no debug ip pim (vrf NAME|) timer register rst`

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`rst`	Turn on or turn off the PIM Register Stop Timer (rst)

Default

By default, all debug options are disabled.

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#debug ip pim timer register
```

ip msdp default-peer

Use this command to set a Multicast Source Discovery Protocol (MSDP) peer from which to accept Source-Active (SA) messages.

You can have multiple active default peers:

- When you enter multiple `ip msdp default-peer` commands *with* a `prefix-list` keyword, all the default peers are used at the same time for different RP prefixes. This form is typically used in a service provider cloud that connects stub site clouds.
- When you enter multiple `ip msdp default-peer` commands *without* a `prefix-list` keyword, a single active peer accepts all SA messages. If that peer fails, the next configured default peer accepts all SA messages. This form is typically used at a stub site.

Use the `no` option with this command to stop accepting SA messages from a peer.

Command Syntax `ip msdp default-peer A.B.C.D (prefix-list WORD|) ip msdp (vrf NAME|) default-peer A.B.C.D (prefix-list WORD|) no ip msdp default-peer A.B.C.D no ip msdp (vrf NAME|) default-peer A.B.C.D`

Parameters

`A.B.C.D`	IPv4 address of a previously configured MSDP peer
`prefix-list`	Make this the default peer only for an access list of rendezvous points (RPs):
`WORD`	Access list name
`NAME`	Name of the VPN routing/forwarding instance

Default

The IPv4 multicast forwarding is disabled by default

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ip msdp default-peer 192.168.1.26 prefix-list xyz
```

ip msdp mesh-group

Use this command to add a Multicast Source Discovery Protocol (MSDP) peer to a mesh group.

You can set up multiple mesh groups on the same device and multiple peers per mesh group.

Use the `no` option with this command to remove a peer from a mesh group.

Command Syntax `ip msdp mesh-group WORD A.B.C.D ip msdp (vrf NAME|) mesh-group WORD A.B.C.D no ip msdp mesh-group WORD A.B.C.D no ip msdp (vrf NAME|) mesh-group WORD A.B.C.D`

Parameters

`WORD`	Name of the mesh group
`A.B.C.D`	IPv4 address of peer
`NAME`	Name of the VPN routing/forwarding instance

Default

The IPv4 multicast forwarding is disabled by default

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ip msdp mesh-group mg-1 192.168.1.26
```

ip msdp originator-id

Use this command to allow a Multicast Source Discovery Protocol (MSDP) speaker that originates a Source-Active (SA) message to use the IP address of an interface as a rendezvous point (RP) address in the SA message.

By default, SWMRE uses the RP address of the device.

Use the `no` option with this command to use the RP address of the device in SA messages.

Command Syntax `ip msdp originator-id IFNAME ip msdp (vrf NAME|) originator-id IFNAME no ip msdp originator-id IFNAME no ip msdp (vrf NAME|) originator-id IFNAME`

Parameters

`IFNAME`	Use the IP address of this interface as an RP address in SA messages
`NAME`	Name of the VPN routing/forwarding instance

Default

The RP address is used as the originator ID.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ip msdp originator-id eth2
```

ip msdp password

Use this command to set an MD5-shared password key used for authenticating a Multicast Source Discovery Protocol (MSDP) peer. By default, no MD5 password is enabled.

Use the `no` option with this command to remove a password.

Command Syntax `ip msdp password WORD peer A.B.C.D ip msdp (vrf NAME|) password WORD peer A.B.C.D no ip msdp password WORD peer A.B.C.D no ip msdp (vrf NAME|) password WORD peer A.B.C.D`

Parameters

`WORD`	Password
`A.B.C.D`	IPv4 address of peer
`NAME`	Name of the VPN routing/forwarding instance

Default

The MD5 password authentication for TCP connections between MSDP peer is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ip msdp password S#m*u104!! peer 192.168.1.26
```

ip msdp peer

Use this command to configure an Multicast Source Discovery Protocol (MSDP) peer relationship.

Use the `no` option with this command to remove a peer relationship.

Command Syntax `ip msdp peer A.B.C.D ((connect-source (IFNAME))|) ip msdp (vrf NAME|) peer A.B.C.D ((connect-source (IFNAME))|) ip msdp peer A.B.C.D connect-source A.B.C.D ip msdp (vrf Name|) peer A.B.C.D connect-source A.B.C.D no ip msdp peer A.B.C.D no ip msdp (vrf NAME|) peer A.B.C.D`

Parameters

`A.B.C.D`	IP address of the potential peer
`A.B.C.D`	IP address of local peer
`IFNAME`	Use the primary address of this interface for the TCP connection with the peer
`NAME`	Name of the VPN routing/forwarding instance

Default

By default, all ip msdp options are disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ip msdp peer 192.168.1.26 connect-source eth2
```

ip pim accept-register

Use this command to configure the ability to filter out multicast sources specified by the given access-list at the RP, so that the RP will accept/refuse to perform the Register mechanism for the packets sent by the specified sources. By default, the RP accepts Register packets from all multicast sources.

Use the no option with this command to revert to default.

Command Syntax `ip pim accept-register list WORD ip pim (vrf NAME|) accept-register list WORD no ip pim accept-register no ip pim (vrf NAME|) accept-register`

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`WORD`	Name of a standard access list

Default

By default, all ip pim options are disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ip pim accept-register list xyz

(config)#no ip pim accept-register
```

ip pim anycast-rp

Use this command to configure the Anycast RP in the RP set.

Use the no option with this command to remove the configuration.

Command Syntax `ip pim anycast-rp A.B.C.D A.B.C.D ip pim (vrf NAME|) anycast-rp A.B.C.D A.B.C.D no ip pim anycast-rp A.B.C.D no ip pim anycast-rp A.B.C.D A.B.C.D no ip pim (vrf NAME|) anycast-rp A.B.C.D no ip pim (vrf NAME|) anycast-rp A.B.C.D A.B.C.D`

Parameters

`vrf`	The VPN routing/forwarding instance.
`NAME`	Specify the name of the VPN routing/forwarding instance.
`A.B.C.D`	Unicast IP address of the Anycast RP set. An Anycast RP set is a collection of RPs in the same domain.
`A.B.C.D`	Destination IP address where Register messages are copied and sent. A Member RP is an individual RP member in the Anycast RP set.

Default

By default, all ip pim options are disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows how to configure the Anycast RP in the RP set.

```
#configure terminal
(config)#ip pim anycast-rp 1.1.1.1 10.10.10.10
```

The following example shows how to remove the configuration.

```
#configure terminal
(config)#no ip pim anycast-rp 1.1.1.1 10.10.10.10
```

ip pim bsr-border

Use this command to prevent bootstrap router (BSR) messages from being sent or received through an interface.

When this command is configured on an interface, no PIM Version 2 BSR messages are sent or received through the interface. Use this command to configure an interface bordering another PIM domain to avoid the exchange of BSR messages between the two domains. BSR messages should not be exchanged between different domains, because routers in one domain may elect rendezvous points (RPs) in the other domain, resulting in a protocol malfunction or loss of isolation between the domains.

Note: This command does not set up multicast boundaries. It only sets up a PIM domain BSR message border.

Use the `no` option with this command to remove the BSR border configuration.

Command Syntax `ip pim`

`bsr-border no ip pim`

`bsr-border`

Default

By default, the ip pim bsr-border is disabled.

Parameters

None

Default

Bootstrap router border configuration is disabled by default.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example configures the interface to be the PIM domain border:

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim bsr-border

(config)#interface eth0
(config-if)#no ip pim bsr-border
```

ip pim bsr-candidate

Use this command to give the router the candidate BSR status using the specified IP address of the interface.

Use the `no` option with this command to disable this function.

Command Syntax `ip pim bsr-candidate IFNAME ip pim bsr-candidate IFNAME <0-32> ip pim bsr-candidate IFNAME <0-32> <0-255> ip pim (vrf NAME|) bsr-candidate IFNAME ip pim (vrf NAME|) bsr-candidate IFNAME <0-32> ip pim (vrf NAME|) bsr-candidate IFNAME <0-32> <0-255> no ip pim bsr-candidate (IFNAME|) no ip pim (vrf NAME|) bsr-candidate (IFNAME|)`

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`IFNAME`	Specify the name of the interface
`<0-32>`	Specify a hash mask length for RP selection
`<0-255>`	Specify a priority for a BSR candidate

Default

The router is not configured to announce itself as a candidate BSR.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ip pim bsr-candidate eth0 20 30
```

ip pim cisco-register-checksum

Use this command to configure the option to calculate the register checksum over the whole packet. This command is used to inter-operate with older Cisco IOS versions.

Use the no option with this command to revert to the default settings.

Command Syntax `ip pim cisco-register-checksum ip pim cisco-register-checksum group-list WORD ip pim (vrf NAME|) cisco-register-checksum ip pim (vrf NAME|) cisco-register-checksum group-list WORD no ip pim cisco-register-checksum no ip pim cisco-register-checksum group-list WORD no ip pim (vrf NAME|) cisco-register-checksum`

`no ip pim (vrf NAME|) cisco-register-checksum group-list WORD`

Parameters `vrf` The VPN routing/forwarding instance.

`NAME` Specify the name of the VPN routing/forwarding instance.

`group-list` Use this parameter to configure the option to calculate the register checksum over the whole packet on multicast groups specified by the access-list.

`WORD` IP named standard access list.

Default

This command is disabled by default. By default, Register Checksum is calculated only over the header.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ip pim cisco-register-checksum

#configure terminal
(config)#ip pim cisco-register-checksum group-list xyz
(config)#ip access-list 34 permit 224.0.1.3
```

ip pim

Use this command to enable PIM dense-mode or sparse-mode on the current interface.

Use the `no` option with this command to disable PIM dense-mode or sparse-mode or sparse-dense-mode on the interface.

Command Syntax `ip pim (dense-mode|sparse-mode) no ip pim (dense-mode|sparse-mode)`

Parameters `dense-mode` Enable PIM dense-mode operation

`sparse-mode` Enable PIM sparse-mode

Default

By default, the ip pim option is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim dense-mode

(config)#interface eth0
(config-if)#no ip pim dense-mode

(config)#interface eth0
(config-if)#ip pim sparse-mode

(config-if)#no ip pim sparse-mode
```

ip pim passive

Use this command to enable or disable passive mode operation for local members on the interface. Passive mode essentially stops PIM transactions on the interface, allowing only the Internet Group Management Protocol (IGMP) mechanism to be active.

Use the `no` option with this command to disable the passive mode.

Command Syntax `ip pim (dense-mode|sparse-mode) passive no ip pim (dense-mode|sparse-mode) passive`

Parameters `dense-mode` Enable passive operation for PIM dense-mode

`sparse-mode` Enable passive operation for PIM sparse-mode

Default

By default, the ip pim option is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim dense-mode passive

(config)#interface eth0
(config-if)#no ip pim dense-mode passive

#configure terminal
(config)#interface eth0
(config-if)#ip pim sparse-mode passive

(config)#interface eth0
(config-if)#no ip pim sparse-mode passive
```

ip pim dr-priority

Use this command to set the designated router's priority value.

Use the `no` option with this command to remove the priority from the DR.

Command Syntax `ip pim dr-priority <0-4294967294> no ip pim dr-priority (<0-4294967294>|)`

Parameter

`<0-4294967294>` Valid range of values for DR priority, with a higher value resulting in a higher preference

Default

The default DR priority value is 1.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim dr-priority 11234

(config)#interface eth0
```

```
(config-if)#no ip pim dr-priority 11234
```

ip pim exclude-genid

Use this command to exclude the GenID (generated ID) option from Hello packets sent by the PIM module on an interface. This command is used to inter-operate with older Cisco IOS versions.

Use the `no` option with this command to restore PIM to its default setting.

Command Syntax `ip pim exclude-genid no ip pim exclude-genid`

Parameters

None

Default

By default, the ip pim exclude-genid command is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Default

By default, this command is disabled; that is, the GenID option is included.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim exclude-genid

(config)#interface eth0
(config-if)#no ip pim exclude-genid
```

ip pim hello-holdtime

Use this command to configure a hello holdtime other than the default (`3.5 * hello_interval` seconds).

When configuring `hello-holdtime`, if the configured value is less than the current `hello_interval`, it is refused.

When removing a configured `hello_holdtime`, the value is reset to (`3.5 *` current `hello_interval)` value.

Every time the hello_interval is updated, the hello-holdtime is also updated according to rules below:

If the hello_holdtime is not configured, or if the hello_holdtime is configured, but is less than the current hello_interval value, it is modified to (3.5 * hello_interval). Otherwise, the configured value is maintained.

Use the `no` option with this command to remove the configured hello-holdtime.

Command Syntax `ip pim hello-holdtime <1-65535> no ip pim hello-holdtime`

Parameter

`<1-65535>`	Range of values for hello-holdtime, in seconds

Default

The default hello-holdtime is 105 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim hello-holdtime 123

(config)#interface eth0
(config-if)#no ip pim hello-holdtime
```

ip pim hello-interval

Use this command to configure a hello interval value other than the default. When a hello-interval is configured and hello-holdtime is not configured, or when the hello-holdtime value configured is less than the new hello-interval value, the holdtime value is modified to (3.5 * hello_interval). Otherwise, the hello-holdtime value is the configured value.

Use the `no` option with this command to reset the hello-interval to its default value.

Command Syntax `ip pim hello-interval <1-18724> no ip pim hello-interval`

Parameter

`<1-18724>`	Range of values for the hello-interval. No fractional values are allowed in seconds.

Default

The default value for hello-interval is 30 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim hello-interval 123

(config)#interface eth0
(config-if)#no ip pim hello-interval
```

ip pim ignore-rp-set-priority

Use this command to ignore the RP-SET priority value, and use only the hashing mechanism for RP selection. This command is used to inter-operate with older Cisco IOS versions.

Use the `no` option with this command to remove this setting.

Command Syntax `ip pim ignore-rp-set-priority ip pim (vrf NAME|) ignore-rp-set-priority no ip pim ignore-rp-set-priority no ip pim (vrf NAME|) ignore-rp-set-priority`

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance

Default

By default, all ip pim options are disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip pim ignore-rp-set-priority

#configure terminal
(config)#no ip pim ignore-rp-set-priority
```

ip pim jp-timer

Use this command to set a PIM join/prune timer.

Use the `no` option with this command to remove the join/prune timer.

Command Syntax `ip pim jp-timer <1-65535> ip pim (vrf NAME|) jp-timer <1-65535> no ip pim jp-timer no ip pim jp-timer <1-65535> no ip pim (vrf NAME|) jp-timer no ip pim (vrf NAME|) jp-timer <1-65535>`

Parameters `vrf` The VPN routing/forwarding instance

`NAME` Specify the name of the VPN routing/forwarding instance

`<1-65535>` Range of values for the Join/Prune timer, in seconds

Default

The ip pim jp-timer default value is 60 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip pim jp-timer 234

#configure terminal
(config)#no ip pim jp-timer 234
```

ip pim neighbor-filter

Use this command to enable filtering of neighbors on the interface. When configuring a neighbor filter, PIM either not establish adjacency with neighbor or terminates adjacency with existing neighbors, when denied by filtering access list.

Use the `no` option with this command to disable filtering of neighbors on the interface.

Command Syntax `ip pim neighbor-filter WORD no ip pim neighbor-filter WORD`

Parameters

`WORD` Name of an IP standard access list

Default

By default, the ip pim option is disabled.

Command Mode

Interface mode

Default

This command is disabled by default there is no filtering.

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim neighbor-filter xyz
(config-if)#exit
(config)#ip access-list deny 192.168.1.53
(config)#ip access-list permit any
```

ip pim propagation-delay

Use this command to configure a propagation delay value for PIM.

Use the no option with this command to return the propagation delay to its default value.

Command Syntax `ip pim propagation-delay <0-32767> no ip pim propagation-delay`

Parameter

`<0-32767>`	Range of values for propagation delay, in milliseconds

Default

The default propagation delay is 500 milliseconds.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim propagation-delay 1000

(config)#interface eth0
(config-if)#no ip pim propagation-delay
```

ip pim register-rate-limit

Use this command to configure the rate of Register packets sent by this designated router (DR), in number of packets per second.

Use the no option to remove the register-rate-limit configuration.

Note: The configured rate is per (S,G) state, and is not a system-wide rate.

Command Syntax `ip pim register-rate-limit <1-65535> ip pim (vrf NAME|) register-rate-limit <1-65535> no ip pim register-rate-limit <1-65535|> no ip pim (vrf NAME|) register-rate-limit <1-65535|>`

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`<1-65535>`	Range of values for packets to send per second

Default

No rate limit is set for PIM-SM register packets.

Command mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ip pim register-rate-limit 3444

#configure terminal
(config)#no ip pim register-rate-limit
```

ip pim register-rp-reachability

Use this command to enable the RP reachability check for PIM Registers at the DR.

Use the no option to reset to disable the RP reachability check for PIM Registers at the DR.

Note: “ip pim register-rp-reachability” is default configuration and it would not be shown in running-configuration, even if admin configures it. If admin does "no" command of this configuration, it would be shown in runningconfiguration.

Command Syntax `ip pim register-rp-reachability ip pim (vrf NAME|) register-rp-reachability no ip pim register-rp-reachability no ip pim (vrf NAME|) register-rp-reachability`

Parameter

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance

Default

The default setting is checking for rendezvous point reachability,

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ip pim register-rp-reachability
```

ip pim register-source

Use this command to configure the source address of Register packets sent by this DR, overriding the default source address, which is the address of the RPF interface toward the source host.

Use the `no` option to remove the source address of register packets sent by this DR, and reset it to use the default source address, that is, the address of the RPF interface toward the source host.

The configured address must be a reachable address so the RP can send corresponding Register-Stop messages in response. This address is usually the loopback interface address, but can also be other physical addresses. The address must be advertised by unicast routing protocols on the DR. Note: The interface configured does not require PIM to be enabled.

Command Syntax

```
ip pim register-source A.B.C.D ip pim register-source IFNAME ip pim (vrf NAME|)
register-source A.B.C.D ip pim (vrf NAME|)
register-source IFNAME no ip pim register-source (A.B.C.D|) no ip pim register-source (IFNAME|) no ip pim (vrf NAME|) register-source (A.B.C.D|) no ip pim (vrf NAME|) register-source (IFNAME|)
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
A.B.C.D	The IP address to use as the source of the register packets
IFNAME	The name of the interface to use as the source of the register packets

Default

By default, the IP address of the outgoing interface of the DR leading toward the RP is used as the IP source address of a register message.

Command mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ip pim register-source 3.3.3.2
```

ip pim register-suppression

Use this command to configure the register-suppression time, in seconds, overriding the default value of 60 seconds. Configuring this value modifies register-suppression time at the DR; configuring this value at the RP modifies the RPkeepalive-period value if the `ip pim rp-register-kat` command is not used.

Use the no option to remove the register-suppression setting.

Command Syntax `ip pim register-suppression <1-65535> ip pim (vrf NAME|) register-suppression <1-65535> no ip pim register-suppression no ip pim (vrf NAME|) register-suppression`

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`<1-65535>`	Range of values for register suppression time in seconds

Default

By default, the ip pim option is disabled.

Command mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip pim register-suppression 555
```

```
#configure terminal
(config)#no ip pim register-suppression
```

ip pim router-id

Use this command to configure PIM router-ID to uniquely identify the router.By default, PIM registers for the NSM router-id service. This command will override the router-id received from NSM.

Use the `no` option with this command to unconfigure PIM router-ID. This will make PIM fall back to the NSM router-id

Command Syntax `ip pim (vrf NAME|) router-id`

`A.B.C.D no ip pim (vrf NAME|) router-id`

`A.B.C.D`

Parameters `vrf` The VPN routing/forwarding instance

`NAME` Specify the name of the VPN routing/forwarding instance

`A.B.C.D` Specify the Router ID

Default

By default, the ip pim option is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip pim router-id 1.1.1.1

(config)#no ip pim router-id 1.1.1.1
```

ip pim rp-address

Use this command to statically configure Rendezvous Point (RP) address for multicast groups.

Use the `no` option to remove the RP address.

SWMRE PIM supports multiple static RPs. It also supports static-RP and Bootsrtrap Router (BSR) mechanism simultaneously. The following list states the correct usage of this command:

- If RP-address configured through BSR and RP-address configured statically are both available for a group range, the RP-address configured through BSR is chosen over statically configured RP-address.
- One static-RP can be configured for multiple group ranges using Access Lists. However, configuring multiple static RPs (using `ip pim rp-address` command) with the same RP address is not allowed. The static-RP can either be configured for the whole multicast group range `224/4` (without ACL) or for specific group ranges (using ACL). For example, configuring `ip pim rp-address 1.2.3.4` will configure static-RP 1.2.3.4 for the default group range `224/4`. Configuring `ip pim rp-address 5.6.7.8 grp-list` will configure static-RP `5.6.7.8` for all the group ranges represented by `Permit` filters in `grp-list` ACL.

- If multiple static-RPs are available for a group range, then one with the highest IP address is chosen.
- Only `permit` filters in ACL are considered as valid group ranges. The default `Permit` filter `0.0.0.0/0` is converted to default multicast filter `224/4`.
- When selecting static-RPs for a group range, the first element, with the static-RP with highest IP address, is chosen.
- Group mode and RP address mappings learned through BSR take precedence over mappings statistically defined by the `ip pim rp-address` command without the `override` keyword. Commands with the `override` keyword take precedence over dynamically learned mappings.

Command Syntax `ip pim rp-address A.B.C.D (override|) ip pim rp-address A.B.C.D WORD (override|) ip pim (vrf NAME|) rp-address A.B.C.D (override|) ip pim (vrf NAME|) rp-address A.B.C.D WORD (override|) no ip pim rp-address A.B.C.D no ip pim rp-address A.B.C.D WORD no ip pim (vrf NAME|) rp-address A.B.C.D no ip pim (vrf NAME|) rp-address A.B.C.D WORD`

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`WORD`	Access-list name
`override`	Static RP overrides dynamically-learned RP

Default

No PIM static group-to-RP mappings are configured.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
(config)#ip pim rp-address 3.3.3.3 xyz
```


© Symanitron Proprietary

ip pim rp-candidate

Use this command to give the router a candidate RP status using the IP address of the specified interface.

The groups specified will operate in PIM sparse mode; group-list specifies the standard IP access list number or name that defines the group prefixes that are advertised in association with the RP address.

Use the `no` option along with this command to remove the settings.

Command Syntax

```
ip pim rp-candidate IFNAME (bidir|) ((group-list WORD)|) (interval <0-16383>|)
  (priority <0-255>|) ip pim (vrf NAME) rp-candidate IFNAME (bidir|) ((group-list
WORD)|) (interval <0-
  16383>|) (priority <0-255>|) no ip pim
rp-candidate (IFNAME|) no ip pim (vrf
NAME) rp-candidate (IFNAME|)
```

Parameters

`vrf NAME`	The VPN routing/forwarding instance
`IFNAME`	Specify an interface name
`WORD`	A named standard access list
`group-list`	Group Ranges for this C-RP
`interval`	C-RP advertisement interval
`priority`	Candidate-RP priority
`<0-16383>`	Range of values for candidate-RP advertisement interval, in seconds
`<0-255>`	Range of values for priority of an RP candidate

Default

The ip pim rp-candidate default priority is 192 and interval is 60 seconds.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip pim rp-candidate eth0

(config)#no ip pim rp-candidate eth0
```

ip pim rp-register-kat

Use this command to configure a Keepalive Timer (KAT) value for (S,G) states at RP to monitor PIM register packets, overriding the generic KAT timer value. Use the no option to remove this configuration.

Command Syntax `ip pim rp-register-kat <1-65535>`
`ip pim (vrf NAME|) rp-register-kat <1-65535>`
`no ip pim rp-register-kat no ip pim (vrf NAME|) rp-register-kat`

Parameters `vrf` The VPN routing/forwarding instance
`NAME` Specify the name of the VPN routing/forwarding instance
`<1-65535>` Range of values for a KAT time in seconds

Default

The ip pim rp-register-kat default is 60 seconds.

Command mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ip pim rp-register-kat 3454

(config)#no ip pim rp-register-kat
```

ip pim spt-threshold

Use this command to turn on the ability of the last-hop PIM router to switch to SPT.

Use the `no` option with this command to turn off the ability of the last-hop PIM router to switch to SPT.

Note: This option is binary, meaning that the switching to SPT happens either at the receiving of the first data packet or not at all. It is not rate-based.

Command Syntax `ip pim spt-threshold ip pim spt-threshold group-list WORD ip pim (vrf NAME|) spt-threshold ip pim (vrf NAME|) spt-threshold group-list WORD no ip pim spt-threshold no ip pim spt-threshold group-list WORD no ip pim (vrf NAME|) spt-threshold`
`no ip pim (vrf NAME|) spt-threshold group-list WORD`

Parameters `vrf` The VPN routing/forwarding instance

`NAME` Specify the name of the VPN routing/forwarding instance `group-list` Enable the ability for the last-hop PIM router to switch to SPT for multicast group addresses indicated by the given access-list

A named standard access list

Default

When this command is not used, the PIM leaf router joins the shortest path tree immediately after the first packet arrives from a new source.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip pim spt-threshold

#configure terminal
(config)#ip pim spt-threshold group-list LIST1
(config)#ip access-list permit 224.0.1.3

#configure terminal
(config)#no ip pim spt-threshold
```

ip pim ssm

Use this command to configure Source Specific Multicast (SSM) and define the range of multicast IP addresses. The keyword `default` defines the SSM range as 232/8. To define an SSM range other than the default, specify an accesslist.

When an SSM range of IP multicast addresses is defined with this command, the no (*,G) or (S,G,rpt) state is initiated for groups in the SSM range.

The messages corresponding to these states are not accepted and originate in the SSM range.

Use the `no` form of this command to disable the SSM range.

Command Syntax `ip pim ssm default ip`

```
pim ssm range WORD ip pim (vrf
NAME|) ssm default ip pim (vrf
NAME|) ssm range WORD no ip pim
ssm no ip pim (vrf NAME|) ssm
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`default`	This keyword defines the 232/8 group range for SSM
`range`	Define an access-list for group range to use for SSM

A named standard access list

Default

By default, all ip pim options are disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following example shows how to configure SSM service for the IP address range defined by access list 10:

```
#configure terminal
(config)#access-list 10 permit 225.1.1.1
(config)#ip pim ssm range xyz
```

ip pim state-refresh origination-interval

Use this command to configure a PIM-DM State-Refresh origination interval other than the default value. The origination interval is the number of seconds between PIM-DM State Refresh control messages.

Use the `no` option with this command to return the origination interval to its default value.

Command Syntax `ip pim state-refresh origination-interval <1-100> no ip pim state-refresh origination-interval`

Parameter

`<1-100>` Range of values for state-refresh origination interval, in seconds Note: No fractional values are allowed for the interval time.

Default

The default state-refresh origination interval is 60 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim state-refresh origination-interval 65

(config)#interface eth0
(config-if)#no ip pim state-refresh origination-interval
```

ip pim unicast-bsm

Use this command to enable support for sending and receiving unicast Bootstrap Messages (BSM) on an interface. This command supports backward-compatibility with older versions of the Bootstrap Router specification, which specifies unicast BSM to refresh the state of new or restarting neighbors.

Use the `no` option with this command to disable unicast bootstrap messaging on an interface.

Command Syntax `ip pim unicast-bsm` `no ip pim unicast-bsm`

Parameters

None

Default

Unicast bootstrap messaging is disabled by default.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ip pim unicast-bsm

(config)#interface eth0
(config-if)#no ip pim unicast-bsm
```

show debugging ip pim

Use this command to display the debug status for the PIM process.

Command Syntax `show debugging ip pim` `showdebugging ip pim` `(vrf NAME|)`

Parameters `vrf` The VPN routing/forwarding instance

`NAME` Specify the name of the VPN routing/forwarding instance

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show debugging ip pim  PIM Debugging status:
 PIM event debugging is on
 PIM MFC debugging is on
 PIM state debugging is on
 PIM incoming packet debugging is on
 PIM outgoing packet debugging is on
 PIM Hello HT timer debugging is on
 PIM Hello NLT timer debugging is on
 PIM Hello THT timer debugging is on
 PIM Join/Prune JT timer debugging is on
 PIM Join/Prune ET timer debugging is on
 PIM Join/Prune PPT timer debugging is on
 PIM Join/Prune KAT timer debugging is on
 PIM Join/Prune OT timer debugging is on
 PIM Assert AT timer debugging is on
 PIM Register RST timer debugging is on
 PIM Bootstrap BST timer debugging is on
 PIM Bootstrap CRP timer debugging is on
 PIM mib debugging is on
 PIM nexthop debugging is on
 PIM mtrace debugging is on
 PIM NSM debugging is on
 PIM MSDP debugging is on
```

show debugging pim

Use this command to display the status of debugging for PIM.

Command Syntax `show debugging pim`

Parameters

None

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

This command displays one of several status:

```
#show debugging pim
PIM Debugging status:
```

```
PIM event debugging is on
 PIM MFC debugging is on
 PIM state debugging is on
 PIM incoming packet debugging is on
 PIM outgoing packet debugging is on
 PIM Hello HT timer debugging is on
 PIM Hello NLT timer debugging is on
 PIM Hello THT timer debugging is on
 PIM Join/Prune JT timer debugging is on
 PIM Join/Prune ET timer debugging is on
 PIM Join/Prune PPT timer debugging is on
 PIM Join/Prune KAT timer debugging is on
 PIM Join/Prune OT timer debugging is on
 PIM Assert AT timer debugging is on
 PIM Register RST timer debugging is on
 PIM Bootstrap BST timer debugging is on
 PIM Bootstrap CRP timer debugging is on
 PIM mib debugging is on
 PIM nexthop debugging is on
 PIM mtrace debugging is on
 PIM NSM debugging is on
 PIM MSDP debugging is on
```

show ip msdp peer

Use this command to display information about a Multicast Source Discovery Protocol (MSDP) peer.

Command Syntax `show ip msdp peer (A.B.C.D|) show ip msdp (vrf NAME|) peer (A.B.C.D|)`

Parameters

`A.B.C.D`	IPv4 address of peer
`NAME`	Name of the VPN routing/forwarding instance

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip msdp peer

MSDP Peer 11.1.1.12
Connection status
 State: Up (Established)
 Keepalive sent: 1
```

```
Keepalive received: 1
 Number of connect retries: 0
```

Table 1-179: Show ip msdp peer output

Entry	Description
MSDP Peer	IP address of the peer
Connection status	State – Up, Down, Invalid, Disabled, Inactive, Listening, Connecting, Established, or Maximum. Keepalive sent – Keepalive messages sent to peer. Keepalive received – Keepalive messages received from the peer. number of connect retries – Number of peer connect retries.

show ip msdp sa-cache

Use this command to display the (S,G) state learned from Multicast Source Discovery Protocol (MSDP) peers.

You can specify zero, one, or two addresses:

- If you do not specify any address, the entire Source-Active (SA) cache is displayed.
- If you specify only a unicast address it is treated as a source; if you specify only a multicast address it is treated as a group. In either case, entries corresponding to that address are displayed.
- If you specify two addresses, an (S, G) entry corresponding to those addresses is displayed; one address must be unicast and the other address must be multicast.

Command Syntax `show ip msdp sa-cache show ip msdp sa-cache details show ip msdp sa-cache A.B.C.D show ip msdp sa-cache A.B.C.D A.B.C.D show ip msdp (vrf NAME|) sa-cache show ip msdp (vrf NAME|) sa-cache details show ip msdp (vrf NAME|) sa-cache A.B.C.D show ip msdp (vrf NAME|) sa-cache A.B.C.D A.B.C.D`

Parameters

`A.B.C.D` Source and/or group IP address `details`

Detailed sa-cache information

`NAME` Name of the VPN routing/forwarding instance

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip msdp sa-cache
MSDP Source-Active Cache:
(20.1.1.11, 224.1.1.1), RP 10.1.1.11, RPF-Peer 11.1.1.12 Uptime 00:00:02
Exptime 00:03:28P
```

Table 1-180: Show ip msdp sa-cache output

Entry	Description
MSDP Source-Active Cache	•(S,G) address pair – Source address, multicast address •RP – Reverse Path address •RRF-Peer – Reverse Path Forwarding address •Uptime – as stated •Exptime – Time until entry timeout

show ip pim interface

Use this command to display PIM interface information.

Command Syntax `show ip pim interface`

`show ip pim interface detail show`

`ip pim (vrf NAME|) interface show`

`ip pim (vrf NAME|) interface detail`

Parameters `vrf` The VPN routing/forwarding instance

`NAME` Specify the name of the VPN routing/forwarding instance `detail`

Display detailed information about a PIM interface

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
Router_E#show ip pim interface
Address         Interface   VIFindex Ver/   Nbr       DR      DR
                                     Mode   Count    Prior
192.168.1.10        eth1         0         v2/S    1           1
192.168.1.10 172.16.1.10      eth2      2      v2/S   1       1
172.16.1.10
```

The output for PIM ECMP Redirect is as below:

```
rtr6#show  ip pim  interface
detail eth1 (vif 0):
  Address 192.168.10.57, DR 192.168.10.57
  Hello period 30 seconds, Next Hello in 18 seconds
  Triggered Hello period 5 seconds
  Propagation delay is 1000 milli-seconds
Interface  ID:  Router-ID:1.1.1.57  Local-
ID 3
  Neighbors:
   192.168.10.52
 eth2
(vif
2):
  Address 192.168.1.57, DR 192.168.1.152
  Hello period 30 seconds, Next Hello in 20 seconds
```

```
   Triggered Hello period 5 seconds
   Propagation delay is 1000 milli-seconds
   Interface ID: Router-ID:1.1.1.57 Local-ID 4
   ECMP REDIRECT, bundle : ecmpbundle, status :  allowed
 Neighbors:
192.168.1.149
192.168.1.150
192.168.1.152
```

Table 1-181: Show ip pim interface output

Entry	Description
Address	IP address of the interface
Interface	Interface name (eth1, xe3, ge4/1, etc.).
VIFindex	The index number of the Virtual Host Interface (vif).
Ver/Mode	PIM version (either v1, v2, or v3) / PIM Mode – Either S (sparse mode) or D (dense mode).
Nbr Count	Neighbor Count.
DR Prior	Designated Router Priority.
DR	Address of the Designated Router.
Hello Period	Routing devices send hello messages at a fixed interval on all PIM-enabled interfaces. By using hello messages, routing devices advertise their existence as PIM routing devices on the subnet.
Next Hello	When the interval counts down to 0, the routing device sends another hello message, and the timer is reset. A routing device that receives no response from a neighbor in 3.5 times the interval value drops the neighbor.
Propagation Delay	Vif Hello LAN Delay – propagation delay in milliseconds.
ECMP Redirect, bundle	An ECMP bundle is a set of PIM-enabled interfaces on a router, where all interfaces belonging to the same bundle share the same routing metric. The next hops for the ECMP are all one hop away. There can be one or more ECMP bundles on any router, while one individual interface can only belong to a single bundle. ECMP bundles are created on a router via configuration.

Neighbors	A list of the addresses of PIM multicast neighbors.

show ip pim mroute

Use this command to display information in the IP PIM multicast routing table.

Command Syntax `show ip pim mroute (detail|) show ip pim mroute A.B.C.D (detail|) show ip pim mroute A.B.C.D A.B.C.D (detail|) show ip pim (vrf NAME|) mroute (detail|) show ip pim (vrf NAME|) mroute A.B.C.D (detail|) show ip pim (vrf NAME|) mroute A.B.C.D A.B.C.D (detail|)`

Parameter `vrf` The VPN routing/forwarding instance

NAME Specify the name of the VPN routing/forwarding instance

`A.B.C.D` Display all entries for this group IP address

`A.B.C.D` Display all entries for this source IP address

Note: A group IP address and a source IP address cannot be simultaneously

`detail` Display detailed PIM multicast routing table information

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip pim mroute

IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
(*, 224.0.1.3)
RP: 10.10.1.5
RPF nbr: 172.16.1.2
RPF idx: eth2
Upstream State: JOINED
 Local     ..............................
 Joined    j..............................
 Asserted  ..............................
 Outgoing  o..............................
```

Table 1-182: Show ip pim mroute output

Entry	Description
(*, *, RP) Entries:	Source, Group, Rendezvous Point Include entries.
(*, G) Entries:	PIM Include entries
(S, G) Entries:	PIM Include entries (Source, Group)
(S, G, rpt) Entries:	The RPT is the path between the RP and receivers (hosts) in a multicast group. The RPT is built by means of a PIM join message from a receiver's DR.
RP:	Rendezvous Point
RPF nbr:	Reverse Path Forwarding neighbor.
RPF idx:	Reverse Path Forwarding index.
Upstream State:	As stated.

show ip pim neighbor

Use this command to display PIM neighbor information.

Command Syntax `show ip pim neighbor (detail|) show ip pim neighbor IFNAME (detail|) show ip pim neighbor IFNAME A.B.C.D (detail|) show ip pim (vrf NAME|) neighbor (detail|) show ip pim (vrf NAME|) neighbor IFNAME (detail|) show ip pim (vrf NAME|) neighbor IFNAME A.B.C.D (default|)`

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`IFNAME`	Name of the interface
`A.B.C.D`	IPv4 address of the neighbor interface
`detail`	Display detailed information for a PIM neighbor

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show ip pim neighbor
Neighbor      Interface    Uptime/Expires     Ver          DR
Address                                                Priority/Mode
10.10.14.11    eth3       00:14:30/00:01:45    v2         1 / DR
```

The validation command to view PIM ECMP Redirect is as below:

```
rtr6#show  ip pim  neighbor detail
Nbr 192.168.10.52 (eth1)
Expires in 83 seconds, uptime 00:21:52
Holdtime: 105 secs, T-bit: off, Lan delay: 1, Override
interval: 3
DR priority: 1, Gen ID: 1048865461,

Nbr 192.168.1.149 (eth2)
Expires in 99 seconds, uptime 00:22:06
Holdtime: 105 secs, T-bit: off, Lan delay: 1, Override
interval: 3
DR priority: 1, Gen ID: 2102076842,
Interface ID: Router-ID: 1.1.1.149 Local-ID: 4,
ECMP REDIRECT enabled
```

```
Nbr 192.168.1.150 (eth2)
Expires in 77 seconds, uptime 00:22:02
Holdtime: 105 secs, T-bit: off, Lan delay: 1, Override interval:
3
DR priority: 1, Gen ID: 1306457151,
Interface ID: Router-ID: 1.1.1.153 Local-ID:
4, ECMP REDIRECT enabled

Nbr 192.168.1.152 (eth2), DR
Expires in 86 seconds, uptime 00:22:06
Holdtime: 105 secs, T-bit: off, Lan delay: 1, Override interval:
3
DR priority: 1, Gen ID: 170629600,
Interface ID: Router-ID: 1.1.1.152 Local-ID:
4, ECMP REDIRECT enabled
```

Table 1-183: Show ip pim neighbor output

Entry	Description
Neighbor	Neighbor IP address
Interface	Name of the interface (eth1, xe3, xe5/1 etc.).
Uptime/Expires	Neighbor's uptime / time until uptime expires and starts sending hello messages.
Ver	PIM version (version1 =v1, version2 - v2, version3 = v3).
DR Priority/mode	Priority and Mode of neighbor as Designated Router.
Nbr	NEighbor IP address and interface name (eth1, xe3, xe5/1 etc.).
Expires in	Time before the Hello timer expires and must retransmit.
uptime	Neighbor uptime.
Holdtime:	Before an interface goes down or changes primary IP address, a Hello message with a zero HoldTime should be sent immediately (with the old IP address if the IP address changed). This will cause PIM neighbors to remove this neighbor (or its old IP address) immediately. After an interface has changed its IP address, it MUST send a Hello message with its new IP address. If an interface changes one of its secondary IP addresses, a Hello message with an updated Address_List option and a non-zero HoldTime should be sent immediately. This will cause PIM neighbors to update this neighbor's list of secondary addresses immediately.

T-bit:	RPT-bit is a 1-bit value. The RPT-bit is set to 1 for Assert(*,G) messages and 0 for Assert(S,G) messages.

Table 1-183: Show ip pim neighbor output

Entry	Description
Lan delay:	In addition to the information recorded for the DR Election, the following per neighbor information is obtained from the LAN Prune Delay Hello option: In addition to the information recorded for the DR Election, the following per neighbor information is obtained from the LAN Prune Delay Hello option: neighbor.lan_prune_delay_present A flag indicating if the LAN Prune Delay option was present in the Hello message. neighbor.tracking_support A flag storing the value of the T bit in the LAN Prune Delay option if it is present in the Hello message. This indicates the neighbor's capability to disable Join message suppression. neighbor.propagation_delay The Propagation Delay field of the LAN Prune Delay option (if present) in the Hello message. neighbor.override_interval The Override_Interval field of the LAN Prune Delay option (if present) in the Hello message. The additional state described above is deleted along with the DR neighbor state when the neighbor timeout expires.
Override interval:	Hello Override Interval
DR priority:	The DR_Priority Option allows a network administrator to give preference to a particular router in the DR election process by giving it a numerically larger DR Priority.The DR_Priority Option SHOULD be included in every Hello message, even if no DR Priority is explicitly configured on that interface. This is necessary because priority-based DR election is only enabled when all neighbors on an interface advertise that they are capable of using the DR_Priority Option. The default priority is 1.
Gen ID:	Generation Identifier, used to detect reboots.
Interface ID:	As stated.
Router-ID:	As stated.
Local-ID:	As stated.

© Symanitron Proprietary

ECMP REDIRECT	Whether ECMP Redirect is enabled or disabled.

show ip pim nexthop

Displays the nexthop information from NSM as used by PIM.

Command Syntax `show ip pim nexthop show ip pim (vrf NAME|) nexthop`

Parameter `vrf` The VPN routing/forwarding instance

`NAME` Specify the name of the VPN routing/forwarding instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip pim nexthop
```

show ip pim bsr-router

Use this command to show the bootstrap router PIMv2 address.

Command Syntax `show ip pim bsr-router`

`show ip pim (vrf NAME|) bsr-router`

Parameters `vrf` The VPN routing/forwarding instance

`NAME` Specify the name of the VPN routing/forwarding instance

Command Mode

Privileged Exec and Exec mode

Applicability

Entry	Description
BSR address	Bootstrap Router's IP address.
Uptime	As stated
BSR Priority	BSR election priority; can be set manually, but default is 64.

Hash mask length	As stated.
Expires	Group-to-C-RP mapping Expiry Timer.

This command was introduced before SWMRE version 1.3. Examples

```
#show ip pim bsr-router
PIMv2 Bootstrap information
  BSR address: 10.10.11.35 (?)
  Uptime:      00:00:38, BSR Priority: 0, Hash mask length: 10
  Expires:     00:01:32
  Role: Non-candidate BSR
  State: Accept Preferred

#show ip pim bsr-router
PIMv2 Bootstrap information
 BSR address: 20.0.1.21
 Uptime:      00:40:20, BSR Priority: 64, Hash mask length: 10
 Expires:     00:02:07
 Role: Candidate BSR
 State: Candidate BSR
```

Table 1-184: Show ip pim bsr-router output

Table 1-184: Show ip pim bsr-router output (Continued)

Entry	Description
Role	Specifies whether the BSR is the Candidate BSR or a Non-candidate BSR
State	• The current state of a Candidate BSR, one of the following: CandidateBSR, Pending-BSR, or Elected-BSR. • The current state of a Non-candidate BSR, one of the following: Accept Any or Accept Preferred.

show ip pim local-members

Use this command to display information about local membership for PIM interfaces.

Command Syntax `show ip pim local-members show ip pim local-members IFNAME show ip pim (vrf NAME|) local-members show ip pim (vrf NAME|) local-members IFNAME`

Parameters `vrf` The VPN routing/forwarding instance

`NAME` Specify the name of the VPN routing/forwarding instance `IFNAME` Display local membership for an interface name

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip pim vrf q local-members p8p1 PIM Local
membership information

p8p1:
  (*, 233.5.5.5) : Include
  (*, 233.7.7.7) : Include
```

Table 1-185: Show ip pim local-members output

Entry	Description
NAME:	Interface name
(*,G)	The local members in the form (Source/Group). Shows state – either Include or Exclude.

show ip pim rp-hash

Use this command to display the rendezvous point (RP) to chose based on the group selected.

Command Syntax `show ip pim rp-hash A.B.C.D show ip pim (vrf NAME|) rp-hash A.B.C.D`

Parameters `vrf` The VPN routing/forwarding instance

NAME	Specify the name of the VPN routing/forwarding instance
A.B.C.D	Specify a group address

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

A.B.C.D in command refers to the group address to be hashed.

```
#show ip pim rp-hash 224.0.1.3
Group(s): 224.0.0.0/4
    RP: 172.16.1.2
    Info source: 172.16.1.2, via bootstrap
```

Table 1-186: Show ip PIM rp-hash output

Entry	Description
Group(s)	The group address to be hashed.
RP	Rendezvous Point
Info source	The address and identity from which this information was received. In the example above, it was learned from the bootstrap router.

show ip pim rp mapping

Use this command to show group-to-RP (rendezvous point) mappings, and the RP set.

Command Syntax `show ip pim rp mapping show ip`

```
pim (vrf NAME|) rp mapping
```

Parameter `vrf` The VPN routing/forwarding instance

NAME	Specify the name of the VPN routing/forwarding instance

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ip pim rp mapping This system is the
Bootstrap Router (v2)
Group(s): 224.0.0.0/4
 RP: 10.10.1.5
    Info source: 172.16.1.2, via bootstrap, priority 192
         Uptime: 00:00:13, expires: 00:02:29
 RP: 172.16.1.2
    Info source: 172.16.1.2, via bootstrap, priority 2
         Uptime: 00:34:42, expires: 00:01:49
```

Table 1-187: Show ip PIM rp mapping output

Entry	Description
Identity declaration	This system is the Bootstrap Router (PIM version number v1, v2. or, v3) or not the Bootstrap Router.
Group(s):	The Multicast address of this multicast Group.
RP	Addresses of the Rendezvous Points.
Info source:	Address of the info source, whether it was learned from the Bootstrap Router, and the configured priority.

snmp restart pim

Use this command to restart SNMP in (PIM).

Note: This command restarts IPv4 PIM daemon

Command Syntax `snmp restart pim`

Parameters

None

Default

By default, the snmp restart pim is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#snmp restart pim
```

undebug all ip pim

Use this command to disable all PIM debugging from Configure mode.

Command Syntax `undebug all ip pim undebug (vrf NAME|) all ip pim`

Parameter `vrf` The VPN routing/forwarding instance

`NAME` Specify the name of the VPN routing/forwarding instance

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#undebug all ip pim
```

CHAPTER 2 PIMv6 Commands

This chapter describes the commands for Protocol-Independent Multicast (PIM).

- clear ipv6 mroute
- clear ipv6 pim sparse-mode bsr
- debug ipv6 pim
- debug ipv6 pim packet
- debug ipv6 pim timer assert
- debug ipv6 pim timer hello
- debug ipv6 pim timer register
- ipv6 pim accept-register
- ipv6 pim anycast-rp
- ipv6 pim bind ecmp-bundle
- ipv6 pim bsr-border
- ipv6 pim bsr-candidate
- ipv6 pim cisco-register-checksum
- ipv6 pim crp-cisco-prefix
- ipv6 pim passive
- ipv6 pim dense-group
- ipv6 pim dr-priority
- ipv6 pim ecmp-bundle
- ipv6 pim rp embedded
- ipv6 pim exclude-genid
- ipv6 pim hello-holdtime
- ipv6 pim hello-interval
- ipv6 pim ignore-rp-set-priority
- ipv6 pim jp-timer
- ipv6 pim neighbor-filter
- ipv6 pim propagation-delay
- ipv6 pim register-rate-limit
- ipv6 pim register-rp-reachability
- ipv6 pim register-source
- ipv6 pim register-suppression
- ipv6 pim router-id
- ipv6 pim rp-address
- ipv6 pim rp-candidate

- ipv6 pim rp-register-kat
- ipv6 pim spt-threshold
- ipv6 pim ssm
- ipv6 pim state-refresh origination-interval
- ipv6 pim unicast-bsm
- show debugging ipv6 pim
- show ipv6 pim interface • show ipv6 pim mroute
- show ipv6 pim neighbor
- show ipv6 pim nexthop
- show ipv6 pim bsr-router
- show ipv6 pim local-members
- show ipv6 pim rp-hash
- show ipv6 pim rp mapping
- snmp restart pim
- undebug all ipv6 pim

clear ipv6 mroute

Use this command to delete all multicast route table entries and all multicast routes at the PIM protocol level.

Command Syntax `clear ipv6 mroute * clear ipv6 mroute * pim (dense-mode|sparse-mode) clear ipv6 mroute X:X::X:X clear ipv6 mroute X:X::X:X X:X::X:X clear ipv6 mroute X:X::X:X X:X::X:X pim (dense-mode|sparse-mode) clear ipv6 mroute X:X::X:X pim sparse-mode clear ipv6 mroute statistics * clear ipv6 mroute statistics X:X::X:X clear ipv6 mroute statistics X:X::X:X X:X::X:X clear ipv6 mroute (vrf NAME|) * clear ipv6 mroute (vrf NAME|) * pim (dense-mode|sparse-mode) clear ipv6 mroute (vrf NAME|) X:X::X:X clear ipv6 mroute (vrf NAME|) X:X::X:X X:X::X:X clear ipv6 mroute (vrf NAME|) X:X::X:X X:X::X:X pim (dense-mode|sparse-mode) clear ipv6 mroute (vrf NAME|) X:X::X:X pim sparse-mode clear ipv6 mroute (vrf NAME|) statistics * clear ipv6 mroute (vrf NAME|) statistics X:X::X:X clear ipv6 mroute (vrf NAME|) statistics X:X::X:X X:X::X:X`

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`*`	Delete all multicast routes
`statistics`	Clears multicast route statistics
`X:X::X:X`	Clears group IP address
`X:X::X:X`	Clears source IP address
`dense-mode`	Clear multicast rout table for PIM dense-mode
`sparse-mode`	Clear multicast route table for PIM sparse mode

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear ipv6 mroute * pim sparse-mode
                      #clear ipv6 mroute 3ffe::24:3 ff00::3 pim sparse-mode
```

clear ipv6 pim sparse-mode bsr

Use this command to clear all rendezvous point (RP) sets learned through the PIMv2 Bootstrap Router (BSR).

Command Syntax `clear ipv6 pim sparse-mode bsr rp-set *`

```
clear ipv6 pim (vrf NAME|) sparse-mode bsr rp-set *
```

Parameters

`rp-set`	PIMv2 bootstrap router RP set
`*`	Clear all RP sets
`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear ipv6 pim sparse-mode bsr rp-set *
```

debug ipv6 pim

Use this command to enable debugging for PIM.

Use the `no` option with this command to deactivate debugging for PIM.

Command Syntax `debug ipv6 pim (all|events|mfc|mib|mtrace|nexthop|nsm|packet|state|timer) debug ipv6 pim (vrf NAME|) (all|events|mfc|mib|mtrace|nexthop|nsm|packet|state |timer) no debug ipv6 pim (all|events|mfc|mib|mtracenexthop|nsm|packet|state|timer) no debug ipv6 pim (vrf NAME|) (all|events|mfc|mib|mtracenexthop|nsm|packet |state|timer)`

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`all`	Enable debugging for all PIM events
`events`	Enable debugging for general configuration, Virtual Routing (VR), and VRF context
`mfc`	Enable debugging for MFC updates
`mib`	Enable debugging for MIB entries
`mtrace`	Enable debugging for MTRACE messages
`nexthop`	Enable debugging for Reverse Path Forwarding (RPF) neighbor nexthop cache handling
`nsm`	Enable debugging for NSM
`packet`	Enable debugging for PIM packets
`state`	Enable debugging for PIM states
`timer`	Enable debugging for PIM timers

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#debug ipv6 pim state
```

debug ipv6 pim packet

Use this command to activate debugging of incoming or outgoing PIM packets.

Use the `no` option with this command to deactivate debugging of incoming or outgoing PIM packets.

Command Syntax `debug ipv6 pim packet debug ipv6 pim packet in debug ipv6 pim packet out debug ipv6 pim (vrf NAME|) packet debug ipv6 pim (vrf NAME|) packet in debug ipv6 pim (vrf NAME|) packet out no debug ipv6 pim packet no debug ipv6 pim packet in no debug ipv6 pim packet out no debug ipv6 pim (vrf NAME|) packet no debug ipv6 pim (vrf NAME|) packet in no debug ipv6 pim (vrf NAME|) packet out`

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`in`	Debug incoming packets
`out`	Debug outgoing packets

Command Mode

Configure and Privileged Exec modes

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#debug ipv6 pim packet in
```

debug ipv6 pim timer assert

Use this command to enable debugging of the PIM assert timers.

Use the `no` option with this command to disable debugging for PIM assert timers.

Command Syntax `debug ipv6 pim timer assert debug ipv6 pim timer assert at debug ipv6 pim (vrf NAME|) timer assert debug ipv6 pim (vrf NAME|) timer assert at no debug ipv6 pim timer assert no debug ipv6 pim timer assert at no debug ipv6 pim (vrf NAME|) timer assert no debug ipv6 pim (vrf NAME|) timer assert at`

Parameters `vrf` The VPN routing/forwarding instance

`NAME` Specify the name of the VPN routing/forwarding instance `at` Use this option to turn on or turn off debugging of the PIM Assert Timer

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#debug ipv6 pim timer assert at
```

debug ipv6 pim timer bsr

Use this command to enable debugging of the PIM BSR time.

Use the `no` option with this command to disable debugging of the PIM BSR timer.

Command Syntax `debug ipv6 pim timer bsr debug ipv6 pim timer bsr bst debug ipv6 pim timer bsr crp debug ipv6 pim (vrf NAME|) timer bsr debug ipv6 pim (vrf NAME|) timer bsr bst debug ipv6 pim (vrf NAME|) timer bsr crp no debug ipv6 pim timer bsr no debug ipv6 pim timer bsr bst no debug ipv6 pim timer bsr crp no debug ipv6 pim (vrf NAME|) timer bsr no debug ipv6 pim (vrf NAME|) timer bsr bst no debug ipv6 pim (vrf NAME|) timer bsr crp`

Parameters

`bst`	Turn on or turn off the bootstrap debugging timer
`crp`	Turn on or turn off the Candidate-RP debugging timer
`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#debug ipv6 pim timer bsr bst
```

debug ipv6 pim timer hello

Use this command to enable debugging of various PIM Hello timers.

Use the `no` option with this command to disable debugging of the PIM Hello timers.

Command Syntax debug ipv6 pim timer hello debug ipv6 pim timer hello ht debug ipv6 pim timer hello nlt debug ipv6 pim timer hello tht debug ipv6 pim (vrf NAME|) timer hello debug ipv6 pim (vrf NAME|) timer hello ht debug ipv6 pim (vrf NAME|) timer hello nlt debug ipv6 pim (vrf NAME|) timer hello tht no debug ipv6 pim timer hello no debug ipv6 pim timer hello ht no debug ipv6 pim timer hello nlt no debug ipv6 pim timer hello tht no debug ipv6 pim (vrf NAME|) timer hello no debug ipv6 pim (vrf NAME|) timer hello ht no debug ipv6 pim (vrf NAME|) timer hello nlt no debug ipv6 pim (vrf NAME|)
timer hello tht

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
ht	Turn on or turn off the PIM Hello debugging timer (ht)
nlt	Turn on or turn off the PIM Neighbor Liveliness debugging timer (nlt)
tht	Turn on or turn off the Triggered Hello Timer (tht)

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#debug ipv6 pim timer hello ht
```

debug ipv6 pim timer joinprune

Use this command to enable debugging of various PIM JoinPrune timers.

Use the no option with this command to disable the debugging of the PIM JoinPrune timers.

Command Syntax debug ipv6 pim timer joinprune debug ipv6 pim timer joinprune et debug ipv6 pim timer joinprune kat debug ipv6 pim timer joinprune jt debug ipv6 pim timer joinprune ot debug ipv6 pim timer joinprune ppt debug ipv6 pim (vrf NAME|) timer joinprune debug ipv6 pim (vrf NAME|) timer joinprune et debug ipv6 pim (vrf NAME|) timer joinprune kat debug ipv6 pim (vrf NAME|) timer joinprune jt debug ipv6 pim (vrf NAME|) timer joinprune ot debug ipv6 pim (vrf NAME|) timer joinprune ppt no debug ipv6 pim timer

```
joinprune no debug ipv6 pim timer joinprune et no debug ipv6
pim timer joinprune kat no debug ipv6 pim timer joinprune jt no
debug ipv6 pim timer joinprune ot no debug ipv6 pim timer
joinprune ppt no debug ipv6 pim (vrf NAME|) timer joinprune no
debug ipv6 pim (vrf NAME|) timer joinprune et no debug ipv6 pim
(vrf NAME|) timer joinprune kat no debug ipv6 pim (vrf NAME|)
timer joinprune jt no debug ipv6 pim (vrf NAME|) timer
joinprune ot no debug ipv6 pim (vrf NAME|) timer joinprune ppt
```

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`et`	Turn on or turn off the PIM JoinPrune expiry timer (et)
`jt`	Turn on or turn off the PIM JoinPrune upstream Join Timer (jt)
`kat`	Turn on or turn off the PIM JoinPrune Keep Alive timer (kat)

`ot` Turn on or turn off the PIM JoinPrune Upstream Override Timer (ot) `ppt` Turn on or turn off the f PIM JoinPrune PrunePending Timer ((ppt)

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#debug ipv6 pim timer joinprune et
```


© Symanitron Proprietary

debug ipv6 pim timer register

Use this command to enable debugging of the PIM register timer.

Use the `no` option with this command to disable debugging of the PIM register timer.

Command Syntax `debug ipv6 pim timer register debug ipv6 pim timer register rst debug ipv6 pim (vrf NAME|) timer register debug ipv6 pim (vrf NAME|) timer register rst no debug ipv6 pim timer register no debug ipv6 pim timer register rst no debug ipv6 pim (vrf NAME|) timer register no debug ipv6 pim (vrf NAME|) timer register rst`

Parameters `vrf` The VPN routing/forwarding instance

`NAME` Specify the name of the VPN routing/forwarding instance `rst` Turn on or turn off the PIM Register Stop Timer (rst)

Command Mode

Exec mode, Privileged Exec mode, and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#debug ipv6 pim timer register
```

ipv6 pim accept-register

Use this command to configure the ability to filter out multicast sources specified by the given access-list at the RP, so that the RP will accept/refuse to perform the Register mechanism for the packets sent by the specified sources. By default, the RP accepts Register packets from all multicast sources.

Use the no option with this command to revert to default.

Command Syntax `ipv6 pim accept-register list (<100-199>|<2000-2699>|WORD) ipv6 pim (vrf NAME|) accept-register list (<100-199>|<2000-2699>|WORD) no ipv6 pim accept-register no ipv6 pim (vrf NAME|) accept-register`

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`<100-199>`	An IP extended access-list value
`<2000-2699>`	An IP extended access-list value in the expanded range
`WORD`	Name of a standard access list

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ipv6 pim accept-register list 121

(config)#no ipv6 pim accept-register
```

ipv6 pim anycast-rp

Use this command to configure an Anycast-RP in the RP set.

Use the no option with this command to remove the Anycast-RP configuration.

Command Syntax `ipv6 pim anycast-rp X:X::X:X X:X::X:X ipv6 pim (vrf NAME|) anycast-rp X:X::X:X X:X::X:X no ipv6 pim anycast-rp X:X::X:X no ipv6 pim anycast-rp X:X::X:X X:X::X:X no ipv6 pim (vrf NAME|) anycast-rp X:X::X:X no ipv6 pim (vrf NAME|) anycast-rp X:X::X:X X:X::X:X`

Parameters

`vrf`	The VPN routing/forwarding instance.
`NAME`	Specify the name of the VPN routing/forwarding instance.
`X:X::X:X`	Unicast IPv6 address of the Anycast RP set. An Anycast RP set is a collection of RPs in the same domain.
`X:X::X:X`	Destination IPv6 address where Register messages are copied and sent. A Member RP is an individual RP member in the Anycast RP set.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows how to configure the Anycast RP in the RP set.

```
#configure terminal
(config)#ipv6 pim anycast-rp 2:2::2:2 20:20::20:20
```

The following example shows how to remove the configuration.

```
#configure terminal
(config)#no ipv6 pim anycast-rp 2:2::2:2 20:20::20:20
```

ipv6 pim bind ecmp-bundle

Use this command to bind interfaces to an ECMP Bundles.

Use the `no` option with this command to unbind the interfaces from an ECMP Bundles

Command Syntax `ipv6 pim bind ecmp-bundle WORD no ipv6 pim bind ecmp-bundle WORD`

Parameter

`WORD`	ECMP bundle name

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#ipv6 pim bind ecmp-bundle ebund1

(config-if)#no ipv6 pim bind ecmp-bundle ebund1
```

ipv6 pim bsr-border

Use this command to prevent bootstrap router (BSR) messages from being sent or received through an interface.

When this command is configured on an interface, no PIM Version 2 BSR messages are sent or received through the interface. Use this command to configure an interface bordering another PIM domain to avoid the exchange of BSR messages between the two domains. BSR messages should not be exchanged between different domains because routers in one domain may elect rendezvous points (RPs) in the other domain, resulting in a protocol malfunction or loss of isolation between the domains.

Use the `no` option with this command to remove the BSR border configuration.

Note: This command does not set up multicast boundaries. It only sets up a PIM domain BSR message border.

Command Syntax `ipv6 pim bsr-border no ipv6 pim bsr-border`

Parameters

None

Default

Bootstrap router border configuration is disabled by default.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example configures the interface to be the PIM domain border:

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 pim bsr-border

(config)#interface eth0
(config-if)#no ipv6 pim bsr-border
```

ipv6 pim bsr-candidate

Use this command to give the router the candidate BSR status using the name the interface.

Use the `no` option with this command to disable this function.

Note: This command does not set up multicast boundaries. It only sets up a PIM domain BSR message candidate

Command Syntax `ipv6 pim bsr-candidate IFNAME ipv6 pim bsr-candidate IFNAME <0-32> ipv6 pim bsr-candidate IFNAME <0-32> <0-255> ipv6 pim (vrf NAME|) bsr-candidate IFNAME ipv6 pim (vrf NAME|) bsr-candidate IFNAME <0-32> ipv6 pim (vrf NAME|) bsr-candidate IFNAME <0-32> <0-255> no ipv6 pim bsr-candidate (IFNAME|) no ipv6 pim (vrf NAME|) bsr-candidate (IFNAME|)`

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`IFNAME`	Specify the name of the interface
`<0-32>`	Specify a hash mask length for RP selection
`<0-255>`	Specify a priority for a BSR candidate

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ipv6 pim bsr-candidate eth0 20 30
```

ipv6 pim cisco-register-checksum

Use this command to configure the option to calculate the register checksum over the whole packet. This command is used to inter-operate with older Cisco IOS versions.

Use the `no` option with this command to revert to the default settings.

Command Syntax `ipv6 pim cisco-register-checksum ipv6 pim cisco-register-checksum group-list (<1-99>|<1300-1999>|WORD) ipv6 pim (vrf NAME|) cisco-register-checksum ipv6 pim (vrf NAME|) cisco-register-checksum group-list (<1-99>|<1300-1999>|WORD) no ipv6 pim cisco-register-checksum no ipv6 pim cisco-register-checksum group-list (<1-99>|<1300-1999>|WORD) no ipv6 pim (vrf NAME|) cisco-register-checksum no ipv6 pim (vrf NAME|) cisco-register-checksum group-list (<1-99>|<1300-1999>|WORD)`

Parameters

`vrf`	The VPN routing/forwarding instance.
`NAME`	Specify the name of the VPN routing/forwarding instance.
`group-list`	Use this parameter to configure the option to calculate the register checksum over the whole packet on multicast groups specified by the access-list.
`<1-99>`	Specify an IP standard access-list.
`<1300-1999>`	Specify an IP access-list (expanded range).
`WORD`	IP named standard access list.

Default

This command is disabled by default. By default, Register Checksum is calculated only over the header.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ipv6 pim cisco-register-checksum

(config)#ipv6 pim cisco-register-checksum group-list G1
(config)#ipv6 access-list filter permit ff1e:10/128
```

ipv6 pim crp-cisco-prefix

Use this command to turn on or turn the Candidate-RP debugging timerworking with Cisco BSR.

Use the `no` form of this command to turn off the Candidate-RP debugging timerworking with Cisco BSR.

Command Syntax `ipv6 pim crp-cisco-prefix`

`no ipv6 pim crp-cisco-prefix`

Parameters `crp-cisco-prefix`

Candidate-RP debugging timerworking with Cisco BSR.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ipv6 pim crp-cisco-prefix

(config)#noipv6 pim crp-cisco-prefix
```

ipv6 pim

Use this command to enable IPv6 PIM dense-mode or sparse-mode or sparse-dense-mode on the current interface.

Use the `no` option with this command to disable IPv6 PIM dense-mode or sparse-mode or sparse-dense-mode on the interface.

Command Syntax `ipv6 pim (dense-mode|sparse-mode|sparse-dense-mode)` `no ipv6 pim (dense-mode|sparse-mode|sparse-dense-mode)`

Parameters `dense-mode` Enable IPv6 PIM dense-mode operation

`sparse-mode` Enable IPv6 PIM sparse-mode operation

`sparse-dense-mode` Enable IPv6 PIM sparse-dense-mode operation

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 pim dense-mode

(config)#interface eth0
(config-if)#no ipv6 pim dense-mode

(config)#interface eth0
(config-if)#ipv6 pim sparse-dense-mode

(config-if)#no ipv6 pim sparse-dense-mode
```

ipv6 pim passive

Use this command to enable or disable passive mode operation for local members on the interface. Passive mode essentially stops PIM transactions on the interface, allowing only the Internet Group Management Protocol (IGMP) mechanism to be active.

Use the `no` option with this command to disable the passive mode.

Command Syntax `ipv6 pim (dense-mode|sparse-mode) passive no ipv6 pim (dense-mode|sparse-mode) passive`

Parameters

`dense-mode`	Enable passive operation for PIM dense-mode
`sparse-mode`	Enable passive operation for PIM sparse-mode

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 pim dense-mode passive

(config)#interface eth0
(config-if)#no ipv6 pim dense-mode passive

#configure terminal
(config)#interface eth0
(config-if)#ipv6 pim sparse-mode passive

(config)#interface eth0 (config-if)#no ipv6
pim sparse-mode passive
```

ipv6 pim dense-group

Use this command to force a particular group to always follow dense mode irrespective of whether RP mapping is available in SM-DM mode.

Use the `no` option with this command to delete the group-address and follow SM-DM rules.

Command Syntax `ipv6 pim dense-group A.B.C.D ipv6 pim (vrf NAME|) dense-group A.B.C.D no ipv6 pim dense-group A.B.C.D no ipv6 pim (vrf NAME|) dense-group A.B.C.D`

Parameter

A.B.C.D	Specify IP address
NAME	Specify the name of the VRF

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#ipv6 pim dense-group 1ffe:11::11:11

(config-if)# no ip pim dense-group 1ffe:1::11:11
```

ipv6 pim dr-priority

Use this command to set the designated router's priority value.

Use the `no` option with this command to remove the priority from the DR.

Command Syntax `ipv6 pim dr-priority <0-4294967294> no ipv6 pim dr-priority (<0-4294967294>|)`

Parameter

<0-4294967294>	Valid range of values for DR priority, with a higher value resulting in a higher preference

Default

The default DR priority value is 1.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 pim dr-priority 11234

(config)#interface eth0
(config-if)#no ipv6 pim dr-priority 11234
```

ipv6 pim ecmp-bundle

Use this command to create an ECMP bundle.

Use the `no` option with this command to delete an ECMP bundle.

Command Syntax `ipv6 pim ecmp-bundle WORD ipv6 pim (vrf NAME|) ecmp-bundle WORD ipv6 pim ecmp-bundle WORD no ipv6 pim (vrf NAME|) ecmp-bundle WORD`

Parameter

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`WORD`	ECMP bundle name

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ipv6 pim exmp-bundle ebund1

(config)#no ipv6 pim ecmp-bundle ebund1
```

ipv6 pim rp embedded

Use this command to embed the PIM Rendezvous Point.

Use the no option with this command to remove the Rendezvous Point.

Command Syntax `ipv6 pim rp embedded no ipv6 pim rp embedded`

Parameter `embedded` Embed the Rendezvous Point

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ipv6 pim rp embedded

(config)#no ipv6 pim rp embedded
```

ipv6 pim exclude-genid

Use this command to exclude the GenID (generated ID) option from Hello packets sent by the PIM module on an interface.This command is used to inter-operate with older Cisco IOS versions.

Use the `no` option with this command to restore PIM its default setting.

Command Syntax `ipv6 pim exclude-genid` `no ipv6 pim exclude-genid`

Parameters

None

Default

By default, this command is disabled; that is, the GenID option is included.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 pim exclude-genid

(config)#interface eth0
(config-if)#no ipv6 pim exclude-genid
```

ipv6 pim hello-holdtime

Use this command to configure a hello holdtime other than the default (`3.5 * hello_interval` seconds).

When configuring `hello-holdtime`, if the configured value is less than the current `hello_interval`, it is refused.

When removing a configured `hello_holdtime`, the value is reset to (`3.5 *` current `hello_interval)` value.

Every time the hello_interval is updated, the hello-holdtime is also updated according to rules below:

If the hello_holdtime is not configured, or if the hello_holdtime is configured, but is less than the current hello_interval value, it is modified to (3.5 * hello_interval). Otherwise, the configured value is maintained.

Use the `no` option with this command to remove the configured hello-holdtime.

Command Syntax `ipv6 pim hello-holdtime <1-65535>` `no ipv6 pim hello-holdtime`

Parameter

`<1-65535>`	Range of values for hello-holdtime, in seconds

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface fxp0
(config-if)#ipv6 pim hello-holdtime 123

(config)#interface fxp0
(config-if)#no ipv6 pim hello-holdtime
```

ipv6 pim hello-interval

Use this command to configure a hello interval value other than the default. When a hello-interval is configured and hello-holdtime is not configured, or when the hello-holdtime value configured is less than the new hello-interval value, the holdtime value is modified to (3.5 * hello_interval). Otherwise, the hello-holdtime value is the configured value.

Use the `no` option with this command to reset the hello-interval to its default value.

Command Syntax `ipv6 pim hello-interval <1-65535> no ipv6 pim hello-interval`

Parameter

`<1-65535>` Range of values for the hello-interval Note:

No fractional values are allowed.

Default

The default value for hello-interval is 30 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 pim hello-interval 123

(config)#interface eth0
(config-if)#no ipv6 pim hello-interval
```

ipv6 pim ignore-rp-set-priority

Use this command to ignore the RP-SET priority value, and use only the hashing mechanism for RP selection. This command is used to inter-operate with older Cisco IOS versions.

Use the `no` option with this command to remove this setting.

Command Syntax `ipv6 pim ignore-rp-set-priority ipv6 pim (vrf NAME|) ignore-rp-set-priority no ipv6 pim ignore-rp-set-priority no ipv6 pim (vrf NAME|) ignore-rp-set-priority`

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ipv6 pim ignore-rp-set-priority

#configure terminal
(config)#no ipv6 pim ignore-rp-set-priority
```

ipv6 pim jp-timer

Use this command to set a PIM join/prune timer.

Use the `no` option with this command to remove the join/prune timer.

Command Syntax `ipv6 pim jp-timer <1-65535> ipv6 pim (vrf NAME|) jp-timer <1-65535> no ipv6 pim jp-timer no ipv6 pim jp-timer <1-65535> no ipv6 pim (vrf NAME|) jp-timer no ipv6 pim (vrf NAME|) jp-timer <1-65535>`

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`<1-65535>`	Range of values for the Join/Prune timer, in seconds

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ipv6 pim jp-timer 234

#configure terminal
(config)#no ipv6 pim jp-timer 234
```

ipv6 pim neighbor-filter

Use this command to enable filtering of neighbors on the interface.

When configuring a neighbor filter and when denied by filtering access list, PIM either does not establish adjacency with a neighbor or terminates adjacency with existing neighbors.

Use the `no` option with this command to disable filtering of neighbors on the interface.

Command Syntax `ipv6 pim neighbor-filter (<1-99>|WORD) no ipv6 pim neighbor-filter (<1-99>|WORD)`

Parameters

`<1-99>`	An IP standard access-list number
`WORD`	Name of an IP standard access list

Command Mode

Interface mode

Default

This command is disabled; by default, there is no filtering.

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
(config)#interface fxp0
(config-if)#ipv6 pim neighbor-filter F1
(config-if)#exit
(config)#ipv6 access-list filter deny fe80:20e:cff:fe01:facc
(config)#ipv6 access-list filter permit any
```

ipv6 pim propagation-delay

Use this command to configure the propagation delay value.

Use the no option with this command to return the propagation delay to its default value.

Command Syntax `ipv6 pim propagation-delay <1000-5000> no ipv6 pim propagation-delay`

Parameter

`<1000-5000>`	Range of values for propagation delay, in milliseconds

Default

The default propagation delay is 500 milliseconds.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 pim propagation-delay 1000

(config)#interface eth0
(config-if)#no ipv6 pim propagation-delay
```

ipv6 pim register-rate-limit

Use this command to configure the rate of Register packets sent by this designated router (DR), in number of packets per second.

Use the no option to remove the register-rate-limit configuration.

Note: The configured rate is per (S,G) state, and is not a system-wide rate.

Command Syntax `ipv6 pim register-rate-limit <1-65535>`

`ipv6 pim (vrf NAME|) register-rate-limit <1-65535>`

`no ipv6 pim register-rate-limit no ipv6 pim (vrf NAME|) register-rate-limit`

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`<1-65535>`	Range of values for packets to send per second

Command mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ipv6 pim register-rate-limit 3444

#configure terminal
(config)#no ipv6 pim register-rate-limit
```

ipv6 pim register-rp-reachability

Use this command to enable the RP reachability check for PIM Registers at the DR.

Use the no option to reset to the default state.

Command Syntax `ipv6 pim register-rp-reachability ipv6 pim (vrf NAME|) register-rp-reachability no ipv6 pim register-rp-reachability no ipv6 pim (vrf NAME|) register-rp-reachability`

Parameter `vrf` The VPN routing/forwarding instance

`NAME` Specify the name of the VPN routing/forwarding instance

Command Mode

Configure mode

Default

The default setting is no checking for rendezvous point reachability,

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ipv6 pim register-rp-reachability
```

ipv6 pim register-source

Use this command to configure the source address of Register packets sent by this DR, overriding the default source address, which is the address of the RPF interface toward the source host.

Use the `no` option to remove the source address of register packets sent by this DR, and reset it to use the default source address, that is, the address of the RPF interface toward the source host.

The configured address must be a reachable address so the RP can send corresponding Register-Stop messages in response. This address is usually the loopback interface address, but can also be other physical addresses. The address must be advertised by unicast routing protocols on the DR. Note: The interface configured does not require PIM to be enabled.

Command Syntax `ipv6 pim register-source IFNAME ipv6 pim register-source X:X::X:X ipv6 pim (vrf NAME|) register-source IFNAME ipv6 pim (vrf NAME|) register-source X:X::X:X no ipv6 pim register-source no ipv6 pim (vrf NAME|) register-source`

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`X:X::X:X`	The IP address to be used as the source of the register packets
`IFNAME`	The name of the interface to be used as the source of the register packets

Command mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ipv6 pim register-source 3ffe:406::1

#configure terminal
(config)#no ipv6 pim register-source
```

ipv6 pim register-suppression

Use this command to configure the register-suppression time, in seconds, overriding the default value of 60 seconds. Configuring this value modifies register-suppression time at the DR; configuring this value at the RP modifies the RPkeepalive-period value if the `ipv6 pim rp-register-kat` command is not used.

Use the no option to remove the register-suppression setting.

Command Syntax `ipv6 pim register-suppression <1-65535>`

`ipv6 pim (vrf NAME|) register-suppression <1-65535>`

`no ipv6 pim register-suppression no ipv6 pim (vrf NAME|) register-suppression`

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`<1-65535>`	Register suppression time, in seconds

Command mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ipv6 pim register-suppression 555

#configure terminal
(config)#no ipv6 pim register-suppression
```

ipv6 pim router-id

Use this command to configure PIM router-ID to uniquely identify the router.By default, PIM registers for the NSM router-id service. This command will override the router-id received from NSM.

Use the `no` option with this command to unconfigure PIM router-ID. This will make PIM fall back to the NSM router-id

Command Syntax `ipv6 pim (vrf NAME|) router-id`

`A.B.C.D no ipv6 pim (vrf NAME|) router-id`

`A.B.C.D`

Parameters `vrf` The VPN routing/forwarding instance

`NAME` Specify the name of the VPN routing/forwarding instance

`A.B.C.D` Specify the Router ID

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ipv6 pim router-id 1.1.1.1

(config)#no ipv6 pim router-id 1.1.1.1
```

ipv6 pim rp-address

Use this command to statically configure an RP address for multicast groups.

Use the `no` option to remove the RP address.

SWMRE PIMv6 supports multiple static RPs. It also supports usage of static-RP and BSR mechanism simultaneously. The following list states the correct usage of this command:

- To support embedded RP, the router configured as the RP must use a configured access-list that permits the embedded RP group ranges derived from the embedded RP address. If embedded RP support is available, only the RP must be statically configured as the RP for the embedded RP ranges – no additional configuration is required on other PIMv6 routers. The other routers will discover the RP address from the IPv6 group address. For these routers to select a static RP instead of the embedded RP, the specific embedded RP group range must be configured in the access list of the static RP, and embedded RP support must be disabled.
- If RP-address configured through BSR and RP-address configured statically are both available for a group range, the RP-address configured through BSR is chosen over statically configured RP-address.
- A single static-RP can be configured for multiple group ranges using Access Lists. However, configuring multiple static RPs (using `ipv6 pim rp-address` command) with the same RP address is not allowed. The static-RP can be configured either for the whole multicast group range `ff00::/8` (without ACL) or for specific group ranges (using ACL).

  For example, configuring `ipv6 pim rp-address 3ffe:10:10:5::153` will configure static-RP `3ffe:10:10:5::153` for the default group range `ff00::/8`. Configuring `ipv6 pim rp-address 3ffe:20:20:5::153 grp-list` will configure static-RP `3ffe:20:20:5::153` for all the group ranges represented by `permit` filters in `grp-list` ACL.
- If multiple static-RPs are available for a group range, then one with the highest IP address is chosen.
- `vrf` The VPN routing/forwarding instance

  `NAME` Specify the name of the VPN routing/forwarding instance

- Only `permit` filters in ACL are considered as valid group ranges. The default `permit` filter `::/0` is converted to default multicast filter `ff00::/8`.
- When selecting static-RPs for a group range, the first element, with static-RP with the highest IP address is chosen.
- Group mode and RP address mappings learned through BSR take precedence over mappings statistically defined by the `ipv6 pim rp-address` command without the `override` keyword. Commands with the `override` keyword take precedence over dynamically learned mappings.

Command Syntax `ipv6 pim rp-address X:X::X:X (override|) ipv6 pim rp-address X:X::X:X (<1-99>|<1300-1999>|WORD)(override|) ipv6 pim (vrf NAME|) rp-address X:X::X:X (override|) ipv6 pim (vrf NAME|) rp-address X:X::X:X (<1-99>|<1300-1999>|WORD)(override|) no ipv6 pim rp-address X:X::X:X`

`no ipv6 pim rp-address X:X::X:X (<1-99>|<1300-1999>|WORD)`

`no ipv6 pim (vrf NAME|) rp-address X:X::X:X`

`no ipv6 pim (vrf NAME|) rp-address X:X::X:X (<1-99>|<1300-1999>|WORD)`

Parameters

X:X::X:X	IPv6 address for the RP
<1-99>	An IP Standard access-list
<1300-1999>	An IP Standard access-list (expanded range)
WORD	Access-list name
override	Static RP overrides dynamically-learned RP

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
                (config)#ipv6 pim rp-address 30:30:5::153 4

#configure terminal
(config)#no ipv6 pim rp-address 30:30:5::153 4
```


© Symanitron Proprietary

ipv6 pim rp-candidate

Use this command to give the router a candidate RP status using the IPv6 address of the specified interface.

Additionally, the groups specified will operate in PIM sparse mode; group-list specifies the standard IP access list number or name that defines the group prefixes that are advertised in association with the RP address.

Use the `no` option along with this command to remove the settings.

Command Syntax

```
ipv6 pim (vrf NAME) rp-candidate IFNAME(group-list(<1-99>|WORD))|)(interval <1-
  16383>|) (priority <0-255>|) no ipv6 pim (vrf
NAME) rp-candidate (IFNAME|)
```

Parameters

`vrf NAME`	The VPN routing/forwarding instance
`IFNAME`	Specify an interface name
`<1-99>`	An IP Standard access-list
`WORD`	A named standard access list
`<0-16383>`	Range of values for candidate-RP advertisement interval, in seconds
`<0-255>`	Range of values for priority of an RP candidate

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ipv6 pim rp-candidate eth3

(config)#no ipv6 pim rp-candidate eth3
```

ipv6 pim rp-register-kat

Use this command to configure a Keepalive Timer (KAT) value for (S,G) states at RP to monitor PIM register packets, overriding the generic KAT timer value. Use the no option to remove this configuration.

Command Syntax `ipv6 pim rp-register-kat <1-65535>`

```
ipv6 pim (vrf NAME|) rp-register-kat <1-65535>
no ipv6 pim rp-register-kat no ipv6 pim (vrf
NAME|) rp-register-kat
```

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
<1-65535>	Range of values for a KAT time in seconds

Command mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ipv6 pim rp-register-kat 3454

(config)#no ipv6 pim rp-register-kat
```

ipv6 pim spt-threshold

Use this command to configure an SPT (System Posture Token) threshold.

Use the `no` option with this command to remove a configured SPT threshold.

Note: This option is binary, meaning that switching to SPT happens either the first data packet is received, or not at all. It is not rate-based.

Command Syntax `ipv6 pim spt-threshold ipv6 pim spt-threshold group-list (<1-99>|<1300-1999>|WORD) ipv6 pim (vrf NAME|) spt-threshold ipv6 pim (vrf NAME|) spt-threshold group-list (<1-99>|<1300-1999>|WORD) no ipv6 pim spt-threshold no ipv6 pim spt-threshold group-list (<1-99>|<1300-1999>|WORD) no ipv6 pim (vrf NAME|) spt-threshold`

`no ipv6 pim (vrf NAME|) spt-threshold group-list (<1-99>|<1300-1999>|WORD)`

Parameters

vrf	The VPN routing/forwarding instance
NAME	Specify the name of the VPN routing/forwarding instance
group-list	Enable the ability for the last-hop PIM router to switch to SPT for multicast group addresses indicated by the given access-list
<1-99>	An IP Standard access-list
<1300-1999>	An IP Standard access-list (expanded range)
WORD	A named standard access list

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ipv6 pim spt-threshold group-list LIST1

#configure terminal
(config)#no ipv6 pim spt-threshold
```

ipv6 pim ssm

Use this command to configure Source Specific Multicast (SSM), and define a range of IP multicast addresses. The `default` keyword defines the SSM range as ff3x::/32. To define a SSM range other than the default, specify an access-list.

When an SSM range of IP multicast addresses is defined with this command, the no (*,G) or (S,G,rpt) state is initiated for groups in the SSM range.

The messages corresponding to these states are not accepted or originated in the SSM range.

Use the `no` form of this command to disable the SSM range.

Command Syntax `ipv6 pim ssm default ipv6 pim ssm range (<1-99>|WORD) ipv6 pim (vrf NAME|) ssm default ipv6 pim (vrf NAME|) ssm range (<1-99>|WORD) no ipv6 pim ssm no ipv6 pim (vrf NAME|) ssm`

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`default`	Defines the FF3x::/32 group range for SSM
`range`	Define an access-list for group range to use for SSM
`<1-99>`	Range of values for a standard access-list
`WORD`	A named standard access list

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following example shows how to configure SSM service for the IP address range defined by access list 10:

```
#configure terminal
(config)#access-list 10 permit 225.1.1.1
(config)#ipv6 pim ssm range 4
```

ipv6 pim state-refresh origination-interval

Use this command to configure a PIM State-Refresh origination interval other than the default value. The origination interval is the number of seconds between PIM State Refresh control messages. Use the `no` option with this command to return the origination interval to its default value.

Command Syntax `ipv6 pim state-refresh origination-interval <1-100> no ipv6 pim state-refresh origination-interval`

Parameter

`<1-100>` Range of values for state-refresh origination interval, in seconds Note: No fractional values are allowed for the interval time.

Default

The default state-refresh origination interval is 60 seconds.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 pim state-refresh origination-interval 65

(config)#interface eth0
(config-if)#no ipv6 pim state-refresh origination-interval
```

ipv6 pim unicast-bsm

Use this command to enable support for sending and receiving unicast Bootstrap Messages (BSM) on an interface. This command supports backward-compatibility with older versions of the Bootstrap Router specification, which specifies unicast BSM to refresh the state of new or restarting neighbors.

Use the `no` option with this command to disable unicast bootstrap messaging on an interface.

Command Syntax `ipv6 pim unicast-bsm no ipv6 pim unicast-bsm`

Parameters

None

Default

Unicast bootstrap messaging is disabled by default.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth0
(config-if)#ipv6 pim unicast-bsm

(config)#interface eth0
(config-if)#no ipv6 pim unicast-bsm
```

show debugging ipv6 pim

Use this command to display the debug status for the IPv6 PIM process.

Command Syntax `show debugging ipv6 pim show debugging ipv6 pim (vrf NAME|)`

Parameters `vrf` The VPN routing/forwarding instance

`NAME` Specify the name of the VPN routing/forwarding instance

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
# show debugging ipv6 pim
PIMv6 Debugging status:
  PIMv6 event debugging is on
  PIMv6 MFC debugging is on
  PIMv6 state debugging is on
  PIMv6 incoming packet debugging is on
  PIMv6 outgoing packet debugging is on
  PIMv6 Hello HT timer debugging is on
```

```
PIMv6 Hello NLT timer debugging is on
  PIMv6 Hello THT timer debugging is on
  PIMv6 Join/Prune JT timer debugging is on
  PIMv6 Join/Prune ET timer debugging is on
  PIMv6 Join/Prune PPT timer debugging is on
  PIMv6 Join/Prune KAT timer debugging is on
  PIMv6 Join/Prune OT timer debugging is on
  PIMv6 Assert AT timer debugging is on
  PIMv6 Register RST timer debugging is on
  PIMv6 Bootstrap BST timer debugging is on
  PIMv6 Bootstrap CRP timer debugging is on
  PIMv6 mib debugging is on
  PIMv6 nexthop debugging is on
  PIMv6 mtrace debugging is on
  PIMv6 NSM debugging is on
  PIMv6 MSDP debugging is on
```

show ipv6 pim interface

Use this command to display information about interfaces configured for PIM.

Command Syntax `show ipv6 pim interface show ipv6 pim interface detail show ipv6 pim (vrf NAME|) interface show ipv6 pim (vrf NAME|) interface detail`

Parameters `vrf` The VPN routing/forwarding instance

`NAME` Specify the name of the VPN routing/forwarding instance `detail` Display detailed information about a PIM interface

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show  ipv6  pim interface detail eth1 (vif 0):
  Address fe80::5054:ff:fe14:857, DR fe80::5054:ff:fe14:857
  Hello period 30 seconds, Next Hello in 20 seconds
  Triggered Hello period 5 seconds
  Propagation delay is 1000 milli-seconds Interface ID: Router-
ID:1.1.1.1 Local-ID 3
  Secondary addresses:
   3ffe:192:168:10::53
```

```
   Neighbors:  eth2 (vif 2):
   Address fe80::5054:ff:fe52:219e, DR fe80::5054:ff:fe63:c0ae
   Hello period 30 seconds, Next Hello in 20 seconds
   Triggered Hello period 5 seconds
   Propagation delay is 1000 milli-seconds
   Interface ID: Router-ID:1.1.1.1 Local-ID 4   ECMP REDIRECT, bundle
 : bundle1, status :  allowed
   Secondary addresses:3ffe:192:168:1::53
   Neighbors:    fe80::5054:ff:fe21:5e56
 fe80::5054:ff:fe29:f7f3    fe80::5054:ff:fe63:c0ae
```

Table 2-188:

Entry	Description
Interface name	As stated
Address	The IPv6 address of the interface.
DR	The IPv6 address of the Designated Router (DR).
Hello period	When PIM is enabled on an interface or a router first starts, the Hello Timer of that interface is set to a random value between 0 and Triggered_Hello_Delay. This prevents synchronization of Hello messages if multiple routers are powered on simultaneously. After the initial randomized interval, Hello messages MUST be sent every Hello_Period seconds. The Hello Timer should not be reset except when it expires.
Next Hello	The time period before the next Hello is sent.
Triggered Hello period	A per-interface Hello Timer (HT(I)) is used to trigger sending Hello messages on each active interface. When PIM is enabled on an interface or a router first starts, the Hello Timer of that interface is set to a random value between 0 and Triggered_Hello_Delay.
Propagation delay	The Propagation Delay field of the LAN Prune Delay option (if present) in the Hello message.
ECMP REDIRECT	Whether Equal-Cost Multiple-Path (ECMP) is allowed and on which bundle.
Secondary address	As stated.
Neighbors	The IPv6 addresses of known Multicast neighbors.

show ipv6 pim mroute

Use this command to display information the IPv6 multicast routing table, or the IPv6 multicast routing table based on the specified address or addresses.

Command Syntax `show ipv6 pim mroute (detail|) show ipv6 pim mroute X:X::X:X (detail|) show ipv6 pim mroute X:X::X:X X:X::X:X (detail|) show ipv6 pim (vrf NAME|) mroute (detail|) show ipv6 pim (vrf NAME|) mroute X:X::X:X (detail|) show ipv6 pim (vrf NAME|) mroute X:X::X:X X:X::X:X (detail|)`

Parameter `vrf` The VPN routing/forwarding instance

`NAME` Specify the name of the VPN routing/forwarding instance

`X:X::X:X` Display all entries for this group IPv6 address `X:X::X:X`

Display all entries for this source IPv6 address `detail` Display

detailed PIM multicast routing table information

Note: A group IP address and a source IP address cannot be used simultaneously.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
    #show ipv6 pim mroute

    IPv6 Multicast Routing Table

    (*,*,RP) Entries: 0
    (*,G) Entries: 2
    (S,G) Entries: 1
    (S,G,rpt) Entries: 1
    FCR Entries: 1

    (*, ff05::2)
    RP: 3ffe:192:168:1::53
    RPF nbr: ::
    RPF idx: None
    Upstream State: JOINED
     Local     i.i.............................
     Joined    j.............................
     Asserted  ..............................
    FCR:
(*, ff1e::10)
RP: 3ffe:192:168:1::53
RPF nbr: ::
RPF idx: None
Upstream State: JOINED
 Local     ..............................
 Joined    ..j............................
 Asserted  ..............................
FCR:
Source: 3ffe:172:31:1::96
 Outgoing  ..o............................
 KAT timer running, 207 seconds remaining
 Packet count 1

(3ffe:172:31:1::96, ff1e::10)
RPF nbr: fe80::202:a5ff:fe4f:1073
```

```
RPF idx: eth3
SPT bit: 0
Upstream State: JOINED
 Local     ..............................
 Joined    ..............................
 Asserted  ..............................
 Outgoing  ..o...........................

(3ffe:172:31:1::96, ff1e::10, rpt) RP: 3ffe:192:168:1::53
RPF nbr: ::
RPF idx: None
Upstream State: NOT PRUNED
 Local     ..............................
 Pruned    ..............................
 Outgoing  ..............................
#
```

Table 2-189: Show ipv6 pim mroute

Entries	Description
(*,*,RP) Entries	Optional (*,*,RP) (RFC 4601), PIM Multicast Border Router feature and authentication using IPsec that lack sufficient deployment experience. this is obsoleted by RFC 7761.
(*,G) Entries	A wild card Group entry for all sources within group G.
(S,G) Entries	Source Specific to a Group. IGMPv3 permits a receiver to join a group and specify that it only wants to receive traffic for a group if that traffic comes from a particular source.
(S, G, rpt) Entries	Source Specific to a Group and Rendezvous Point Tree entries.
RP	Rendezvous Point address
RPF nbr	“Reverse Path Forwarding Neighbor” address. The RPF Neighbor of a router with respect to an address is the neighbor that the MRIB indicates should be used to forward packets to that address.

Table 2-189: (Continued)Show ipv6 pim mroute

Entries	Description
RPF idx	RPF interface (RP) is the interface the MRIB indicates would be used to route packets to the RP, except at the RP when it is the decapsulation interface (the “virtual” interface on which Register packets are received).
SPT bit	The SPT bit is used to indicate whether forwarding is taking place on the (S,G) Shortest Path Tree (SPT) or on the (*,G) tree.
Upstream State	The state of the a particular entry. States are: Local, Joined, Pruned Not Pruned, Asserted, or Outgoing.
KAT timer running	Keep Alive Timer.
Source	The Source address.

show ipv6 pim neighbor

Use this command to display IPv6 PIM neighbor information.

Command Syntax `show ipv6 pim neighbor (detail|) show ipv6 pim neighbor IFNAME (detail|) show ipv6 pim neighbor IFNAME X:X::X:X (detail|) show ipv6 pim (vrf NAME|) neighbor (detail|) show ipv6 pim (vrf NAME|) neighbor IFNAME (detail|) show ipv6 pim (vrf NAME|) neighbor IFNAME X:X::X:X (detail|)`

Parameters

`vrf`	The VPN routing/forwarding instance
`NAME`	Specify the name of the VPN routing/forwarding instance
`IFNAME`	Name of the interface
`X:X::X:X`	IPv6 address of the neighbor interface
`detail`	Display detailed information for a PIM neighbor

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show ipv6 pim neighbor detail rtr6# show ipv6 pim
neighbor detail Nbr fe80::5054:ff:fe21:5e56 (eth2)
Expires in 83 seconds, uptime 01:37:14
Holdtime: 105 secs, T-bit: off, Lan delay: 1, Override interval: 3
DR priority: 1, Gen ID: 321289676,
Interface ID: Router-ID: 4.4.4.4 Local-ID: 4, ECMP
REDIRECT enabled
Secondary addresses:
  3ffe:192:168:1::150

Nbr fe80::5054:ff:fe29:f7f3 (eth2)
Expires in 79 seconds, uptime 01:37:15
Holdtime: 105 secs, T-bit: off, Lan delay: 1, Override interval: 3
DR priority: 1, Gen ID: 847253139,
Interface ID: Router-ID: 2.2.2.2 Local-ID: 4, ECMP
REDIRECT enabled
Secondary addresses:
  3ffe:192:168:1::149
```

Table 2-190: Show ipv6 pim Neighbor

Entry	Description
Interface name	As stated
Address	The IPv6 address of the interface.
DR	The IPv6 address of the Designated Router (DR).
Hello period	When PIM is enabled on an interface or a router first starts, the Hello Timer of that interface is set to a random value between 0 and Triggered_Hello_Delay. This prevents synchronization of Hello messages if multiple routers are powered on simultaneously. After the initial randomized interval, Hello messages MUST be sent every Hello_Period seconds. The Hello Timer should not be reset except when it expires.
Next Hello	The time period before the next Hello is sent.
Triggered Hello period	A per-interface Hello Timer (HT(I)) is used to trigger sending Hello messages on each active interface. When PIM is enabled on an interface or a router first starts, the Hello Timer of that interface is set to a random value between 0 and Triggered_Hello_Delay.
Propagation delay	The Propagation Delay field of the LAN Prune Delay option (if present) in the Hello message.
ECMP REDIRECT	Whether Equal-Cost Multiple-Path (ECMP) is allowed and on which bundle.
Secondary address	As stated.

show ipv6 pim nexthop

Use this command to display the nexthop information from NSM as used by IPv6 PIM.

Command Syntax `show ipv6 pim nexthop`

```
show ipv6 pim (vrf NAME|) nexthop
```

Parameter `vrf` The VPN routing/forwarding instance

`NAME` Specify the name of the VPN routing/forwarding instance

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ipv6 pim nexthop

Flags: N = New, R = RP, S = Source, U = Unreachable
Destination           Type  Nexthop Nexthop Nexthop  Nexthop Metric    Pref
Refcnt
                            Num     Addr    Ifindex  Name
_____________________________________________________________________________
_______
2001:db8:10:5::153    .RS.  1       fe80::20e:cff:fe01:facc  2     30  110
1
```

show ipv6 pim bsr-router

Use this command to show the bootstrap router v2 address.

Command Syntax `show ipv6 pim bsr-router show ipv6 pim (vrf NAME|) bsr-router`

Parameters `vrf` The VPN routing/forwarding instance

`NAME` Specify the name of the VPN routing/forwarding instance

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before SWMRE version 1.3. Example

```
#show ipv6 pim bsr-router
  PIMv2 Bootstrap information
  This system is the Bootstrap Router (BSR)
    BSR address: 3ffe:b00:c18:1::10
    Uptime:      00:37:12, BSR Priority: 64, Hash mask length: 10
    Next bootstrap message in 00:00:04
    Role: Candidate BSR
    State: Elected BSR
    Candidate RP: fe80::5054:ff:fe21:5e56(eth1)
    Advertisement interval 60 seconds
```

```
Next C-RP advertisement in 00:00:27
```

Table 2-191: Show ipv6 pim bsr-router

Entry	Description
BSR address	Address of the Bootstrap router (BSR).
Uptime	As Stated.
BSR Priority	The current priority of the BSR (this is configurable).
Hash mask length	For Rendezvous Point (RP) addresses in the matching group-range-to-RP mappings, compute a value — Value(G,M,C(i))= (1103515245 * ((1103515245 * (G&M)+12345) XOR C(i)) + 12345) mod 2^31 where C(i) is the RP address and M is a hash-mask.
Next bootstrap message	Time until next boostrap message.
Role	AS stated..
State	As stated..

Table 2-191: Show ipv6 pim bsr-router

Entry	Description
Candidate RP	Address of the rendezvous point (RP).
Advertisement interval	As stated.
Next C-RP advertisement	Time before the next Candidate RP is advertised.

show ipv6 pim local-members

Use this command to display information about local membership for PIM interfaces.

Command Syntax `show ipv6 pim local-members show ipv6 pim local-members IFNAME show ipv6 pim (vrf NAME|) local-members show ipv6 pim (vrf NAME|) local-members IFNAME`

Entries	Description
Port	Port name
(*, G)	State that maintains the Rendezvous Point for the Group (G).

Parameters `vrf` The VPN routing/forwarding instance

`NAME` Specify the name of the VPN routing/forwarding instance `IFNAME` Display neighbors for an interface name

Command Mode

Privileged Exec and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ipv6 pim local-members PIM Local
membership information

eth1:
  (*, ff05::2) : Include

eth2:
  (*, ff05::2) : Include
  (*, ff1e::10) : Include
#
```

Table 2-192: Show ipv6 pim local-members output

show ipv6 pim rp-hash

Use this command to display the rendezvous point (RP) based on the group selected.

Command Syntax `show ipv6 pim rp-hash X:X::X:X show ipv6 pim (vrf NAME|) rp-hash X:X::X:X`

Parameters `vrf` The VPN routing/forwarding instance

`NAME` Specify the name of the VPN routing/forwarding instance `X:X::X:X` Specify a group address

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ipv6 pim rp-hash ff1e::10
    RP: 3ffe:192:168:1::57
    Info source: 3ffe:192:168:1::57, via bootstrap
#
```

Table 2-193: Show ipv6 pim rp-hash

Entries	Description
RP	Address of the Rendezvous Point
Info source	Address of the information source. In this case the information comes from the Bootstrap router.

show ipv6 pim rp mapping

Use this command to display the mappings for the PIM group to the active rendezvous points.

Command Syntax `show ipv6 pim rp mapping show ipv6 pim (vrf NAME|) rp mapping`

Parameter `vrf` The VPN routing/forwarding instance

`NAME` Specify the name of the VPN routing/forwarding instance

Command

Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#sh ipv6 pim rp mapping
PIM Group-to-RP Mappings Override RP cnt: 0


Group(s): ff00::/8, Static
    RP: aab1:23::1
         Uptime: 00:05:44
    RP: a121:33::1
         Uptime: 00:00:29
    RP: 3ffe:172:31:12::2
         Uptime: 00:14:54 Embedded RP Groups:
```

undebug all ipv6 pim

Use this command to disable all PIM debugging.

Command Syntax `undebug all ipv6 pim undebug (vrf NAME|) all ipv6 pim`

Parameter `vrf` The VPN routing/forwarding instance

`NAME` Specify the name of the VPN routing/forwarding instance

Command Mode

Privileged Exec mode and Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#undebug all ipv6 pim
```

SECTION 8 Data Center Bridging

Data Center Bridging Configuration Guide

Contents

This guide contains these chapters:

- Chapter 1, *Enhanced Transmission Selection Configuration*
- Chapter 2, *Priority-based Flow Control Configuration*
- Chapter 3, *Quantized Congestion Notification Configuration*
- Chapter 4, *DCBx Configuration*

CHAPTER 1 Enhanced Transmission Selection Configuration

This chapter shows how to:

- Enable ETS on a bridge and interface
- Configure priorities and bandwidth for ETS

Topology

Figure 1-147: ETS-Enabled Bridge

Configuring a Bridge and Interface for ETS

`#configure terminal`	Enter configure mode
`(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge 1 as an IEEE VLAN-enabled bridge
`(config)#data-center-bridging enable bridge 1`	Enables DCB on the bridge
`(config)#enhanced-transmission-selection enable bridge 1`	Enables ETS on the bridge
`(config)#interface eth1`	Configure interface eth1
`(config-if)#switchport`	Configure eth1 as a layer 2 port
`(config-if)#bridge-group 1`	Configure eth1 in bridge group 1
`(config-if)#lldp-agent`	Enter into LLDP agent mode.
`(lldp-agent)#set lldp enable txrx`	Configure LLDP for transmit and receive mode on eth1
`(lldp-agent)#lldp tlv-select ieee-8021-orgspecific`	Configure LLDP to send an IEEE 802.1 organizationally specific TLV
`(lldp-agent)#exit`	Exit from LLDP mode.

(config-if)#enhanced-transmission-selection mode on	Start sending DCBX TLVs in LLDP messages

Configuring Priorities and Bandwidth for ETS

#configure terminal	Enter configure mode
(config)#bridge 1 protocol ieee vlan-bridge	Create bridge 1 as an IEEE VLAN-enabled bridge

Enhanced Transmission Selection Configuration

(config)#data-center-bridging enable bridge 1	Enables DCB on the bridge
(config)#enhanced-transmission-selection enable bridge 1	Enables ETS on the bridge
(config)#interface eth1	Configure interface eth1
(config-if)#switchport	Configure eth1 as a layer 2 port
(config-if)#bridge-group 1	Configure eth1 in bridge group 1
(config-if)#lldp-agent	Enter into LLDP agent mode.
(lldp-agent)#set lldp enable txrx	Configure LLDP for transmit and receive mode on eth1
(lldp-agent)#lldp tlv-select ieee-8021-orgspecific	Configure LLDP to send an IEEE 802.1 organizationally specific TLV
(lldp-agent)#exit	Exit from LLDP mode.
(config-if)#enhanced-transmission-selection mode on	Configure the advertise flag and start sending DCBX TLVs in LLDP messages
(config-if)#traffic-class-group 1 add priority 0 1 2	Configure TCG 1 and add priorities 0, 1, and 2
(config-if)#traffic-class-group 0 add priority 3 4 5	Configure TCG 0 and add priorities 3, 4, and 5
(config-if)#bandwidth-percentage 0 40 1 60	Configure bandwidth percentages for TCG 1 and 1

Validation

Verify the ETS parameters configuration on the port specified.

```
#show enhanced-transmission-selection interface eth1
Interface : eth1
Enhanced Transmission Selection : on

Admin Configuration

Mode Advertise Willing Max-TCG TCG-ID BW% Priorities
================================================================================
On    On        Off        0        0       40      3 4 5
On    On        Off        0        1       60      0 1 2
On    On        Off        0        15      NA      6 7

Operational Configuration
```

```
Oper  Max_TCG TCG-ID  BW%   Priorities
State
================================================================================
On     0       0       40      3 4 5
On     0       1       60      0 1 2
On     0       15      NA      6 7
```

Priority-based Flow Control Configuration

CHAPTER 2 Priority-based Flow Control Configuration

This chapter shows how to:

- Enable PFC on a bridge and interface
- Configure priorities and link delay allowance for PFC
- Configuring application priority for PFC

Topology

Figure 2-148: PFC Enabled Bridge

Configuring a Bridge and Interface for PFC

`#configure terminal`	Enter configure mode
`(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge 1 as an IEEE VLAN-enabled bridge
`(config)#data-center-bridging enable bridge 1`	Enables DCB on the bridge
`(config)#priority-flow-control enable bridge 1`	Enables PFC on the bridge
`(config)#interface eth1`	Configure interface eth1
`(config-if)#switchport`	Configure eth1 as a layer 2 port
`(config-if)#bridge-group 1`	Configure eth1 in bridge group 1
`(config-if)#lldp-agent`	Enter into LLDP agent mode.
`(lldp-agent)#set lldp enable txrx`	Configure LLDP for transmit and receive mode on eth1

(lldp-agent)#lldp tlv-select ieee-8021-orgspecific	Configure LLDP to send an IEEE 802.1 organizationally specific TLV set in the packet
(lldp-agent)#exit	Exit from LLDP mode.
(config-if)#priority-flow-control mode on	Configure the advertise flag and start sending DCBX TLVs in LLDP messages

Configuring Priorities and Link Delay Allowance for PFC

#configure terminal	Enter Configure Mode.
(config)#bridge 1 protocol ieee vlan-bridge	Create bridge 1 as an IEEE VLAN-enabled bridge

Priority-based Flow Control Configuration

(config)#data-center-bridging enable bridge 1	Enables DCB on the bridge
(config)#priority-flow-control enable bridge 1	Enables PFC on the bridge
(config)#interface eth1	Configure interface eth1
(config-if)#switchport	Configure eth1 as a layer 2 port
(config-if)#bridge-group 1	Configure eth1 in bridge group 1
(config-if)#lldp-agent	Enter into LLDP agent mode.
(lldp-agent)#set lldp enable txrx	Configure LLDP for transmit and receive mode on eth1
(lldp-agent)#lldp tlv-select ieee-8021-orgspecific	Configure LLDP to send an IEEE 802.1 organizationally specific TLV set in the packet
(lldp-agent)#exit	Exit from LLDP mode.
(config-if)#priority-flow-control mode on	Configure the advertise flag and start sending DCBX TLVs in LLDP messages
(config-if)#priority-flow-control cap 4	Configure the maximum number of PFC priorities
(config-if)#priority-flow-control enable priority 2 4 5	Enable PFC on priorities 2, 4, and 5
(config-if)#priority-flow-control linkdelay-allowance allowance 34567	Configure the link delay

Validation

1. Verify the default data set.

```
#sh priority-flow-control statistics bridge
1 bridge : 1
interface pri pause sent     pause received
=========================================
eth1      0  00             00 eth1      1
00              00 eth1      2  00
00 eth1      3  00             00 eth1     4
00              00 eth1      5  00
```

```
00 eth1      6  00            00 eth1      7
00              00

#sh priority-flow-control details bridge 1

Admin Configuration
interface  mode  advertise willing   cap    link delay     priorities allowance
================================================================================

eth1       on     on      off       4      34567            2 4 5

Operational Configuration ------------------------
-
interface state cap   link delay   priorities allowance
============================================== eth1
on     4       34567          2 4 5
```

Priority-based Flow Control Configuration

Configuring Application Priority for PFC

`#configure terminal`	Enter configure mode
`(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge 1 as an IEEE VLAN-enabled bridge.
`(config)#data-center-bridging enable bridge 1`	Enables DCB on the bridge
`(config)#application-priority enable bridge 1`	Enables application priority on the bridge
`(config)#interface eth1`	Configure interface eth1
`(config-if)#switchport`	Configure eth1 as a layer 2 port
`(config-if)#bridge-group 1`	Configure eth1 in bridge group 1
`(config-if)#lldp-agent`	Enter into LLDP agent mode.
`(lldp-agent)#set lldp enable txrx`	Configure LLDP for transmit and receive mode on eth1
`(lldp-agent)#lldp tlv-select ieee-8021-orgspecific`	Configure LLDP to send an IEEE 802.1 organizationally specific TLV set in the packet
`(lldp-agent)#exit`	Exit from LLDP mode.
`(config-if)#application-priority enable`	Configure the advertise flag and start sending DCBX TLVs in LLDP messages
`(config-if)#tcp port-no 23 priority 6`	Enable priority for protocol using port number
`(config-if)#tcp service-name telnet priority 6`	Enable priority for protocol using TCP service-name

Validation

1. Verify the default data set.

```
#show application-priority interface eth1
bridge : 1
Application Priority : On

Admin Configuration
intf  Admin Config Protocol  ProtoId Priorities Mode
      Advertise

================================================================================
eth1 On    On        tcp          telnet     6
```

Priority-based Flow Control Configuration

CHAPTER 3 Quantized Congestion Notification Configuration

This chapter shows how to:

- Enable QCN on a bridge and interface
- Enable a Congestion Notification Priority Value (CNPV) and create a Congestion Point (CP)

Topology

Figure 3-149: PFC-Enabled Bridge

Configuring a Bridge and Interface for QCN

`#configure terminal`	Enter configure mode
`(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge 1 as an IEEE VLAN-enabled bridge
`(config)#data-center-bridging enable bridge 1`	Enable DCB on the bridge
`(config)#qcn enable bridge 1`	Enable QCN on the bridge
`(config-qcn)#exit`	Exit QCN mode
`(config)#interface eth1`	Configure interface eth1
`(config-if)#switchport`	Configure eth1 as a layer 2 port
`(config-if)#bridge-group 1`	Configure eth1 in bridge group 1
`(config-if)#lldp-agent`	Enter into LLDP agent mode.
`(lldp-agent)#set lldp enable txrx`	Configure LLDP for transmit and receive mode on eth1
`(lldp-agent)#lldp tlv-select ieee-8021-orgspecific`	Configure LLDP to send an IEEE 802.1 organizationally specific TLV
`(lldp-agent)#exit`	Exit from LLDP mode.

Validation

```
#show qcn configuration bridge 1

 QCN:   Enable
 CNM Transmit Priority: 6
 Discarded Frames: 0
 Errored Port List: NONE
 Priority       CNPV
 ========       ====
```

Quantized Congestion Notification Configuration

```
 0              No
 1              No
 2              No
 3              No
 4              No
 5              No
 6              No
 7              No CNPV details:

 CNPV  DefModeChoice  AltPriority  DefenseMode
 ====  =============  ===========  ==============

 CNPV details per interface:
 Interface       CNPV  DefModeChoice  AltPriority  DefenseMode     XmitReady
 ==============  ====  =============  ===========  ==============  =========

 Congestion Point Details:
 Interface       CpId      W     SampleBase  MinHdrOctet  Qsp
 ==============  ========  ====  ==========  ===========  ===
```

Enable a CNPV and Create a CP

`#configure terminal`	Enter configure mode
`(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge 1 as an ieee vlan enabled bridge
`(config)#data-center-bridging enable bridge 1`	Enables DCB on the bridge
`(config)#qcn enable bridge 1`	Enables QCN on the bridge
`(config-qcn)#cnpv 5`	Set the CNPV value on the QCN enabled bridge
`(config-qcn)#exit`	Exit QCN mode
`(config)#interface eth1`	Configure interface eth1
`(config-if)#switchport`	Configure eth1 asa layer 2 port
`(config-if)#bridge-group 1`	Configure eth1 in bridge group 1
`(config-if)#lldp-agent`	Enter into LLDP agent mode.

(lldp-agent)#set lldp enable txrx	Configure LLDP for transmit and receive mode on eth1
(lldp-agent)#lldp tlv-select ieee-8021-orgspecific	Configure LLDP to send an IEEE 802.1 organizationally specific TLV
(lldp-agent)#exit	Exit from LLDP mode.
(config-if)#cp enable cnpv 5 sample-base 10000 weight 2	Configure the congestion point

Validation

1. Verify the QCN configuration on the bridge.

```
#show qcn configuration bridge 1
```

Quantized Congestion Notification Configuration

```
QCN:   Enable
CNM Transmit Priority: 6
Discarded Frames: 0
Errored Port List: NONE

Priority       CNPV
========       ====
0              No
1              No
2              No
3              No
4              No
5              Yes
6              No
7              No CNPV details:

CNPV  DefModeChoice  AltPriority  DefenseMode
====  =============  ===========  ==============
5     AUTO           0            EDGE

CNPV details per interface:
Interface       CNPV  DefModeChoice  AltPriority  DefenseMode     XmitReady
==============  ====  =============  ===========  ==============  =========
eth1            5     COMP           0            EDGE             FALSE
Congestion Point Details:
Interface            CpId        W     SampleBase  MinHdrOctet   Qsp
==============      ========    ====  ==========   ===========  =====
eth1           00ecf4bb530b0005  2      10000            0        31200
```

2. Verify the CNPV value on the QCN enabled bridge.

```
#show qcn cnpv bridge 1

Priority       CNPV
========       ====
0              No
1              No
```

```
 2              No
 3              No
 4              No
 5              Yes
 6              No
 7              No CNPV details:

 CNPV  DefModeChoice  AltPriority  DefenseMode
 ====  =============  ===========  ==============
 5     AUTO           0            EDGE

 CNPV details per interface:
 Interface    CNPV    DefModeChoice    AltPriority    DefenseMode    XmitReady
============== ==== ============= =========== ============== ========= eth1
5 COMP 0 EDGE FALSE
```

3. Verify the CP on the QCN bridge. Quantized

Congestion Notification Configuration

```
# sh qcn cp interface eth1

Congestion Point Details:
 Interface         CpId                  W       SampleBase   MinHdrOctet   Qsp
==============  ================   ====   ==========   ===========   ====== eth1
00ecf4bb530b0005  2      10000       0           31200
```

CHAPTER 4 DCBx Configuration

This chapter show how to:

- Configure ETS parameter exchange
- Configure PFC parameter exchange

Topology

Figure 4-150: DCBx Configuration

Configuring ETS Parameter Exchange

SW1

`#configure terminal`	Enter configure mode
`(config)#bridge 1 protocol ieee vlan-bridge`	Create bridge 1 as an IEEE VLAN-enabled bridge.
`(config)#data-center-bridging enable bridge 1`	Enable DCB on the bridge
`(config)#enhanced-transmission-selection enable bridge 1`	Enable ETS on the bridge
`(config)#interface eth1`	Configure interface eth1
`(config-if)#switchport`	Configure eth1 as a layer 2 port
`(config-if)#bridge-group 1`	Configure eth1 in bridge group 1
`(config-if)#lldp-agent`	Enter into LLDP agent mode.
`(lldp-agent)#set lldp enable txrx`	Configure LLDP for transmit and receive mode on eth1
`(lldp-agent)#lldp tlv-select ieee-8021-orgspecific`	Configure LLDP to send an IEEE 802.1 organizationally specific TLV set in the packet
`(lldp-agent)#exit`	Exit from LLDP mode.
`(config-if)#enhanced-transmission-selection mode on`	Configure the advertise flag and start sending DCBx TLVs in LLDP messages
`(config-if)#traffic-class-group 0 add priority 0 1 2`	Configure TCG 0 and add priorities 0, 1, and 2
`(config-if)#traffic-class-group 1 add priority 3 4 5`	Configure TCG 1 and add priorities 3, 4, and 5
`(config-if)#bandwidth-percentage 0 40 1 60`	Configure the bandwidth percentage for TCG 0and 1

SW2

#configure terminal	Enter configure mode
(config)#bridge 1 protocol ieee vlan-bridge	Create bridge 1 as an IEEE VLAN-enabled bridge.
(config)#data-center-bridging enable bridge 1	Enable DCB on the bridge
(config)#enhanced-transmission-selection enable bridge 1	Enable ETS on the bridge
(config)#interface eth1	Configure interface eth1
(config-if)#switchport	Configure eth1 as a layer 2 port
(config-if)#bridge-group 1	Configure eth1 in bridge group 1
(config-if)#lldp-agent	Enter into LLDP agent mode.
(lldp-agent)#set lldp enable txrx	Configure LLDP for transmit and receive mode on eth1
(lldp-agent)#lldp tlv-select ieee-8021-orgspecific	Configure LLDP to send an IEEE 802.1 organizationally specific TLV set in the packet
(lldp-agent)#exit	Exit from LLDP mode.
(config-if)#enhanced-transmission-selection mode on	Configure the advertise flag and start sending DCBx TLVs in LLDP messages
(config-if)#traffic-class-group 0 add priority 0 1 2	Configure TCG 0 and add priorities 0, 1 and 2
(config-if)# traffic-class-group 1 add priority 3 4 5	Configure TCG 1 and add priorities 3, 4, and 5
(config-if)# bandwidth-percentage 0 40 1 60	Configure the bandwidth percentage for TCG 0 and 1

Validation

SW1

Verify the data set on SW1

```
#show enhanced-transmission-selection interface eth1
Interface : eth1
Enhanced Transmission Selection : on

Admin Configuration

Mode Advertise Willing Max-TCG TCG-ID BW% Priorities
================================================================================
On    On        Off        0        0       40      0 1 2
On    On        Off        0        1       60      3 4 5
On    On        Off        0        15      NA      6 7

Operational Configuration
Oper  Max_TCG TCG-ID  BW%   Priorities
State
================================================================================
On     0      0       40      0 1 2
On     0      1       60      3 4 5
On     0      15      NA      6 7
```

SW2

Verify the data set on SW2

```
#show enhanced-transmission-selection interface eth1
Interface : eth1
Enhanced Transmission Selection : on

Admin Configuration

Mode Advertise Willing Max-TCG TCG-ID BW% Priorities
================================================================================
On    On        Off        0        0       40      0 1 2
On    On        Off        0        1       60      3 4 5
On    On        Off        0        15      NA      6 7

Operational Configuration
Oper  Max_TCG TCG-ID  BW%   Priorities
State
================================================================================
On     0      0       40      0 1 2
On     0      1       60      3 4 5
On     0      15      NA      6 7
```

Configuring PFC Parameter Exchange

SW2

#configure terminal	Enter configure mode
(config)#bridge 1 protocol ieee vlan-bridge	Create bridge 1 as an IEEE VLAN-enabled bridge
(config)#data-center-bridging enable bridge 1	Enable DCB on the bridge
(config)#priority-flow-control enable bridge 1	Enable PFC on the bridge
(config)#interface eth1	Configure interface eth1
(config-if)#switchport	Configure eth1 as a layer 2 port
(config-if)#bridge-group 1	Configure eth1 in bridge group 1
(config-if)#lldp-agent	Enter into LLDP agent mode.
(lldp-agent)#set lldp enable txrx	Configure LLDP for transmit and receive mode on eth1
(lldp-agent)#lldp tlv-select ieee-8021-orgspecific	Configure LLDP to send an IEEE 802.1 organizationally specific TLV set in the packet
(lldp-agent)#exit	Exit from LLDP mode.
(config-if)#priority-flow-control mode on	Configure the advertise flag and start sending DCBx TLVs in LLDP messages
(config-if)#priority-flow-control cap 4	Configure the maximum number of PFC priorities

(config-if)#priority-flow-control enable priority 2 4 5	Enables PFC on priorities 2,4, and 5
(config-if)#priority-flow-control linkdelay-allowance 34567	Configure the link delay allowance

SW1

#configure terminal	Enter configure mode
(config)#bridge 1 protocol ieee vlan-bridge	Create bridge 1 as an IEEE VLAN-enabled bridge
(config)#data-center-bridging enable bridge 1	Enable DCB on the bridge
(config)#priority-flow-control enable bridge 1	Enable PFC on the bridge
(config)#interface eth1	Configure interface eth1
(config-if)#switchport	Configure eth1 as a layer 2 port
(config-if)#bridge-group 1	Configure eth1 in bridge group 1
(config-if)#lldp-agent	Enter into LLDP agent mode.
(lldp-agent)#set lldp enable txrx	Configure LLDP for transmit and receive mode on eth1
(lldp-agent)#lldp tlv-select ieee-8021-orgspecific	Configure LLDP to send an IEEE 802.1 organizationally specific TLV set in the packet
(lldp-agent)#exit	Exit from LLDP mode.
(config-if)#priority-flow-control mode on	Configure the advertise flag and start sending DCBx TLVs in LLDP messages
(config-if)#priority-flow-control cap 4	Configure the maximum number of PFC priorities
(config-if)#priority-flow-control enable priority 2 4 5	Enables PFC on priorities 2,4, and 5
(config-if)#priority-flow-control linkdelay-allowance allowance 34567	Configure the link delay

Validation

SW1

Verify the data set.

```
#show priority-flow-control details interface eth1 bridge
: 1
priority flow control : on interface
: eth1

Admin Configuration
mode  advertise willing   cap   link        priorities
delay                                  allowance
================================================================================
on    on        off       4     34567       2 4 5
```

```
Operational Configuration state cap
link        priorities
delay             allowance
================================================================================
on     4     34567      2 4 5
```

SW2

Verify the data set.

```
#show priority-flow-control details interface eth1 bridge
: 1
priority flow control : on interface
: eth1

Admin Configuration
mode  advertise willing   cap   link        priorities
delay                                  allowance
================================================================================
==
on    on        off        4     34567      2 4 5

Operational Configuration state cap
link        priorities
delay              allowance
================================================================================
==
on     4     34567      2 4 5
```

Data Center Bridging Command Reference

Contents

This document contains these chapters:

- Chapter 1, *Enhanced Transmission Selection Commands*
- Chapter 2, *Quantized Congestion Notification Commands*
- Chapter 3, *Priority-based Flow Control Commands*

© Symanitron

CHAPTER 1 Enhanced Transmission Selection Commands

This section list and describe the commands that can be used to configure Enhanced Transmission Selection (ETS) in a Data Center Bridging (DCB) environment. It includes the following commands:

- application-priority advertise-local-config
- application-priority enable (interface)
- application-priority enable (switch)
- bandwidth-percentage
- data-center-bridging
- dcbx enable
- enhanced-transmission-selection accept-peer-config
- enhanced-transmission-selection advertise-local-config
- enhanced-transmission-selection (switch)
- enhanced-transmission-selection (interface)
- ethertype
- max-traffic-class-group
- show application-priority bridge
- show application-priority interface
- show data-center-bridging
- show enhanced-transmission-selection bridge
- show enhanced-transmission-selection interface
- tcp
- traffic-class-group
- udp

application-priority advertise-local-config

Use this command to enable advertising mode for ETS feature on the interface.

Use the no form of this command to disable advertising mode for the interface.

Command Syntax `application-priority advertise-local-config no application-priority advertise-local-config`

Parameters

None

Default

By default, advertising mode for ETS feature on the interface is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth1
                        (config-if)#application-priority advertise-local-config
```

application-priority enable (interface)

Use this command to enable the application priority feature of DCB on an interface.

Use the no form of this command to disable application priority on an interface.

Command Syntax `application-priority enable no application-priority`

Parameters

None

Default

By default, application priority feature of DCB on an interface is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#application-priority enable
```

application-priority enable (switch)

Use this command to enable the application priority feature of DCB on a switch (bridge).

Use the no form of this command to disable application priority on a switch.

Command Syntax `application-priority enable bridge <1-32> no application-priority bridge <1-32>`

Parameters

`<1-32>`	Specify the Bridge ID.

Default

By default, application priority feature of DCB on a switch is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#application-priority enable bridge 2
```

bandwidth-percentage

Use this command to assign a percentage of bandwidth to a traffic class group. The total percentage bandwidth should be equal to 100 percent.

Command Syntax `bandwidth-percentage (<0-1> <0-100> | <0-1> <0-100> <0-1> <0-100>)`

Parameters

`<0-1>`	Specify the traffic class group ID. You can set a bandwidth percentage for up to two IDs.
`<0-100>`	Specify the bandwidth percentage for the traffic class group.

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
(config)#interface eth1
(config-if)#bandwidth-percentage 0 40 0 60
```

data-center-bridging

Use this command to enable DCB (Data Center Bridging) on a switch (bridge).

Use the `no` form of this command to disable DCB.

Command Syntax `data-center-bridging enable bridge <1-32> no data-center-bridging enable bridge <1-32>`

Parameters

`bridge`	Bridge ID.

Default

By default, DCB on a switch is disabled.

Command Mode

Configure mode

Default

DCB is enabled.

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
              (config)#data-center-bridging enable bridge 1


#configure terminal
              (config)#no data-center-bridging enable bridge 1
```

dcbx enable

Use this command to enables DCBX (Data Center Bridging Exchange) on the interface in lldp-agent mode.

Use the `no` form of this command to disable DCBX.

Command Syntax `dcbx enable no dcbx enable`

Parameters

`None`

Default

By default, DCBX is disabled.

Command Mode

LLDP Agent mode

Default

DCB is enabled.

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#lldp-agent
(lldp-agent)#dcbx enable
```

enhanced-transmission-selection accept-peer-config

Use this command to enable willing mode for ETS on the interface.

Use the `no` form of this command to disable willing mode.

Command Syntax `enhanced-transmission-selection accept-peer-config no enhanced-transmission-selection accept-peer-config`

Parameters

None

Default

By default, willing mode is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
                (config-if)#enhanced-transmission-selection accept-peer-config
```

enhanced-transmission-selection advertise-local-config

Use this command to enable advertising mode for ETS on the interface.

Use the `no` form of this command to disable advertising mode.

Command Syntax `enhanced-transmission-selection advertise-local-config no enhanced-transmission-selection advertise-local-config`

Parameters

None

Default

By default, advertising mode for ETS on the interface is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
            (config-if)#enhanced-transmission-selection advertise-local-config
```

enhanced-transmission-selection (switch)

Use this command to enable the ETS feature of DCB on a switch (bridge).

Use the `no` form of this command to disable ETS.

Command Syntax `enhanced-transmission-selection enable bridge <1-32> no enhanced-transmission-selection bridge <1-32>`

Parameters

`<1-32>`	Bridge ID.

Default

By default, ETS feature is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
                        (config)#enhanced-transmission-selection enable bridge 1


#configure terminal
           (config)#no enhanced-transmission-selection bridge 1
```

enhanced-transmission-selection (interface)

Use this command to enable the ETS feature of DCB on an interface.

Use the `no` from of this command to disable the ETS at an interface.

Command Syntax `enhanced-transmission-selection mode (on|auto) no enhanced-transmission-selection`

Parameters

`auto`	Select auto to negotiate ETS capabilities.
`on`	Select on to force enable ETS.

Default

Default is Auto.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#interface eth1
                          (config-if)#enhanced-transmission-selection mode on

(config)#interface eth1
             (config-if)#no enhanced-transmission-selection
```

ethertype

Use this command to set the application priority based on the Ethertype.

Use the `no` parameter along with this command to unset the application priority based on the Ethertype.

Command Syntax `ethertype (value ETHERTYPE | name ETHERNAME) priority <0-7> no ethertype (value ETHERTYPE | name ETHERNAME) priority <0-7>`

Parameters `value`

`ETHERTYPE`

Ethertype value in hexadecimal notation (such as “0xhhhh”).

`name ETHERNAME`

Enter a well-known Ethertype string. Ethertype supports the following protocol names:

ip (IPv4), ipv6 (IPv6), ipx (IPX), x25 (CCITT X.25), arp (Address Resolution), rarp (Reverse Address Resolution), atalkddp (Appletalk DDP), atalkaarp (Appletalk AARP), atmmulti (MultiProtocol over ATM), atmtransport (Frame-based ATM Transport), pppdiscovery (PPPoE discovery), pppsession (PPPoE Session), xeroxpup (Xerox PUP), xeroxaddrtrans (Xerox PUP Address Translation), g8bpqx25 (G8BPQ AX.25), ieeepup (Xerox IEEE802.3 PUP), ieeeaddrtrans (Xerox IEEE802.3 PUP Address Translation), dec

	(DEC Assigned), decdnadumpload (DEC DNA Dump/Load), decdnaremoteconsole (DEC DNA Remote Console), decdnarouting (DEC DNA Routing), declat (DEC LAT), decdiagnostics (DEC Diagnostics), deccustom (DEC Customer Use), decsyscomm (DEC Systems Comms Arch)
`priority`	User priority value <0-7>.

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#ethertype value 0x0800 priority 6

(config)#interface eth1
(config-if)#ethertype name arp priority 6

(config)#interface eth1
(config-if)#no ethertype value 0x0800 priority 6

(config)#interface eth1
```

```
(config-if)#no ethertype name arp priority 6
```

max-traffic-class-group

Use this command to configure the maximum number of traffic classes that you can enable on ETS.

Use the `no` form of this command to set the maximum number of traffic classes to 0 which is the default.

If the value is 0, you can add priorities for all 8 traffic classes with the traffic-class-group command. When the number of traffic classes is not 0, you can add priorities with the traffic-class-group command until the maximum is reached.

Command Syntax `max-traffic-class-group <0-2>` `no max-traffic-class-group`

Parameters

`<0-2>`	The maximum number of traffic class groups.

Default

Default maximum number of traffic classes is 0.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#max-traffic-class-group 2
(config-if)#
```

show application-priority bridge

Use this command to display application priority table for a bridge (switch).

Command Syntax `show application-priority bridge <1-32>`

Parameter

`<1-32>`	Bridge ID.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example 1

```
#show application-priority bridge 2 bridge
: 2

Admin Configuration
intf  Admin Config Protocol ProtoId Priorities Mode
      Advertise

================================================================================
eth1  On     On         Ethertype    ip          6 eth1   On     On         Ethertype
arp        6 eth1  On     On        udp         telnet     6 eth1  On     On        tcp
telnet     6
```

Table 1-197 Explains the show command output fields

Table 1-197: Show application-priority output fields

Field	Description
intf	Number of maximum intf admin session.
Admin mode	Allows the user to configure and monitor security data.
Config Advertise	Allows the user to configure and advertise security data.
Protocol	Used to interconnect network devices on the internet.
Proto Id	Used to identify the network devices on the internet.
Priorities	Used to provide the priorities for the data.

show application-priority interface

Use this command to display application priority table for an interface.

Command Syntax `show application-priority interface IFNAME`

Parameter

`IFNAME` Name of the interface.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example 1

```
#show application-priority interface eth1 bridge
: 2
Application Priority : On

Admin Configuration
intf  Admin Config    Protocol     ProtoId   Priorities
      Mode  Advertise
================================================================================
eth1  On    On        Off          -           -         -
```

Table 1-198 Explains the show command output fields

Table 1-198: Show application-priority interface output fields

Field	Description
intf	Number of maximum intf admin session.
Admin mode	Allows the user to configure and monitor security data.
Config Advertise	Allows the user to configure and advertise security data.
Protocol	Used to interconnect network devices on the internet.
Proto Id	Used to identify the network devices on the internet.
Priorities	Used to provide the priorities for the data.

show data-center-bridging

Use this command to display administrative, operational, and remote parameters for DCBX.

Command Syntax

```
  show data-center-bridging (admin-details | operational-details | remote-details)
interface IFNAME
```

Parameter `admin-details` Administrative details.

`operational-details`

Operational details.

`remote-details` Remote details.

`interface` Interface.

`IFNAME` Name of the interface.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example 1

```
#show data-center-bridging operational-details interface eth1
PFC Operational details interface :
eth1
state cap    syncd priorities
================================================================================    Off
0      Off


ETS Operational details interface :
eth1
State MAX_TCGs  TCG-ID    BW%  priorities
================================================================================
On     0         0         0
On     0         1         0          1234567
On     0         2         0
On     0         3         0
On     0         4         0
On     0         5         0
On     0         6         0
On     0         7         0
```

```
On     0          15         NA      0


Application priority operational details
interface : eth1
State Adv   Will  Proto ProtoID    priorities    app
================================================================================
```

Table 1-199 Explains the show command output fields

Table 1-199: show data-center-bridging output fields

Field	Description
State	State of the session.
Cap	Allows the user to configure and monitor security data.
MAX TCGs	Maximum trusted computing group in the interface.
TCG-ID	Trusted computing group identification.
BW	Bandwidth of network.
Will	Used to send and receive the data.
app	Network application.
Protocol	Used to interconnect network devices on the internet.
Proto Id	Used to identify the network devices on the internet.
Priorities	Used to provide the priorities for the data.

show enhanced-transmission-selection bridge

Use this command to display all traffic class groups for a bridge (switch).

Command Syntax `show enhanced-transmission-selection bridge <1-32>`

Parameter

<1-32> Bridge ID.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example 1

```
#show enhanced-transmission-selection bridge
2 bridge : 2
Admin Configuration
intf  Admin Config Willing Max-TCG TCGID BW% Priorities Mode
      Advertise

================================================================================
eth1   On    On         On          0         15    NA   01234567

Operational Configuration
intf  Oper  Max-Tcg  TCGID BW% Priorities
      State
================================================================================
eth1  On     15    NA  01234567
```

Table 1-200 Explains the show command output fields

Table 1-200: show enhanced-transmission-selection bridge output fields

Field	Description
intf	Number of maximum intf admin session.
Admin mode	Allows the user to configure and monitor security data.
Config Advertise	Allows the user to configure and advertise security data.
State	State of the session.
MAX TCGs	Maximum trusted computing group in the interface.

Field	Description
TCG-ID	Trusted computing group identification.
BW	Bandwidth of network.
Willing	Used to send and receive the data.
Protocol	Used to interconnect network devices on the internet.
Proto Id	Used to identify the network devices on the internet.
Priorities	Used to provide the priorities for the data.

show enhanced-transmission-selection interface

Use this command to display all traffic class groups for an interface.

Command Syntax `show enhanced-transmission-selection interface IFNAME`

Parameter

`IFNAME` Name of the interface.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example 1

```
#show enhanced-transmission-selection interface eth1
Interface : eth1
Enhanced Transmission Selection : on

Admin Configuration

Mode Advertise Willing Max-TCG TCG-ID BW% Priorities
================================================================================
On    On        On        0         15     NA           01234567

Operational Configuration
Oper  Max_TCG TCG-ID   BW%   Priorities
State
================================================================================
On    0       15      NA     01234567
```

Table 1-201 Explains the show command output fields

Table 1-201: show enhanced-transmission-selection interface output fields

Field	Description
Admin mode	Allows the user to configure and monitor security data.
Config Advertise	Allows the user to configure and advertise security data.

State	State of the session.
MAX TCGs	Maximum trusted computing group in the interface.
TCG-ID	Trusted computing group identification.

Field	**Description**
BW	Bandwidth of network.
Willing	Used to send and receive the data.
Protocol	Used to interconnect network devices on the internet.
Proto Id	Used to identify the network devices on the internet.
Priorities	Used to provide the priorities for the data.

tcp

Use this to set the application priority based on TCP. The protocol ID is the protocol number in decimal value or protocol service name.

Use the `no` parameter along with this command to unset the application priority based on the selection type.

Command Syntax `tcp (port-no <1-1023>) priority <0-7> no tcp (port-no <1-1023>) priority <0-7> tcp (service-name [PROTOSERV]) priority <0-7> no tcp (service-name [PROTOSERV]) priority <0-7>`

Parameters `port-no` Enter a well-known protocol number in decimal <1-1023>.

`service-name[PROTOSERV]`

Protocol service name. Enter a well-known service name, such as telnet.

`priority` Default priority for CFM frames to be relayed <0-7>.

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#tcp port-no 23 priority 6

(config)#interface eth1 (config-if)#tcp
service-name telnet priority 6

(config)#interface eth1
(config-if)#no tcp port-no 23 priority 6

(config)#interface eth1
(config-if)#no tcp service-name telnet priority 6
```

traffic-class-group

Use this command to add or remove priorities for a traffic class group.

Use the `no` form of this command to remove all traffic-class-groups.

Command Syntax

```
traffic-class-group <0-1> add priority <0-7> (<0-7>(<0-7>(<0-7>(<0-7>(<0-7>(<0-7>(<0-
  7>|)|)|)|)|)|)|) traffic-class-group <0-1> remove priority <0-7> (<0-7>(<0-
7>(<0-7>(<0-7>(<0-7>(<0-
  7>(<0-7>|)|)|)|)|)|)|)
no traffic-class-groups
```

Parameters

`<0-1>`	Specify traffic-class-group ID.
`add priority`	Specify to add a traffic class group
`<0-7>`	Traffic-priority value. Up to seven priorities can be added.
`remove priority`	Specify to remove a traffic class group
`<0-7>`	Traffic-priority value. Up to seven priorities can be removed.

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#traffic-class-group 1 add priority 1 2 3 4 5 6 7

(config)#interface eth1
(config-if)#traffic-class-group 1 remove priority 3 6

(config)#interface eth1
(config-if)#no traffic-class-group
```

udp

Use this to set the application priority based on UDP. The protocol ID is the protocol number in decimal value or protocol service name.

Use the `no` parameter along with this command to unset the application priority.

Command Syntax `udp (port-no <1-1023>) priority <0-7> no udp (port-no <1-1023>) priority <0-7> udp (service-name [PROTOSERV]) priority <0-7> no udp (service-name [PROTOSERV]) priority <0-7>`

Parameters `port-no` Enter a well-known protocol number in decimal <1-1023>.

`service-name [PROTOSERV]`

Protocol service name. Enter a well-known service name, such as telnet.

`priority` Default priority for CFM frames to be relayed <0-7>.

Default

None

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#udp port-no 23 priority 6

(config)#interface eth1 (config-if)#udp
service-name telnet priority 6

(config)#interface eth1
(config-if)#no udp port-no 23 priority 6

(config)#interface eth1
(config-if)#no udp service-name telnet priority 6
```

CHAPTER 2 Quantized Congestion Notification Commands

This section describes the commands that you use to configure Quantized Congestion Notification (QCN) in a Data Center Bridging (DCB) environment. QCN is a IEEE 802.1Qau mechanism that manages network congestion. When a queue reaches a configured threshold, QCN throttles traffic at the source of the congestion by transmitting messages that propagate back to the source and temporarily stop the source from transmitting. When the queue crosses the threshold that indicates the congestion has dissipated, QCN sends a message to allow the source to resume transmitting frames. QCN includes the following commands:

- cnpv
- cp enable
- defense-mode cnpv
- qcn enable
- show qcn configuration
- show qcn cnpv
- show qcn cp

cnpv

Use this command to enable Congestion Notification Priority Values (CNPV). A CNPV corresponds to a class of applications or a single application, such as interprocess communications or disk storage, that have different requirements for network resources as such as latency or bandwidth. There are total of eight CNPVs with one reserved for “best-effort” traffic, meaning you can assign up to seven CNPVs.

Use the `no` form of this command to disable CNPVs.

Command Syntax `cnpv <0-7> (<0-7>(<0-7>(<0-7>(<0-7>(<0-7>(<0-7>|)|)|)|)|)|) no cnpv <0-7> (<0-7>(<0-7>(<0-7>(<0-7>(<0-7>(<0-7>|)|)|)|)|)|)`

Parameters

`<0-7>` Congestion notification priority values (up to seven).

Default

By default, CNPV is disabled.

Command Mode

QCN mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#qcn enable bridge 1
(config-qcn)#cnpv 4 6
```

cp enable

Use this command to create a Congestion Point (CP) for a Congestion Notification Priority Value (CNPV).

Use the `no` form of this command to disable a CP.

Command Syntax `cp enable ((cnpv <0-7>|) (sample-base <10000-4294967295>|) (weight WEIGHT|) no cp (cnpv <0-7>|)`

Parameters `cnpv` Congestion notification priority.

`<0-7>` Congestion notification priority value. `sample-base`

Sample base.

`<10000-4294967295>`

The minimum number of octets to enqueue in the Congestion Point's queue between transmissions of Congestion Notification Messages (CNMs). The default is 150,000.

`weight` Weight in offset calculation.

WEIGHT	The weight change in queue length used to calculate whether the queue length is moving toward or away from the target number of octets for the CP's queue <-10 - 10>. The default is one (1).

Default

Default sample base value is 150,000 and WEIGHT value is 1.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
>ena
#con term
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#interface eth0
(config-if)#cp enable sample-base 100000 weight 2
```

defense-mode cnpv

Use this command to set the defense mode for a Congestion Notification Priority Value (CNPV).

In QCN mode, you can:

- Specify an `admin` type to explicitly set the defense mode and the alternate priority.
- Specify `auto` to derive the defense mode from LLDP Congestion Notification TLVs.

In addition, in interface mode, you can specify `component` to set the defense mode the same as the bridge-level defense mode.

Command Syntax

QCN mode:

```
defense-mode cnpv <0-7> (admin (disabled|edge|interior|interior-ready)
  alternatepriority <0-7> | auto)
```

Interface mode:

```
defense-mode cnpv <0-7> (admin (disabled|edge|interior|interior-ready) alternate-
  priority <0-7> |auto |component)
```

Parameters

`cnpv`	CNPV.
`<0-7>`	CNPV.
`admin`	Explicitly set the defense mode:
`disabled`	Congestion notification is disabled for this CNPV and interface.
`edge`	On this interface and for this CNPV, the priority parameters of input frames are remapped to an alternate value. Congestion notification tags are not output.
`interior`	On this interface and for this CNPV, the priority parameters of input frames are not remapped to another value. Congestion notification tags are not output.

`interior-ready`

On this interface and for this CNPV, the priority parameters of input frames are not remapped to another value. Congestion notification tags can be output.

`alternate-priority`

Explicitly set the alternate priority.

`<0-7>` Alternate priority value.

`auto` Set the defense mode according to LLDP Congestion Notification TLVs and set the alternate priority to the cncpAutoAltPri variable as defined in the 802.1Qau standard.

`component` Set the defense mode the same as the bridge-level defense mode and set the alternate priority to the cncpAutoAltPri variable as defined in the 802.1Qau standard.

Default

None

Command Mode

QCN mode and interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#qcn enable bridge 1
(config-qcn)#defense-mode cnpv 4 admin edge alternate-priority 6

#configure terminal config)#interface eth1
(config-if)#defense-mode cnpv 4 component
```

qcn enable

Use this command to enable QCN at the switch (bridge) level. This command initializes the QCN module with default values.

Use the `no` form of this command to disable QCN.

Command Syntax `qcn enable bridge <1-32> (cnm-transmit-priority <0-7> | ) no qcn bridge <1-32>`

Parameters

`<1-32>`	Bridge ID.
`<0-7>`	Priority to use when transmitting Congestion Notification Messages (CNMs).

Default

By default, QCN is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
>enable
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#qcn enable bridge 1 cnm-transmit-priority 4
```

show qcn configuration

Use this command to show the configuration of the QCN module.

Command Syntax `show qcn configuration bridge <1-32>`

Parameters

`<1-32>`	Bridge ID.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show qcn configuration bridge 2

 QCN:   Enable
 CNM Transmit Priority: 6
 Discarded Frames: 0
 Errored Port List: NONE

  Priority      CNPV
  ========      ====
 0             No
 1             No
 2             Yes
 3             Yes
 4             No
 5             No
 6             No
 7             No CNPV details:

 CNPV  DefModeChoice  AltPriority  DefenseMode
 ====  =============  ===========  ==============
2      AUTO           0            EDGE
3      AUTO           0            EDGE

 CNPV details per interface:
  Interface         CNPV  DefModeChoice  AltPriority  DefenseMode      XmitReady
============== ====  =============  ===========  ==============  =========  eth1
2       ADMIN           1             INTERIOR         TRUE  eth1              3
ADMIN           6           EDGE            FALSE   Congestion Point Details:
```

```
Interface          CpId       W       SampleBase  MinHdrOctet   Qsp  ==============
========    ====   ==========  ==========  === eth1            ********  2.00  0
0             0
```

Table 2-202 Explains the show command output fields.

Table 2-202: show qcn configuration output fields

Field	Description
QCN	Enable the QCN on the bridge and interface.
CNM Transmit Priority	Details of the CNM transmit priority on the interface.
Discarded Frames	Discarded frames detail from the interface.
Errored Port List	List of the port error.
Priority	QCN priority on the interface.
CNPV details	Details of the CNPV on the bridge and interface.
CNPV details per interface	Details of the CNPV per interface.
Congestion Point Details	Details of the configured congestion point value.

show qcn cnpv

Use this command to display application priority table per interface.

Command Syntax `show qcn cnpv ((bridge BRIDGE_ID) | (interface PORT_ID ))`

Parameter

`bridge`	Bridge.
`<1-32>`	Bridge ID.
`interface`	Interface.
`PORT_ID`	Interface name.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example 1

```
#show qcn cnpv bridge 2

  Priority       CNPV
  ========       ====
 0              No
 1              No
 2              Yes
 3              Yes
 4              No
 5              No
 6              No
 7              No CNPV details:

 CNPV  DefModeChoice  AltPriority  DefenseMode
 ====  =============  ===========  ==============
2      AUTO           0            EDGE
3      AUTO           0            EDGE

 CNPV details per interface:
  Interface         CNPV  DefModeChoice   AltPriority   DefenseMode       XmitReady
============== ====  =============  ===========  ==============  =========  eth1
2       ADMIN           1             INTERIOR         TRUE  eth1               3
ADMIN           6           EDGE             FALSE

#show qcn cnpv interface eth1
```

```
                                                                    CNPV
details per interface:
 Interface         CNPV   DefModeChoice    AltPriority  DefenseMode       XmitReady
==============   ====   ============ ===========  ==============  =========  eth1
2      ADMIN             1             INTERIOR          TRUE   eth1               3
ADMIN            6             EDGE             FALSE
```

Table 2-203 Explains the show command output fields.

Table 2-203: show qcn cnpv output fields

Field	Description
Priority	QCN priority on the interface.
CNPV	Status of the CNPV on the bridge and interface.
CNPV details	Details of the CNPV on the bridge and interface.
CNPV details per interface	Details of the CNPV per interface.
Congestion Point Details	Details of the configured congestion point value.

show qcn cp

Use this command to show the configuration of all congestion points on the interface.

Command Syntax `show qcn cp ((bridge <1-32> )|(interface PORT_ID))`

Parameters

`bridge`	Bridge.
`<1-32>`	Bridge ID.
`interface`	Interface.
`PORT_ID`	Interface name.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show qcn cp bridge 2

 Congestion Point Details:
 Interface         CpId      W      SampleBase  MinHdrOctet   Qsp  ==============
========    ====  ========== ===========   === eth1            ********  2.00 0
0             0

#show qcn cp interface eth1

Congestion Point Details:
 Interface         CpId      W      SampleBase  MinHdrOctet   Qsp  ==============
========    ====  ========== ===========   === eth1            ********  2.00 0
0             0
```

Table 2-204 Explains the show command output fields.

Table 2-204: show qcn cp output fields

Field	Description
Congestion Point Details	Details of the configured congestion point value.

CHAPTER 3 Priority-based Flow Control Commands

This section lists and describes the commands that can be used to configure Priority-based Flow Control (PFC) in a Data Center Bridging (DCB) environment.It includes the following commands:

- priority-flow-control accept-peer-config
- priority-flow-control advertise-local-config
- priority-flow-control enable
- priority-flow-control cap
- priority-flow-control enable priority
- priority-flow-control link-delay-allowance
- priority-flow-control mode
- show priority-flow-control details
- show priority-flow-control statistics

priority-flow-control accept-peer-config

Use this command to enable willing mode for PFC on the interface.

If willing is enabled, then by default advertise mode is also enabled.

Use the `no` form of this command to disable willing mode.

Command Syntax `priority-flow-control accept-peer-config` `no priority-flow-control accept-peer-config`

Parameters

None

Default

By default, willing mode for PFC on the interface is disabled. If willing is enabled, then by default advertise mode is also enabled.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#priority-flow-control accept-peer-config
```

priority-flow-control advertise-local-config

Use this command to enable advertising mode for PFC on the interface.

Use the `no` form of this command to disable advertising mode.

Command Syntax `priority-flow-control advertise-local-config` `no priority-flow-control advertise-local-config`

Parameters

None

Default

By default, advertising mode for PFC on the interface is disabled. If willing is enabled, then by default advertise mode is also enabled.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#priority-flow-control advertise-local-config
```

priority-flow-control enable

Use this command to enable Priority-based Flow Control (PFC) on a switch (bridge).

Use the `no` form of this command to disable PFC.

Command Syntax `priority-flow-control enable bridge <1-32> no priority-flow-control bridge <1-32>`

Parameters

`<1-32>`	Bridge ID.

Default

By default, PFC is disabled.

Command Mode

Configure mode

Default

PFC is disabled by default.

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#priority-flow-control enable bridge 32
```

```
#configure terminal
(config)#no priority-flow-control bridge 32
```

priority-flow-control cap

Use this command to configure a priority-flow-control cap for the number of priorities allowed on an interface.

Use the `no` parameter along with this command to return the value to its default level.

Command Syntax `priority-flow-control cap <0-8> no priority-flow-control cap`

Parameters

<0-8>Select a cap value. Zero indicates that there is no limitations.

Default

By default, priority-flow-control cap value is 8.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth2
(config-if)#priority-flow-control cap 7
```

priority-flow-control enable priority

Use this command to enable the PFC at the interface level for a specific priority.

Use the no parameter along with this command to disable PFC for a priority.

Command Syntax

```
priority-flow-control enable priority <0-7> (<0-7>(<0-7>(<0-7> (<0-7>(<0-7>(<0-
  7>(<0-7>|)|)|)|)|)|) no priority-flow-control enable priority <0-7> (<0-7>(<0-
7>(<0-7>(<0-7>(<0-7>(<07>(<0-7>|)|)|)|)|)|)
```

Parameter

<0-7>	Traffic-priority value. You can specify up to seven priorities.

Default

None

Command Mode

Interface mode

Default

PFC is disabled by default.

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#interface eth1
(config-if)#priority-flow-control enable priority 1 2 3 4 5 6 7

(config)#interface eth1
```

```
(config-if)#no priority-flow-control enable priority 2 3 4
```

priority-flow-control link-delay-allowance

Use this command to set PFC link delay allowance on an interface. This command provides allowance for round-trip propagation delay of the link in bits; moreover, it is one of the factors that determines when to trigger PAUSE.

Use the `no` parameter along with this command to unset PFC link delay allowance on an interface.

Command Syntax `priority-flow-control link-delay-allowance <0-4294967296> no priority-flow-control link-delay-allowance`

Parameter

`<0-4294967296>` Link characteristics that affect the link delay (for example, link length).

Command Mode

Interface mode

Default

Default value is zero.

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#priority-flow-control link-delay-allowance 5

(config)#interface eth1
(config-if)#no priority-flow-control link-delay-allowance
```

priority-flow-control mode

Use this command to enable Priority-based Flow Control (PFC) on an interface.

Us the `no` form of this command to disable PFC on an interface.

Command Syntax `priority-flow-control mode (on | auto) no priority-flow-control`

Parameters

`auto`	Negotiate ETS capabilities.
`on`	Force-enable ETS, overriding negotiation.

Default

By default, PFC is disabled.

Command Mode

Interface mode

Default

PFC is disabled by default.

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#priority-flow-control mode auto
```

show priority-flow-control details

Use this command to display the PFC details for a specified interface or bridge.

Command Syntax `show priority-flow-control details ((interface IFNAME)|(bridge <1-32>))`

Parameters

`IFNAME`	Name of the input or output interface.
`<1-32>`	Specify a bridge ID.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Table 3-205: Show priority-flow control details output

Entry	Description
bridge	The bridge number to which this interface is associated (1-32).
priority flow control	Show whether priority flow control is either `on` or `off`.

Example

```
#show priority-flow-control details interface eth1 bridge : 2
priority flow control : on interface : eth1

Admin Configuration
mode  advertise willing   cap   link       priorities
```

```
                                delay
allowance
================================================================================     on
on         off       5     128            2345

Operational Configuration state cap
link        priorities             delay
allowance
================================================================================     on
5      128         2  3 4  5
```

Table 3-205: Show priority-flow control details output (Continued)

Entry	Description
interface	The interface name.
Admin Configuration	The configuration as entered on this device.
mode	The priority flow control operating mode – `on`, `off`, or `auto`.
advertise	Status of advertisement of the configuration to the peer device.
willing	The willingness of the local interface to learn the PFC configuration from the peer. Values are either `on` or `off`.
cap	Cap is a limit set that specifies the maximum number of PFC priorities.
link delay allowance	The allowance made for round-trip propagation delay of the link in bits.
Priorities	Shows the PFCs that have been to be used on the priorities.
Operational Configuration	The actual configuration that exists between this device and its PFC peer.

state	Shows whether PFC is functioning. Values are `on`, `off`, or `auto`.
cap	Cap is the limit that specifies the maximum number of PFC priorities.
link delay allowance	The allowance being used for round-trip propagation delay of the link in bits.
priorities	The PFCs actually being used by this device and its peer.

show priority-flow-control statistics

Use this command to display statistics about the number of PFC Pause frames sent and received for a specified interface or bridge. If you do not specify a bridge or interface, this commands shows statistics for the bridge.

Command Syntax `show priority-flow-control statistics ((interface IFNAME)|(bridge <1-32>))`

Parameters

`<1-32>`	Specify bridge ID.
`IFNAME`	Name of the input or output interface.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show priority-flow-control statistics interface
eth1 bridge : 2 interface : eth1 pause sent
pause received ==============================
5968061499624837205834574861
```

SECTION 9 Virtual Router Redundancy Protocol

Virtual Router Redundancy Protocol Configuration Guide

Contents

This guide contains these chapters:

- Chapter 1, *VRRP Configuration*
- Chapter 2, *VRRP IPv6 Configuration*

© Symanitron Proprietary

CHAPTER 1 VRRP Configuration

This chapter provides an overview of Virtual Router Redundancy Protocol (VRRP) and its implementation with SWMRE. VRRP eliminates the risk of a single point of failure inherent in a static default routing environment. It specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. One of the major advantages of VRRP is that it makes default path available without requiring configuration of dynamic routing on every end-host.

SWMRE only supports VRRP protocol version 3.

For details about the commands used, see the *Virtual Router Redundancy Protocol Command Reference*.

Terminology

Terms related to VRRP configuration are defined in the table below.

Backup Router	The VRRP router that is backing up an IP address. It assumes forwarding responsibility for the virtual IP address if the Master fails.
Critical IP	The IP address that a VRRP router sends/receives messages on for a particular session.
IP Address Owner	The VRRP Router that has the virtual router's IP address(es) as real interface address(es). This is the router that, when up, will respond to packets addressed to one of these IP addresses for ICMP pings, TCP connections, and so on
Master Router	The VRRP router that owns the IP address (i.e., is being backed up), and which is the default router for forwarding for that IP address.
Virtual IP	The IP address that is being backed up by a VRRP session.
Virtual Router	A router managed by VRRP that acts as a default router for hosts on a shared LAN. It consists of a Virtual Router Identifier and a set of associated IP addresses across a common LAN. A VRRP Router might backup one or more virtual routers.
VRRPv2 Router	A router running the Virtual Router Redundancy Protocol version 2. It might participate in one or more virtual routers.
VRRPv3 Router	A router running the Virtual Router Redundancy Protocol version 3. It might participate in one or more virtual routers.

VRRP Process

Typically, end hosts are connected to the enterprise network through a single router (first-hop router) that is in the same Local Area Network (LAN) segment. The most popular method of configuration is for the end hosts to configure statically this router as their default gateway. This minimizes configuration and processing overhead. The main problem with this configuration method is that it produces a single point of failure if this first-hop router fails.

Topology

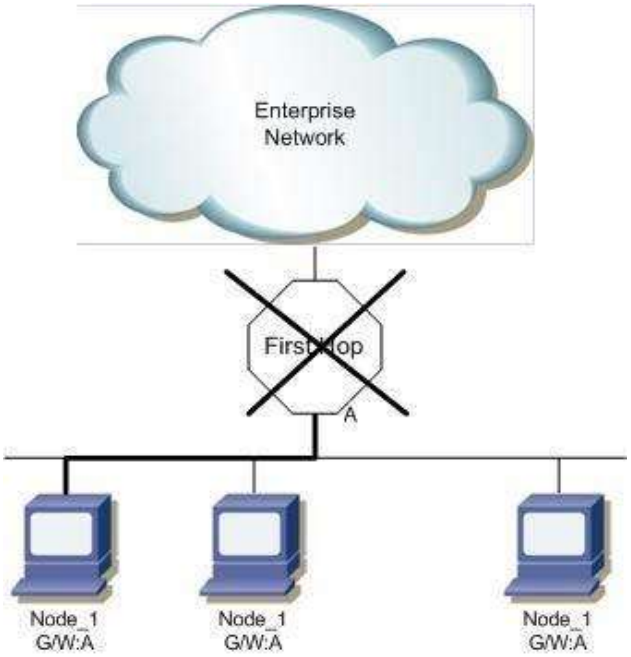


Figure 1-185: VRRP Process - First-Hop Not Reachable

The Virtual Router Redundancy Protocol attempts to solve this problem by introducing the concept of a virtual router, composed of two or more VRRP routers on the same subnet. The concept of a virtual IP address is also introduced, which is the address that end hosts configure as their default gateway. One of the routers called the “Master” forwards packets on behalf of this IP address. In the event that the Master router fails, one of the other routers (Backup) assumes forwarding responsibility for it.

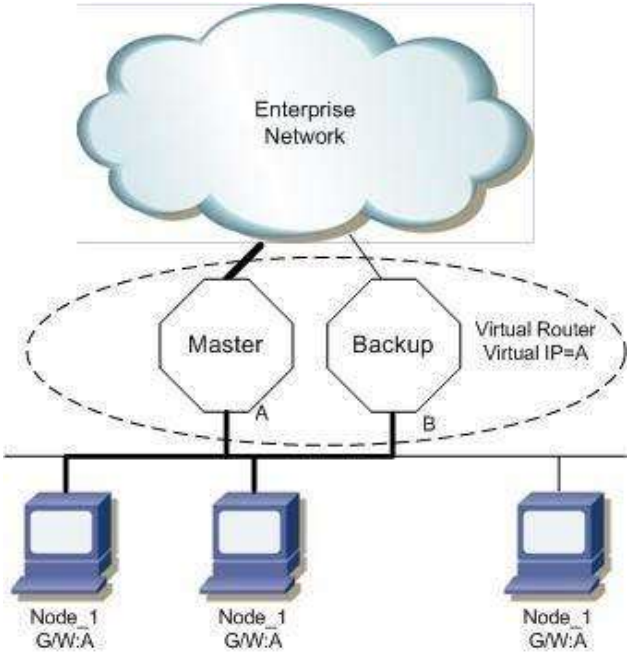


Figure 1-186: VRRP Process - Master and Backup VR

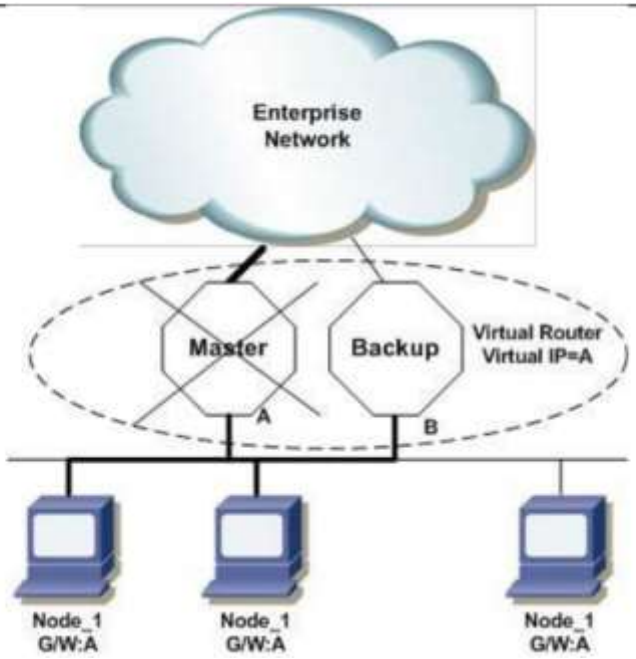


Figure 1-187: VRRP Process - Master Down and Backup Takeover

At first glance, the configuration outlined in might not seem very useful, as it doubles the cost, and leaves one router idle at all times. This, however, can be avoided by creating two virtual routers and splitting the traffic between them.

WARNING -- POTENTIAL DATA LOSS: Adding a default route in the kernel on the interface that is used for VRRP might cause loss of network connectivity. According to the VRRP guidelines, when the VRRP session changes, the MAC address for the machine that attains the master state also changes. The change causes the default route from the kernel to disappear and leads to loss of connectivity. To avoid this situation, add the default route in the NSM and not in the kernel. This ensures that the default route remains on the machine across changes in the VRRP state.

To add default route through NSM, run the following command in NSM:

`ip route 0.0.0.0/0 <IPADDRESS>` where `<IPADDRESS>` is the IP address of the default gateway.

Configuration

One Virtual Router

In this configuration, the end-hosts install a default route to the IP address of virtual router 1(VRID = 1), and both routers R1 and R2 run VRRP. R1 is configured to be the Owner for virtual router 1 (VRID = 1) and R2 as a Backup for virtual router 1. If R1 fails, R2 will take over virtual router 1 and its IP addresses, and provide uninterrupted service for the hosts. Configuring only one virtual router doubles the cost, and leaves R2 idle at all times.

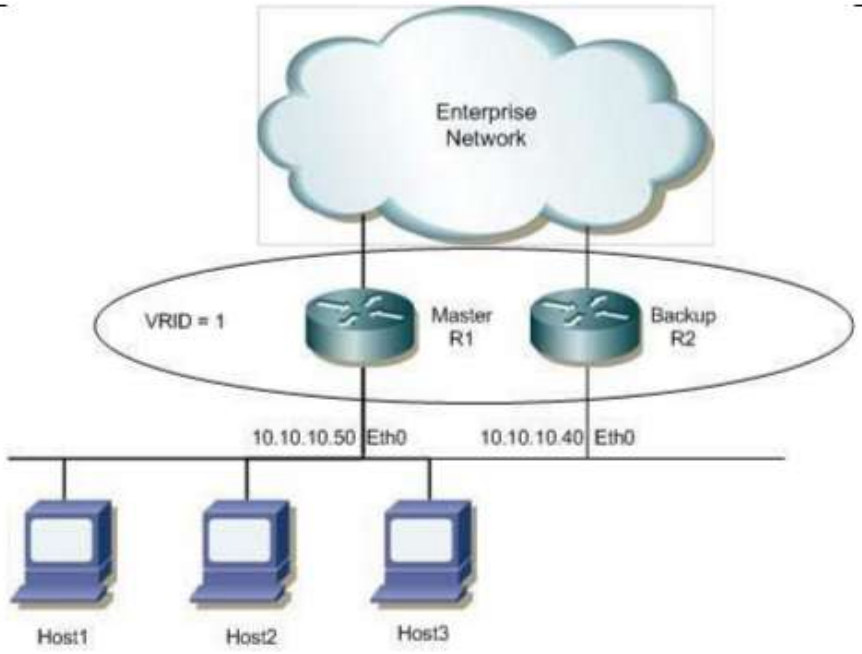


Figure 1-188: VRRP with One Virtual Router

R1

`#configure terminal`	Enter the `Configure` mode.
`(config)#router vrrp 1 eth0`	Create a VRRP instance for interface eth0.
`(config-router)#virtual-ip 10.10.10.50 owner`	Set the virtual IP address for the VRRP session. Define the default state (owner) of the VRRP router within the virtual router.
`(config-router)#preempt-mode true`	Set the preempt mode to specify that the highest priority will function as a backup to master when master is unavailable.
`(config-router)#advertisement-interval 100`	Configure the advertisement interval to 100 centi seconds (value must be a multiple of 5).
`(config-router)#enable`	Enable the VRRP session on the router.

R2

`#configure terminal`	Enter the `Configure` mode.
`(config)#router vrrp 1 eth0`	Create a VRRP instance for interface eth0.
`(config-router)#virtual-ip 10.10.10.50`	Set the virtual IP address for the VRRP session.
`(config-router)#priority 200`	Configure the priority to 200 (less than 255), because R2 is the Backup router.
`(config-router)#preempt-mode true`	Set the preempt mode to specify that the highest priority will function as a backup to master when master is unavailable.
`(config-router)#advertisement-interval 100`	Configure the advertisement interval to 100 centi seconds (value must be a multiple of 5).
`(config-router)#enable`	Enable the VRRP session on the router.

Validation

show vrrp

Two Virtual Routers

In the previous, one virtual router example, R2 is not backed up by R1. This example illustrates how to back up R2 by configuring a second virtual router. In this configuration, R1 and R2 are two virtual routers, and the hosts split their traffic between R1 and R2. R1and R2 functions as backups for each other.

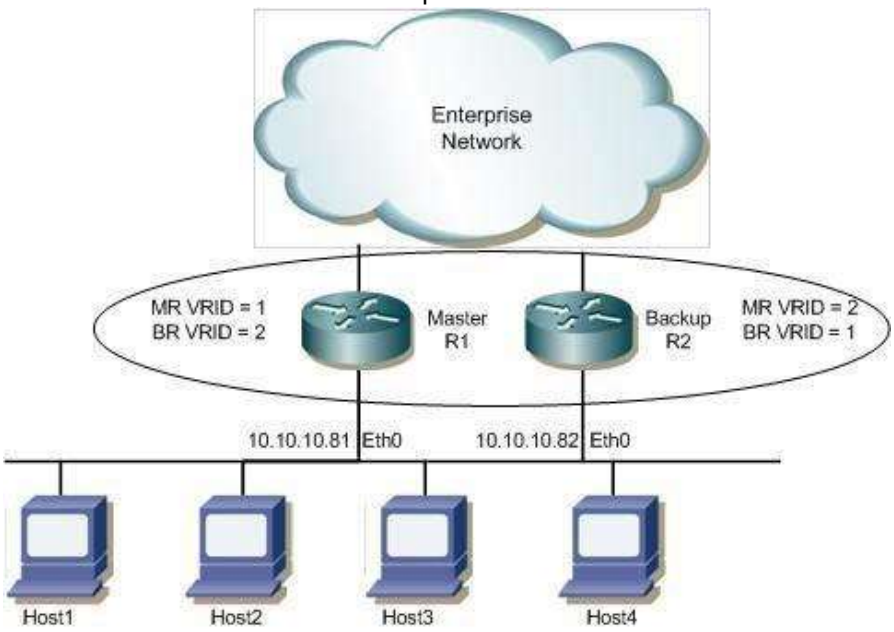


Figure 1-189: Configuring VRRP with Two Virtual Routers

R1

`#configure terminal`	Enter the `Configure` mode.
`(config)#router vrrp 1 eth0`	Create a VRRP instance for interface eth0.
`(config-router)#virtual-ip 10.10.10.81 owner`	Set the virtual IP address for the VRRP session. Define the default state (owner) of the VRRP router within the virtual router.
`(config-router)#preempt-mode true`	Set the preempt mode to specify that the highest priority will function as a backup to master when master is unavailable.
`(config-router)#advertisement-interval 100`	Configure the advertisement interval to 100 centi seconds (value must be a multiple of 5).
`(config-router)#enable`	Enable the VRRP session 1 on the router.
`(config-router)#exit`	Exit `Router` mode and enter the `Configure` mode.
`(config)#router vrrp 2 eth0`	Create a VRRP instance for interface eth0.
`(config-router)#virtual-ip 10.10.10.82`	Set the virtual IP address for the VRRP session.
`(config-router)#priority 200`	Configure the priority to 200 (less than 255), because R2 is the Backup router.
`(config-router)#preempt-mode true`	Set the preempt mode to specify that the highest priority will function as a backup to master when master is unavailable.
`(config-router)#advertisement-interval 100`	Configure the advertisement interval to 100 centi seconds (value must be a multiple of 5).
`(config-router)#enable`	Enable the VRRP session two on the router.

R2

`#configure terminal`	Enter the `Configure` mode.
`(config)#router vrrp 1 eth0`	Create a VRRP instance for interface eth0.
`(config-router)#virtual-ip 10.10.10.81`	Set the virtual IP address for the VRRP session.
`(config-router)#priority 200`	Configure the priority to 200 (less than 255), because R2 is the Backup router.
`(config-router)#preempt-mode true`	Set the preempt mode to specify that the highest priority will function as a backup to master when master is unavailable.
`(config-router)#advertisement-interval 100`	Configure the advertisement interval to 100 centi seconds (value must be a multiple of 5).
`(config-router)#enable`	Enable the VRRP session 1 on the router.
`(config-router)#exit`	Exit the `Router` mode and enter the `Configure` mode.
`(config)#router vrrp 2 eth0`	Create a VRRP instance for interface eth0.
`(config-router)#virtual-ip 10.10.10.82 owner`	Set the virtual IP address for the VRRP session. Define the default state (owner) of the VRRP router within the virtual router.
`(config-router)#preempt-mode true`	Set the preempt mode to specify that the highest priority will function as a backup to master when master is unavailable.
`(config-router)#advertisement-interval 100`	Configure the advertisement interval to 100 centi seconds (value must be a multiple of 5).
`(config-router)#enable`	Enable the VRRP session two on the router.

Validation

The following outputs on R1and R2 display the complete configuration for each session on R1 and R2. In session one, R1 is the master router, and in session two R2 is the master router.

```
R1#sh vrrp 1 eth0
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled
Address family IPv4
VRRP Id: 1 on interface: eth0
 State: AdminUp   - Master
 Virtual IP address: 10.10.10.81 (Owner)
 Priority is 255
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Skew time: 0 centi sec
 Accept mode: FALSE
 Preempt mode: TRUE
 Multicast membership on IPv4 interface eth0: JOINED ---------------------------------
-----------
R1#sh vrrp 2 eth0
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled
Address family IPv4
```

```
VRRP Id: 2 on interface: eth0
 State: AdminUp   - Backup
 Virtual IP address: 10.10.10.82 (Not-owner)
 Priority is 100
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Skew time: 60 centi sec
 Accept mode: FALSE
 Preempt mode: TRUE
 Multicast membership on IPv4 interface eth0: JOINED
-------------------------------------------
R2#sh vrrp 1 eth0
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled
Address family IPv4
VRRP Id: 1 on interface: eth0
 State: AdminUp   - Backup
 Virtual IP address: 10.10.10.81 (Not-Owner)
 Priority is 100
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Skew time: 0 centi sec
 Accept mode: FALSE
 Preempt mode: TRUE
 Multicast membership on IPv4 interface eth0: JOINED
-------------------------------------------
R2#sh vrrp 2 eth0
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled
Address family IPv4
VRRP Id: 2 on interface: eth0
 State: AdminUp   - Master
 Virtual IP address: 10.10.10.82 (Owner)
 Priority is 255
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Skew time: 60 centi sec
 Accept mode: FALSE
 Preempt mode: TRUE
 Multicast membership on IPv4 interface eth0: JOINED
```

Two Backup Routers

In this configuration, Host B could be a gateway router. As such, interface eth1 on Routers R1, R2, and R3, and the gateway router, would run the IGP protocol.

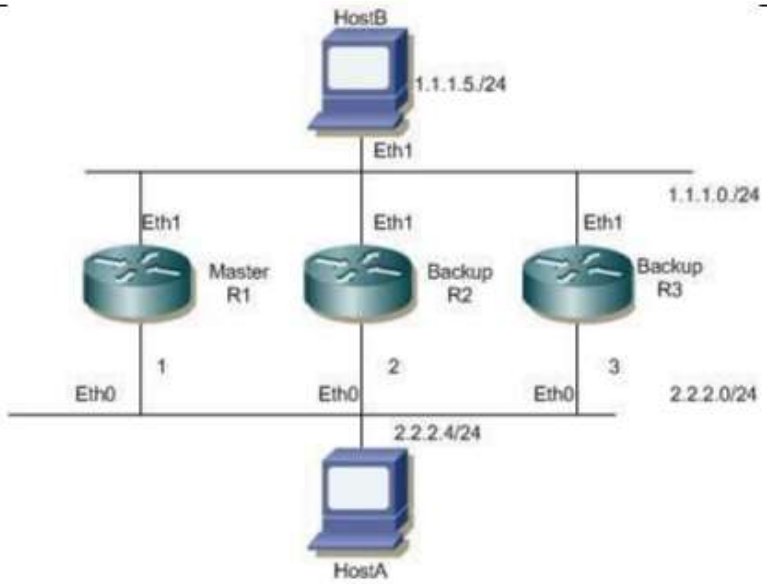


Figure 1-190: Configuring VRRP with Two Backup Routers

R1

`#configure terminal`	Enter the Configure mode.
`(config)#interface eth0`	Enter the Interface mode for eth0.
`(config-if)#ip address 2.2.2.1/24`	Configure the IP address for interface eth0 to be in network 0.
`(config-if)#exit`	Exit the Interface mode.
`(config)#interface eth1`	Enter the Interface mode for eth1.
`(config-if)#ip address 1.1.1.1/24`	Configure the IP address for interface eth1 to be in network 1.
`(config-if)#exit`	Exit the Interface mode.
`(config)#router vrrp 1 eth0`	Create a VRRP instance for interface eth0.
`(config-router)#virtual-ip 2.2.2.1 owner`	Configure R1 as the owner.
`(config-router)#advertisement-interval 100`	Configure the default value for the advertisement interval. The configurable range is 5 to 4095 centi seconds (value must be a multiple of 5).
`(config-router)#preempt-mode true`	Set `true` as the default value for the field.
`(config-router)#enable`	Enable the VRRP session on the router.
`(config-router)#exit`	Exit Router mode.

R2

`#configure terminal`	Enter the Configure mode.
`(config)#interface eth0`	Enter the Interface mode for eth0.
`(config-if)#ip address 2.2.2.2/24`	Configure the IP address for interface eth0 to be in network 0.
`(config-if)#exit`	Exit the Interface mode.
`(config)#interface eth1`	Enter the Interface mode for `eth1`.

`(config-if)#ip address 1.1.1.2/24`	Configure the IP address for interface `eth1` to be in network 1.
`(config-if)#exit`	Exit the Interface mode.
`(config)#router vrrp 1 eth0`	Create a VRRP instance for interface eth0.
`(config-router)#virtual-ip 2.2.2.1`	Configure R2 as the backup.
`(config-router)#advertisement-interval 100`	Configure the default value for the advertisement interval. The configurable range is 5 to 4095 centi seconds (value must be a multiple of 5).
`(config-router)#priority 100`	Set the default value for the backup router.
`(config-router)#preempt-mode true`	Set `true` as the default value for the field.
`(config-router)#enable`	Enable the VRRP session on the router.
`(config-router)#exit`	Exit Router mode.

R3

`#configure terminal`	Enter the Configure mode.
`(config)#interface eth0`	Enter the Interface mode for eth0.
`(config-if)#ip address 2.2.2.3/24`	Configure the IP address for interface eth0 to be in network 0.
`(config-if)#exit`	Exit the Interface mode.
`(config)#interface eth1`	Enter the Interface mode for eth1.
`(config-if)#ip address 1.1.1.3/24`	Configure the IP address for interface eth1 to be in network 1.
`(config-if)#exit`	Exit the Interface mode.
`(config)#router vrrp 1 eth0`	Create a VRRP instance for interface eth0.
`(config-router)#virtual-ip 2.2.2.1`	Configure R3 as the backup.
`(config-router)#advertisement-interval 100`	Configure the default value for the advertisement interval. The configurable range is 5 to 4095 centi seconds (value must be a multiple of 5).
`(config-router)#priority 254`	Configure the priority for R3. The configurable range is 1255.
`(config-router)#preempt-mode true`	Set `true` as the default value for the field.
`(config-router)#enable`	Enable the VRRP session on the router.
`(config-router)#exit`	Exit Router mode.

Validation

Router 1

```
R1#sh vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled
Address family IPv4
VRRP Id: 1 on interface: eth2
 State: AdminUp   - Master
```

```
 Virtual IP address: 2.2.2.1 (Owner)
 Operational primary IP address: 2.2.2.1
 Operational master IP address: 2.2.2.1
 Priority is 255
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Skew time: 0 centi sec
 Accept mode: FALSE
 Preempt mode: TRUE
 Multicast membership on IPv4 interface eth2: JOINED  V2-Compatible: FALSE
```

Router 2

```
R2#sh vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: eth2
 State: AdminUp   - Backup
 Virtual IP address: 2.2.2.1 (Not-owner)
 Operational primary IP address: 2.2.2.2
 Operational master IP address: 2.2.2.1
 Priority is 100
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Skew time: 60 centi sec
 Accept mode: FALSE
 Preempt mode: TRUE
 Multicast membership on IPv4 interface eth2: JOINED  V2-Compatible: FALSE
```

Router 3

```
R3#sh vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: eth0
 State: AdminUp   - Backup
 Virtual IP address: 2.2.2.1 (Not-Owner)
 Operational primary IP address: 2.2.2.3
 Operational master IP address: 2.2.2.1
 Priority is 254
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Skew time: 0 centi sec
 Accept mode: FALSE
 Preempt mode: TRUE
 Multicast membership on IPv4 interface eth0: JOINED  V2-Compatible: FALSE
```

Ping Output at Host A

```
[root@HstA root]#ping 1.1.1.5
PING 1.1.1.5 (1.1.1.5) 56(84) bytes of data.
64 bytes from 1.1.1.5: icmp_seq=1 ttl=63 time=0.486 ms
64 bytes from 1.1.1.5: icmp_seq=2 ttl=63 time=0.290 ms
```

Disabling the Master/Owner

#configure terminal	Enter the Configure mode.
(config)#router vrrp 1 eth0	Create a VRRP instance for interface eth0.
(config-router)#disable	Disable the VRRP session.

Output After Disabling the Master

```
R1#sh vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: eth2
 State: AdminDown - Init (admin state down)
 Virtual IP address: 2.2.2.1 (Owner)
 Operational primary IP address: 2.2.2.1
 Operational master IP address: 2.2.2.1
 Priority is 255
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Skew time: 0 centi sec
 Accept mode: FALSE
 Preempt mode: TRUE
 Multicast membership on IPv4 interface eth2: LEFT
 V2-Compatible: FALSE

R3#sh vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv4
VRRP Id: 1 on interface: eth2
 State: AdminUp   - Master
 Virtual IP address: 2.2.2.1 (Not-owner)
 Operational primary IP address: 2.2.2.2
 Operational master IP address: 2.2.2.2
 Priority is 100
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Skew time: 60 centi sec
 Accept mode: FALSE
 Preempt mode: TRUE
```

```
    Multicast membership on IPv4 interface eth2: JOINED  V2-
    Compatible: FALSE
[root@HstA root]#ping 1.1.1.5
PING 1.1.1.5 (1.1.1.5) 56(84) bytes of data.
64 bytes from 1.1.1.5: icmp_seq=1 ttl=63 time=0.572 ms
64 bytes from 1.1.1.5: icmp_seq=2 ttl=63 time=0.291 ms
```

Interface Tracking

The need for VRRP Interface Tracking arose because VRRPv2 was unable to track the gateway interface status. The VRRP Interface Tracking feature provides dynamic failover of an entire circuit, in the event that one member of the group fails. It introduces the concept of a circuit, where two or more Virtual Routers on a single system can be grouped. In the event that a failure occurs, and one of the Virtual Routers performs the Master to Backup transition, the other Virtual Routers in the group are notified, and are forced into the Master to Backup transition, so that both incoming and outgoing packets are routed through the same gateway router, eliminating the problem for Firewall/NAT environments. Note: Only one interface is supported in an interface tracking for a VRRP session.

To configure VRRP Interface Tracking, each circuit is configured to have a corresponding priority-delta value, which is passed to VRRP when a failure occurs. The priority of each Virtual Router on the circuit is decremented by the prioritydelta value, causing the VR Master to VR Backup transition.

In this example, two routers, R1 and R2, are configured as backup routers with different priorities. The priority-delta value is configured to be greater than the difference of both the priorities. R1 is configured to have a priority of 100, and R2 has a priority of 90. R1, with a greater priority, is the Virtual Router Master. The priority-delta value is 20, greater than 10 (100 minus 90). On R1, when the external interface `eth1` fails, the priority of R1 becomes 80 (100 minus 20). Since R2 has a greater priority (90) than R1, R2 becomes the VR Master, and routing of packages continues without interruption. When this VR Backup (R1) is up again, it regains its original priority (100), and becomes the VR Master again.

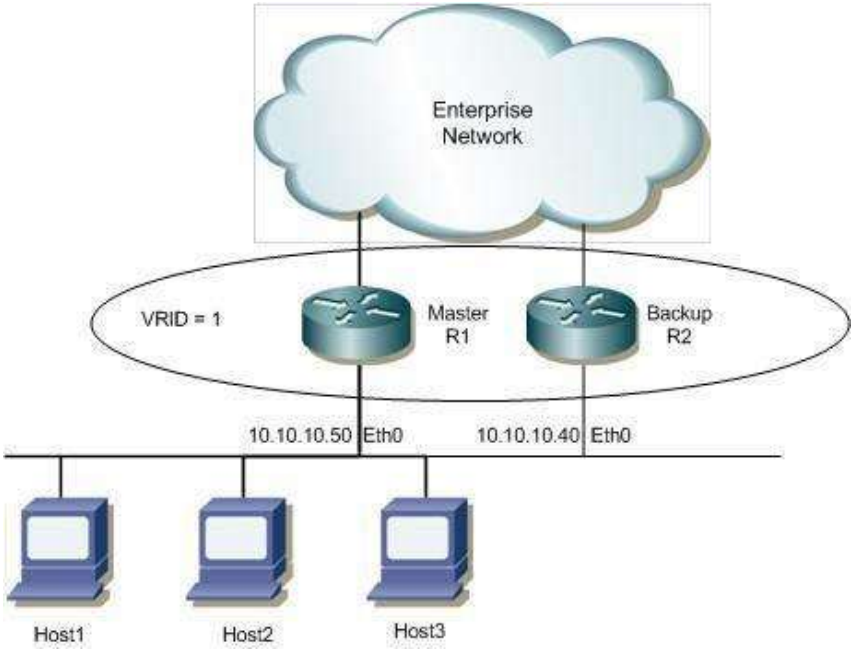


Figure 1-191: VRRP Interface Tracking

R1

`#configure terminal`	Enter the `Configure` mode.

(config)#router vrrp 1 eth0	Create a new VRRP instance for interface eth0.
(config-router)#virtual-ip 10.10.10.1	Set the virtual IP address for the VRRP session.
(config-router)#priority 100	Configure the priority to 100.
(config-router)#preempt-mode true	Set the preempt mode to specify that the highest priority will own the external ip address when there is a failure.
(config-router)#advertisement-interval 100	Configure the advertisement interval to 100 centi seconds (value must be a multiple of 5).
(config-router)#circuit-failover eth1 20	Configure the priority-delta value to be 20. In case of failover, this priority-delta value is subtracted from the current VR Master.
(config-router)#enable	Enable the VRRP session on the router.
R2	
#configure terminal	Enter the Configure mode.
(config)#router vrrp 1 eth0	Create a new VRRP instance for interface eth0.
(config-router)#virtual-ip 10.10.10.1	Set the virtual IP address for the VRRP session.
(config-router)#priority 90	Configure the priority to 90 (less than 100), because R2 is the VR Backup router.
(config-router)#preempt-mode true	Set the preempt mode to specify that the highest priority will function as a primary backup router in case of failure.
(config-router)#advertisement-interval 100	Configure the advertisement interval to 100 centi seconds (value must be a multiple of 5).
(config-router)#enable	Enable the VRRP session on the router.

Validation

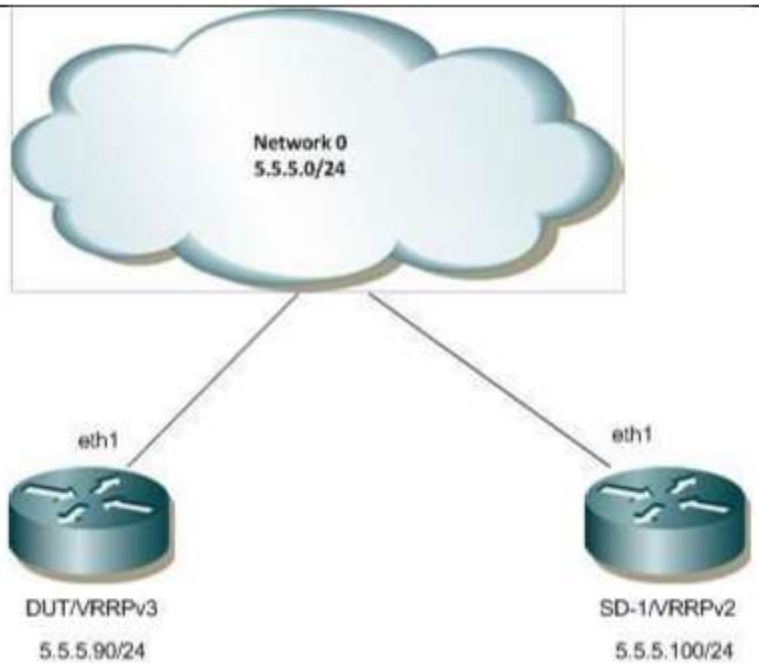
show vrrp

VRRP-Backward Compatibility

This section contains VRRP Backward Compatibility configuration examples.

The backward compatibility feature which implements version 3 of VRRP protocol recognizes the presence of VRRP version 2 compatible routers in the network and performs all operations normally. This support is intended for upgrade scenarios and is not recommended for permanent deployments. This should only occur when a router is transitioning from VRRPv2 to VRRPv3.

VRRP Backward Compatibility is applicable only for VRRP IPv4.



DUT

`#configure terminal`	Enter the Configure mode.
`(config)# interface eth1`	Enter Interface configuration mode.
`(config-if)# ip address 5.5.5.90/24`	Configure IP address on the interface.
`(config-if)#end`	Exit from configuration mode.
`#configure terminal`	Enter Configuration mode.
`(config)# router vrrp 1 eth1`	Configure VRRP on DUT with Virtual router Identifier as 1 on the interface eth1.
`(config-router)#virtual-ip 5.5.5.190`	Configure Virtual-IP address as the interface IP address of Owner which is not actually present in the LAN.
`(config-router)#enable`	Enable VRRP session on DUT.
`(config-router)#end`	Exit router VRRP mode.
`#configure terminal`	Enter Configuration mode.
`(config)#vrrp compatible-v2 enable`	Enable VRRP-Backward compatibility feature on a VRRPv3 running router.

SD-1

`#configure terminal`	Enter the Configure mode.
`(config)# interface eth1`	Enter Interface configuration mode.
`(config-if)# ip address 5.5.5.100/24`	Configure IP address on the interface.
`(config-if)#end`	Exit from configuration mode.
`#configure terminal`	Enter Configuration mode.
`(config)#router vrrp 1 eth1`	Configure VRRP on DUT with Virtual router Identifier as 1 on the interface eth1.

(config-router)#virtual-ip 5.5.5.190	Configure Virtual-IP address as the interface IP address of Owner which is not actually present in the LAN.
(config-router)#enable	Enable VRRP session on DUT.
(config-router)#end	Exit router VRRP mode.

Validation

```
DUT# sh vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility enabled
Address family IPv4
VRRP Id: 20 on interface: eth1
 State: AdminUp   - Master
 Virtual IP address: 5.5.5.190 (Not-Owner)
 Priority is 100
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Skew time: 0 centi sec
 Accept mode: FALSE
 Preempt mode: TRUE
 Multicast membership on IPv4 interface eth1: JOINED

SD-1#sh vrrp
VRRP Version: 2
VMAC enabled
Address family IPv4
VRRP Id: 20 on interface: eth1
 State: AdminUp   - Backup
 Virtual IP address: 5.5.5.190 (Not-owner)
 Priority is 100
 Advertisement interval: 1 sec
 Preempt mode: TRUE
 Multicast membership on IPv4 interface eth1: JOINED
```

Redundancy Using VRRP and OSPF: Two Virtual Routers

This example illustrates a configuration of two routers between two end-hosts. R1 and R2 are two virtual routers functioning as backups for each other, with VRRP running on the 10.10.12.0/24 network (LAN), and OSPF running on the 10.10.10.0/24 network (ISP).

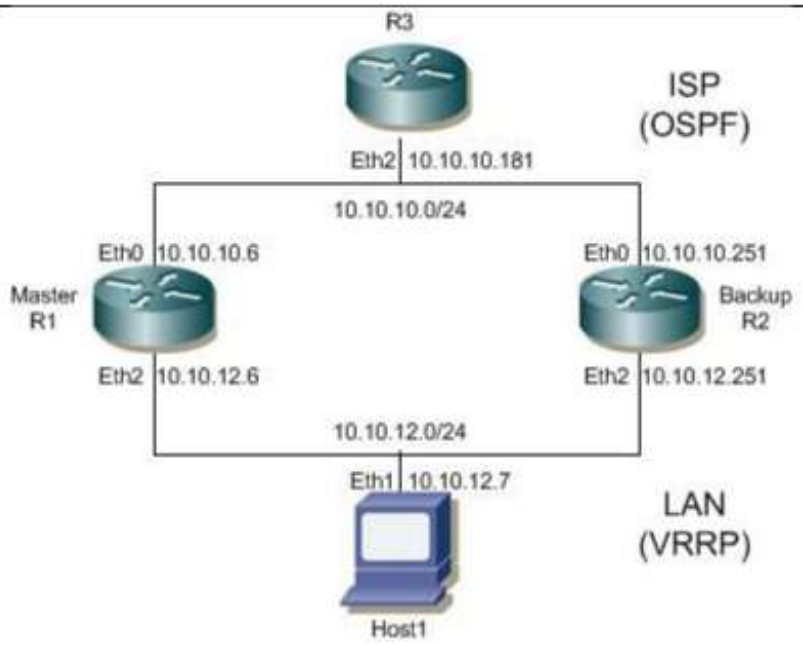


Figure 1-192: Redundancy Using VRRP and OSPF

In this example:

- R3 is an OSPF router representing an OSPF network to an ISP.
- R1 is the VRRP Master/OSPF router.
- R2 is the VRRP Backup/OSPF router.
- Host 1 is an end-host.

VRRP handles any failure of the Master's link to the LAN. Failures in the OSPF network that could cause the Master to lose routing information would cause packets from Host 1 that are targeted for R3 to be dropped. Running VRRP on the OSPF network to create redundancy is undesirable, because doing so would cause erroneous VRRP packets to be sent to the ISP.

An alternative method to achieve redundancy is to run OSPF on the LAN side. By running OSPF on the LAN, any routing information lost by the Master would be regained from the Backup on the LAN interface, resulting in ICMP redirects to R2 for traffic received from Host 1. To reduce OSPF control traffic, R1 and R2 are configured as Area Border Routers (ABR), and the LAN is configured as a stub network to reduce LSA advertisement traffic on the LAN. Before enabling OSPF on the LAN, verify that VRRP is running with R1 as the Master and R2 as the Backup.

```
R1#show vrrp
 VrId <1>
 State is Master
 Virtual IP is 10.10.12.6 (IP owner)
 Interface is eth0
 Priority is 255
 Advertisement interval: 5 centi sec
 Preempt mode is TRUE
R2#show vrrp
 VrId <1>
  State is Backup
  Virtual IP is 10.10.12.6 (Not IP owner)
  Interface is eth0
  Priority is 100
  Advertisement interval: 5 centi sec
```

```
Preempt mode is TRUE
```

Steps to configure OSPF on the LAN are given below.

R3

`#configure terminal`	Enter the Configure mode.
`(config)#router ospf 1`	Configure the routing process and specify the process ID (`1`). The process ID should be a unique integer.
`(config-router)#ospf router-id 10.10.10.181`	Specify the OSPF router ID.
`(config-router)#timers spf exp 0 0`	Set `timers` to minimum time for quick convergence.
`(config-router)#network 10.10.10.0/24 area 0`	Define one interface (`10.10.10.0/24`) on which OSPF runs and associate the area ID (0).

R1

`#configure terminal`	Enter the Configure mode.
`(config)#router ospf 1`	Configure the routing process and specify the process ID (`1`). The process ID should be a unique integer.
`(config-router)#ospf router-id 10.10.12.6`	Specify the OSPF router ID.
`(config-router)#area 1 stub`	Define area 1 as a stub network.
`(config-router)#network 10.10.10.0/24 area 0`	Define one interface (`10.10.10.0/24`) on which OSPF runs and associate the area ID (0).
`(config-router)#network 10.10.12.0/24 area 1`	Define the other interface (`10.10.12.0/24`) on which OSPF runs and associate the area ID (`1`)

R2

`#configure terminal`	Enter the Configure mode.
`(config)#router ospf 1`	Configure the routing process, and specify the process ID (`1`). The process ID should be a unique integer
`(config-router)#ospf router-id 10.10.12.251`	Specify the OSPF router ID.
`(config-router)#area 1 stub`	Define area 1 as a stub network.
`(config-router)#network 10.10.10.0/24 area 0`	Define one interface (`10.10.10.0/24`) on which OSPF runs and associate the area ID (0).
`(config-router)#network 10.10.12.0/24 area 1`	Define the other interface (`10.12.10.0/24`) on which OSPF runs and associate the area ID (`1`)

Verification

1. Set gateway on the end-host (statically):

```
(root@host1)#route add -net 10.10.10.0 netmask 255.255.255.0 gw 10.10.12.6
```

2. Verify end-host reachability via traceroute:

```
(root@host1)#traceroute 10.10.10.181
traceroute to 10.10.10.181 (10.10.10.181), 30 hops max, 38 byte packets
 1  10.10.12.6 (10.10.12.6)  0.835 ms  0.350 ms  0.341 ms  2  10.10.10.181
(10.10.10.181)  9.557 ms  0.572 ms  0.545 ms
```

3. Bring down eth0 of R1:

```
[root@r1 sbin]#ifconfig eth0 down
```

4. Verify end-host reachability via traceroute:

```
(root@host1)#traceroute 10.10.10.181
traceroute to 10.10.10.181 (10.10.10.181), 30 hops max, 38 byte packets
 1 10.10.12.6 (10.10.12.6)  0.461 ms  0.352 ms  0.334 ms
 2 10.10.12.251  (10.10.12.251)  0.425 ms  0.432 ms  0.410 ms
 3 10.10.10.181  (10.10.10.181)  0.691 ms  0.639 ms  0.607 ms
```

5. Bring up eth0 of R1:

```
[root@r1 sbin]#ifconfig eth0 up
```

6. Verify end-host reachability via traceroute:

```
(root@host1)#traceroute 10.10.10.181
traceroute to 10.10.10.181 (10.10.10.181), 30 hops max, 38 byte packets
 1 10.10.12.6 (10.10.12.6)  0.457 ms  0.356 ms  0.443 ms
 2 10.10.10.181 (10.10.10.181)  0.698 ms  0.642 ms  0.618 ms
```

CHAPTER 2 VRRP IPv6 Configuration

This chapter contains a Virtual Router Redundancy Protocol IPv6 (VRRPv6) configuration example.

VRRPv6 eliminates the risk of a single point of failure inherent in a static default routing environment. It specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRPv6 routers on a LAN. In this sample, OSPFv3 is enabled on Router 1 (R1), the master router, and the backup router. In R1, the connected routes are redistributed.

Note: IPv6 VRRP can be configured only on a link-local address.

Topology

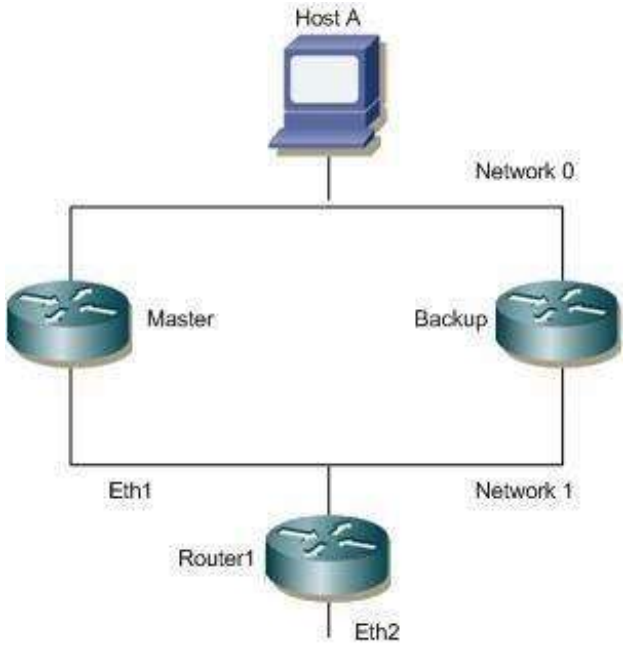


Figure 2-193: Topology

Configuration

Owner/Master Router

#configure terminal	Enter the Configure mode.
(config)#interface eth0	Enter the Interface mode for eth0.
(config-if)#ipv6 address fe80::3037:3aff:fe3a:3a32/64	Configure the IPv6 address for interface eth0 to be in network 0.
(config-if)#exit	Exit the Interface mode.
(config)#interface eth1	Enter the Interface mode for eth1.
(config-if)#ipv6 address fe80::3037:a0ff:fea4:3539/64	Configure the IPv6 address for interface eth1 to be in network 1.

(config-if)#exit	Exit the Interface mode.
(config)#router ipv6 vrrp 1 eth0	Create a VRRPv6 instance for interface eth0.
(config-router)#virtual-ipv6 fe80::3037:3aff:fe3a:3a32 owner	Configure R1 as the owner.
(config-router)#advertisement-interval 100	Configure the default value for the advertisement interval. The configurable range is <5-4095> (value must be a multiple of 5).
(config-router)#preempt-mode true	Set `true` as the default value for the field.
(config-router)#enable	Enable the VRRPv6 session on the router.
(config-router)#exit	Exit Router mode.

Backup Router

#configure terminal	Enter the Configure mode.
(config)#interface eth0	Enter the Interface mode for eth0.
(config-if)#ipv6 address fe80::3037:3aff:fe3a:3b45/64	Configure the IPv6 address for interface eth0 to be in network 0.
(config-if)#exit	Exit the Interface mode.
(config)#interface eth1	Enter the Interface mode for eth1.
(config-if)#ipv6 address fe80::3037:a0ff:fea4:3a40/64	Configure the IPv6 address for interface eth1 to be in network 1.
(config-if)#exit	Exit the Interface mode.
(config)#router ipv6 vrrp 1 eth0	Create a VRRPv6 instance for interface eth0.
(config-router)#virtual-ipv6 fe80::3037:3aff:fe3a:3a32	Configure Router 2 (R2) as the backup.
(config-router)#advertisement-interval 100	Configure the default value for the advertisement interval. The configurable range is <5-4095> (value must be a multiple of 5).
(config-router)#priority 100	Set the default value for the backup router.
(config-router)#preempt-mode true	Set `true` as the default value for the field.
(config-router)#enable	Enable the VRRPv6 session on the router.
(config-router)#exit	Exit Router mode.

Host A

#configure terminal	Enter the Configure mode.
(config)#interface eth0	Enter the Interface mode for eth0.
(config-if)#ipv6 address fe80::3037:3aff:fe3a:3a11/64	Configure the IPv6 address for interface eth0 to be in network 0.
(config-if)#exit	Exit the Interface mode.
(config)#ipv6 route 5ffe:14:14:14::/64 fe80::3037:3aff:fe3a:3a32	Configure a static route to reach interface eth2 of R1 through the virtual IPv6 address.

Router 1

#configure terminal	Enter the Configure mode.
(config)#interface eth1	Enter the Interface mode for eth1.
(config-if)#ipv6 address fe80::3037:a0ff:fea4:1111/64	Configure the IPv6 address for interface eth1 to be in network 1.
(config-if)#exit	Exit the Interface mode.
(config)#interface eth2	Enter the Interface mode for eth2.
(config-if)#ipv6 address fe80::3437:30ff:fe35:a6ac/64	Configure the IPv6 address of interface eth2.

Validation

Master Router

```
R1#sh vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv6
VRRP Id: 1 on interface: eth0
 State: AdminUp   - Master
 Virtual IP address: fe80::3037:3aff:fe3a:3a32 (Owner)
 Priority is 255
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Skew time: 0 centi sec
 Accept mode: FALSE
 Preempt mode: TRUE
 Multicast membership on IPv6 interface  eth0: JOINED
```

Backup Router

```
R1#sh vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv6
VRRP Id: 1 on interface: eth0
 State: AdminUp   - Backup
 Virtual IP address: fe80::3037:3aff:fe3a:3a32 (Not-Owner)
 Priority is 100
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Skew time: 0 centi sec  Accept mode: FALSE
 Preempt mode: TRUE
 Multicast membership on IPv6 interface  eth0: JOINED
```

Ping Output at Host A

```
[[root@HstA root]#ping ipv6 fe80::3437:30ff:fe35:a6ac
```

```
PING fe80::3437:30ff:fe35:a6ac(fe80::3437:30ff:fe35:a6ac) 56 data bytes
64 bytes from fe80::3437:30ff:fe35:a6ac: icmp_seq=1 ttl=63 time=0.398 ms 64 bytes from
fe80::3437:30ff:fe35:a6ac: icmp_seq=2 ttl=63 time=0.230 ms 64 bytes from
fe80::3437:30ff:fe35:a6ac: icmp_seq=3 ttl=63 time=0.234 ms
64 bytes from fe80::3437:30ff:fe35:a6ac: icmp_seq=4 ttl=63 time=0.230 ms
```

Disabling the Master

#configure terminal	Enter the Configure mode.
(config)#interface eth0	Enter the Interface mode for eth0.
(config-router)#shutdown	Shut down the interface

Validation

```
R1#sh vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv6
VRRP Id: 1 on interface: eth0
 State: AdminUp   - Init (interface is not running)
 Virtual IP address: fe80::3037:3aff:fe3a:3a32 (Owner)
 Priority is 255
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Skew time: 0 centi sec
 Accept mode: FALSE
 Preempt mode: TRUE
 Multicast membership on IPv6 interface eth0: LEFT
```

Backup Router

```
R1#sh vrrp
VRRP Version: 3
VMAC enabled
Backward Compatibility disabled

Address family IPv6
VRRP Id: 1 on interface: eth0
 State: AdminUp   - Backup
 Virtual IP address: fe80::3037:3aff:fe3a:3a32 (Not-Owner)
 Priority is 100
 Advertisement interval: 100 centi sec
 Master Advertisement interval: 100 centi sec
 Skew time: 0 centi sec
 Accept mode: FALSE
 Preempt mode: TRUE
 Multicast membership on IPv6 interface  eth0: LEFT
```

Ping Output at Host A

```
[root@HstA root]#ping ipv6 fe80::3437:30ff:fe35:a6ac
PING fe80::3437:30ff:fe35:a6ac(fe80::3437:30ff:fe35:a6ac) 56 data bytes
64 bytes from fe80::3437:30ff:fe35:a6ac: icmp_seq=1 ttl=63 time=0.423 ms 64 bytes from
fe80::3437:30ff:fe35:a6ac: icmp_seq=2 ttl=63 time=0.291 ms
```

Virtual Router Redundancy Protocol Command Reference

Contents

This document contains these chapters:

- Chapter 1, *VRRP Commands*
- Chapter 2, *VRRP v6 Commands*

CHAPTER 1 VRRP Commands

This chapter describes the commands for VRRP.

- accept-mode
- advertisement-interval
- circuit-failover
- debug vrrp
- disable
- enable
- operational-ip
- preempt-mode
- router vrrp
- show debugging vrrp
- show running-config router vrrp
- show vrrp
- show vrrp <1-255>
- show vrrp statistics
- snmp restart vrrp
- switch-back-delay
- undebug vrrp
- virtual-ip
- vrrp compatible-v2
- vrrp vmac

accept-mode

Use this command to enable accept mode for the session

Use the `no` parameter with this command to restore the default setting.

Command Syntax `accept-mode true accept-mode false`

Parameter

`None`

Default

By default, accept mode for the session is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The example below shows how to set and unset the accept mode.

```
#configure terminal
(config)#router vrrp 2 eth0
(config-router)#accept-mode false
```

advertisement-interval

Use this command to configure the advertisement interval of a virtual router. This is the length of time, in seconds, between each advertisement sent from the master to its backup(s). The master virtual router sends VRRP advertisements to other VRRP routers in the same group. The advertisements communicate the priority and state of the master virtual router. The VRRP advertisements are encapsulated in IP packets and sent to the multicast address assigned to the VRRP group (224.0.0.18). Advertisements are sent every second by default.

Note: VRRP Master router and backup routers should be configured with the same advertisement interval. If there is a mismatch in the configuration, VRRP goes to the INIT state.

Use the `no` parameter with this command to restore the default setting.

Command Syntax `advertisement-interval <5-4095> no advertisement-interval`

Parameter

`<5-4095>`	Specify the advertisement interval in centi-seconds (in multiples of 5) when VRRPv3 is enabled

Default

By default, advertisements are sent every second

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The example below shows how to configure an advertisement interval of 50 centi-seconds for the virtual router with VR ID 2 on interface eth0.

```
#configure terminal
(config)#router ip vrrp 2 eth0
(config-router)#advertisement-interval 50
```

circuit-failover

Use this command to enable the VRRP circuit failover feature.

Use the `no` parameter with this command to disable this feature.

Command Syntax `circuit-failover [IFNAME] |<1-253> no circuit-failover [IFNAME] |<1-253>`

Parameters

`IFNAME`	Specify an interface of the router that is monitored by the virtual router. This is usually an upstream interface. Should the interface go down, another router, configured as backup within the VRRP group, may take over as a master.
`<1-253>`	Specify the delta value. The value by which the virtual router decrements its priority value during a circuit failover event. Configure this value to be greater than the difference of priorities between the master and backup routers.

Default

By default, circuit failover feature is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The example below shows how to configure circuit failover for the VRRP session with VR ID 1. Interface eth1 is considered the monitored interface.

```
#configure terminal
(config)#router vrrp 1 eth0
(config-router)#circuit-failover eth1 30
```

debug vrrp

Use this command to specify debugging options for VRRP.

Use the `no` parameter with this command to disable debugging.

Command Syntax `debug vrrp (all|event|packet [send|recv|]) no debug vrrp (all|event|packet [send|recv|])`

Parameters

`all`	Specify debugging options for all VRRP events.
`event`	Specify debugging options for VRRP event troubleshooting.
`packet`	Specify debugging options for VRRP packets
`send`	Specify the debug option set for sent packets.
`recv`	Specify the debug option set for received packets.

Command Mode

Configure mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The example below shows how to enable all VRRP debug options.

```
#configure terminal
(config)#debug vrrp all
```

The example below shows how to enable debugging options for VRRP events.

```
#configure terminal
(config)#debug vrrp events
```

The example below shows how to enable debug options for VRRP packets sent.

```
#configure terminal
(config)#debug vrrp packet send
```

The example below shows how to enable debug options for VRRP packets received.

```
#configure terminal
(config)#debug vrrp packet recv
```

disable

Use this command to disable a VRRP session on the router (to stop the router from participating in virtual routing). When this command is configured, a backup Router assumes the Role of Master depending on its priority.

Command Syntax `disable`

Parameters

None

Default

By default, VRRP session on the router is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The example below shows how to disable a VRRP session.

```
#configure terminal
(config)#router vrrp 1 eth0
(config-router)#disable
```

enable

Use this command to enable a VRRP session on the router (to make it participate in virtual routing). To make any changes to the VRRP configuration, first disable the router from participating in virtual routing using the `disable` command.

Note: Configure the virtual IP address and define an interface for the VRRP session (using the `virtual-ip` and `interface` commands) before using this command.

Command Syntax

```
enable
```

Parameters

None

Default

By default, VRRP session on the router is disabled

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The example below shows how to enable a VRRP session with VR ID 1 on interface eth0.

```
#configure terminal
(config)#router vrrp 1 eth0
(config-router)#enable
```

operational-ip

Use this command to set the primary IPv4 address.

Use the no parameter with this command to remove a primary IPv4 address.

Command Syntax `operational-ip A.B.C.D no operational-ip`

Parameters

A.B.C.D	IPv4 address.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router vrrp 1 eth0
(config-router)#operational-ip 1.2.3.4
```

preempt-mode

Use this command to configure preempt mode. If set to `true`, the highest priority backup is always the master when the default master is unavailable. If set to `false`, a higher priority backup does not preempt a lower priority backup which is acting as master.

When the master router fails, the backup routers come online in priority order — highest to lowest. Preempt mode set to `true` allows a higher priority backup router to relieve a lower priority backup.

By default, a preemptive scheme is enabled whereby a higher priority backup virtual router that becomes available takes over for the backup virtual router that was elected to become master virtual router. This preemptive scheme can be disabled using the `preempt-mode false` command. If preemption is disabled, the backup virtual router that is currently elected as Master does not transition to backup again when the alternate backup router with higher priority becomes available.

Command Syntax `preempt-mode`

```
(true|false)
```

Parameters

true	Specify that preemption is enabled.
false	Specify that preemption is disabled.

Default

By default, preempt mode is true

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The example below shows how to enable the preempt mode.

```
#configure terminal
(config)#router vrrp 1 eth0
(config-router)#preempt-mode false

#configure terminal
(config)#router vrrp 1 eth0
(config-router)#preempt-mode true
```

router vrrp

Use this command to enable a VRRP routing process.

Use the `no` form of this command to disable a VRRP routing process.

Command Syntax `router vrrp <1-255> IFNAME no router vrrp <1-255> IFNAME`

Parameters

`<1-255>`	Virtual router identifier
`IFNAME`	Interface name

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router vrrp 1 eth0
```

show debugging vrrp

Use this command to display the set VRRP debugging option.

Command Syntax `show debugging vrrp`

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show debugging vrrp
VVRRP debugging status:
VRRP event debugging is on
VRRP packet debugging is on
```

show running-config router vrrp

Use this command to show the running configuration for VRRP.

Command Syntax `show running-config`

`router vrrp`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The example below shows the running configuration of VRRP. Virtual Router is configured as Master and Owner of IP address.

```
#show running-config router vrrp
! router vrrp 1 eth0
virtual-ip 39.0.0.24 owner
advertisement-interval 5
preempt-mode false enable
!
```

show vrrp

Use this command to display a list of virtual router identifiers that are configured on the router.

Command Syntax `show vrrp`

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show vrrp

R1#show vrrp
VrId <1>
State is Master
```

```
Virtual IP is 10.10.12.6 (IP owner)
Interface is eth0
Priority is 255
Advertisement interval: 5 centi sec
Preempt mode is TRUE

R2#show vrrp
VrId <1>
State is Backup
Virtual IP is 10.10.12.6 (Not IP owner)
Interface is eth0
Priority is 100
Advertisement interval: 5 centi sec Preempt mode is TRUE
```

Table 1-236 Explains the show command output fields.

Table 1-236: show vrrp output fields

Field	Description
VrID	Type of vr identifier by the system on the interface.
State	VRRP State: Master — The interface is acting as the master router interface. Backup —The interface is acting as the backup router interface.
Virtual IP	List of virtual IP addresses configured on the interface.
Interface	Name of the logical interface.

Field	Description
Priority	Configured VRRP priority for the interface.
Advertisement interval	Configured VRRP advertisement interval.
Preempt mode	Whether preemption is allowed on the interface.

© Symanitron Proprietary

show vrrp <1-255>

Use this command to display VRRP information for a virtual router.

Command Syntax `show vrrp <1-255> IFNAME`

Parameters

`<1-255>`	Virtual router identifier
`IFNAME`	Interface name

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show vrrp 7 eth0
```

show vrrp statistics

Use this command to display VRRP IPv4 router statistics.

Command Syntax `show vrrp statistics <1-255> IFNAME`

Parameters

`<1-255>`	Virtual router identifier
`IFNAME`	Interface name

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show vrrp statistics 15 eth1
```

snmp restart vrrp

Use this command to restart SNMP in Virtual Routing Redundancy Protocol (VRRP).

Command Syntax `snmp restart vrrp`

Parameters

None

Default

By default, SNMP restart is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#snmp restart vrrp
```

switch-back-delay

Use this command to set a switch-back delay timer for the master VRRP router. This feature prevents the original master VRRP router from transitioning back to the master state after coming back online until the configured delay timer has expired.

Command Syntax `switch-back-delay <1-500000> no switch-back-delay`

Parameters

`<1-500000>`	Specify a switch-back delay in milliseconds.

Command Mode

Router mode

Default

By default, the switch-back delay is set to 0

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The example below shows how to set a switch-back delay timer of 7000 milliseconds.

```
#configure terminal
(config)#router vrrp 5 eth1
(config-router)#switch-back-delay 7000
```

undebug vrrp

Use this command to disable debugging options for VRRP.

Command Syntax `undebug vrrp (all|event|packet [send|recv|]) no undebug vrrp (all|event|packet [send|recv|])`

Parameters

`all`	Specify debugging options for all VRRP events.
`event`	Specify debugging options for VRRP event troubleshooting.
`packet`	Specify debugging options for VRRP packets
`send`	Specify the debug option set for sent packets.
`recv`	Specify the debug option set for received packets.

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#undebug vrrp all
```

The example below shows how to disable debug options for VRRP events.

```
#undebug vrrp events
```

The example below shows how to disable debug options for VRRP packets sent.

```
#undebug vrrp packet send
```

The example below shows how to disable debug options for VRRP packets received.

```
#undebug vrrp packet recv
```

virtual-ip

Use this command to set the virtual IP address for the VRRP virtual router as VRRP Owner. This is the IP address used by end hosts to address their default gateway.

The VRRP Owner of the Virtual IP address only responds to packets destined to the Virtual IP address (for example, ICMP packets destined to the Virtual IP address).

Use the `no` parameter with this command to remove a virtual IP address assignment.

Syntax Description

```
virtual-ip
A.B.C.D     (owner|)      no
virtual-ip
```

Parameters

`A.B.C.D` Specify the virtual IP address of the interface that participates in virtual routing. `owner`

Specify the IP address as the owner.

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The example below shows how to configure the router as VRRP owner.

```
#configure terminal
(config)#router vrrp 1 eth0
(config-router)#virtual-ip 10.10.20.30 owner
```

The example below removes the virtual IP address assignment.

```
#configure terminal
(config)#router vrrp 1 eth0
(config-router)#no virtual-ip
```

vrrp compatible-v2

Use this command to enable the backward-compatibility feature. When enabled, both VRRPv3 and VRRPv2 interoperation are supported.

Command Syntax `vrrp compatible-v2 (enable| disable)`

Parameters

`enable`	Enable VRRPv2 inter-operation
`disable`	Disable VRRPv2 inter-operation

Default

By default, vrrp compatible-v2 is enabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#vrrp compatible-v2 enable
```

vrrp vmac

Use this command to enable or disable Virtual MAC (VMAC).

This command affects all VRRP groups in a router. On a single network segment, multiple VRRP groups can be configured, each using a different VMAC. The use of VMAC addressing allows for faster switchover when a backup router assumes the master role. When this command is used to enable a VMAC, the virtual router forwards packets with a special-purpose multicast VMAC address (0:0:5e:0:01:<VR ID>). Otherwise, it forwards with is interface's physical address.

The VMAC address is assigned to a router interface at the time the VRRP group is enabled in the router.

Command Syntax `vrrp vmac (enable|disable)`

Parameters

`enable`	Enable virtual MAC addressing.
`disable`	Disable virtual MAC addressing and use physical MAC addressing.

Default

By default, VMAC is disabled

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The example below shows how to enable a virtual MAC address on the router.

```
#configure terminal
(config)#vrrp vmac enable
```

The example below shows how to disable a virtual MAC address on the router.

```
#configure terminal
(config)#vrrp vmac disable
```

CHAPTER 2 VRRP v6 Commands

This chapter describes the commands for VRRP IPv6.

- advertisement-interval
- circuit-failover
- disable
- enable
- preempt-mode
- priority
- router ipv6 vrrp
- router ipv6 vrrp vlan
- show running-config router ipv6 vrrp
- virtual-ipv6

advertisement-interval

Use this command to configure the advertisement interval of a virtual router. This is the length of time, in seconds, between each advertisement sent from the master to its backup(s). The master virtual router sends VRRP advertisements to other VRRP routers in the same group. The IPV6 VRRP advertisements are sent to the multicast address assigned to the VRRP IPV6 group (FF02:0:0:0:0:0:XXXX:XXXX) and a backup virtual router has to join all multicast groups within this range. As a convenient assignment, SWMRE sends a VRRP advertisement to the multicast address FF02::12.The advertisements are sent every second by default.

Note: VRRP Master router and backup routers should be configured with the same advertisement interval. If there is a mismatch in the configuration, VRRP goes to the INIT state.

Use the `no` parameter with this command to restore the default setting.

Command Syntax `advertisement-interval <5-4095> no advertisement-interval`

Parameter

`<5-4095>`	Specify the advertisement interval in centi-seconds (multiples of 5) when VRRPv3 is enabled

Command Mode

Router mode

Examples

The example below shows how to configure an advertisement interval of 10 seconds for the virtual router with VR ID 3 on interface eth0.

```
#configure terminal
(config)#router ipv6 vrrp 3 eth0
(config-router)#advertisement-interval 10
```

circuit-failover

Use this command to enable the VRRP circuit failover feature.

Use the `no` parameter with this command to disable this feature.

Command Syntax `circuit-failover IFNAME <1-253> no circuit-failover IFNAME <1-253>`

`no circuit-failover (IFNAME|)`

Parameters

`IFNAME`	Specify an interface of the router that is monitored by the virtual router. This is usually an upstream interface. Should the interface go down, another router, configured as backup within the VRRP group, may take over as a master.
`<1-253>`	Specify the delta value. The value by which the virtual router decrements its priority value during a circuit failover event. Configure this value to be greater than the difference of priorities between the master and backup routers.

Command Mode

Router mode

Examples

The example below shows how to configure circuit failover for the VRRP session with VR ID 1. Interface eth1 is considered the monitored interface.

```
#configure terminal
(config)#router ipv6 vrrp 1 eth0
(config-router)#circuit-failover eth1 30
```

disable

Use this command to disable a VRRP session on the router (to stop the router from participating in virtual routing). Refer to enable to enable a VRRP session on the router.

When this command is configured, a backup router assumes the role of master depending on its priority.

Command Syntax `disable`

Parameters

None

Command Mode

Router mode

Example

The example below shows to disable VRRP session.

```
#configure terminal
(config)#router ipv6 vrrp 1 eth0
(config-router)#disable
```

enable

Use this command to enable a VRRP session on the router, so the router participates in virtual routing. To make any changes to the VRRP configuration, first disable the Router from participating in Virtual Routing using the `disable` command.

Note: Configure the virtual IP address and define an interface for the VRRP session (using the `virtual-ip` and `interface` commands) before using this command.

Command Syntax

```
enable
```

Parameters

None

Command Mode

Router mode

Example

The example below shows to enable VRRP session with VR ID 1 on interface eth0

```
#configure terminal
(config)#router ipv6 vrrp 1 eth0
(config-router)#enable
```

preempt-mode

Use this command to configure preempt mode. If set to `true`, the highest priority backup is always the master when the default master is unavailable. If set to `false`, a higher priority backup does not preempt a lower priority backup that is acting as master.

When the master router fails, the backup routers come online in priority order — highest to lowest. Preempt mode set to `true` allows a higher priority backup router to relieve a lower priority backup.

By default, a preemptive scheme is enabled whereby a higher priority backup virtual router that becomes available takes over for the backup virtual router that was elected to become master virtual router. This preemptive scheme can be disabled using the `preempt-mode false` command. If preemption is disabled, the backup virtual router that is currently elected as Master does not transition to backup again when the alternate backup router with higher priority becomes available.

Command Syntax

```
preempt-mode true
preempt-mode
false
```

Parameters

`true`	Specify that preemption is enabled.
`false`	Specify that preemption is disabled.

Default

Default is `true`.

Command Mode

Router mode

Example

The example below shows to configure preempt mode as False.

```
#configure terminal
(config)#router ipv6 vrrp 1 eth0
(config-router)#preempt-mode false
```

priority

Use this command to configure the VRRP router priority within the virtual router. Priority determines the role that each VRRP router plays and what happens if the master virtual router fails. If a VRRP router owns the IP address of the virtual router and the IP address of the physical interface, this router functions as the master virtual router.

Priority also determines whether a VRRP router functions as a backup virtual router and the order of ascendancy to becoming a master virtual router if the master virtual router fails. Use the `no` parameter with this command to disable this feature.

Command Syntax

```
priority <1-255>
no priority
```

Parameter

`<1-255>`	Specify a priority. For the master router, specify 255; otherwise use any number in the range <1-254>.

Default

Default values for priority are:

- master router = 255
- backup = 100

Command Mode

Router mode

Examples

The example below shows to set the priority

```
#configure terminal
(config)#router ipv6 vrrp 1 eth0
(config-router)#priority 101
```

router ipv6 vrrp

Use this command to associate an IPv6 interface with a VRRP session. When issued, this command enters the `Router` mode.

Use the `no` parameter with this command to remove the IPv6 VRRP configuration. Disable the IPv6 VRRP session before using this command.

Command Syntax `router ipv6 vrrp <1-255>`

`IFNAME no router ipv6 vrrp <1-255>`

`IFNAME`

Parameters

`<1-255>`	Specify the ID of the virtual router session to create.
`IFNAME`	Specify the name of the IPv6 interface on which VRRP is enabled.

Command Mode

Configure mode

Example

The example below shows how to enable an IPv6 VRRP session with VR ID 1 on interface eth0.

```
#configure terminal
(config)#router ipv6 vrrp 1 eth0
(config-router)#
```

router ipv6 vrrp vlan

Use this command to associate a VLAN with a VRRP session. When issued, this command enters the `Router` mode.

Use the `no` parameter with this command to remove the IPv6 VRRP configuration. Disable the IPv6 VRRP session before using this command.

Command Syntax `router ipv6 vrrp <1-255> vlan`

`<1-4094> no router ipv6 vrrp <1-255> vlan`

`<1-4094>`

Parameters

<1-255>	Specify a virtual router identifier. Must be unique for each routing process.
<1-4094>	Specify the actual VLAN identifier

Command Mode

Configure mode

Examples

This example shows the use of the `router vrrp` command to enter router mode. Note the change in the prompt.

```
#configure terminal
(config)#router ipv6 vrrp 100 vlan 123
(config-router)#
```

show running-config router ipv6 vrrp

Use this command to show the running configuration for VRRP.

Command Syntax `show running-config router ipv6 vrrp`

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Example

The example below shows the running configuration of IPv6 VRRP. Virtual Router is configured as Master and Owner of IP address.

```
#show running-config router ipv6 vrrp
! router ipv6 vrrp
1 eth0
 virtual-ip fe80::202:b3ff:fed5:983e
master circuit-failover eth1 30
```

```
advertisement-interval 6  preempt-mode
false  enable
!
#
```

virtual-ipv6

Use this command to set the virtual IPv6 address for the VRRP session. The virtual IPv6 address is the IPv6 address of the virtual router that end-hosts set as their default gateway.

VRRP Owner of the Virtual IP address only responds to the packets destined to the Virtual IP address (for example, ICMP packets destined to the Virtual IP address).

Use the `no` parameter with this command to disable this feature.

Syntax Description `virtual-ipv6`

```
X:X::X:X  owner  no  virtual-
ipv6
```

Parameters

`X:X::X:X` Specify the virtual IP address of the interface that participates in virtual routing

Note: The virtual-ip address should be the IPv6 link-local address of the interface. `owner`

Specify the IP address as the owner.

Command Mode

Router mode

Example

The example below shows how to configure a router as VRRP Master and Owner:

```
#configure terminal
(config)#router ipv6 vrrp 1 eth0
(config-router)#virtual-ipv6 fe80::202:b3ff:fed5:983e owner
```

The example below removes the virtual IP address assignment.

```
#configure terminal
```

```
(config)#router ipv6 vrrp 1 eth0
(config-router)#no virtual-ipv6
```

© Symanitron Proprietary

SECTION 10 Bidirectional Forwarding Detection

Bidirectional Forwarding Detection Configuration Guide

Contents

This document contains these chapters and appendices:

- Chapter 1, *Base BFD Configuration*
- Chapter 2, *BFD Protocol Configurations*
- Chapter 3, *BFD Static Route Configuration*
- Chapter 5, *BFD Authentication*

CHAPTER 1 Base BFD Configuration

This chapter provides the steps for configuring the base Bidirectional Forwarding Detection (BFD) setup.

Overview

This section provides an overview of Bidirectional Forwarding Detection (BFD). BFD is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols like BGP, EIGRP, IS-IS, and OSPF. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators.The configuration and command reference for BFD is given in the following chapters in this section.

Topology

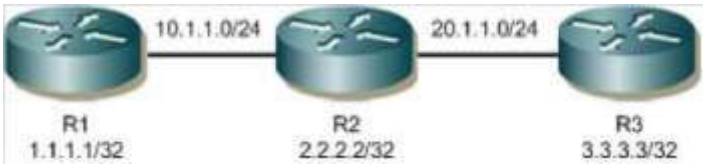


Figure 1-194: Basic Topology of Three Routers

BFD Echo Function

R1

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#interface eth1`	Enter interface Mode.
`R1(config-if)#ip address 10.1.1.1/24`	Assign IP address for interface
`R1(config-if)#bfd session 10.1.1.1 10.1.1.2`	Configure BFD session on interface.
`R1(config-if)#exit`	Exit from interface mode.
`R1(config)#bfd echo`	Enable BFD echo mode.

R2

`R2#configure terminal`	Enter the Configure mode.
`R2(config)#interface eth1`	Enter interface Mode.
`R2(config-if)#ip address 10.1.1.2/24`	Assign IP address for interface
`R2(config-if)#bfd session 10.1.1.2 10.1.1.1`	Configure BFD session on interface.
`R2(config-if)#exit`	Exit from interface mode.
`R2(config)#bfd echo`	Enable BFD echo mode.

Validation

R1

```
#sh bfd session detail

Session Interface Index : 3             Session Index : 1
Lower Layer : IPv4                      Version : 1
Session Type : Single Hop               Session State : Down
Local Discriminator : 1                 Local Address : 10.1.1.1/32
Remote Discriminator : 1                Remote Address : 10.1.1.2/32
Local Port : 49152                      Remote Port : 3784
Local Echo Port : 49153
Options :
Echo Enabled
Diagnostics : None

Timers in Milliseconds :
Min Tx: 250             Min Rx: 250             Multiplier: 3
Neg Tx: 2000            Neg Rx: 2000            Neg detect mult: 3
Min echo Tx: 1000       Min echo Rx: 1000       Neg echo intrvl: 1000
Storage type : 2
Sess down time : 00:00:01
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 000000000000010a               Pkt Out : 00000000000001f7
Echo Out : 00000000000000ab             IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000          IPv6 Pkt Out : 0000000000000000
UP Count : 57                           UPTIME : 00:00:00

Protocol Client Info:
BFD-> Client ID: 28      Flags: 4
------------------------------------------------------Number
of Sessions:     1
```

R2

```
#sh bfd session detail

Session Interface Index : 3             Session Index : 1
Lower Layer : IPv4                      Version : 1
Session Type : Single Hop               Session State : Up
Local Discriminator : 1                 Local Address : 10.1.1.2/32
Remote Discriminator : 1                Remote Address : 10.1.1.1/32
Local Port : 49152                      Remote Port : 3784
Local Echo Port : 49153
Options :
Echo Enabled
```

```
Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 2000              Neg Rx: 2000              Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 1000
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000000ad                Pkt Out : 0000000000000105
Echo Out : 0000000000000063              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 33                            UPTIME : 00:00:03

Protocol Client Info:
BFD-> Client ID: 28      Flags: 4
------------------------------------------------------------Number
of Sessions:     1
```

BFD Slow Timer

R1

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#interface eth1`	Enter interface Mode.
`R1(config-if)#ip address 10.1.1.1/24`	Assign IP address for interface
`R1(config-if)#bfd session 10.1.1.1 10.1.1.2`	Configure BFD session on interface.
`R1(config-if)#exit`	Exit from interface mode.
`R1(config)#bfd slow-timer 1000`	Configure BFD `slow-timer` in milliseconds.

R2

`R2#configure terminal`	Enter the Configure mode.
`R2(config)#interface eth1`	Enter interface Mode.
`R2(config-if)#ip address 10.1.1.2/24`	Assign IP address for interface
`R2(config-if)#bfd session 10.1.1.2 10.1.1.1`	Configure BFD session on interface.
`R2(config-if)#exit`	Exit from interface mode.
`R2(config)#bfd slow-timer 1000`	Configure BFD `slow-timer` in milliseconds.

BFD Multihop Peer Timer

R1

`R1#configure terminal`	Enter the Configure mode.

`R1(config)#interface eth1`	Enter interface Mode.
`R1(config-if)#ip address 10.1.1.1/24`	Assign IP address for interface
`R1(config-if)#exit`	Exit from interface mode.
`R1(config)#router ospf 1`	Enter router OSPF mode
`R1(config-router)#network 10.1.1.0/24 area 0`	Advertise the network to area 0
`R1(config-router)#redistribute connected`	
`R1(config-router)#exit`	Exit router OSPF mode
`R1(config)#bfd multihop-peer 20.1.1.3 interval 100 minrx 100 multiplier 3`	Configure BFD `multihop-peer` timer and reception intervals in milliseconds and the Hello multiplier.
R2	
`R2#configure terminal`	Enter the Configure mode.
`R2(config)#interface eth1`	Enter interface Mode.
`R2(config-if)#ip address 10.1.1.2/24`	Assign IP address for interface
`R2(config-if)#exit`	Exit from interface mode.
`R2(config)#interface eth2`	Enter interface Mode.
`R2(config-if)#ip address 20.1.1.2/24`	Assign IP address for interface
`R2(config-if)#exit`	Exit from interface mode.
`R2(config)#router ospf 1`	Enter router OSPF mode
`R2(config-router)#network 10.1.1.0/24 area 0`	Advertise the network to area 0
`R2(config-router)#network 20.1.1.0/24 area 0`	Advertise the network to area 0
`R2(config-router)#redistribute connected`	
`R2(config-router)#exit`	Exit router OSPF mode
R3	
`R1#configure terminal`	Enter the Configure mode.
`R1(config)#interface eth2`	Enter interface Mode.
`R1(config-if)#ip address 20.1.1.3/24`	Assign IP address for interface
`R1(config-if)#exit`	Exit from interface mode.
`R1(config)#router ospf 1`	Enter router OSPF mode
`R1(config-router)#network 20.1.1.0/24 area 0`	Advertise the network to area 0
`R1(config-router)#redistribute connected`	
`R1(config-router)#exit`	Exit router OSPF mode
`R1(config)#bfd multihop-peer 20.1.1.3 interval 100 minrx 100 multiplier 3`	Configure BFD `multihop-peer` timer and reception intervals in milliseconds and the Hello multiplier.

Validation:

R1

```
#sh bfd session detail


Session Interface Index : 0              Session Index : 2
Lower Layer : IPv4                       Version : 1
Session Type : Multihop Arbit Path       Session State : Up
Local Discriminator : 2                  Local Address : 10.1.1.1/32
Remote Discriminator : 0                 Remote Address : 20.1.1.3/32
Local Port : 49153                       Remote Port : 4784 Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 100               Min Rx: 100               Multiplier: 3
Neg Tx: 0                 Neg Rx: 0                 Neg detect mult: 0
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 0000000000000000                Pkt Out : 0000000000000097
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 0                             UPTIME : 00:00:00

Protocol Client Info:
BFD-> Client ID: 28      Flags: 4
------------------------------------------------------------Number
of Sessions:     1
```

R3

```
#sh bfd session detail


Session Interface Index : 0              Session Index : 1
Lower Layer : IPv4                       Version : 1
Session Type : Multihop Arbit Path       Session State : Up
Local Discriminator : 1                  Local Address : 20.1.1.3/32
Remote Discriminator : 1                 Remote Address : 10.1.1.1/32
Local Port : 49152                       Remote Port : 4784 Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 100               Min Rx: 100               Multiplier: 3
Neg Tx: 100               Neg Rx: 100               Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
```

```
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000001df                  Pkt Out : 00000000000001e0
Echo Out : 0000000000000000                IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000             IPv6 Pkt Out : 0000000000000000
UP Count : 1                               UPTIME : 00:01:26

Protocol Client Info:
BFD-> Client ID: 28      Flags: 4
------------------------------------------------------------Number
of Sessions:    1
```

BFD Single-hop Session Timer

R1

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#interface eth1`	Enter interface Mode.
`R1(config-if)#ip address 10.1.1.1/24`	Assign IP address for interface
`R1(config-if)#bfd session 10.1.1.1 10.1.1.2`	Configure BFD session on interface.
`R1(config-if)#bfd interval 100 minrx 100 multiplier 4`	Configure BFD single-hop sessions timer and reception interval in millisecond and the Hello multiplier.
`R1(config-if)#exit`	Exit from interface mode.

R2

`R2#configure terminal`	Enter the Configure mode.
`R2(config)#interface eth1`	Enter interface Mode.
`R2(config-if)#ip address 10.1.1.2/24`	Assign IP address for interface
`R2(config-if)#bfd session 10.1.1.2 10.1.1.1`	Configure BFD session on interface.
`R2(config-if)#bfd interval 100 minrx 100 multiplier 4`	Configure BFD single-hop sessions timer and reception interval in millisecond and the Hello multiplier.
`R2(config-if)#exit`	Exit from interface mode.

Validation:

R1

```
#sh bfd session detail

Session Interface Index : 3                Session Index : 1
Lower Layer : IPv4                         Version : 1
Session Type : Single Hop                  Session State : Up
```

```
Local Discriminator : 1                  Local Address : 10.1.1.1/32
Remote Discriminator : 1                 Remote Address : 10.1.1.2/32
Local Port : 49152                       Remote Port : 3784 Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 100              Min Rx: 100              Multiplier: 4
Neg Tx: 100              Neg Rx: 100              Neg detect mult: 4
Min echo Tx: 100         Min echo Rx: 1000        Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 000000000000156e                Pkt Out : 0000000000001748
Echo Out : 000000000000019b              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 139                           UPTIME : 00:14:23

Protocol Client Info:
BFD-> Client ID: 28      Flags: 4
------------------------------------------------------------Number
of Sessions:     1
```

R2

```
#sh bfd session detail

Session Interface Index : 3              Session Index : 1
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                  Local Address : 10.1.1.2/32
Remote Discriminator : 1                 Remote Address : 10.1.1.1/32
Local Port : 49152                       Remote Port : 3784 Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 100              Min Rx: 100              Multiplier: 4
Neg Tx: 100              Neg Rx: 100              Neg detect mult: 4
Min echo Tx: 100         Min echo Rx: 1000        Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 000000000000181d                Pkt Out : 00000000000019ab
```

```
Echo Out : 00000000000001b5                IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000             IPv6 Pkt Out : 0000000000000000
UP Count : 145                             UPTIME : 00:15:19

Protocol Client Info:
BFD-> Client ID: 28      Flags: 4
-------------------------------------------------------------------------------
                                                                Number of
Sessions:     1
```

BFD Echo Interval

R1

R1#configure terminal	Enter the Configure mode.
R1(config)#interface eth1	Enter interface Mode.
R1(config-if)#ip address 10.1.1.1/24	Assign IP address for interface
R1(config-if)#bfd session 10.1.1.1 10.1.1.2	Configure BFD session on interface.
R1(config-if)#bfd echo interval 100	.
R1(config-if)#exit	Exit from interface mode.
R1(config)#bfd echo	Enable BFD echo mode.

R2

R2#configure terminal	Enter the Configure mode.
R2(config)#interface eth1	Enter interface Mode.
R2(config-if)#ip address 10.1.1.2/24	Assign IP address for interface
R2(config-if)#bfd session 10.1.1.2 10.1.1.1	Configure BFD session on interface.
R1(config-if)#bfd echo interval 100	.
R2(config-if)#exit	Exit from interface mode.
R2(config)#bfd echo	Enable BFD echo mode.

Validation

R1

```
#sh bfd session detail

Session Interface Index : 3                Session Index : 1
Lower Layer : IPv4                         Version : 1
Session Type : Single Hop                  Session State : Down
Local Discriminator : 1                    Local Address : 10.1.1.1/32
Remote Discriminator : 1                   Remote Address : 10.1.1.2/32
Local Port : 49152                         Remote Port : 3784 Local
Echo Port : 49153
Options :
Echo Enabled
```

```
Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 2000              Neg Rx: 2000              Neg detect mult: 3
Min echo Tx: 100          Min echo Rx: 1000         Neg echo intrvl: 1000
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000001ea                Pkt Out : 0000000000000398
Echo Out : 0000000000000147              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 109                           UPTIME : 00:00:00

Protocol Client Info:
BFD-> Client ID: 28      Flags: 4
------------------------------------------------------------Number
of Sessions:     1
```

R2

```
#sh bfd session detail

Session Interface Index : 3              Session Index : 1
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Down
Local Discriminator : 1                  Local Address : 10.1.1.2/32
Remote Discriminator : 1                 Remote Address : 10.1.1.1/32
Local Port : 49152                       Remote Port : 3784
Local Echo Port : 49153
Options :
Echo Enabled
Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 2000              Neg Rx: 2000              Neg detect mult: 3
Min echo Tx: 100          Min echo Rx: 1000         Neg echo intrvl: 1000
Storage type : 2
Sess down time : 00:00:01
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 000000000000028f                Pkt Out : 00000000000003b8
Echo Out : 0000000000000183              IPv6 Echo Out : 0000000000000000
```

```
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 129                           UPTIME : 00:00:00

Protocol Client Info:
BFD-> Client ID: 28       Flags: 4
------------------------------------------------------------
Number of Sessions:     1
```

CHAPTER 2 BFD Protocol Configurations

This chapter describes the BFD protocol configurations.

OSPF—BFD Single-Hop Session

This section provides the steps for configuring BFD for Single-Hop OSPF.

Topology

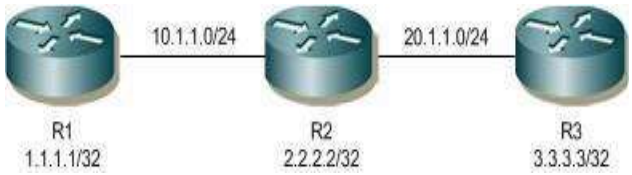


Figure 2-195: Single-Hop OSPF Topology

Configuration for R1

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#interface eth1`	Enter the Interface configuration mode for `eth1`.
`R1(config-if)#ip address 10.1.1.1/24`	Assign IP Address.
`R1(config-if)#exit`	Exit the Interface configuration mode.
`R1(config)#router ospf 100`	Enter the Router mode for OSPF.
`R1(config-router)#network 10.1.1.0/24 area 1`	Advertise network `10.1.1.0/24` in OSPF `area 1`.
`R1(config-router)#network 1.1.1.1/32 area 1`	Advertise loopback network `1.1.1.1/32` in OSPF `area 1`.
`R1(config-router)#bfd all-interfaces`	Enable BFD for all neighbors.
`R1(config-router)#exit`	Exit the router mode.

Configuration for R2

`R2#configure terminal`	Enter the Configure mode.
`R2(config)#interface eth1`	Enter the Interface configuration mode for `eth1`.
`R2(config-if)#ip address 10.1.1.2/24`	Assign IP Address.
`R2(config-if)#exit`	Exit the Interface configuration mode.
`R2(config)#interface eth2`	Enter the Interface configuration mode for `eth1`.
`R2(config-if)#ip address 20.1.1.1/24`	Assign IP Address.
`R2(config-if)#exit`	Exit the Interface configuration mode.
`R2(config)#router ospf 100`	Enter the Router mode for OSPF.
`R2(config-router)#network 10.1.1.0/24 area 1`	Advertise network `10.1.1.0/24` in OSPF `area 1`.

R2(config-router)#network 20.1.1.0/24 area 1	Advertise network 20.1.1.0/24 in OSPF area 1.
R2(config-router)#network 2.2.2.2/32 area 1	Advertise loopback network 2.2.2.2/32 in OSPF area 1.
R2(config-router)#bfd all-interfaces	Enable BFD for all neighbors.
R2(config-router)#exit	Exit the router mode.

Configuration for R3

R3#configure terminal	Enter the Configure mode.
R3(config)#interface eth2	Enter the Interface configuration mode for eth1.
R3(config-if)#ip address 20.1.1.1/24	Assign IP Address.
R3(config-if)#exit	Exit the Interface configuration mode.
R3(config)#router ospf 100	Enter the Router mode for OSPF.
R3(config-router)#network 20.1.1.0/24 area 1	Advertise network 20.1.1.0/24 in OSPF area 1.
R3(config-router)#network 3.3.3.3/32 area 1	Advertise loopback network 3.3.3.3/32 in OSPF area 1.
R3(config-router)#bfd all-interfaces	Enable BFD for all neighbors
R3(config-router)#exit	Exit the router mode.

Validation

```
R1#sh bfd session
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Remote-Addr
1          1            IPv4         Single-Hop  Up          00:12:09  10.1.1.2/32
Number of Sessions:     1
-------------------------------------------------------------------------------
-

R2#sh bfd session
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Remote-Addr
1          1            IPv4         Single-Hop  Up          00:12:36  10.1.1.1/32
2          1            IPv4         Single-Hop  Up          00:12:21  20.1.1.2/32
Number of Sessions:     2

-------------------------------------------------------------------------------
-

R1#sh bfd session
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Remote-Addr
1          2            IPv4         Single-Hop  Up          00:13:07  20.1.1.1/32
Number of Sessions:    1

-------------------------------------------------------------------------------
-

R1#sh bfd session detail
```

```
=====================================================

Session Interface Index : 3              Session Index : 1
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                  Local Address : 10.1.1.1/32
Remote Discriminator : 1                 Remote Address : 10.1.1.2/32 Local Port :
49152                       Remote Port : 3784 Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 250               Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 0000000000000cf3                Pkt Out : 0000000000000cfc
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 1                             UPTIME : 00:12:12

Protocol Client Info:
OSPF-> Client ID: 4      Flags: 4
-----------------------------------------------------------
Number of Sessions:    1

R2#sh bfd session detail
=====================================================

Session Interface Index : 3              Session Index : 1
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                  Local Address : 10.1.1.2/32
Remote Discriminator : 1                 Remote Address : 10.1.1.1/32 Local Port :
49152                       Remote Port : 3784 Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 2000              Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
```

```
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled
Counters values:
Pkt In : 0000000000000d6f                Pkt Out : 0000000000000da5
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 1                             UPTIME : 00:12:39

Protocol Client Info:
OSPF-> Client ID: 4      Flags: 4
------------------------------------------------------------

Session Interface Index : 4              Session Index : 2
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 2                  Local Address : 20.1.1.1/32
Remote Discriminator : 1                 Remote Address : 20.1.1.2/32 Local Port :
49153                       Remote Port : 3784 Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 2000              Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 0000000000000d30                Pkt Out : 0000000000000d5e
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 1                             UPTIME : 00:12:24

Protocol Client Info:
OSPF-> Client ID: 4      Flags: 4
------------------------------------------------------------
Number of Sessions:    2

R3#sh bfd session detail
============================================================

Session Interface Index  : 4             Session Index : 1
Lower  Layer : IPv4                      Version : 1
Session  Type : Single Hop               Session State : Up
Local  Discriminator : 1                 Local Address : 20.1.1.2/32
```

```
Remote Discriminator : 2                Remote Address : 20.1.1.1/32 Local Port :
49152                       Remote Port : 3784 Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250              Min Rx: 250              Multiplier: 3
Neg Tx: 250              Neg Rx: 250              Neg detect mult: 3
Min echo Tx: 1000        Min echo Rx: 1000        Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 0000000000000e0b                Pkt Out : 0000000000000e06
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 1                             UPTIME : 00:13:09

Protocol Client Info:
OSPF-> Client ID: 4      Flags: 4
-----------------------------------------------------------------------------
                                                        Number  of  Sessions:
1
```

OSPF—BFD Multi-Hop Session

This section provides the steps for configuring BFD for OSPF multi-hop sessions.

Topology

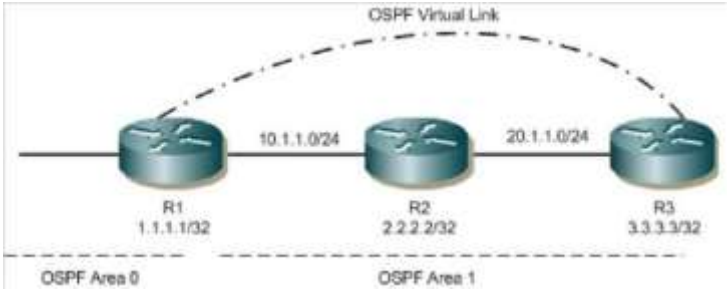


Figure 2-196: Multi-hop OSPFv2 Topology

Configuration

R1

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#router ospf 100`	Enter the Router mode for OSPF.

R1(config-router)#network 10.1.1.0/24 area 1	Advertise network 20.1.1.0/24 in OSPF area 1.
R1(config-router)#network 1.1.1.1/32 area 1	Advertise loopback network 1.1.1.1/32 in OSPF area 1.
R1(config-router)#network 30.1.1.0/24 area 0	Advertise network 30.1.1.0/24 in OSPF area 0.
R1(config-router)#area 1 virtual-link 3.3.3.3 fall-over bfd	Create a virtual link to R3 with BFD.

R2

R2#configure terminal	Enter the Configure mode
R2(config)#router ospf 100	Enter the Router mode for OSPF.
R2(config-router)#network 10.1.1.0/24 area 1	Advertise network 10.1.1.0/24 in OSPF area 1.
R2(config-router)#network 20.1.1.0/24 area 1	Advertise network 20.1.1.0/24 in OSPF area 1.
R2(config-router)#network 2.2.2.2/32 area 1	Advertise loopback network 2.2.2.2/32 in OSPF area 1.

R3

R3#configure terminal	Enter the Configure mode.
R3(config)#router ospf 100	Enter the Router mode for OSPF.
R3(config-router)#network 20.1.1.0/24 area 1	Advertise network 20.1.1.0/24 in OSPF area 1.
R3(config-router)#network 3.3.3.3/32 area 1	Advertise loopback network 3.3.3.3/32 in OSPF area 1.
R3(config-router)#area 1 virtual-link 1.1.1.1 fall-over bfd	Create a virtual link to R1 with BFD.

Validation

```
R1#sh bfd session
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Remote-Addr
5          5            IPv4         Multi-Hop   Up          00:02:27  20.1.1.68/32
Number of Sessions:     1

-------------------------------------------------------------------------------
-

R2#sh bfd session
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Remote-Addr
Number of Sessions:    0 ------------------------------------------------------------
--------------------------

R3#sh bfd session
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Remote-Addr
5           5             IPv4          Multi-Hop   Up           00:03:03  10.1.1.66/32
Number of Sessions:    1
```

```
--------------------------------------------------------------------------------
-


R1#sh bfd session detail
=======================================================

Session Interface Index : 0              Session Index : 5
Lower Layer : IPv4                       Version : 1
Session Type : Multihop Arbit Path       Session State : Up
Local Discriminator : 5                  Local Address : 10.1.1.66/32
Remote Discriminator : 5                 Remote Address : 20.1.1.68/32
Local Port : 49156                       Remote Port : 4784 Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 2000              Neg detect mult: 3 Min
echo Tx: 1000          Min echo Rx: 1000        Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 0000000000000452                Pkt Out : 0000000000000457
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 1                             UPTIME : 00:04:08

Protocol Client Info:
OSPF-> Client ID: 4       Flags: 4
-------------------------------------------------------
Number of Sessions:     1


R2#sh bfd session detail
=======================================================
Number of Sessions:    0


R3#sh bfd session detail
=======================================================

Session  Interface Index : 0             Session Index : 5
Lower  Layer : IPv4                      Version : 1
Session  Type : Multihop Arbit Path      Session State : Up
Local  Discriminator : 5                 Local Address : 20.1.1.68/32
```

```
Remote Discriminator : 5                Remote Address : 10.1.1.66/32 Local Port :
49156                        Remote Port : 4784 Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 2000              Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000004f6                Pkt Out : 00000000000004f1
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 1                             UPTIME : 00:04:39

Protocol Client Info:
OSPF-> Client ID: 4      Flags: 4
------------------------------------------------------------
Number of Sessions:    1
```

BFD Configuration in IS-IS

This section provides the steps for configuring BFD for the IS-IS protocol.

Topology

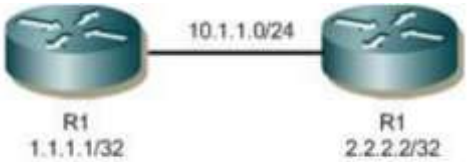


Figure 2-197: Basic Topology for BFD-ISIS

R1

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#interface eth1`	Enter Interface mode.
`R1(config-if)#ip address 10.1.1.1/24`	Configure IP address.
`R2(config-if)#ip router isis`	Configure ISIS router
`R1(config-if)#exit`	Exit Interface mode.
`R1(config)#router isis`	Enter the Router mode for IS-IS.
`R1(config-router)#net 10.0000.0000.0001.00`	Advertise network `10.0000.0000.0001.00` in IS-IS.

R1(config-router)#bfd all-interfaces	Enable BFD for all neighbors.

R2

R2#configure terminal	Enter the Configure mode.
R2(config)#interface eth1	Enter Interface mode.
R2(config-if)#ip address 10.1.1.2/24	Configure IP address.
R2(config-if)#ip router isis	Configure ISIS router
R2(config-if)#exit	Exit Interface mode.
R2(config)#router isis	Enter the Router mode for IS-IS.
R2(config-router)#net 10.0000.0000.0002.00	Advertise network 10.0000.0000.0002.00 in IS-IS.
R2(config-router)#bfd all-interfaces	Enable BFD for all neighbors.

Validation

```
R1#sh bfd session
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Remote-Addr
2          3            IPv4         Single-Hop  Up          00:02:17  10.1.1.2/32
Number of Sessions:    1

--------------------------------------------------------------------------------
-

R2#sh bfd session
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   Remote-Addr
3          2            IPv4         Single-Hop  Up          00:02:40  10.1.1.1/32 Number
of Sessions:    1

--------------------------------------------------------------------------------
-

R1#sh bfd session detail
=======================================================

Session Interface Index : 3              Session Index : 2
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 2                  Local Address : 10.1.1.1/32
Remote Discriminator : 3                 Remote Address : 10.1.1.2/32
Local Port : 49153                       Remote Port : 3784 Options
:

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250              Min Rx: 250              Multiplier: 3
Neg Tx: 250              Neg Rx: 2000             Neg detect mult: 3 Min
echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
```

```
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 000000000000027b                Pkt Out : 0000000000000278
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 1                             UPTIME : 00:02:19

Protocol Client Info:
ISIS-> Client ID: 6       Flags: 4
------------------------------------------------------------
Number of Sessions:     1

R2#sh bfd session detail
============================================================

Session Interface Index : 3              Session Index : 3
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 3                  Local Address : 10.1.1.2/32
Remote Discriminator : 2                 Remote Address : 10.1.1.1/32
Local Port : 49154                       Remote Port : 3784 Options
:

Diagnostics : None
```

```
Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 250               Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000002db                Pkt Out : 00000000000002dd
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 1                             UPTIME : 00:02:42

Protocol Client Info:
ISIS-> Client ID: 6      Flags: 4
------------------------------------------------------------Number
of Sessions:    1
```

BFD Configuration in BGP

This section provides the steps for configuring BFD for the BGP protocol.

Topology

Figure 2-198: Basic Topology for BFD in BGP

R1

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#router bgp 100`	Enter the Router mode for BGP.
`R1(config-router)#neighbor 3.3.3.3 remote-as 100 100`	Add the neighbor `3.3.3.3/32` to remote-as
`R1(config-router)#neighbor 3.3.3.3 fall-over bfd multihop`	Enable the BFD option for the neighbor.

R2

`R2#configure terminal`	Enter the Configure mode.
`R2(config)#router bgp 100`	Enter the Router mode for BGP.
`R2(config-router)#neighbor 2.2.2.2 remote-as 100. 100`	Add the neighbor `2.2.2.2` to remote-as

```
Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
```

R2(config-router)#neighbor 2.2.2.2 fall-over bfd multihop	Enable the BFD option for the neighbor.

R3

R3#configure terminal	Enter the Configure mode.
R3(config)#router bgp 100	Enter the Router mode for BGP.
R3(config-router)#neighbor 1.1.1.1 remote-as 100. 100	Add the neighbor 1.1.1.1 to remote-as
R3(config-router)#neighbor 1.1.1.1 fall-over neighbor. bfd multihop	Enable the BFD option for the

Validation

```
R1#sh bfd session
Sess-Idx    Remote-Disc   Lower-Layer   Sess-Type    Sess-State   UP-Time
Remote-Addr
6           3             IPv4          Single-Hop   Up           00:01:22
10.1.1.67/32
Number of Sessions:    1

------------------------------------------------------------------------
------------

R2#sh bfd session
Sess-Idx    Remote-Disc   Lower-Layer   Sess-Type    Sess-State   UP-Time
Remote-Addr
3           6             IPv4          Single-Hop   Up           00:01:16
10.1.1.66/32 4            6               IPv4           Single-Hop   Up
00:00:01  20.1.1.68/32
Number of Sessions:    2

------------------------------------------------------------------------
--------------

R3#sh bfd session
Sess-Idx    Remote-Disc   Lower-Layer   Sess-Type    Sess-State   UP-Time
Remote-Addr
6           4             IPv4          Single-Hop   Up           00:01:26
20.1.1.67/32
Number of Sessions:    1



R1#sh bfd session detail
=======================================================

Session Interface Index : 4             Session Index : 6
```

```
Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Lower Layer : IPv4                          Version : 1
Session Type : Single Hop                   Session State : Up
Local Discriminator : 6                     Local Address : 10.1.1.66/32
Remote Discriminator : 3                    Remote Address :
10.1.1.67/32 Local Port : 49157
Remote Port : 3784 Options :

Diagnostics : None
Neg Tx: 250               Neg Rx: 2000              Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 0000000000000318                   Pkt Out : 0000000000000317
Echo Out : 0000000000000000                 IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000              IPv6 Pkt Out : 0000000000000000
UP Count : 1                                UPTIME : 00:02:54

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------------
Number of Sessions:    1


R2#sh bfd session detail
============================================================

Session Interface Index : 4                 Session Index : 3
Lower Layer : IPv4                          Version : 1
Session Type : Single Hop                   Session State : Up
Local Discriminator : 3                     Local Address : 10.1.1.67/32
Remote Discriminator : 6                    Remote Address : 10.1.1.66/32
Local Port : 49154                          Remote Port : 3784 Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 250               Neg detect mult: 3 Min
echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
```

```
Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 0000000000000345                Pkt Out : 0000000000000346
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000            IPv6 Pkt Out : 0000000000000000
UP Count : 1                             UPTIME : 00:03:06

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------------

Session Interface Index : 3              Session Index : 4
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 4                  Local Address : 20.1.1.67/32
Remote Discriminator : 6                 Remote Address : 20.1.1.68/32
Local Port : 49155                       Remote Port : 3784 Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 250               Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 00000000000001f0                Pkt Out : 00000000000001f0
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 1                             UPTIME : 00:01:51

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------------
Number of Sessions:    2


R3#sh bfd session detail
============================================================
```

```
Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Session Interface Index : 3              Session Index : 6
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 6                  Local Address : 20.1.1.68/32
Remote Discriminator : 4                 Remote Address : 20.1.1.67/32
Local Port : 49157                       Remote Port : 3784 Options :

Diagnostics : None
Neg Tx: 250               Neg Rx: 2000              Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 000000000000024c                Pkt Out : 000000000000024b
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 1                             UPTIME : 00:02:10

Protocol Client Info:
BGP-> Client ID: 44      Flags: 4
------------------------------------------------------------Number
of Sessions:     1
```

BFD Configuration in RIP

This section provides the steps for configuring BFD for the RIP protocol.

Topology

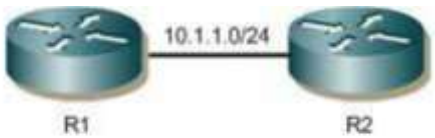


Figure 2-199: Basic Topology for BFD in RIP

R1

`R1#configure terminal`	Enter the Configure mode.
`R1(config)#interface eth2`	Enter Interface mode.
`R1(config-if)#ip address 10.1.1.1/24`	Configure IP address.
`R2(config-if)#ip router isis`	Configure ISIS router
`R1(config-if)#exit`	Exit Interface mode.

```
Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
```

R1(config)#router rip	Enter the Router mode for RIP.
R1(config-router)#network 10.1.1.0/24	Advertise network 10.1.1.0/24 in RIP.
R1(config-router)#bfd all-interfaces	Enable BFD for all neighbors.
	or
R1(config-router)#neighbor 10.1.1.2 fallover bfd	Enable BFD for a specific RIP neighbor
R2	
R2#configure terminal	Enter the Configure mode.
R2(config)#interface eth1	Enter Interface mode.
R2(config-if)#ip address 10.1.1.2/24	Configure IP address.
R2(config-if)#ip router isis	Configure ISIS router
R2(config-if)#exit	Exit Interface mode.
R2(config)#router rip	Enter the Router mode for RIP.
R2(config-router)#network 10.1.1.0/24	Advertise network 10.1.1.0/24 in RIP.
R2(config-router)#bfd all-interfaces	Enable BFD for all neighbors.
	or
R2(config-router)#neighbor 10.1.1.1 fallover bfd	Enable BFD for a specific RIP neighbor.

Validation

```
R1#sh bfd session
Sess-Idx    Remote-Disc   Lower-Layer   Sess-Type    Sess-State   UP-Time
Remote-Addr
1           1             IPv4          Single-Hop   Up           00:00:14
10.1.1.68/32
Number of Sessions:    1

------------------------------------------------------------------------
------------

R2#sh bfd session
Sess-Idx    Remote-Disc   Lower-Layer   Sess-Type    Sess-State   UP-Time
Remote-Addr
1           1             IPv4          Single-Hop   Up           00:00:10
10.1.1.67/32
Number of Sessions:    1

------------------------------------------------------------------------
------------
```

```
Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
R1#sh bfd session detail
=======================================================

Session Interface Index : 3             Session Index : 1
Lower Layer : IPv4                      Version : 1
Session Type : Single Hop               Session State : Up
Local Discriminator : 1                 Local Address : 10.1.1.67/32
Remote Discriminator : 1                Remote Address :
10.1.1.68/32 Local Port : 49152
Remote Port : 3784 Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 2000              Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
```

```
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 0000000000000040                Pkt Out : 000000000000003f
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 1                             UPTIME : 00:00:16

Protocol Client Info:
RIP-> Client ID: 2        Flags: 4
------------------------------------------------------------
Number of Sessions:     1



R2#sh bfd session detail
============================================================

Session Interface Index : 3              Session Index : 1
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                  Local Address : 10.1.1.68/32
Remote Discriminator : 1                 Remote Address : 10.1.1.67/32 Local Port :
49152                         Remote Port : 3784 Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250                Min Rx: 250              Multiplier: 3
Neg Tx: 250                 Neg Rx: 250               Neg detect mult: 3 Min echo Tx: 1000
Min echo Rx: 1000          Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 0000000000000055                Pkt Out : 0000000000000057
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 1                             UPTIME : 00:00:22

Protocol Client Info:
RIP-> Client ID: 2       Flags: 4 ------------------------------------------------------------
--
Number of Sessions:     1
```

CHAPTER 3 BFD Static Route Configuration

This chapter describes the configurations for BFD static routes.

In order to establish alternate paths to destinations that have the least possible delay it is important to quickly detect any changes to static route validity. BFD detects the liveliness of a static route's nexthop and then uses the nexthop's reachability information to determine whether routes are valid. Using BFD to reach a static route's nexthop also ensures that a static route is inserted in the forwarding database only when the nexthop neighbor is reachable.

Topology

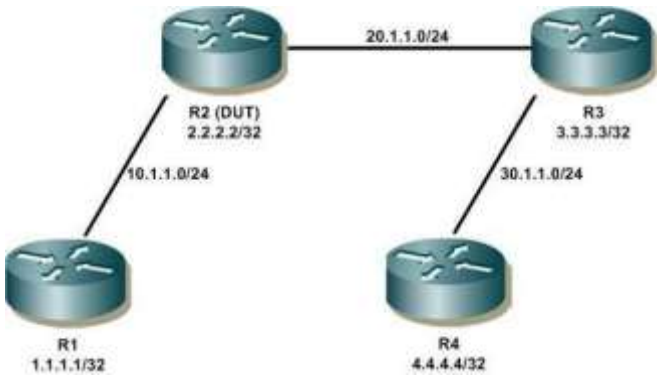


Figure 3-200: BFD Static Route Basic Topology

R1

`R1(config)#interface eth2`	Enter the Interface configuration mode for `eth2`.
`R1(config-if)#ip address 10.1.1.1/24`	Assign IP address on interface.
`R1(config-if)#exit`	Exit the Interface configuration mode.

R2

`R2#configure terminal`	Enter the Configure mode.
`R2(config)#ip route 30.1.1.0/24 20.1.1.3`	Configure static route.
`R2(config)#ip bfd static all-interfaces`	Enable BFD for all static routes.
`R2(config)#interface eth1`	Enter the Interface configuration mode for `eth1`.
`R2(config-if)#ip static bfd`	Enable static BFD on the interface.
`R2(config-if)#ip address 20.1.1.2/24`	Assign IP address on interface.
`R2(config-if)#exit`	Exit the Interface configuration mode.
`R2(config)#ip static 30.1.1.0/24 20.1.1.3 fall-over bfd`	Enable static BFD at static route level.
`R2(config)#interface eth2`	Enter the Interface configuration mode for `eth2`.

`R2(config-if)#ip address 10.1.1.2/24`	Assign IP address on interface.
`R2(config-if)#exit`	Exit the Interface configuration mode.

BFD Static Route Configuration

R3

R3#configure terminal	Enter the Configure mode.
R3(config)#ip route 10.1.1.0/24 20.1.1.2	Configure static route.
R3(config)#ip bfd static all-interfaces	Enable BFD for all static routes.
R3(config)#interface eth1	Enter the Interface configuration mode for eth1.
R3(config-if)#ip address 20.1.1.3/24	Assign IP address on interface.
R3(config-if)#ip static bfd	Enable static BFD at interface level.
R3(config-if)#exit	Exit the Interface configuration mode.
R3(config)#ip static 10.1.1.0/24 20.1.1.2 fall-over bfd	Enable static BFD at static route level.
R3(config)#interface eth2	Enter the Interface configuration mode for eth2.
R3(config-if)#ip address 30.1.1.2/24	Assign IP address on interface.
R3(config-if)#exit	Exit the Interface configuration mode.

R4

R3(config)#interface eth2	Enter the Interface configuration mode for eth2.
R3(config-if)#ip address 30.1.1.1/24	Assign IP address on interface.
R3(config-if)#exit	Exit the Interface configuration mode.

Validation

R2

```
#sh bfd session
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   RemoteAddr
5          1            IPv4         Single-Hop  Up          00:09:32
20.1.1.3/32
Number of Sessions:     1
VPC2#sh bfd session detail
=======================================================

Session Interface Index : 3              Session Index : 5
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 5                  Local Address : 20.1.1.2/32
Remote Discriminator : 1                 Remote Address : 20.1.1.3/32
Local Port : 49156                       Remote Port : 3784 Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx:  250              Min Rx: 250              Multiplier: 3
Neg Tx:  250              Neg Rx: 2000             Neg detect mult: 3
```

```
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
```



```
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 0000000000000a29                Pkt Out : 0000000000000bb6
Echo Out : 0000000000000000              IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000           IPv6 Pkt Out : 0000000000000000
UP Count : 1                             UPTIME : 00:09:34

Protocol Client Info:
RIB-> Client ID: 42      Flags: 4
------------------------------------------------------------Number of
Sessions:     1
```

R3

```
#sh bfd session
Sess-Idx   Remote-Disc  Lower-Layer  Sess-Type   Sess-State  UP-Time   RemoteAddr
1          5            IPv4         Single-Hop  Up          00:09:39
20.1.1.2/32
Number of Sessions:    1
VPC3#sh bfd session detail
=======================================================

Session Interface Index : 3              Session Index : 1
Lower Layer : IPv4                       Version : 1
Session Type : Single Hop                Session State : Up
Local Discriminator : 1                  Local Address : 20.1.1.3/32
Remote Discriminator : 5                 Remote Address : 20.1.1.2/32
Local Port : 49152                       Remote Port : 3784 Options :

Diagnostics : None

Timers in Milliseconds :
Min Tx: 250               Min Rx: 250               Multiplier: 3
Neg Tx: 250               Neg Rx: 250               Neg detect mult: 3
Min echo Tx: 1000         Min echo Rx: 1000         Neg echo intrvl: 0
Storage type : 2
Sess down time : 00:00:00
Sess discontinue time : 00:00:00
Bfd GTSM Disabled
Bfd Authentication Disabled

Counters values:
Pkt In : 0000000000000a59                Pkt Out : 0000000000000a53
```

```
Echo Out : 0000000000000000                IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000             IPv6 Pkt Out : 0000000000000000
UP Count : 1                               UPTIME : 00:09:41

Protocol Client Info:
RIB-> Client ID: 42       Flags: 4
------------------------------------------------------------
Number of Sessions:     1
```

BFD Static Route Configuration

Bidirectional Forwarding Detection Command Reference

Contents

This document contains these chapters:

- Chapter 1, *Bidirectional Forwarding Commands*
- Chapter 2, *Protocol Commands for BFD*
- Chapter 3, *BFD Static Route Commands*

CHAPTER 1 Bidirectional Forwarding Commands

This chapter explains the commands used to configure Bidirectional Forwarding (BFD):

- bfd auth type
- bfd
- bfd echo
- bfd echo interval
- bfd-firmware
- bfd interval
- bfd multihop-peer
- bfd multihop-peer A.B.C.D interval
- bfd multihop-peer X:X::X:X interval
- bfd notification
- bfd slow-timer
- debug bfd
- key
- key chain
- send-lifetime
- show bfd
- show bfd interface
- show bfd session
- show bfd session A.B.C.D
- show bfd session ipv6
- show debugging bfd
- snmp restart bfd

bfd auth type

Use this command to enable BFD authentication on an interface that has either an IPv4 or an IPv6 BFD session. The configured key-chain option identifies the key-chain name. A key-chain consists of a configured key-id and authentication string, which can be configured under key-chain mode (refer to key chain for more information). BFD authentication uses the active key-id when there are multiple key-ids under a key-chain. Use the `no` form of the command to disable BFD authentication.

Command Syntax

```
bfd auth type (simple | keyed-sha1 | meticulous-keyed-sha1) (key-id <0-255> key
  LINE) no
bfd auth
```

Parameters `simple` Specify a simple authentication type. `keyed-sha1` Specify a keyed secure hashing algorithm authentication type.

`meticulous-keyed-sha1`
Specify an authentication key meticulous keyed secure hashing algorithm authentication.

`key-id` Indicate the `key-id` keyword.

`<0-255>` Specify the key ID value. `key`
Indicate the `key` keyword.

`LINE` Specify the authentication key name.

Command Mode

Interface mode

Applicability

This command was introduced in a version before SWMRE version 1.3.

Example

Do the following to configure a single-key support:

```
(config)#interface eth1
(config-if)#bfd auth type simple key-id 14 key myid1
```

bfd

Use this command to enable and disable all the BFD sessions on this interface.

Command Syntax `bfd (enable|disable)`

Parameters

`enable` Enable BFD `disable` Disable BFD.

Command Mode

Interface mode

Applicability

This command was introduced in a version before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#bfd disable
```

bfd echo

Use this command to set BFD sessions to echo mode.

Use the `no` form of the command to return a BFD session to its default mode.

Command Syntax `bfd echo no bfd echo`

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced in a version before SWMRE version 1.3.

Example

```
#configure terminal
(config)#bfd echo
```

bfd echo interval

Use this command to set the BFD echo interval.

Use the `no` form of this command to reset the echo interval to its default value.

Command Syntax `bfd echo interval <1-4294967> no bfd echo interval <1-4294967>`

Parameter

`<1-4294967>` Transmit interval in milliseconds.

Command Mode

Interface mode

Applicability

This command was introduced in a version before SWMRE version 1.3.

Example

The following command sets the BFD echo with no values.

```
#configure terminal
(config)#interface eth1
(config-if)#bfd echo interval 234
```

bfd-firmware

Use this command to enable multi-hop or micro-BFD processing in hardware.

Note: For LAG interfaces, you must specify `micro-bfd`. With `micro-bfd` only single hop sessions are supported.

Command Syntax `bfd-firmware (multi-hop|micro-bfd)`

Parameter `multi-hop` Enable multihop sessions

`micro-bfd` Enable micro-BFD sessions (default)

Default

By default, micro-BFD sessions are enabled.

Command Mode

Configure mode

Applicability

This command was introduced in a version before SWMRE version 1.3.

Example

```
#configure terminal
```

```
(config)#bfd-firmware multi-hop
```

bfd interval

Use this command to configure BFD transmit and receive intervals, and the hello multiplier value.

Use the `no` form of the command to set the intervals and multiplier to their default values.

Command Syntax `bfd interval <3-999> minrx <3-999> multiplier <3-50> no bfd interval <3-999> minrx <3-999> multiplier <3-50>`

Parameters

`<3-999>`	Transmit interval in milliseconds.
`minrx`	Receive interval.
`<3-999>`	Receive interval in milliseconds.
`multiplier`	Hello multiplier.
`<3-50>`	Hello multiplier value.

Defaults

The default for the transmit and receive intervals is 250 milliseconds.

The default hello multiplier value is 3.

Command Mode

Interface mode

Applicability

This command was introduced in a version before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#bfd interval 100 minrx 100 multiplier 5 (config-if)#
```

bfd multihop-peer

Use this command to enable authentication over either a multihop IPv4 or IPv6

session Use the `no` form of the command to disable BFD authentication.

Command Syntax

```
bfd multihop-peer (A.B.C.D|X:X::X:X) auth type (simple | keyed-sha1 | meticulous-keyed-sha1) key-id <0-255> key LINE
no bfd multihop-peer (A.B.C.D) auth
```

Parameters

`A.B.C.D`	Specify an IPv4 address.
`auth type`	Specify an authentication type.

`simple` Specify a simple authentication type. `keyed-sha1` Specify a keyed secure hashing algorithm authentication type.

`meticulous-keyed-sha1`
Specify an authentication key Meticulous Keyed Secure hashing algorithm authentication type.

`key-id` Indicate the `key-id` keyword.

`<0-255>` Specify the key ID value. `key`

Indicate the `key` keyword.

`LINE` Specify the authentication key name.

Command Mode

Configure mode

Applicability

This command was introduced in a version before SWMRE version 1.3.

Example

Do the following to configure a single-key support:

```
#configure terminal
(config)#bfd multihop-peer 123.12.1.2 auth-type simple key-id 14 key myid1
```

bfd multihop-peer A.B.C.D interval

Use this command to configure IPv4 BFD multihop peer timer values.

Use the `no` form of the command to reset the IPv4 multihop peer timer value.

Command Syntax `bfd multihop-peer A.B.C.D interval <50-999> minrx <50-999> multiplier <3-50> no bfd multihop-peer A.B.C.D interval <50-999> minrx <50-999> multiplier <3-50>`

Parameters

`interval` Indicate the interval parameter.

`<50-999>` Specify the actual transmit interval in milliseconds.

`minrx` Indicate the minrx parameter.

`<50-999>` Specify the actual reception interval in milliseconds.

`multiplier` Indicate the multiplier parameter.

`<3-50>` Specify the actual hello multiplier value.

Command Mode

Configure mode

Default

Multiplier value is 3

Applicability

This command was introduced in a version before SWMRE version 1.3.

Example

```
#configure terminal
(config)#bfd multihop-peer 10.1.1.67 interval 100 minrx 100 multiplier
3 (config)#
```

bfd multihop-peer X:X::X:X interval

Use this command to configure an IPv6 BFD multihop peer timer values.

Use the `no` form of the command to reset the IPv6 multihop peer timer values.

Command Syntax `bfd multihop-peer X:X::X:X interval <50-999> minrx <50-999> multiplier <3-50> no bfd multihop-peer X:X::X:X interval <50-999> minrx <50-999> multiplier <3-50>`

Parameters

`interval`	Indicate the interval parameter.
`<50-999>`	Specify the actual transmit interval in milliseconds.
`minrx`	Indicate the minrx parameter.
`<50-999>`	Specify the actual reception interval in milliseconds.
`multiplier`	Indicate the multiplier parameter.
`<3-50>`	Specify the actual hello multiplier value.

Command Mode

Configure mode

Default

Default multiplier value is 3

Applicability

This command was introduced in a version before SWMRE version 1.3.

Example

```
#configure terminal
 (config)#bfd multihop-peer 10.1.1.1 interval 100 minrx 100 multiplier 3
```

bfd notification

Use this command to enable or disable BFD notification.

Command Syntax `bfd notification (enable | disable)`

Parameters

`disable`	Disable BFD notification.
`enable`	Enable BFD notification.

Command Mode

Configure mode

Applicability

This command was introduced in a version before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#bfd notification enable

(config)#bfd notification disable
```

bfd slow-timer

Use this command to set a BFD slow timer interval.

Use the `no` form of the command to reset the timer to default values.

Command Syntax `bfd slow-timer <1000-3000> no bfd slow-timer <1000-3000>`

Parameter

`<1000-3000>`	Interval for the slow-timer in milliseconds

Command Mode

Configure mode

Default

Default slow-timer value is 2000

Applicability

This command was introduced in a version before SWMRE version 1.3.

Example

```
#configure terminal
(config)#bfd slow-timer 1500
(config)#
```

debug bfd

Use this command to enable debugging for BFD.

Use the `no` form of the command to disable all debugging for BFD.

Command Syntax `debug bfd (all|) debug bfd (event|ipc-error|ipc-event|nsm|packet|session) no debug bfd (all|) no debug all no debug all bfd no debug bfd (event|ipc-error|ipc-event|nsm|packet|session)`

Parameters

`all`	Enable all debugging.
`event`	Enable BFD event debugging.
`ipc-error`	Enable BFD IPC-error debugging
`ipc-event`	Enable BFD IPC-event debugging.
`nsm`	Enable BFD NSM debugging.
`packet`	Enable BFD packet debugging.
`session`	Enable BFD session debugging.

Command Mode

Exec, Privileged Exec and Configure Mode

Applicability

This command was introduced in a version before SWMRE version 1.3.

Examples

```
#debug bfd all
#no debug bfd all
#debug bfd event
#debug bfd ipc-error
#debug bfd ipc-event
#debug bfd nsm
#debug bfd packet
#debug bfd session
```

key

Use this command to manage, add or delete authentication keys in a key chain. This command allows you to enter the keychain-key mode to set a password for the key.

Command Syntax `key <0-2147483647> no key <0-2147483647>`

Parameters

`<0-2147483647>` Specify a key identifier.

Default

By default, BFD uses level-1-2 if there is no Level-2 instance nor a Level-1-2 instance. Otherwise, it uses level-1.

Command Mode

Keychain mode

Applicability

This command was introduced in a version before SWMRE version 1.3.

Examples

The following example configures a key number 1 and shows the change to keychain-key command mode.

```
#configure terminal
(config)#key chain mychain
(config-keychain)#key 1
(config-keychain-key)#
```

key chain

Use this command to enter key chain mode to configure a key chain with a key chain name. This command allows you to enter the keychain mode to specify keys on this key chain.

Command Syntax `key`

`chain WORD no key`

`chain WORD`

Parameters

`WORD`	Specify the name of the key chain to manage.

Command Mode

Configure mode

Applicability

This command was introduced in a version before SWMRE version 1.3.

Examples

The following example shows the creation of a key chain named `mychain` and the change to keychain mode:

```
#configure terminal
(config)#key chain mychain
(config-keychain)#
```

send-lifetime

Use this command to specify the time period during which the authentication key on a key chain can be sent.

Use the `no` parameter with this command to negate this command.

Command Syntax `send-lifetime HH:MM:SS <1-31> MONTH <1993-2035> HH:MM:SS <1-31> MONTH <1993-2035> send-lifetime HH:MM:SS <1-31> MONTH <1993-2035> HH:MM:SS MONTH <1-31> <1993-2035> send-lifetime HH:MM:SS MONTH <1-31> <1993-2035> HH:MM:SS <1-31> MONTH <1993-2035> send-lifetime HH:MM:SS MONTH <1-31> <1993-2035> HH:MM:SS MONTH <1-31> <1993-2035> send-lifetime HH:MM:SS <1-31> MONTH <1993-2035> infinite send-lifetime HH:MM:SS MONTH <1-31> <1993-2035> infinite send-lifetime HH:MM:SS <1-31> MONTH <1993-2035> duration <1-2147483646> send-lifetime HH:MM:SS MONTH <1-31> <1993-2035> duration <1-2147483646> no send-lifetime`

Parameters

`HH:MM:SS`	Specify the start time of accept-lifetime in hours, minutes and seconds.
`<1-31>`	Specify the day of the month to start.
`MONTH`	Specify the month of the year to start as the first three letters of the month, for example, Jan.
`<1993-2035>`	Specify the year to start.
`HH:MM:SS`	Specify the end time of accept-lifetime in hours, minutes and seconds.
`<1-31>`	Specify the day of the month to end.

MONTH	Specify the month of the year to end as the first three letters of the month, for example, Jan.
<1993-2035>	Specify the year to end.
duration	Indicate the duration parameter.
<1-2147483646>	Specify the actual end time duration of a key in seconds.
infinite	Specify the end time to never expire.

Command Mode

Keychain-key mode

Applicability

This command was introduced in a version before SWMRE version 1.3.

Examples

The following example shows the setting of `send-lifetime` for `key 1` on the key chain named `mychain`:

```
#configure terminal
```

```
(config)#key chain mychain
(config-keychain)#key 1
(config-keychain-key)#send-lifetime 03:03:01 Jan 3 2004 04:04:02 Dec 6 2006
```

show bfd

Use this command to display information about the BFD process.

Command Syntax `show bfd`

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in a version before SWMRE version 1.3.

Example

The example below displays the command syntax and sample output from the command.

```
#show bfd
BFD ID: 00      Start Time:Fri May 1 09:55:06 2009
Number of Sessions:     1
Slow Timer: 1000        Image type: MONOLITHIC
Echo Mode: Disabled     Next Session Discriminator:    2 #
```

Table 1-237 explains the output fields.

Table 1-237: Show BFD fields

Entry	Description
BFD ID	ID number of the BFD session.
Start Time	The date and time when the BFD session was started
BFD Admin State	State of the BFD session: Initializing: session is initializing Up: session is up. Down: session is down
Number of Sessions	Number of BFD sessions running on the device.
Slow Timer	Required minimum transmission time for the BFD session.
Image Type	Distributed or Monolithic.

Echo Mode	Either enabled or disabled.
Next Session Discriminator	An opaque discriminator value that identifies each session on the device that is used to demultiplex multiple BFD sessions between the same pair of devices.

show bfd interface

Use this command to display details for an interface running BFD or for all interfaces configured for BFD.

Command Syntax `show bfd interface (ifindex <0-4294967295>|all|)`

Parameters `all` Display all interfaces.

`ifindex` Display an interface index.

`<0-4294967295>`

Display an ID of an interface in this range.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in a version before SWMRE version 1.3.

Example

The example below displays the command syntax and sample output from the command.

```
#show bfd interface all
Interface:         lo ifindex: 1 state:   UP
Interface level configuration: NO ECHO, NO SLOW TMR
Timers in Milliseconds
Min Tx: 20 Min Rx: 20 Multiplier: 5

Interface:       eth0 ifindex: 2 state:   UP
Interface level configuration: NO ECHO, NO SLOW TMR
Timers in Milliseconds
Min Tx: 20 Min Rx: 20 Multiplier: 5

Interface:       eth1 ifindex: 3 state: DOWN
Interface level configuration: NO ECHO, NO SLOW TMR
Timers in Milliseconds
Min Tx: 20 Min Rx: 20 Multiplier: 5

Interface:       sit0 ifindex: 4 state: DOWN
Interface level configuration: NO ECHO, NO SLOW TMR
Timers in Milliseconds
Min Tx: 20 Min Rx: 20 Multiplier: 5
```

```
Interface:       gre0 ifindex: 5 state: DOWN
Interface level configuration: NO ECHO, NO SLOW TMR
Timers in Milliseconds
Min Tx: 20 Min Rx: 20 Multiplier: 5
```

Table 1-238 explains the output fields.

Table 1-238: Show BFD interface fields

Entry	Description
interface	Interface on which BFD is running
ifindex	Interface index number
state	State of the BFD session for the interface: UP: session is up. DOWN: session is down
Interface level configuration	State of interface-level properties: echo on or off slow-timer (timer dampening) on or off
Min Tx	The minimum interval that the local device would like to use when transmitting BFD control packets.
Min Rx	The minimum interval between received BFD control packets that this device is capable of supporting
Multiplier	The negotiated transmit interval, multiplied by this value, provides the detection time for the receiving device in asynchronous mode.

show bfd session

Use this command to display BFD sessions.

Command Syntax `show bfd session (detail|)`

`show bfd session (detail|) (vrf VRFNAME|)`

Parameters

`detail`	Session details.
`VRFNAME`	Sessions for this user-defined Virtual Routing and Forwarding instance name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in a version before SWMRE version 1.3 and updated in SWMRE version 1.3.5.

Example

```
#show bfd session detail
Session Interface Index : 3                Session Index : 1
Lower Layer : IPv4                         Version : 1
Session Type : Single Hop                  Session State : Down
Local Discriminator : 1                    Local Address : 19.19.19.2/32
Remote Discriminator : 0                   Remote Address : 19.19.19.1/32
Local Port : 49152                         Remote Port : 3784 Options :

Diagnostics: None

Timers in Milliseconds :
Min Tx: 20                Min Rx: 20                Multiplier: 5
Neg Tx: 0                 Neg Rx: 0                 Neg detect mult: 0
Min echo Tx: 20           Min echo Rx: 10           Neg echo intrvl: 0
Storage type: 2
Sess down time: 00:00:00
Bfd Authentication Enabled
Authentication type : simple
Auth-Key-Id: 47

Counters values:
Pkt In : 0000000000000000                  Pkt Out : 0000000000000011
Echo Out : 0000000000000000                IPv6 Echo Out : 0000000000000000
IPv6 Pkt In : 0000000000000000             IPv6 Pkt Out : 0000000000000000
UP Count : 0                               UPTIME : 00:00:00

Protocol Client Info:
BFD-> Client ID: 28      Flags: 4
```

Table 1-239 explains the output fields.

Table 1-239: show bfd session detail fields

Entry	Description
Session Interface Index	ID number of the interface.
Session Index	ID number of this BFD session.
Lower Layer	The lower layer protocol on which BFD is carried: IPv4 IPv6 MPLS LSP MPLS VCCV MPLS-TP
Version	Session version number; generally 1.
Session Type	Single Hop Multihop Arbit Path Multihop OOB Signalled Multihop Unidirectional.
Session State	The State of the session: Init: The session is initializing Up: The session is up. Down: The session is down AdminDown: The session has been administratively shutdown indefinitely.
Local Discriminator	A unique discriminator value generated by the transmitting device used to demultiplex multiple BFD sessions between the same pair of devices.
Local Address	Local address of the transmitting device.
Remote Discriminator	The discriminator received from the corresponding remote device; zero if that value is unknown.
Remote Address	Remote address of the receiving device.
Local Port	UDP port number of the transmitting device.
Remote Port	UDP port number of destination.

Options	Fate Shared Echo Enabled Demand Enabled Remote Demand Enbl Remote admin Down Poll seq Init.

Table 1-239: show bfd session detail fields (Continued)

Entry	Description
Diagnostics	Performance diagnostics: None Control Detection Time Expired Echo Failed Neighbor Session Down Forwarding Plane Reset Path Down Concatenated Path Down Admin Down Reverse Concatenated Path Down
Min Tx	Minimum transmit interval.
Min Rx	Minimum receive interval.
Multiplier	The negotiated transmit interval, multiplied by this value, provides the detection time for the receiving system in asynchronous mode.
Neg Tx	Negotiated transmit interval.
Neg Rx	Negotiated receive interval in milliseconds.
Neg detect mult	Negotiated detection multiplier.
Min echo Tx	Minimum echo transmit interval in milliseconds.
Min echo Rx	Minimum echo receive interval in milliseconds.
Neg echo intrvl	Negotiated echo interval.

Storage type	SNMPv2 storage type (usually be set to 2): other(1) volatile(2) non-Volatile(3) permanent(4 read-Only(5)
Sess down time	Length of time this BFD session has been down.
Bfd GTSM	Whether the BFD session has enabled or disabled the Generalized TTL Security Mechanism (GTSM), which uses the time to live (TTL) or hop count to prevent off-link attackers from spoofing packets.
Bfd Authentication Enabled	When authentication is enabled.
Authentication type	Type of authentication: simple: Simple Password keyed- md5: Keyed message digest keyed- sha1: Keyed Secure hashing algorithm meticulous-keyed-md5: Meticulous Keyed message digest meticulous-keyed-sha1: Meticulous Keyed Secure hashing algorithm
Authentication Key-id	ID number of the authentication key.

Table 1-239: show bfd session detail fields (Continued)

Entry	Description
Pkt In	Number of packets that have been received during this BFD session.
Pkt Out	Number of packets that have been transmitted during this BFD session.
Echo Out	Number of Echo-packets that have been transmitted during this BFD session.
IPv6 Pkt In	Number of IPv6 packets that have been received during this BFD session.
IPv6 Pkt Out	Number of IPv6 packets that have been transmitted during this BFD session.
UP Count	Number of times the BFD session has been up.
UPTIME	Length of time this BFD session has been up.

BGP-> Client ID	Protocol and module ID number of this BFD session’s neighboring device.
Flags	Session state of the neighboring device.

show bfd session A.B.C.D

Use this command to display information about an IPv4 BFD session neighbor.

Command Syntax `show bfd session A.B.C.D A.B.C.D (detail|) show bfd session A.B.C.D A.B.C.D <0-4294967295> (detail|)`

Parameters

`A.B.C.D` Display the local IPv4 address.

`A.B.C.D` Display the neighbor IPv4 address.

`<0-4294967295>` Display the interface index of the address.

`detail` Display detailed information.

Command Mode

Exec mode and Privileged Exec mode

Entry	Description
Session Interface Index	ID number of the Interface.

Session Index	ID number for this BFD session.
Lower Layer	The lower layer protocol on which BFD is carried (IPv4 or IPv6).

Applicability

This command was introduced in a version before SWMRE version 1.3.

Example

The example below displays the command syntax and sample output from the command.

```
#show bfd session 10.1.1.66 10.1.1.67 3
Session Interface Index: 3     Session Index: 1
Lower Layer: IPv4     Single Hop
Session State: Up
Local Discriminator: 1 Remote Discriminator: 163
Local Address: 10.1.1.66/32    Remote Address: 10.1.1.67/32
Local Port: 49152      Remote Port: 3784
Timers in Milliseconds
Min Tx: 1000 Min Rx: 1000 Multiplier: 4 UP
Count: 1 UPTIME: 00:10:08
```

Table 1-240 explains the output fields.

Table 1-240: show BFD session fields

Table 1-240: show BFD session fields

Entry	Description
Session State	The state of the session: Init: session is initializing Up: session is up. Down: session is down AdminDown: session has been administratively shutdown indefinitely
Local Discriminator	A unique value generated by the transmitting device used to demultiplex multiple BFD sessions between the same pair of devices.
Remote Discriminator	The discriminator received from the corresponding remote device. This field is zero if the value is unknown.
Local Address	Local address of the transmitting device.

Remote Address	Remote address of the receiving device.
Local Port	UDP port number of the transmitting device.
Remote Port	UDP port number of the receiving device.
Min Tx	Minimum transmit interval in milliseconds.
Min Rx	Minimum receive interval in milliseconds.
Multiplier	The negotiated transmit interval, multiplied by this value, provides the detection time for the receiving system in asynchronous mode.
UP Count	The number of times the BFD session has been in up state.
UPTIME	The length of time this BFD session has been in the up state.

show bfd session ipv6

Use this command to display information about an IPv6 BFD session neighbor.

Command Syntax `show bfd session ipv6 X:X::X:X X:X::X:X (detail|) show bfd session ipv6 X:X::X:X X:X::X:X <0-4294967295> (detail|)`

Parameters

`X:X::X:X` Display the local IPv6 address.

`X:X::X:X` Display the neighbor IPv6 address.

`<0-4294967295>` Display the interface index of the address.

`detail` Display detailed information.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in a version before SWMRE version 1.3.

Example

The example below displays the command syntax and sample output from the command.

```
#show bfd session 2001::1222 2001::1223 3
```

```
Session Interface Index : 3     Session Index: 1
Lower Layer: IPv6     Single Hop
Session State : Up
Local Discriminator : 1 Remote Discriminator: 163
Local Address : 2001::1222/128    Remote Address: 2001::1223/128
Local Port : 49152      Remote Port: 3784
Timers in Milliseconds
Min Tx: 1000 Min Rx: 1000 Multiplier: 4
UP Count: 1 UPTIME: 00:06:03
```

Table 1-241 explains the output fields.

Table 1-241: show BFD session fields

Entry	Description
Session Interface Index	ID number of the Interface.
Session Index	ID number for this BFD session.
Lower Layer	The lower layer protocol on which BFD is carried (IPv4 or IPv6).

Table 1-241: show BFD session fields

Entry	Description
Session State	The state of the session: Init: session is initializing Up: session is up. Down: session is down AdminDown: session has been administratively shutdown indefinitely
Local Discriminator	A unique value generated by the transmitting device used to demultiplex multiple BFD sessions between the same pair of devices.
Remote Discriminator	The discriminator received from the corresponding remote device. This field is zero if the value is unknown.
Local Address	Local address of the transmitting device.
Remote Address	Remote address of the receiving device.

Local Port	UDP port number of the transmitting device.
Remote Port	UDP port number of the receiving device.
Min Tx	Minimum transmit interval in milliseconds.
Min Rx	Minimum receive interval in milliseconds.
Multiplier	The negotiated transmit interval, multiplied by this value, provides the detection time for the receiving system in asynchronous mode.
UP Count	The number of times the BFD session has been in up state.
UPTIME	The length of time this BFD session has been in the up state.

show debugging bfd

Use this command to display debugging information for BFD processes.

Command Syntax `show debugging bfd`

Parameters

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced in a version before SWMRE version 1.3.

Example

The example below displays the command syntax and sample output from the command.

```
#show debugging bfd
BFD debugging status:
BFD events debugging is on
BFD packet debugging is on
BFD ipc-error debugging is on
BFD ipc-event debugging is on
BFD session debugging is on
```

```
BFD nsm debugging is on
#
```

snmp restart bfd

Use this command to restart SNMP in Bidirectional Forwarding (BFD)

Command Syntax `snmp restart bfd`

Parameters

None

Command Mode

Configure mode

Applicability

This command was introduced in a version before SWMRE version 1.3.

Examples

```
#snmp restart bfd
```


© Symanitron Proprietary

CHAPTER 2 Protocol Commands for BFD

The chapter describes the commands used to manage BFD functionality for OSPF, IS-IS and BGP.

- area virtual-link
- bfd all-interfaces
- debug bgp bfd
- debug isis bfd
- debug ospf bfd
- debug rip bfd
- ip ospf bfd
- isis bfd
- neighbor fall-over bfd (RIP)

area virtual-link

Use this command to enable the BFD option for a specified virtual-link neighbor.

Use the `no` form of the command to disable BFD on a virtual-link neighbor.

Command Syntax `area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D {fall-over bfd} no area (A.B.C.D|<0-4294967295>) virtual-link A.B.C.D {fall-over bfd}`

Parameters

`A.B.C.D` Indicate an area IP address

`<0-429467295>` Indicate an area ID in integer format `virtual-link` Indicate a virtual link and its parameters `A.B.C.D` Indicate the IP address of the virtual link `fall-over` Indicate fall-over detection

`bfd` Specify the Bidirectional Forwarding Detection (BFD)

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router ospf
 (config-router)#area 1 virtual-link 192.168.0.1 fall-over bfd
```

bfd all-interfaces

Use this command to enable BFD for all neighbors maintained by an OSPF or RIP process, or an ISIS instance.

Use the `no` form of the command to disable BFD.

Note: This command does not apply BFD to virtual-link neighbors.

Command Syntax `bfd all-interfaces no bfd all-interfaces`

Parameters

None

Default

By default, bfd all interface is disabled

Command Mode

Configure router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#router ospf
(config-router)#bfd all-interfaces

#configure terminal
(config)#router isis
(config-router)#bfd all-interfaces

#configure terminal
(config)#router rip
```

```
(config-router)#bfd all-interfaces
```

debug bgp bfd

Use this command to debug BFD processes in BGP. Use the `no` form of the command to stop debugging.

Command Syntax `debug bgp bfd no debug bgp bfd undebug bgp bfd`

Parameters

None

Command Mode

Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#debug bgp bfd
```

debug isis bfd

Use this command to debug BFD processes in IS-IS.

Use the `no` form of the command to stop debugging.

Command Syntax `debug isis bfd no debug isis bfd undebug isis bfd`

Parameters

None

Command Mode

Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#debug isis bfd
```

debug ospf bfd

Use this command to debug BFD processes in OSPF.

Use the `no` form of the command to stop debugging.

Command Syntax `debug ospf bfd no debug ospf bfd undebug ospf bfd`

Parameters

None

Command Mode

Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#debug ospf bfd
```

debug rip bfd

Use this command to debug BFD processes in RIP.

Use the `no` form of the command to stop debugging.

Command Syntax `debug rip bfd no debug rip bfd`

Parameters

None

Command Mode

Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#debug rip bfd
```

ip ospf bfd

Use this command to enable the BFD option for OSPF neighbors on an interface. Use the `no` form of the command to disable the BFD option for OSPF neighbors on an interface.

Command Syntax `ip ospf bfd`

`(disable|) no ip ospf`

`bfd (disable|)`

Parameter `disable` Disable the BFD option for neighbors on an interface

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip ospf bfd
```

isis bfd

Use this command to enable the BFD option for IS-IS neighbors on an interface. Use the `no` form of the command to disable the BFD option for neighbors on an interface.

Command Syntax `isis bfd`

`(disable|) no isis bfd`

`(disable|)`

Parameter `disable` Used to disable the BFD option for neighbors on an interface

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#isis bfd disable
```

neighbor fall-over bfd (RIP)

Use this command to enable the BFD option on an IPv4 RIP peer.

Use the `no` form of the command to disable the BFD option on an IPv4 RIP peer.

Command Syntax `neighbor A.B.C.D fall-over bfd no neighbor A.B.C.D fall-over bfd`

Parameters

`A.B.C.D` Peer address in an IPv4 format

Default

No default value is specified

Command Mode

Router mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
(config)#router rip
            (config-router)#neighbor 10.10.2.9 fall-over bfd
```

CHAPTER 3 BFD Static Route Commands

Bidirectional Forwarding Detection (BFD) support for static routes can be configured on a static route basis, interface basis, or on a global level:

- When BFD is configured for an IPv4 or IPv6 static route, BFD provides the next-hop reachability detection for the given static route.
- When BFD is configured for an interface, BFD provides the data plane next-hop reachability information for any IPv4 or IPv6 static route configured through the given interface.
- When BFD is configured globally, BFD is applied on all interfaces with a single command. In all these cases, the BFD session update for NSM governs the state of the static routes.

This chapter includes the following commands:

- ip bfd static all-interfaces
- ip static fall-over bfd
- ip static bfd
- ipv6 bfd static all-interfaces
- ipv6 static fall-over bfd
- ipv6 static bfd

ip bfd static all-interfaces

Use this command to enable BFD support for IPv4 static routes configured on all interfaces.

Use the `no` option with this command to disable BFD support for IPv4 static routes configured on all interfaces.

Command Syntax `ip bfd static all-interfaces`

`ip bfd vrf NAME static all-interfaces no`

`ip bfd static all-interfaces no ip bfd vrf NAME static all-interfaces`

Parameters

`NAME` Enable/disable IPv4 static BFD on all interfaces bound to this user-defined Virtual Routing and Forwarding instance name.

Command Mode

Configure mode

Applicability

This command was introduced in a version before SWMRE version 1.3 and updated in SWMRE version 1.3.5.

Example

```
#configure terminal
(config)#ip bfd static all-interfaces

#configure terminal
(config)#ip  bfd  vrf vrf1 static all-interfaces
```

ip static fall-over bfd

Use this command to enable BFD support for a specific IPv4 static route.

Use the `no` form of the command to disable the BFD support for a specific IPv4 static route.

Command Syntax `ip static A.B.C.D/M A.B.C.D fall-over bfd (disable|) ip static vrf NAME A.B.C.D/M A.B.C.D fall-over bfd (disable|) no ip static A.B.C.D/M A.B.C.D fall-over bfd (disable|) ip static vrf NAME A.B.C.D/M A.B.C.D fall-over bfd (disable|)`

Parameters

`A.B.C.D/M`	The IPv4 destination prefix and mask length.
`A.B.C.D`	The IPv4 gateway address.
`disable`	Disable BFD.
`NAME`	Enable/disable BFD for the IPv4 routes for this user-defined Virtual Routing and Forwarding instance name.

Command Mode

Configure mode

Applicability

This command was introduced in a version before SWMRE version 1.3 and updated in SWMRE version 1.3.5.

Example

```
#configure terminal
(config)#ip static 4.4.4.4/32 20.0.10.82 fall-over bfd

#configure terminal
(config)# ip static vrf vrf1 4.4.4.4/32 20.0.10.82 fall-over bfd
```

ip static bfd

Use this command to enable or disable BFD support for IPv4 static route(s) configured on an interface.

Use the `no` option with this command to reset BFD support for IPv4 static route(s) configured on an interface.

Command Syntax `ip static bfd`

`(disable|) no ip static bfd`

`(disable|)`

Parameters

None

Command Mode

Interface mode

Default

By default, BFD static route support is disabled at all levels.

Applicability

This command was introduced in a version before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ip static bfd disable

(config)#interface eth1
(config-if)#ip static bfd
```

ipv6 bfd static all-interfaces

Use this command to enable BFD support for IPv6 static routes on all interfaces.

Use the `no` option with this command to disable BFD support for IPv6 static routes on all interfaces.

Command Syntax `ipv6 bfd static all-interfaces`

`ipv6 bfd vrf NAME static all-interfaces no`

`ipv6 bfd static all-interfaces no ipv6 bfd vrf NAME static all-interfaces`

Parameters

NAME	Enable/disable IPv6 static BFD on all interfaces bound to this user-defined Virtual Routing and Forwarding instance name.

Command Mode

Configure mode

Applicability

This command was introduced in a version before SWMRE version 1.3 and updated in SWMRE version 1.3.5.

Example

```
#configure terminal
(config)#ipv6 bfd static all-interfaces

#configure terminal
(config)#ipv6 bfd vrf vrf1 static all-interfaces
```

ipv6 static fall-over bfd

Use this command to enable BFD support for a specific IPv6 static route.

Use the no option with this command to disable BFD support for a specific IPv6 static route.

Command Syntax ipv6 static X:X::X:X/M X:X::X:X fall-over bfd (disable|) ipv6 static vrf NAME X:X::X:X/M X:X::X:X fall-over bfd (disable|) no ipv6 static X:X::X:X/M X:X::X:X fall-over bfd (disable|) no ipv6 static vrf NAME X:X::X:X/M X:X::X:X fall-over bfd (disable|)

Parameters

X:X::X:X/M	The IPv6 destination prefix and mask length.
X:X::X:X	The IPv6 gateway address.
NAME	Enable/disable BFD for the IPv6 routes for this user-defined Virtual Routing and Forwarding instance name.
disable	Disable BFD.

Command Mode

Configure mode

Applicability

This command was introduced in a version before SWMRE version 1.3 and updated in SWMRE version 1.3.5.

Examples

```
#configure terminal
(config)#ipv6 static 2345:6::0:1/28 2345:6::0:2 fall-over bfd

#configure terminal
(config)#ipv6 static 2345:12::1/64 2345:12::2 fall-over bfd disable

#configure terminal
(config)#ipv6 static vrf vrf1 2345:6::0:1/28 2345:6::0:2 fall-over bfd
```

ipv6 static bfd

Use this command to disable BFD support for IPv6 static route(s) configured on an interface.

Use the `no` option with this command to reset BFD support for IPv6 static route(s) configured on an interface.

Command Syntax `ipv6 static bfd`

`(disable|) no ipv6 static bfd`

`(disable|)`

Parameters

None

Command Mode

Interface mode

Applicability

This command was introduced in a version before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface eth1
(config-if)#ipv6 static bfd disable
```

© Symanitron Proprietary

SECTION 11 Policy Based Routing

Policy Based Routing Configuration Guide

Contents

This document contains this chapter:

- Chapter 1, *Policy Based Routing Configuration*

CHAPTER 1 Policy Based Routing Configuration

This chapter contains a sample Policy Based Routing (PBR) configuration.

Overview

Policy Based Routing (PBR) allows the forwarding and routing of data packets based on policies defined by network administrators. By design, it is a way to have a policy override a routing protocol decision based on the destination IP address. PBR includes a mechanism for selectively applying policies based on an access list or other criteria. Actions taken might include routing a packet on a user-defined route or routing the packet using the default route.

PBR applies on ingress interfaces. Define a routing policy by creating a route map. A route map is a combination of match and set clauses/commands. The match clauses define the criteria conditions to meet. The set commands define how the packets should route once they have met the match criteria. Match clauses utilizes access control lists (ACLs) to define a matching criteria.

For each combination of match and set commands in a route map statement, all sequential match clauses must meet simultaneously by the packet for the set clauses to be applied. There may be multiple sets of combinations of match and set commands in a route map statement.

You can also mark a route map statement as permit or deny. If the statement is marked as deny, the packets meeting the match criteria are sent back through the normal forwarding path (that is, via destination-based routing). If the statement is marked as permit and the packets meet the match criteria, then all set clauses are applied. If the statement is marked as permit and the packets do not meet the match criteria, then those packets are forwarded through the normal routing channel.

The routing policy applies only on incoming interfaces. A routing policy can contain multiple rules defined with different sequence numbers for a same route-map-name. The system evaluates the rules in the order of their sequence number until the first match occurs. If no match occurs, then those packets are forwarded through the normal routing channel.

Router

`#configure terminal`	Enter the `Configure` mode.
`(config)#access-list SWMRE TEST deny ip 1.1.1.1/24 any`	Create an access list TEST, to deny all ip packets coming from source address 1.1.1.1.
`(config)#route-map FILTER deny 1`	Create a route-map FILTER.
`(config-route-map)#match ip address TEST`	Set the matching IP address to access list TEST.
`(config-route-map)#set ip next-hop 2.2.2.2`	Set the primary next hop as 2.2.2.2
`(config-route-map)#set ip next-hop 2.2.2.3`	Set the secondary next hop as 2.2.2.3
(c`onfig-route-map`**)**`#exit`	Exit the router map mode
`(config)#interface eth1`	Enter the interface configuration mode for eth1.
(config-if)`#ip policy route-map FILTER`	Configure ip policy FILTER on the interface eth1.

(config-if)#exit	Exit the interface mode.

Validation

```
#>show ip policy
        Interface         Route map         eth1                FILTER
```

SECTION 12 Virtual Routing

Virtual Routing Command Reference

Contents

This document contains these chapters:

- Chapter 1, *Virtual Routing Commands*
- Chapter 2, *Logical Switch Router Commands*

CHAPTER 1 Virtual Routing Commands

This chapter includes an alphabetical listing of all available virtual router commands. It includes the following commands:

- configuration file
- description
- ip vrf
- load
- load IPv6
- login virtual-router
- show ip route virtual-router
- show nsm virtual-router
- show running-config virtual-router
- show VR and VRF
- show virtual-router ip
- username
- virtual-router

- virtual-router forwarding

configuration file

This command loads the default configuration file for the VR/VRF Use the `no` parameter to resume the use of the default.

Command Syntax `configuration file WORD no configuration file`

Parameters

`WORD`	Specify the full path and file name of the configuration file.
`default`	Specify the configuration filename as default.

Default

No default value is specified

Command Mode

VR mode

Examples

```
#configure terminal
(config)#virtual-router VR1
(config-vr)#configuration file default

(config)#virtual-router VR1
(config-vr)#no configuration file
(config)#ip vrf vrf1
(config)#no ip vrf vrf1
```

description

Use this command to add a description tag to a virtual router instance.

Use the `no` parameter to remove a description.

Command Syntax `description LINE no description`

Parameters

`LINE`	Specify a description for the virtual router.

Default

No default value is specified

Command Mode

VR mode

Examples

```
#configure terminal
(config)#virtual-router VR1
(config-vr)#description VR1 has been created for CLI testing

(config)#virtual-router VR1
(config-vr)#no description
#configure terminal
(config)#ip vrf vrf1
(config-vr)#description vrf1 has been created for CLI testing
```

ip vrf

Use this command to

- Create new VRF
- Enter the Configure mode to configure VRF parameters. Use

the no parameter with this command to disable the specified vrf.

Command Syntax `ip vrf WORD no vrf WORD`

Parameters

`WORD`	Specify the name of the virtual router.

Default

No default value is specified

Command Mode

Configure mode

Example

In this configuration, interface `eth1` is bound to the Virtual Router `VR1`.

```
#configure router
```

```
(config)#ip vrf vrf1
(config-vrf)#
```

load

Use this command to load IPv4 protocol modules to a virtual router.

Use the `no` parameter with this command to remove the specified protocol module from the VR.

Command Syntax `load (ospf|bgp|rip|trill|isis|ptp|pim) no load (ospf|bgp|rip|trill|isis|ptp|pim)`

Parameters

`bgp`	Loads the BGP module to this VR.
`isis`	Loads the ISIS module to this VR.
`ospf`	Loads the OSPF module to this VR.
`pim`	Loads the PIM module to this VR.
`rip`	Loads the RIP module to this VR.
`trill`	Loads the TRILL module to this VR.
`ptp`	Loads the PTP module to this VR.

Default

No default value is specified

Command Mode

VR mode

Examples

```
#configure terminal
(config)#virtual-router VR1
(config-vr)#load bgp

#configure terminal
(config)#virtual-router VR1
(config-vr)#no load bgp
```

load IPv6

Use this command to load IPv6 protocol modules to a virtual router.

Use the `no` parameter with this command to remove the specified protocol module from the VR.

Command Syntax `load ipv6 (ospf|rip)`

Parameters

`ospf`	Loads the OSPFv3 module to this VR for the IPv6 protocol module.
`rip`	Loads the RIPng module to this VR for the IPv6 protocol module.

Default

No default value is specified

Command Mode

VR mode

Examples

```
(config)#virtual-router VR1
(config-vr)#load ipv6 ospf
```

login virtual-router

This command is used to jump from global configuration mode to a particular VR configuration mode.

Note: This command can be used only by the administrator. The administrator can login from GMA to VR for administration purposes.

Command Syntax `login virtual-router WORD`

Parameters

`WORD`	Specify the name of the virtual router.

Default

No default value is specified

Command Mode

Privileged Exec mode

Example

```
1#login virtual-router VR1

 version 7.7.2.t78 candidiasis 06/23/10 18:49:52
1>>en
#con t
(config)#ip vrf vrf1
(config)#router ospf 1 vrf1
(config)#no router ospf 1
(config-router)#router rip (config-
router)#address-family ipv4 vrf vrf1
(config)#no router rip
```

show ip route virtual-router

Use this command to display the IP routing table for a virtual router.

Command Syntax `show ip route virtual-router WORD (database|) show ip route virtual-router WORD (database|) (bgp|connected|isis|kernel|ospf|rip|static)`

Parameters

`bgp`	Display Border Gateway Protocol (BGP) information.
`connected`	Display connected information.
`database`	Display IPv6 routing table database information.
`isis`	Display ISO IS-IS information.
`kernel`	Display kernel information.
`ospf`	Display Open Shortest Path First (OSPF) information.
`rip`	Display Routing Information Protocol (RIP) information.
`static`	Display static routes.

Command Mode

Exec mode and Privileged Exec mode

Examples

```
#show ip route virtual-router new-vr
```

show nsm virtual-router

Use this command to display NSM information for a virtual router.

Command Syntax `show nsm virtual-router (brief|detail|)`

Parameters `brief` Display brief NSM information. `detail` Display connected NSM information.

Command Mode

Privileged Exec mode

Examples

```
#show nsm virtual-router brief

#
```

show running-config virtual-router

Use this command to display the contents of the running configuration on a virtual router.

Command Syntax `show running-config virtual-router <1-512> show running-config virtual-router WORD`

Parameters

`WORD`	Display the name of the virtual router.
`<1-512>`	Display the current configuration mode.

Command Mode

Exec mode and Privileged Exec mode

Example

The following is a sample output of this command displaying running configuration for the specified Virtual Router `v1`.

```
#show running-config virtual-router v1
 !
 no service password-encryption
 !  interface
eth1
  ip address 10.10.10.121/24
  ipv6 address fe80::202:b3ff:fed5:9553/64
!
end
localhost.localdomain#show running-config
!
no service password-encryption
!
mpls propagate-ttl
!
no feature dhcp
! line con 0
login line
```

```
vty 0 39
login
!
end
```

show VR and VRF

Use this command to display a list of all virtual routers and their descriptions.

Command Syntax `show virtual-router show virtual-router WORD show virtual-router <1-512>`

Parameters

`WORD`	Display the name of the virtual router.
`<1-512>`	Display the current configuration mode.

Command Mode

Exec mode and Privileged Exec mode

Example

The following is a sample output of this command displaying two Virtual Routers and their descriptions:

```
#show virtual-router
Virtual Router vr1
  VR-ID: 1
  Router-ID: (unset)
  Interfaces: eth1

Virtual Router vr2
  VR-ID: 2
  Router-ID: (unset)
  Interfaces: eth2
localhost.localdomain#show ip vrf vrf0
VRF vrf0, FIB ID 3
Router ID: 3.3.3.1 (automatic)
Interfaces:
  eth1   eth2
localhost.localdomain#show ip vrf vrf1
```

```
VRF vrf1, FIB ID 4
Router ID is not set
Interfaces:
```

show virtual-router ip

Use this command to display a list of all virtual routers and their descriptions.

Command Syntax `show virtual-router WORD ip route (database|)`

`show virtual-router WORD ip route (database|)`

`(bgp|connected|isis|kernel|ospf|rip|static)`

Parameters

`WORD`	Display the name of the virtual router.
`database`	Display IP routing table database information.
`bgp`	Display Border Gateway Protocol (BGP) information.
`connected`	Display connected information.
`isis`	Display ISO IS-IS information.
`kernel`	Display kernel information.
`ospf`	Display Open Shortest Path First (OSPF) information.
`rip`	Display Routing Information Protocol (RIP) information.
`static`	Display static routes.

Command Mode

Exec mode and Privileged Exec mode

Example

The following is a sample output of this command displaying two Virtual Routers and their descriptions:

```
#show virtual-router
Virtual Router vr1
  VR-ID: 1
  Router-ID: (unset)
  Interfaces: eth1

Virtual Router vr2
  VR-ID: 2
  Router-ID: (unset)
```

```
   Interfaces: eth2
#
```

show vlog virtual-routers

Use this command to display virtual log information for a virtual router.

Command Syntax `show vlog virtual-routers`

Parameters

None

Command Mode

Privileged Exec mode

Examples

```
#show vlog virtual-routers

#
```

username

This command is used by the global administrator to add a login username to a virtual router. Use the `no` parameter to remove the username.

Command Syntax

```
username
WORD       no
username
```

Parameters

`WORD`	Specify the user name.

Default

No default value is specified

Command Mode

VR mode

Example

```
#configure terminal
(config)#virtual-router VR1
(config-vr)#username QA 3 QA123
```

virtual-router

The Global administrator executes this command to create a new virtual router and to configure VR parameters.

Commands that appear in VR mode set startup parameters for the virtual router prior. Only some of these commands can be executed once the VR has been loaded.

Use the `no` parameter with this command to disable the specified virtual router.

Command Syntax `virtual-router WORD no virtual-router WORD`

Parameters

`WORD`	Specify the name of the VR.

Default

No default value is specified

Command Mode

Configure mode

Example

```
#router
(config)#virtual-router VR1
(config-vr)#
```

virtual-router forwarding

Use this command to bind an interface name to the virtual router name. This command informs all SWMRE clients about it.

Use the `no` parameter to remove the association.

Command Syntax `virtual-router forwarding WORD no virtual-router forwarding WORD`

Parameters

`WORD`	Specify the name of the virtual router.

Default

No default value is specified

Command Mode

Interface mode

Example

In this configuration, interface `eth1` is bound to the Virtual Router `VR1`.

```
#configure terminal
(config)#interface eth1
(config-if)#virtual-router forwarding VR1

(config)#interface eth1 (config-if)#no
virtual-router forwarding VR1
```

CHAPTER 2 Logical Switch Router Commands

This chapter includes an alphabetical listing of all available Logical Switch Router commands. It includes the following commands:

- allocate interface
- lsr name
- feature daemon
- lsr-move
- mac-address
- leave lsr
- switch lsr
- show lsr
- show lsr process-list
- show lsr membership

allocate interface

Use this command to bind the interface to LSR instance.

Use the `no` parameter to unbind the interface to LSR instance.

Note:This command can be used in default LSR only.

Command Syntax `allocate interface IFNAME no allocate interface IFNAME`

Parameters

`IFNAME`	Specify the interface name.

Default

No default value is specified

Command Mode

LSR-config mode

Examples

```
#configure terminal
(config)#virtual-router VR1
                (config-test-lsr)#allocate interface eth1

                                    (config-test-lsr)#no allocate interface eth1
```

lsr name

Used this command to create or specify a LSR and enter LSR configuration mode.

Use the `no` parameter to delete a LSR.

Command Syntax `lsr NAME no lsr NAME`

Parameters

NAMESpecify the name of a LSR.

Default

No default value is specified

Command Mode

Configuration mode

Examples

```
#configure terminal
(config)#lsr test-lsr
Test-lsr-SWMRE#

#configure terminal
(config)#no lsr test-lsr
```

feature daemon

Use this command to load a feature in the LSR specified.

Use the no parameter to unload features in the LSR specified.

Note:This command can be used in default LSR only.

Command Syntax feature daemon-name no feature daemon-name

Parameters daemon Specify the daemon name.

Default

No default value is specified

Examples

```
#(config)#lsr first
#(config-lsr)#feature ospfd

#(config-lsr)#no feature ospfd
```

```
#(config-lsr)#
```

lsr-move

Used this command to specifies whether an interface can be moved from the default LSR to a non-default LSR.

Every interface by default can be moved.

Command Syntax `lsr-move (enable|disable)`

Default

No default value is specified

Command Mode

Interface mode

Examples

```
(config)#interface p2p3
(config-if)#lsr-move enable
```

mac-address

Used this command to set the MAC address for an LSR.

Use the `no` parameter to remove the mac address for an LSR.

Command Syntax `mac-address MAC no mac-address MAC`

Parameters

`MAC`	Specify the MAC address.

Default

No default value is specified

Command Mode

LSR mode

Examples

```
(config)#lsr first
                    (config-lsr)#mac-address 1234.1234.1234

(config)#lsr first
                                          (config-lsr)#no mac-address 1234.1234.1234
```

leave lsr

Use this command to switch back to the default LSR.

Command Syntax `leave lsr`

Default

No default value is specified

Command Mode

Configure mode

Example

```
#leave lsr
```

switch lsr

Use this command to switch to another LSR from the default LSR.

Note:This command can be used in the default LSR only.

Command Syntax `switch-lsr LSR-NAME`

Parameters

`LSR-NAME`	Name of the LSR

Default

No default value is specified

Command Mode

Privileged exec mode

Example

```
#switch-lsr test-lsr
Test-lsr-SWMRE#
```

show lsr

Use this command to display LSR information.

Note: In the default LSR, this command displays a list of all LSRs and their descriptions. In non-default LSRs, this command displays the LSR description for the current LSR only.

Command Syntax `show lsr (LSR_NAME ) (detail)`

Parameters

`LSR-NAME`	Name of the LSR
`detail`	Details

Command Mode

Privileged Exec mode

Examples

```
# show lsr lsr_id
lsr_name state ------
-------- -----
1   switch active
2   Payroll active
3   MyLSR active

switch# show lsr detail
lsr id: 1 lsr name:
switch lsr state: active
lsr start time: Thu May 14 08:14:39 2009 lsr
restart count: 0

lsr id: 2 lsr
name: payroll lsr
state: active
lsr start time: Thu May 14 08:15:22 2009 lsr
restart count: 0
```

show lsr process-list

Use this command to display the process names and identifiers that are running.

Note:This command can be used in the default LSR only.

Command Syntax `show lsr process-list (lsr-name LNAME|)`

Parameters

`LSR-NAME` Name of the LSR

Command Mode

Privileged Exec mode

Examples `show lsr process-list LSR Process Details:`

```
LSR ID: 2,  LSR Name: first

  PROCESS NAME                     PID
  -------------------------------- --Process_name
Process_name_pid  nsm                              1914   ribd
1917   imi                            1920   hostpd
1934 LSR ID: 3,  LSR Name: test

  PROCESS NAME                     PID   --------------------------
------ --  nsm                           2340   ribd
2343   imi                            2351
```

show lsr membership

Use this command to display the interface membership information for the LSR.

Note: In the default LSR, this command displays a list of all LSRs and their descriptions. In non-default LSRs, this command displays the LSR description for the current LSR only.

Command Syntax `show lsr membership`

Example

```
(config)# show lsr membership

lsr_id: 1  lsr_name: switch  interfaces:
eth0  eth1  eth3  eth4 eth6
eth8

lsr_id: 2  lsr_name: Payroll  interfaces:
eth2  eth5

lsr_id: 3 lsr_name: MyLSR interfaces: eth7
eth9



switch# show LSR membership status LSR_id:
1 LSR_name: switch interfaces:
Port   Status ----
---------eth1   OK
eth2   OK eth3
OK eth4   OK
```

SECTION 23 sFlow

© Symanitron Proprietary

Sampling Flow Configuration Guide

Contents

This document contains this chapter:

- Chapter 1, *sFlow Configuration*

CHAPTER 1 sFlow Configuration

This chapter provides the steps for configuring Sampled Flow (sFlow).

sFlow is the standard for monitoring high-speed switched and routed networks. The sFlow monitoring system consists of an sFlow Agent which is embedded in a switch or router and an sFlow Collector.

The sFlow agent samples packets as well as polling traffic statistics for the device it is monitoring. The packet sampling is performed by the switching/routing device at wire speed. The sFlow agent forwards the sampled traffic statistics in sFlow PDUs as well as sampled packets to an sFlow collector for analysis.

The sFlow agent uses the following forms of sampling:

- Sampling packets: samples one packet out of a defined sampling rate. This sampling is done by hardware at wire speed.
- Sampling counters: polls interface statistics such as generic and Ethernet counters at a defined interval.

You must enable the sFlow feature and collector before enabling sFlow sampling on an interface.

You cannot globally enable sFlow sampling monitoring on all interfaces with a single command. Instead you must enable sFlow sampling on the required interfaces individually.

sFlow feature is supported on physical interface as well as LAG interface. Configuring sampling on a LAG interface will enable the same on all member ports part of that LAG interface.

Topology

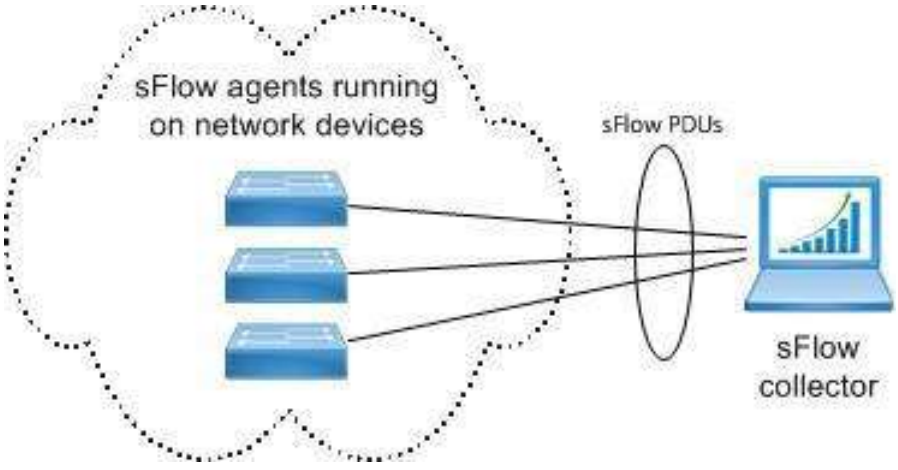


Figure 1-213: Basic sFlow topology

Configuration

sFlow Agent

`#configure terminal`	Enter configure mode.

(config)#feature sflow	Enable the sFlow feature.
(config)#sflow collector 2.2.2.2 port 6343 receiver-time-out 0 max-datagram-size 200	Configure the sFlow collector
(config)#interface xe1	Enter interface mode

© Symanitron

sFlow Configuration

(config-if)#sflow interface xe1 pollinterval 5	Set the counter poll Interval on the interface.
(config-if)#sflow interface xe1 samplingrate 1024 direction ingress max-header-size 200	Set the sFlow sampling interval on the interface in ingress directions.
(config-if)#sflow interface xe1 samplingrate 1024 direction egress max-header-size 200	Set the sFlow sampling interval on the interface in egress directions.
(config-if)#sflow enable	Start packet sampling on the interface
(config-if)#end	Exit interface and configure mode.

Validation

```
#show sflow detail sFlow
Feature: Enabled sFlow
Version: 5 sFlow Global
Information : Agent
IP: 10.10.26.101
Collector IP: 2.2.2.2          Port:  6343
Maximum Datagram Size(bytes): 0
Receiver timout(sec)        : 188
 sFlow       Port       Detailed
Information:
Interface   Packet-Sampling              Packet-Sampling                 Counter-Polling
Maximum Header
                 Rate                        Count                  Interval        Count
Size(bytes)
           Ingress      Egress       Ingress      Egress       (sec)
Ingress     Egress
---------   ----------------------    ----------------------  ----------------------
--------------------
xe1             1024          1024        172505        146891             5           432
256          256
```

Sampling Flow Command Reference

Sampling Flow Command Reference

Contents

This document contains this chapter:

- Chapter 1, *sFlow Commands*

CHAPTER 1 sFlow Commands

This chapter describes the Sampled Flow (sFlow) commands.

- clear sflow statistics
- debug sflow
- feature sflow
- sflow collector
- sflow poll-interval
- sflow sampling enable
- sflow sampling-rate
- show sflow
- show sflow interface
- show sflow statistics

clear sflow statistics

Use this command to clear sFlow sampling-related counters such as the number of packets sampled and the number of counters sampled.

Command Syntax `clear sflow statistics`

`(interface IFNAME|)`

Parameters

`IFNAME`	Interface name

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear sflow statistics
```

debug sflow

Use this command to display sFlow debugging messages.

Command Syntax `debug sflow (all|agent|sampling|polling|)`

Parameters

`all`	Debug all (agent,sampling,polling)
`agent`	Debug sFlow agent
`sampling`	Debug sFlow sampling
`polling`	Debug sFlow polling

Default

By default, debug command is disabled.

Command Mode

Exec mode and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#debug sflow all
#debug sflow agent

#configure terminal
(config)#debug sflow agent
```

feature sflow

Use this command to enable the sFlow feature.

Use the no form to disable the sFlow feature.

Command Syntax `feature sflow no feature sflow`

Parameters

None

Default

By default, sFlow feature is disabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
(config)#feature sflow
```

sflow collector

Use this command to configure the collector details such as the collector IPv4 address, port number, receiver time-out and datagram size.

Use the `no` form of this command to disable the sFlow collector.

Command Syntax

```
sflow collector A.B.C.D port <1024-65535> receiver-time-out <0-2147483647>
  max-datagram-size <200-9000>

no sflow collector (A.B.C.D port <1024-65535> receiver-time-out <0-2147483647>
  max-datagram-size <200-9000> |)
```

Parameter

`A.B.C.D`	Collector IPv4 address
`<1024-65535>`	Collector UDP Port number. The standard sFlow UDP Port : 6343
`<0-2147483647>`	Receiver time out value in seconds. Zero means no timeout. Upon timeout, value collector information is removed, stopping any ongoing sampling.
`<200-9000>`	Maximum datagram size in bytes that can be sent Collector

Default

By default, sFlow collector is disabled. Default port number is 6343.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
```

```
(config)#sflow collector 2.2.2.2 port 1111 receiver time-out 30
max-datagramsize 500

(config)#no sflow collector
```

sflow poll-interval

Use this command to configure the sFlow counter polling interval. Any change in the polling interval restarts ongoing polling of existing data source interfaces, if any.

Use the `no` form of this command to disable the sFlow counter polling interval.

Command Syntax `sflow poll-interval <5-60> no sflow poll-interval <5-60>`

Parameters

`<5-60>`	Interface counter. Polling interval in seconds

Default

By default, sFlow counter polling interval is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#sflow poll-interval 25
(config-if)#no sflow poll-interval 25
```

sflow sampling enable

Use this command to enable or disable sampling on an interface after giving the sflow sampling-rate command on the same interface.

Command Syntax `sflow enable no sflow enable`

Default

By default, sFlow sampling is disabled.

Command Mode

Interface mode

Parameters

None

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
(config)#interface xe1
(config-if)#sflow sampling-rate 1024 direction ingress max-datagram-size 200
(config-if)#sflow enable
(config-if)#no sflow enable
```

sflow sampling-rate

Use this command to set the sampling rate on an interface. Any change in the sampling rate restarts the ongoing sampling of existing data-source interfaces, if any.

Use the `no` form of this command to disable the sFlow sampling rate.

Note: Packets to CPU is rate limited. In case of unknown unicast, rate limit is applied to such packets as well as sampled data packets.

Command Syntax

```
sflow sampling-rate <1024-1073741823> direction (ingress | egress) max-header-size
  <128-256> no sflow sampling-rate <1024-1073741823> direction (ingress | egress)
max-header-
  size <128-256>
```

Parameters

`<1024-1073741823>`

Sampling rate

`direction`	The direction of sampling an interface:
`ingress`	Ingress traffic
`egress`	Egress traffic
`<128-256>`	Maximum header size in bytes

Default

By default, sFlow sampling rate is disabled.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#sflow sampling-rate 1024 direction ingress max-header-size 200
(config-if)#no sflow sampling-rate 1024 direction ingress max-header-size 200
```

show sflow

Use this command to display sFlow agent configuration along with statistics for all interfaces.

Command Syntax `show sflow (brief | detail)`

Parameters

`brief`	Display configuration parameters on interfaces along with sampling rate and poll interval.
`detail`	Same as `brief` along with configured and default attributes and values of sFlow agent, sFlow collector, and sampling information.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show sflow sFlow Feature: Enabled sFlow
Version: 5 sFlow Global Information :
Agent     IP: 10.12.16.38
Collector IP: 10.12.16.17      Port:  6343
Maximum Datagram Size(bytes): 200 Receiver timeout(sec)
: 0

sFlow Port Detailed Information:
Interface  Packet-Sampling           Packet-Sampling            Counter-Polling         Maximum Header
                 Rate                      Count               Interval       Count        Size(bytes)
```

```
Ingress      Egress       Ingress      Egress       (sec)                      Ingress     Egress ---------  -----------------
------   ----------------------  ----------------------   --------------------xe1            1024           0            0
0           6            3     128            0

#
#show sflow brief sFlow Feature:
Enabled
Collector IP: 10.12.16.17      Port:  6343
Maximum Datagram Size(bytes): 200 Receiver timeout(sec)
: 0

sFlow Port Configuration:
Interface   Status               Sample Rate               Counter-Polling
            Ingress    Egress    Ingress      Egress       Interval(sec) ---------   --------
----------   ------------------------   --------------xe1       Enabled    Disabled
1024            0      6
```

Table 1-242: Show sflow output

Entry	Description
sFlow feature	Shows whether sFlow is enabled or disabled.
sFlow Version	Displays the sFlow version. Version 5 is the current global standard.
sFlow Global Information	Global Information consists of the Agent IP address, Collector IP, Port number, Maximum Datagram Size, and the Receiver timeout.
Agent IP	IPv4 address of this switch/router.
Collector IP	IPv4 address of the sFlow collector server.
Port	Port number on the sFlow collector server. Standard is port 6343.
Maximum Datagram Size	The maximum size of the datagrams sent by the agent
Receiver timeout	The number of seconds between each sampling – zero means sample continuously.
sFlow Port Interface	The interface of this switch/router on which sFlow is running (e.g. xe1/1).
Packet-Sampling Rate	the number of packets received or transmitted before a sample is taken.
Packet-Sampling Count	The number of sample packets that have been sampled on both the ingress and egress of the interface.
Counter-Polling	Shows the amount of time between polling samples and the count of the total number of polling samples taken.

Maximum Header Size	The maximum header size for both the ingress and egress of the interface.

show sflow interface

Use this command to display the sFlow configuration for the input interface.

Command Syntax `show sflow interface IFNAME`

Parameters

`IFNAME` Interface name

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

Note: For information on the output values of this command, see the show sflow command.

```
#show sflow interface xe1
sFlow feature: Enabled sFlow
Version: 5 sFlow Global
Information : Agent      IP:
10.10.26.104
Collector IP: 10.12.16.18      Port:   6343
Maximum  Datagram  Size(bytes):  200  Receiver
timeout(sec)         : 0

sFlow Port Detailed Information:
Interface  Packet-Sampling           Counter-Polling          Maximum Header
```

```
           Rate          Count         Interval(sec) Count       Size(bytes) ----
-----  ----------------------   ------------------------  -------------xe1
1024            0           6            41      128
```

show sflow statistics

Use this command to display sFlow counter information.

Command Syntax `show sflow statistics (interface IFNAME|)`

Parameters

`IFNAME`	Interface name.

Default

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

Note: For information on the output values of this command, see the show sflow command.

```
#show sflow statistics

sFlow Port Statistics:
Interface  Packet-Sampling   Counter-Polling
               Count              Count ---------  ------
---------   --------------xe1                     0
19
```

SECTION 13 Quality of Service

Quality of Service Configuration Guide (Helix4)

Contents

This document contains these chapters and appendices:

- Chapter 1, *Basic Helix4 QoS Configuration*
- Chapter 2, *Marking/Remarking Configuration*
- Chapter 3, *Policing Configuration*
- Chapter 4, *Aggregate Policing*
- Chapter 5, *Shaping Configuration*
- Chapter 6, *Tail-Drop Configuration*
- Chapter 7, *WRED Configuration*

CHAPTER 1 Basic Helix4 QoS Configuration

Configuration Guidelines

The following provides information to consider before configuring QoS for the Helix4 platform.

- QoS policing cannot be configured over EtherChannel.
- Traffic can be classified per ingress port or per-port per-VLAN.
- There can be only one ACL configuration command per class map. An ACL can have multiple commands (access control entries) that match fields against the packet contents.
- Policing cannot be done at the switch virtual level. A policer can be configured only on an ingress physical port.
- As a part of egress queue configuration, define which packets (identified by the CoS value) are assigned to one of the eight egress queues.

`#configure terminal`	Enter configure mode

(config)#ip-access-list 1 permit 192.5.255.0 192.5.255.0 0.0.0.255	Creating a permit access list for

Enabling and Disabling QoS

Enable QoS

The following globally enables QoS.

#configure terminal	Enter configure mode
(config)#mls qos enable	Enable QoS
(config)#exit	Exit configure mode.

Disable QoS

The following globally disables QoS.

#configure terminal	Enter configure mode.
(config)#no mls qos	Disable QoS
(config)#exit	Exit configure mode.

Classify Traffic Using ACLs

IP traffic can be classified using IP standard or IP extended ACLs.

The following example shows allowing access only for hosts on three specified networks. Wildcard bits correspond to the network address host portions. If a host has an address that does not match the access list, it is rejected.

Basic Helix4 QoS Configuration

(config)#ip-access-list 1 permit 128.88.0.0 0.0.255.255	Creating a permit access list for 128.88.0.0
(config)#ip-access-list 1 permit 36.0.0.0 0.0.0.255	Creating a permit access list for 36.0.0.0
(config)#exit	Exit configure mode

Creating a Class Map

The following shows creating a class map and defining the match criterion.

#configure terminal	Enter configuration mode.
(config-cmap)#class-map cmap1	Enter a name (cmap1) for the class-map.
(config-cmap)#exit	Exit class-map mode.
(config)#exit	Exit configure mode/

Classify Traffic on a Per-VLAN Basis

The following shows classifying traffic on a per-VLAN basis using class maps. This involves creating a class map and defining the match criterion.

The following example shows configuring a class map named cmap1 with criterion that matches IP DSCP 56.

`#configure terminal`	Enter configure mode.
`(config)#class-map cmap1`	Create a class-map named cmap1.
`(config-cmap)#match ip-dscp 56`	Match it to DSCP value 56.
`(config-cmap)#match vlan-range 20 to 30`	Match to VLANs 20 through 30.
`(config-cmap)#exit`	Exit class-map mode.
`(config)#exit`	Exit config mode.

Create Policy Map

The following example shows creating a policy map and attaching it to an ingress interface. In this example, the IP standard ACL allows traffic from network 10.1.0.0. If the matched traffic exceeds a 48000-bps average traffic rate and an 8000-byte normal burst size, its DSCP is marked down, and sent.

`#configure terminal`	Enter the configuration mode.
`(config)#ip-access-list 1 permit 10.1.0.0 0.0.255.255`	Create an access-list with number 1 that permits traffic from 10.1.0.0.
`(config)#class-map cmap1`	Create a class-map with name cmap1.
`(config-cmap)#match access-group 1`	Match the class-map to access-group 1.
`(config-cmap)#exit`	Exit class-map mode.
`(config)#policy-map pmap1`	Create a policy-map with name pmap1
`(config-pmap)#class cmap1`	The class-map name (cmap1) for which to define the traffic classification.

`(config-pmap-c)#police colour-blind srtcm 48000 8000 12 exceed-action drop`	Specify the policing parameters for the service-policy.
`(config-pmap-c)#exit`	Exit the policy-map-class mode.
`(config-pmap)#exit`	Exit the policy-map mode.
`(config)#interface fe0`	Enter the interface mode.
`(config-if)#service-policy input pmap1`	Assign the service-policy to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit the configuration mode.

Create Aggregate Policer

The following example shows creating an aggregate policer and attaching it to multiple classes within a policy map. In this example, the IP ACLs allow traffic from network 10.1.0.0 and host 11.3.1.1. The traffic rate from network

10.1.0.0 and host 11.3.1.1 is policed. If the traffic exceeds a 48000-bps average traffic rate and an 8000-byte normal burst size, it is considered out of profile, and is dropped. The policy map is attached to an ingress interface.

`#configure terminal`	Enter configuration more.
`(config)#ip-access-list 1 permit 10.1.0.0 0.0.255.255`	Create access-list 1 that permits traffic from 10.1.0.0.
`(config)#ip-access-list 2 permit 11.3.1.1`	Create access-list 2 that permits traffic from 11.3.1.1
`(config)#mls qos aggregate-police transmit1 48000 8000`	Create a policer (transmit1) that allows 48000 bps traffic, with a maximum burst rate of 8000 bytes.
`(config)#class-map cmap1`	Create class-map cmap1.
`(config-cmap)#match access-group 1`	Match to access-group 1.
`(config-cmap)#exit`	Exit class-map mode.
`(config)#class-map cmap2`	Create class-map cmap2.
`(config-cmap)#match access-group 2`	Match to access-group 2.
`(config-cmap)#exit`	Exit class-map mode.
`(config)#policy-map aggflow1`	Create policy-map aggflow1.
`(config-pmap)#class cmap1`	Assign class-map cmap1 to policy-map aggflow1.
`(config-pmap-c)#police-aggregate transmit1`	Assign policer transmit1 to aggflow1 and cmap1.
`(config-pmap-c)#exit`	Exit policy-map class mode.
`(config-pmap)#class cmap2`	Enter policy-map-class mode with cmap2.
`(config-pmap-c)#set ip-dscp 56`	set the DSCP value to 56.
`(config-pmap-c)#police-aggregate transmit1`	Assign policer transmit1 to aggflow1 and cmap2.
`(config-pmap-c)#exit`	Exit policy-map-class mode.
`(config-pmap)#exit`	Exit policy-map mode.
`(config)#interface fe0`	Enter interface mode.
`(config-if)#service-policy input aggflow1`	Assign the service-policy (aggflow1) to the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit configure mode.

Basic Helix4 QoS Configuration

Validation

The following sections display the show commands to use to validate the above configurations.

```
#show class-map cmap1
    CLASS-MAP-NAME: cmap1
      Set IP DSCP: 56
      Match IP DSCP: 7


#show mls qos aggregate-policer agp1
```

```
 AGGREGATOR-POLICER-NAME: agp1
    Police:    Average rate(1 kbps), burst size(1 bytes)      Exceed-action drop


#show policy-map pmap1
  POLICY-MAP-NAME: pmap1
    State: detached
    CLASS-MAP-NAME: cmap1
      Match IP DSCP: 7
      Set IP DSCP: 56
```

CHAPTER 2 Marking/Remarking Configuration

This chapter contains a complete sample of configuring Marking/Remarking.

Topology

Figure 2-214: Simple configuration of Marking/Remarking

L2 Interface

Do the following to configure Marking/Remarking on an L2 interface.

`#configure terminal`	Enter configure mode.
`(config)#mls qos enable`	Enable the QOS globally
`(config)#bridge 1 protocol rstp vlan-bridge`	Configure bridge 1 as RSTP-VLAN aware.
`(config)#vlan 2-6 bridge 1`	Configure vlans
`(config)#interface xe2`	Enter interface mode.
`(config-if)#switchport`	Configure xe2 as a layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.
`(config-if)#switchport mode trunk`	Configure port as a trunk.
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe1 interface.
`(config-if)#exit`	Exit the xe1 interface mode.
`(config)#interface xe3`	Enter interface mode.
`(config-if)#switchport`	Configure xe1 as a layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.
`(config-if)#switchport mode trunk`	Configure port as a trunk.
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe1 interface.

(config-if)#exit	Exit the xe1 interface mode.
(config)# class-map cmap1	Enter Class-map mode
(config-cmap)# match cos 2	Configure match criteria as CoS with Value 2
(config-cmap)# exit	Exit Class-map mode
(config)# policy-map pmap1	Enter policy-map mode

Marking/Remarking Configuration

(config-pmap)#class cmap1	Assign Class camp1 to Policy-map pmap1
(config-pmap-c)# set cos 5	Remark cos from cos 2 to cos 5
(config-pmap-c)#exit	Exit out of policy-class-map mode
(config-pmap)#exit	Exit out of Policy-map mode
(config)#interface xe2	Enter xe1 interface
(config-if)#service-policy input pmap1	Assign service-policy to interface on in-direction
(config-if)#exit	Exit out of interface mode
(config)#interface xe3	Enter xe2 interface
(config-if)#service-policy input pmap1	Assign service-policy to interface on in-direction
(config-if)#exit	Exit out of interface mode

Validation

Enter the commands below to confirm the configurations.

```
#show class-map cmap1

     CLASS-MAP-NAME: cmap1       Match Cos: 2

#show policy-map pmap1

  POLICY-MAP-NAME: pmap1     State: attached

    CLASS-MAP-NAME: cmap1
      Match Cos: 2       Set CoS: 5
```

L3 Interface

Do the following to configure Marking/Remarking on an L3 interface.

#configure terminal	Enter configure mode.
(config)#mls qos enable	Enable the QOS globally
(config)#interface xe2	Enter interface mode.
(config-if)#ip address 10.1.1.2/24	Configure ip address on interface xe2.
(config-if)#exit	Exit the xe1 interface mode.

(config)#interface xe3	Enter interface mode.
(config-if)#ip address 20.1.1.2/24	Configure ip address on interface xe3.
(config-if)#exit	Exit the xe1 interface mode.
(config)# class-map cmap1	Enter Class-map mode
(config-cmap)# match ip-dscp 45	Configure match criteria as CoS with Value 2
(config-cmap)# exit	Exit Class-map mode

Marking/Remarking Configuration

(config)# policy-map pmap1	Enter policy-map mode
(config-pmap)#class cmap1	Assign Class camp1 to Policy-map pmap1
(config-pmap-c)# set ip-dscp 54	Remark cos from dscp 45 to dscp 54
(config-pmap-c)#exit	Exit out of policy-class-map mode
(config-pmap)#exit	Exit out of Policy-map mode
(config)#interface xe2	Enter xe1 interface
(config-if)#service-policy input pmap1	Assign service-policy to interface on in-direction
(config-if)#exit	Exit out of interface mode
(config)#interface xe3	Enter xe2 interface
(config-if)#service-policy input pmap1	Assign service-policy to interface on in-direction
(config-if)#exit	Exit out of interface mode

Validation

Enter the commands below to confirm the configurations.

```
#show class-map cmap1
        CLASS-MAP-NAME: cmap1
      Match IP DSCP: 45
#show policy-map pmap1
  POLICY-MAP-NAME:      pmap1
State: attached

    CLASS-MAP-NAME: cmap1
      Match IP DSCP: 45
      Set IP DSCP: 54
```

Marking/Remarking Configuration

CHAPTER 3 Policing Configuration

This chapter contains a complete sample of configuring Marking/Remarking.

Topology

Figure 3-215: Simple configuration of Policing

L2 Interface

The following steps describe how to configure Marking/Remarking.

`#configure terminal`	Enter configure mode.
`(config)#mls qos enable`	Enable the QOS globally
`(config)#bridge 1 protocol rstp vlan- bridge`	Configure bridge 1 as RSTP-VLAN aware.
`(config)#vlan 2-6 bridge 1`	Configure vlans
`(config)#interface xe2`	Enter interface mode.
`(config-if)#switchport`	Configure xe2 as a layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.
`(config-if)#switchport mode trunk`	Configure port as a trunk.
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe1 interface.
`(config-if)#exit`	Exit the xe1 interface mode.
`(config)#interface xe3`	Enter interface mode.
`(config-if)#switchport`	Configure xe1 as a layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.
`(config-if)#switchport mode trunk`	Configure port as a trunk.
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe1 interface.
`(config-if)#exit`	Exit the xe1 interface mode.
`(config)# class-map cmap1`	Enter Class-map mode
`(config-cmap)# match cos 2`	Configure match criteria as CoS with Value 2

(config-cmap)# exit	Exit Class-map mode
(config)# policy-map pmap1	Enter policy-map mode
(config-pmap)#class cmap1	Assign Class camp1 to Policy-map pmap1
(config-pmap-c)# police colour-blind srtcm 2048 2048 5120 exceed-action set-cos-transmit 1 violate-action drop	Police the above classified traffic
(config-pmap-c)#exit	Exit out of policy-class-map mode
(config-pmap)#exit	Exit out of Policy-map mode
(config)#interface xe2	Enter xe1 interface
(config-if)#service-policy input pmap1	Assign service-policy to interface on in-direction
(config-if)#exit	Exit out of interface mode
(config)#interface xe3	Enter xe2 interface
(config-if)#service-policy input pmap1	Assign service-policy to interface on in-direction
(config-if)#exit	Exit out of interface mode

Validation

Enter the commands below to confirm the configurations.

```
#show class-map cmap1

     CLASS-MAP-NAME: cmap1
      Match Cos: 2


#show policy-map pmap1

  POLICY-MAP-NAME: pmap1      State:
attached

    CLASS-MAP-NAME: cmap1
      Match Cos: 2
      Police: Type colour-blind      Mode:
SrTCM
              average rate (2048 Kbits/sec)
burst size (2048 Kbits/sec)               exceed-action
(Remarked to policed-cos-tx)               excess burst size
(5120 Kbits/sec)               flow control mode (none)
violate-action (drop)
```

L3 Interface

Do the following to configure policing on an L3 interface.

#configure terminal	Enter configure mode.
(config)#mls qos enable	Enable the QOS globally
(config)#interface xe2	Enter interface mode.
(config-if)#ip address 10.1.1.2/24	Configure ip address on interface xe2.
(config-if)#exit	Exit the xe1 interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#ip address 20.1.1.2/24	Configure ip address on interface xe3.
(config-if)#exit	Exit the xe1 interface mode.
(config)# class-map cmap1	Enter Class-map mode
(config-cmap)# match ip-dscp 45	Configure match criteria as CoS with Value 2
(config-cmap)# exit	Exit Class-map mode
(config)# policy-map pmap1	Enter policy-map mode
(config-pmap)#class cmap1	Assign Class camp1 to Policy-map pmap1
(config-pmap-c)# police colour-blind srtcm 13312 3072 2048 exceed-action set-dscptransmit 8 violate-action drop	Police the above classified traffic
(config-pmap-c)#exit	Exit out of policy-class-map mode
(config-pmap)#exit	Exit out of Policy-map mode
(config)#interface xe2	Enter xe1 interface
(config-if)#service-policy input pmap1	Assign service-policy to interface on in-direction
(config-if)#exit	Exit out of interface mode
(config)#interface xe3	Enter xe2 interface
(config-if)#service-policy input pmap1	Assign service-policy to interface on in-direction
(config-if)#exit	Exit out of interface mode

Validation

Enter the commands below to confirm the configurations.

```
#show class-map cmap1

       CLASS-MAP-NAME: cmap1
      Match IP DSCP: 45

#show policy-map pmap1

POLICY-MAP-NAME: pmap1     State:
attached

    CLASS-MAP-NAME: cmap1
```

```
      Match Cos: 2
      Police:      Type:      colour-blind
Mode: SrTCM
               average rate (13312 Kbits/sec)
burst size (3072 Kbits/sec)               exceed-action
(Remarked to policed-dscp-tx)               excess burst size
(2048 Kbits/sec)               flow control mode (none)
violate-action (drop)
```

TRTCM Policing

The following steps describe how to configure TRTCM policing.

L2 Interface

Do the following to configure policing on an L2 interface.

`#configure terminal`	Enter configure mode.
`(config)#mls qos enable`	Enable the QOS globally
`(config)#bridge 1 protocol rstp vlan- bridge`	Configure bridge 1 as RSTP-VLAN aware.
`(config)#vlan 2-6 bridge 1`	Configure vlans
`(config)#interface xe2`	Enter interface mode.
`(config-if)#switchport`	Configure xe2 as a layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.
`(config-if)#switchport mode trunk`	Configure port as a trunk.
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe1 interface.
`(config-if)#exit`	Exit the xe1 interface mode.
`(config)#interface xe3`	Enter interface mode.
`(config-if)#switchport`	Configure xe1 as a layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.
`(config-if)#switchport mode trunk`	Configure port as a trunk.
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe1 interface.
`(config-if)#exit`	Exit the xe1 interface mode.
`(config)# class-map cmap1`	Enter Class-map mode
`(config-cmap)# match cos 2`	Configure match criteria as CoS with Value 2
`(config-cmap)# exit`	Exit Class-map mode
`(config)# policy-map pmap1`	Enter policy-map mode
`(config-pmap)#class cmap1`	Assign Class camp1 to Policy-map pmap1

(config-pmap-c)# police colour-aware trtcm 2000 1000 1000 2000 exceed-action set-costransmit 0 violate-action drop	Police the above classified traffic
(config-pmap-c)#exit	Exit out of policy-class-map mode
(config-pmap)#exit	Exit out of Policy-map mode
(config)#interface xe2	Enter xe1 interface
(config-if)#service-policy input pmap1	Assign service-policy to interface on in-direction
(config-if)#exit	Exit out of interface mode
(config)#interface xe3	Enter xe2 interface
(config-if)#service-policy input pmap1	Assign service-policy to interface on in-direction
(config-if)#exit	Exit out of interface mode

Validation

Enter the commands below to confirm the configurations.

```
#show class-map cmap1

     CLASS-MAP-NAME: cmap1      Match
Cos: 2

#show policy-map pmap1

  POLICY-MAP-NAME: pmap1      State:
attached

    CLASS-MAP-NAME: cmap1
      Match Cos: 2
      Police:      Type:      colour-aware
Mode: TrTCM
              average rate (1000 Kbits/sec)
burst size (1000 Kbits/sec)               exceed-action
(Remarked to policed-cos-tx)               peak rate (2000
Kbits/sec)               peak burst size (2000 Kbits/sec)
flow control mode (none)               violate-action (drop)
```

L3 Interface

Do the following to configure policing on L3 interface.

#configure terminal	Enter configure mode.
(config)#mls qos enable	Enable the QOS globally
(config)#interface xe2	Enter interface mode.
(config-if)#ip address 10.1.1.2/24	Configure ip address on interface xe2.
(config-if)#exit	Exit the xe1 interface mode.

(config)#interface xe3	Enter interface mode.
(config-if)#ip address 20.1.1.2/24	Configure ip address on interface xe3.
(config-if)#exit	Exit the xe1 interface mode.
(config)# class-map cmap1	Enter Class-map mode
(config-cmap)# match ip-dscp 45	Configure match criteria as CoS with Value 2
(config-cmap)# exit	Exit Class-map mode
(config)# policy-map pmap1	Enter policy-map mode
(config-pmap)#class cmap1	Assign Class camp1 to Policy-map pmap1
(config-pmap-c)# police colour-blind trtcm 30000 15000 1500 3000 exceed-action set-dscptransmit 15 violate-action drop	Police the above classified traffic
(config-pmap-c)#exit	Exit out of policy-class-map mode
(config-pmap)#exit	Exit out of Policy-map mode
(config)#interface xe2	Enter xe1 interface
(config-if)#service-policy input pmap1	Assign service-policy to interface on in-direction
(config-if)#exit	Exit out of interface mode
(config)#interface xe3	Enter xe2 interface
(config-if)#service-policy input pmap1	Assign service-policy to interface on in-direction
(config-if)#exit	Exit out of interface mode

Validation

Enter the commands below to confirm the configurations.

```
#show class-map cmap1

       CLASS-MAP-NAME: cmap1
      Match IP DSCP: 45

#show policy-map pmap1

POLICY-MAP-NAME: pmap1     State:
attached

    CLASS-MAP-NAME: cmap1
      Match IP DSCP: 45
      Police:      Type:      colour-blind
Mode: TrTCM
              average rate (15000 Kbits/sec)
burst size (1500 Kbits/sec)               exceed-action
(Remarked to policed-dscp-tx)               peak rate (30000
Kbits/sec)               peak burst size (3000 Kbits/sec)
flow control mode (none)               violate-action (drop)
```

CHAPTER 4 Aggregate Policing

This chapter contains a complete sample of configuring Marking/Remarking.

Topology

L2 Interface

Do the following to configure aggregate policing on anL2 interface.

`#configure terminal`	Enter configure mode.
`(config)#mls qos enable`	Enable the QOS globally
`(config)#bridge 1 protocol rstp vlan- bridge`	Configure bridge 1 as RSTP-VLAN aware.
`(config)#vlan 2-6 bridge 1`	Configure vlans
`(config)#interface xe2`	Enter interface mode.
`(config-if)#switchport`	Configure xe2 as a layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.
`(config-if)#switchport mode trunk`	Configure port as a trunk.
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe1 interface.
`(config-if)#exit`	Exit the xe1 interface mode.
`(config)#interface xe3`	Enter interface mode.
`(config-if)#switchport`	Configure xe1 as a layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.
`(config-if)#switchport mode trunk`	Configure port as a trunk.
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe1 interface.

(config-if)#exit	Exit the xe1 interface mode.
(config)# class-map cmap1	Enter Class-map mode
(config-cmap)# match cos 2	Configure match criteria as CoS with Value 2
(config-cmap)# exit	Exit Class-map mode
(config)# mls qos aggregate-police pagg1 30000 300	Configure aggregate policer

Aggregate Policing

(config)# policy-map pmap1	Enter policy-map mode
(config-pmap)#class cmap1	Assign Class camp1 to Policy-map pmap1
(config-pmap-c)# police-aggregate pagg1	Police the above classified traffic
(config-pmap-c)#exit	Exit out of policy-class-map mode
(config-pmap)#exit	Exit out of Policy-map mode
(config)#interface xe2	Enter xe1 interface
(config-if)#service-policy input pmap1	Assign service-policy to interface on in-direction
(config-if)#exit	Exit out of interface mode
(config)#interface xe3	Enter xe2 interface
(config-if)#service-policy input pmap1	Assign service-policy to interface on in-direction
(config-if)#exit	Exit out of interface mode

Validation

Enter the commands below to confirm the configurations.

```
#show class-map cmap1

     CLASS-MAP-NAME:           cmap1
Match Cos: 2

#show policy-map pmap1

  POLICY-MAP-NAME:          State:
pmap1 attached

    CLASS-MAP-NAME: cmap1
      Match      Cos:       2
Police: Mode: SrTCM
              average rate (30000 Kbits/sec)
burst size (2400 Kbits/sec)               exceed-
action (drop)               excess burst size (0
Kbits/sec)               flow control mode (none)
```

```
violate-action (remark) #show mls qos
aggregate-policer pagg1

 AGGREGATOR-POLICER-NAME: pagg1
    Police:    Average rate(30000 kbps), burst size(300 kbps)    Exceed-action drop
```

L3 Interface

Do the following to configure aggregate policing on anL3 interface.

Aggregate Policing

`#configure terminal`	Enter configure mode.
`(config)#mls qos enable`	Enable the QOS globally
`(config)#interface xe2`	Enter interface mode.
`(config-if)#ip address 10.1.1.2/24`	Configure ip address on interface xe2.
`(config-if)#exit`	Exit the xe1 interface mode.
`(config)#interface xe3`	Enter interface mode.
`(config-if)#ip address 20.1.1.2/24`	Configure ip address on interface xe3.
`(config-if)#exit`	Exit the xe1 interface mode.
`(config)# class-map cmap1`	Enter Class-map mode
`(config-cmap)# match ip-dscp 45`	Configure match criteria as CoS with Value 2
`(config-cmap)# exit`	Exit Class-map mode
`(config)# mls qos aggregate-police pagg1 40000 4000`	Configure aggregate policer
`(config)# policy-map pmap1`	Enter policy-map mode
`(config-pmap)#class cmap1`	Assign Class camp1 to Policy-map pmap1
`(config-pmap-c)# police-aggregate pagg1`	Police the above classified traffic
`(config-pmap-c)#exit`	Exit out of policy-class-map mode
`(config-pmap)#exit`	Exit out of Policy-map mode
`(config)#interface xe2`	Enter xe1 interface
`(config-if)#service-policy input pmap1`	Assign service-policy to interface on in-direction
`(config-if)#exit`	Exit out of interface mode
`(config)#interface xe3`	Enter xe2 interface
`(config-if)#service-policy input pmap1`	Assign service-policy to interface on in-direction
`(config-if)#exit`	Exit out of interface mode

Validation

Enter the commands below to confirm the configurations.

```
#show class-map cmap1

       CLASS-MAP-NAME:      cmap1
Match IP DSCP: 45

#show policy-map pmap1

  POLICY-MAP-NAME:       pmap1
State: attahced

    CLASS-MAP-NAME: cmap1
      Match IP DSCP: 45
      Police: Mode: SrTCM
```

Aggregate Policing

```
              average rate (40000 Kbits/sec)
burst size (32000 Kbits/sec)
exceed-action (drop)               excess burst
size (0 Kbits/sec)               flow control
mode (none)               violate-action
(remark)

#show mls qos aggregate-policer pagg1

 AGGREGATOR-POLICER-NAME: pagg1
    Police:    Average rate(40000  kbps), burst size(4000 kbps)      Exceed-action drop
```

CHAPTER 5 Shaping Configuration

This chapter contains a complete sample of configuring Shaping.

Topology

Figure 5-216: Simple configuration of Shaping

L2 Interface

Do the following to configure shaping on anL2 interface.

`#configure terminal`	Enter configure mode.
`(config)#mls qos enable`	Enable the QOS globally
`(config)#bridge 1 protocol rstp vlan- bridge`	Configure bridge 1 as RSTP-VLAN aware.
`(config)#vlan 2-6 bridge 1`	Configure vlans
`(config)#interface xe2`	Enter interface mode.
`(config-if)#switchport`	Configure xe2 as a layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.
`(config-if)#switchport mode trunk`	Configure port as a trunk.
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe1 interface.
`(config-if)#exit`	Exit the xe1 interface mode.
`(config)#interface xe3`	Enter interface mode.
`(config-if)#switchport`	Configure xe1 as a layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.
`(config-if)#switchport mode trunk`	Configure port as a trunk.
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe1 interface.

(config-if)#exit	Exit the xe1 interface mode.
(config)#interface xe3	Enter xe2 interface
(config-if)# traffic-shape rate 30720 kbps burst 2000	Configure shaping on the egress interface
(config-if)#exit	Exit out of interface mode

Shaping Configuration

Validation

Enter the commands below to confirm the configurations. `rtr2#show mls qos interface xe3`

```
  Trust Mode: Trust the VLAN Tag Priority
  Port Default CoS Priority: 0
  Port Default DSCP value : 0
  COS Priority Overide: Not Configured
  Egress Traffic Shaping: 30720 Kbps  burst rate: 2000 Kb
  Schedule mode: Strict Queues: 0 1 2 3 4 5 6 7
     The number of COS Values mapped: 8
    Cos (Queue): 0(0), 1(1), 2(2), 3(3), 4(4), 5(5), 6(6), 7(7)
    Cos (Cos): 0(0), 1(1), 2(2), 3(3), 4(4), 5(5), 6(6), 7(7)
    Dscp (Queue): 0(0), 1(0), 2(0), 3(0), 4(0), 5(0), 6(0), 7(0)
    Dscp (Queue): 8(1), 9(1), 10(1), 11(1), 12(1), 13(1), 14(1), 15(1)
    Dscp (Queue): 16(2), 17(2), 18(2), 19(2), 20(2), 21(2), 22(2), 23(2)
    Dscp (Queue): 24(3), 25(3), 26(3), 27(3), 28(3), 29(3), 30(3), 31(3)
    Dscp (Queue): 32(4), 33(4), 34(4), 35(4), 36(4), 37(4), 38(4), 39(4)
    Dscp (Queue): 40(5), 41(5), 42(5), 43(5), 44(5), 45(5), 46(5), 47(5)
    Dscp (Queue): 48(6), 49(6), 50(6), 51(6), 52(6), 53(6), 54(6), 55(6)
    Dscp (Queue): 56(7), 57(7), 58(7), 59(7), 60(7), 61(7), 62(7), 63(7)
    Dscp (Dscp): 0(0), 1(1), 2(2), 3(3), 4(4), 5(5), 6(6), 7(7)
    Dscp (Dscp): 8(8), 9(9), 10(10), 11(11), 12(12), 13(13), 14(14), 15(15)
    Dscp (Dscp): 16(16), 17(17), 18(18), 19(19), 20(20), 21(21), 22(22), 23(23)
    Dscp (Dscp): 24(24), 25(25), 26(26), 27(27), 28(28), 29(29), 30(30), 31(31)
    Dscp (Dscp): 32(32), 33(33), 34(34), 35(35), 36(36), 37(37), 38(38), 39(39)
    Dscp (Dscp): 40(40), 41(41), 42(42), 43(43), 44(44), 45(45), 46(46), 47(47)
        Dscp (Dscp): 48(48), 49(49), 50(50), 51(51), 52(52), 53(53), 54(54), 55(55)
      Dscp (Dscp): 56(56), 57(57), 58(58), 59(59), 60(60), 61(61), 62(62), 63(63)
```

L3 Interface

Do the following to configure shaping on an L3 interface.

#configure terminal	Enter configure mode.
(config)#mls qos enable	Enable QOS globally

(config)#interface xe2	Enter interface mode.
(config-if)#ip address 10.1.1.2/24	Configure ip address on interface xe2.
(config-if)#exit	Exit the xe1 interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#ip address 20.1.1.2/24	Configure IP address on interface xe3.
(config-if)#exit	Exit the xe1 interface mode.
(config)#interface xe3	Enter xe3 interface

Shaping Configuration

(config-if)# traffic-shape rate 40960 kbps burst 819	Configure shaping on the egress interface
(config-if)#exit	Exit out of interface mode

Validation

Enter the commands below to confirm the configurations.

```
rtr2#show mls qos interface xe3

  Trust Mode: Trust the IP DSCP Bits
  Port Default CoS Priority: 0
  Port Default DSCP value : 0
  COS Priority Overide: Not Configured
  Egress Traffic Shaping: 40960 Kbps  burst rate: 819 Kb
  Schedule mode: Strict Queues: 0 1 2 3 4 5 6 7
     The number of COS Values mapped: 8
    Cos (Queue): 0(0), 1(1), 2(2), 3(3), 4(4), 5(5), 6(6), 7(7)
    Cos (Cos): 0(0), 1(1), 2(2), 3(3), 4(4), 5(5), 6(6), 7(7)
    Dscp (Queue): 0(0), 1(0), 2(0), 3(0), 4(0), 5(0), 6(0), 7(0)
    Dscp (Queue): 8(1), 9(1), 10(1), 11(1), 12(1), 13(1), 14(1), 15(1)
    Dscp (Queue): 16(2), 17(2), 18(2), 19(2), 20(2), 21(2), 22(2), 23(2)
    Dscp (Queue): 24(3), 25(3), 26(3), 27(3), 28(3), 29(3), 30(3), 31(3)
    Dscp (Queue): 32(4), 33(4), 34(4), 35(4), 36(4), 37(4), 38(4), 39(4)
    Dscp (Queue): 40(5), 41(5), 42(5), 43(5), 44(5), 45(5), 46(5), 47(5)
    Dscp (Queue): 48(6), 49(6), 50(6), 51(6), 52(6), 53(6), 54(6), 55(6)
    Dscp (Queue): 56(7), 57(7), 58(7), 59(7), 60(7), 61(7), 62(7), 63(7)
    Dscp (Dscp): 0(0), 1(1), 2(2), 3(3), 4(4), 5(5), 6(6), 7(7)
    Dscp (Dscp): 8(8), 9(9), 10(10), 11(11), 12(12), 13(13), 14(14), 15(15)
    Dscp (Dscp): 16(16), 17(17), 18(18), 19(19), 20(20), 21(21), 22(22), 23(23)
    Dscp (Dscp): 24(24), 25(25), 26(26), 27(27), 28(28), 29(29), 30(30), 31(31)
    Dscp (Dscp): 32(32), 33(33), 34(34), 35(35), 36(36), 37(37), 38(38), 39(39)
    Dscp (Dscp): 40(40), 41(41), 42(42), 43(43), 44(44), 45(45), 46(46), 47(47)
    Dscp (Dscp): 48(48), 49(49), 50(50), 51(51), 52(52), 53(53), 54(54),
55(55) Dscp (Dscp): 56(56), 57(57), 58(58), 59(59), 60(60), 61(61), 62(62),
63(63) rtr2#
```

Shaping Configuration

CHAPTER 6 Tail-Drop Configuration

This chapter contains a sample of configuring Tail-Drop.

Topology

Figure 6-217: Simple configuration of Tail-Drop

L2 Interface

Do the following to configure tail drop on an L2 interface.

`#configure terminal`	Enter configure mode.
`(config)#mls qos enable`	Enable the QOS globally
`(config)#bridge 1 protocol rstp vlan- bridge`	Configure bridge 1 as RSTP-VLAN aware.
`(config)#vlan 2-6 bridge 1`	Configure vlans
`(config)#interface xe2`	Enter interface mode.
`(config-if)#switchport`	Configure xe2 as a layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.
`(config-if)#switchport mode trunk`	Configure port as a trunk.
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe1 interface.
`(config-if)#exit`	Exit the xe1 interface mode.
`(config)#interface xe3`	Enter interface mode.
`(config-if)#switchport`	Configure xe1 as a layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.
`(config-if)#switchport mode trunk`	Configure port as a trunk.
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe1 interface.

(config-if)#exit	Exit the xe1 interface mode.
(config)#interface xe3	Enter xe2 interface
(config-if)# tail-drop queue-id 2 threshold 60	Configure tail drop on the egress interface
(config-if)#exit	Exit out of interface mode

Tail-Drop Configuration

Validation

Enter the commands below to confirm the configurations. #

```
show mls qos interface xe3

  Trust Mode: Trust the VLAN Tag Priority
  Port Default CoS Prioiry: 0
  Port Default DSCP value : 0
  VLAN Priority Overide: Not Configured
  Egress Traffic Shaping: Not Configured
  Schedule mode: Strict Queues: 0 1 2 3 4 5 6 7
     The number of COS Values mapped: 8
    Cos (Queue): 0(0), 1(1), 2(2), 3(3), 4(4), 5(5), 6(6), 7(7)
    Cos (Cos): 0(0), 1(1), 2(2), 3(3), 4(4), 5(5), 6(6), 7(7)
    Exp (Queue): 0(0), 1(0), 2(0), 3(0), 4(0), 5(0), 6(0), 7(0)
    Exp (Exp): 0(0), 1(0), 2(0), 3(0), 4(0), 5(0), 6(0), 7(0)
    Dscp (Queue): 0(0), 1(0), 2(0), 3(0), 4(0), 5(0), 6(0), 7(0)
    Dscp (Queue): 8(1), 9(1), 10(1), 11(1), 12(1), 13(1), 14(1), 15(1)
    Dscp (Queue): 16(2), 17(2), 18(2), 19(2), 20(2), 21(2), 22(2), 23(2)
    Dscp (Queue): 24(3), 25(3), 26(3), 27(3), 28(3), 29(3), 30(3), 31(3)
    Dscp (Queue): 32(4), 33(4), 34(4), 35(4), 36(4), 37(4), 38(4), 39(4)
    Dscp (Queue): 40(5), 41(5), 42(5), 43(5), 44(5), 45(5), 46(5), 47(5)
    Dscp (Queue): 48(6), 49(6), 50(6), 51(6), 52(6), 53(6), 54(6), 55(6)
    Dscp (Queue): 56(7), 57(7), 58(7), 59(7), 60(7), 61(7), 62(7), 63(7)
    Dscp (Dscp): 0(0), 1(1), 2(2), 3(3), 4(4), 5(5), 6(6), 7(7)
    Dscp (Dscp): 8(8), 9(9), 10(10), 11(11), 12(12), 13(13), 14(14), 15(15)
    Dscp (Dscp): 16(16), 17(17), 18(18), 19(19), 20(20), 21(21), 22(22), 23(23)
    Dscp (Dscp): 24(24), 25(25), 26(26), 27(27), 28(28), 29(29), 30(30), 31(31)
    Dscp (Dscp): 32(32), 33(33), 34(34), 35(35), 36(36), 37(37), 38(38), 39(39)
    Dscp (Dscp): 40(40), 41(41), 42(42), 43(43), 44(44), 45(45), 46(46), 47(47)
        Dscp (Dscp): 48(48), 49(49), 50(50), 51(51), 52(52), 53(53), 54(54), 55(55)
      Dscp (Dscp): 56(56), 57(57), 58(58), 59(59), 60(60), 61(61), 62(62), 63(63)
   Queue-id: 2
      Tail-Drop Algorithm: Enabled
      Min-threshold: 60
      Max-threshold: 60
```

L3 Interface

Do the following to configure tail drop on an L3 interface.

#configure terminal	Enter configure mode.
(config)#mls qos enable	Enable the QOS globally
(config)#interface xe2	Enter interface mode.
(config-if)#ip address 10.1.1.2/24	Configure ip address on interface xe2.
(config-if)#exit	Exit the xe1 interface mode.

Tail-Drop Configuration

(config)#interface xe3	Enter interface mode.
(config-if)#ip address 20.1.1.2/24	Configure ip address on interface xe3.
(config-if)#exit	Exit the xe1 interface mode.
(config)#interface xe3	Enter xe2 interface
(config-if)# tail-drop queue-id 3 threshold 70	Configure tail drop on the egress interface
(config-if)#exit	Exit out of interface mode

Validation

Enter the commands below to confirm the configurations. #

```
show mls qos interface xe3

Trust Mode: Trust the VLAN Tag Priority
  Port Default CoS Prioiry: 0
  Port Default DSCP value : 0
  VLAN Priority Overide: Not Configured
  Egress Traffic Shaping: Not Configured
  Schedule mode: Strict Queues: 0 1 2 3 4 5 6 7
     The number of COS Values mapped: 8
    Cos (Queue): 0(0), 1(1), 2(2), 3(3), 4(4), 5(5), 6(6), 7(7)
    Cos (Cos): 0(0), 1(1), 2(2), 3(3), 4(4), 5(5), 6(6), 7(7)
    Exp (Queue): 0(0), 1(0), 2(0), 3(0), 4(0), 5(0), 6(0), 7(0)
    Exp (Exp): 0(0), 1(0), 2(0), 3(0), 4(0), 5(0), 6(0), 7(0)
    Dscp (Queue): 0(0), 1(0), 2(0), 3(0), 4(0), 5(0), 6(0), 7(0)
    Dscp (Queue): 8(1), 9(1), 10(1), 11(1), 12(1), 13(1), 14(1), 15(1)
    Dscp (Queue): 16(2), 17(2), 18(2), 19(2), 20(2), 21(2), 22(2), 23(2)
    Dscp (Queue): 24(3), 25(3), 26(3), 27(3), 28(3), 29(3), 30(3), 31(3)
    Dscp (Queue): 32(4), 33(4), 34(4), 35(4), 36(4), 37(4), 38(4), 39(4)
    Dscp (Queue): 40(5), 41(5), 42(5), 43(5), 44(5), 45(5), 46(5), 47(5)
    Dscp (Queue): 48(6), 49(6), 50(6), 51(6), 52(6), 53(6), 54(6), 55(6)
    Dscp (Queue): 56(7), 57(7), 58(7), 59(7), 60(7), 61(7), 62(7), 63(7)
    Dscp (Dscp): 0(0), 1(1), 2(2), 3(3), 4(4), 5(5), 6(6), 7(7)
    Dscp (Dscp): 8(8), 9(9), 10(10), 11(11), 12(12), 13(13), 14(14), 15(15)
    Dscp (Dscp): 16(16), 17(17), 18(18), 19(19), 20(20), 21(21), 22(22), 23(23)
```

```
    Dscp (Dscp): 24(24), 25(25), 26(26), 27(27), 28(28), 29(29), 30(30), 31(31)
    Dscp (Dscp): 32(32), 33(33), 34(34), 35(35), 36(36), 37(37), 38(38), 39(39)
    Dscp (Dscp): 40(40), 41(41), 42(42), 43(43), 44(44), 45(45), 46(46), 47(47)
    Dscp (Dscp): 48(48), 49(49), 50(50), 51(51), 52(52), 53(53), 54(54), 55(55)
Dscp (Dscp): 56(56), 57(57), 58(58), 59(59), 60(60), 61(61), 62(62), 63(63)
Queue-id: 3
      Tail-Drop Algorithm: Enabled
      Min-threshold: 70
      Max-threshold: 70
```

Tail-Drop Configuration

CHAPTER 7 WRED Configuration

This chapter contains a complete sample of configuring WRED.

Topology

Figure 7-218: Simple configuration of WRED

L2 Interface

Do the following to configure WRED on an L2 interface.

`#configure terminal`	Enter configure mode.
`(config)#mls qos enable`	Enable the QOS globally
`(config)#bridge 1 protocol rstp vlan- bridge`	Configure bridge 1 as RSTP-VLAN aware.
`(config)#vlan 2-6 bridge 1`	Configure vlans
`(config)#interface xe2`	Enter interface mode.
`(config-if)#switchport`	Configure xe2 as a layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.
`(config-if)#switchport mode trunk`	Configure port as a trunk.
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe1 interface.
`(config-if)#exit`	Exit the xe1 interface mode.
`(config)#interface xe3`	Enter interface mode.
`(config-if)#switchport`	Configure xe1 as a layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.
`(config-if)#switchport mode trunk`	Configure port as a trunk.
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe1 interface.

(config-if)#exit	Exit the xe1 interface mode.
(config)#interface xe3	Enter xe2 interface
(config-if)# wrr-queue random-detect queue-id 2	Configure WRED on the egress interface
min-threshold 50 max-threshold 70 exp-weight 1	
(config-if)#exit	Exit out of interface mode

WRED Configuration

Validation

Enter the commands below to confirm the configurations. #show mls qos interface xe3

```
  Trust Mode: Trust the VLAN Tag Priority
  Port Default CoS Prioiry: 0
  Port Default DSCP value : 0
  VLAN Priority Overide: Not Configured
  Egress Traffic Shaping: Not Configured
  Schedule mode: Strict Queues: 0 1 2 3 4 5 6 7
     The number of COS Values mapped: 8
    Cos (Queue): 0(0), 1(1), 2(2), 3(3), 4(4), 5(5), 6(6), 7(7)
    Cos (Cos): 0(0), 1(1), 2(2), 3(3), 4(4), 5(5), 6(6), 7(7)
    Exp (Queue): 0(0), 1(0), 2(0), 3(0), 4(0), 5(0), 6(0), 7(0)
    Exp (Exp): 0(0), 1(0), 2(0), 3(0), 4(0), 5(0), 6(0), 7(0)
    Dscp (Queue): 0(0), 1(0), 2(0), 3(0), 4(0), 5(0), 6(0), 7(0)
    Dscp (Queue): 8(1), 9(1), 10(1), 11(1), 12(1), 13(1), 14(1), 15(1)
    Dscp (Queue): 16(2), 17(2), 18(2), 19(2), 20(2), 21(2), 22(2), 23(2)
    Dscp (Queue): 24(3), 25(3), 26(3), 27(3), 28(3), 29(3), 30(3), 31(3)
    Dscp (Queue): 32(4), 33(4), 34(4), 35(4), 36(4), 37(4), 38(4), 39(4)
    Dscp (Queue): 40(5), 41(5), 42(5), 43(5), 44(5), 45(5), 46(5), 47(5)
    Dscp (Queue): 48(6), 49(6), 50(6), 51(6), 52(6), 53(6), 54(6), 55(6)
    Dscp (Queue): 56(7), 57(7), 58(7), 59(7), 60(7), 61(7), 62(7), 63(7)
    Dscp (Dscp): 0(0), 1(1), 2(2), 3(3), 4(4), 5(5), 6(6), 7(7)
    Dscp (Dscp): 8(8), 9(9), 10(10), 11(11), 12(12), 13(13), 14(14), 15(15)
    Dscp (Dscp): 16(16), 17(17), 18(18), 19(19), 20(20), 21(21), 22(22), 23(23)
    Dscp (Dscp): 24(24), 25(25), 26(26), 27(27), 28(28), 29(29), 30(30), 31(31)
    Dscp (Dscp): 32(32), 33(33), 34(34), 35(35), 36(36), 37(37), 38(38), 39(39)
    Dscp (Dscp): 40(40), 41(41), 42(42), 43(43), 44(44), 45(45), 46(46), 47(47)
        Dscp (Dscp): 48(48), 49(49), 50(50), 51(51), 52(52), 53(53), 54(54), 55(55)
      Dscp (Dscp): 56(56), 57(57), 58(58), 59(59), 60(60), 61(61), 62(62), 63(63)
   Queue-id: 2
      Random-detect Algorithm: Enabled
      Min-threshold: 50
      Max-threshold: 70
      Gain: 1        Color:
blind
```

L3 Interface

Do the following to configure WRED on an L3 interface.

#configure terminal	Enter configure mode.
(config)#mls qos enable	Enable the QOS globally
(config)#interface xe2	Enter interface mode.
(config-if)#ip address 10.1.1.2/24	Configure ip address on interface xe2.

WRED Configuration

(config-if)#exit	Exit the xe1 interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#ip address 20.1.1.2/24	Configure ip address on interface xe3.
(config-if)#exit	Exit the xe1 interface mode.
(config)#interface xe3	Enter xe2 interface
(config-if)# wrr-queue random-detect queue-id 4 min-threshold 60 max-threshold 80 exp-weight 1	Configure WRED on the egress interface
(config-if)#exit	Exit out of interface mode

Validation

Enter the commands below to confirm the configurations.

```
#show mls qos interface xe3

Trust Mode: Trust the VLAN Tag Priority
  Port Default CoS Prioiry: 0
  Port Default DSCP value : 0
  VLAN Priority Overide: Not Configured
  Egress Traffic Shaping: Not Configured
  Schedule mode: Strict Queues: 0 1 2 3 4 5 6 7
     The number of COS Values mapped: 8
    Cos (Queue): 0(0), 1(1), 2(2), 3(3), 4(4), 5(5), 6(6), 7(7)
    Cos (Cos): 0(0), 1(1), 2(2), 3(3), 4(4), 5(5), 6(6), 7(7)
    Exp (Queue): 0(0), 1(0), 2(0), 3(0), 4(0), 5(0), 6(0), 7(0)
    Exp (Exp): 0(0), 1(0), 2(0), 3(0), 4(0), 5(0), 6(0), 7(0)
    Dscp (Queue): 0(0), 1(0), 2(0), 3(0), 4(0), 5(0), 6(0), 7(0)
    Dscp (Queue): 8(1), 9(1), 10(1), 11(1), 12(1), 13(1), 14(1), 15(1)
    Dscp (Queue): 16(2), 17(2), 18(2), 19(2), 20(2), 21(2), 22(2), 23(2)
    Dscp (Queue): 24(3), 25(3), 26(3), 27(3), 28(3), 29(3), 30(3), 31(3)
    Dscp (Queue): 32(4), 33(4), 34(4), 35(4), 36(4), 37(4), 38(4), 39(4)
    Dscp (Queue): 40(5), 41(5), 42(5), 43(5), 44(5), 45(5), 46(5), 47(5)
    Dscp (Queue): 48(6), 49(6), 50(6), 51(6), 52(6), 53(6), 54(6), 55(6)
```

```
    Dscp (Queue): 56(7), 57(7), 58(7), 59(7), 60(7), 61(7), 62(7), 63(7)
    Dscp (Dscp): 0(0), 1(1), 2(2), 3(3), 4(4), 5(5), 6(6), 7(7)
    Dscp (Dscp): 8(8), 9(9), 10(10), 11(11), 12(12), 13(13), 14(14), 15(15)
    Dscp (Dscp): 16(16), 17(17), 18(18), 19(19), 20(20), 21(21), 22(22), 23(23)
    Dscp (Dscp): 24(24), 25(25), 26(26), 27(27), 28(28), 29(29), 30(30), 31(31)
    Dscp (Dscp): 32(32), 33(33), 34(34), 35(35), 36(36), 37(37), 38(38), 39(39)
    Dscp (Dscp): 40(40), 41(41), 42(42), 43(43), 44(44), 45(45), 46(46), 47(47)
    Dscp (Dscp): 48(48), 49(49), 50(50), 51(51), 52(52), 53(53), 54(54), 55(55)
Dscp (Dscp): 56(56), 57(57), 58(58), 59(59), 60(60), 61(61), 62(62), 63(63)
Queue-id: 4
      Random-detect Algorithm: Enabled
      Min-threshold: 60
      Max-threshold: 80
      Gain: 1
```

WRED Configuration

```
      Color: blind
```

Quality of Service Command Reference (Helix4)

Contents

This document contains these chapters and appendices:

- Chapter 1, *Quality of Service Commands*

© Symanitron

Quality of Service Command Reference (Helix4)

CHAPTER 1 Quality of Service Commands

This chapter is a reference for the Quality of Service (QoS) commands for the Helix4 platform.

- class
- class-map name
- clear mls qos cosq-stat
- ip-access-list (extended named)
- ip-access-list (extended numbered)
- ip-access-list (standard named)
- ip-access-list (standard numbered)
- ip6-access-list (extended named)
- ip6-access-list (extended numbered)
- ip6-access-list (standard named)
- ip6-access-list (standard numbered)
- mac-access-list
- match access-group
- match cos
- match cos inner
- match ethertype
- match ip-dscp
- match ip6-dscp
- match ip-precedence
- match ip6-precedence
- match layer4
- match layer4-range
- match vlan
- match vlan inner
- match vlan-range
- mls qos aggregate-police
- mls qos cos
- mls qos cos-cos
- mls qos cos-queue
- mls qos dscp
- mls qos dscp-dscp
- mls qos dscp-queue • mls qos enable
- mls qos strict-queue
- mls qos trust

- mls qos wrr-weight
- mls qos wrr-weight
- mode
- police
- police-aggregate
- policy-map
- service-policy input
- set cos
- set ip-dscp
- set ip6-dscp
- set ip-precedence
- set ip6-precedence
- set mirror-to-port
- set redirect-to-port
- set vlan
- show class-map name
- show mls qos
- show mls qos aggregate-policer
- show mls qos cosq-stat
- show mls qos interface
- show policy-map name
- show qos-access-list
- strict-queue
- tail-drop threshold
- traffic-shape rate
- wrr-queue queue-id
- wrr-queue random-detect

class

Use this command to enter Policy-class-map mode and create or change a traffic classification for a policy to act upon.

Use the `no` parameter with this command to delete an existing class.

Command Syntax

```
class NAME no
class NAME
```

Parameter

`NAME`	Name of the class to create or change

Default

No default value is specified

Command Mode

Policy-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example creates a policy map and defines the traffic classification.

```
#configure terminal
(config)#policy-map pmap1
(config-pmap)#class cmap1
(config-pmap-c)#
```

class-map name

Use this command to enter class map configuration mode and create or change a class map to use for matching packets to a specified class.

Note: Enable QoS globally before giving this command (see mls qos enable).

Use the `no` parameter with this command to delete an existing class map.

Command Syntax `class-map`

```
NAME no class-map NAME
```

Parameter

`NAME`	Name of the class map.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following example creates a class map.

```
#configure terminal
(config)#class-map cmap1
(config-cmap)#
```

clear mls qos cosq-stat

Use this command to clear CoS queue statistics.

Note: Enable QoS globally before giving this command (see mls qos enable).

Command Syntax `clear mls qos cosq-stats IFNAME ((mcqueue <0-3>) | <0-7> | all )`

Parameter

`IFNAME`	Interface name.
`<0-7>`	Queue identifier.
`all`	All queues.
`mcqueue`	Multicast cos-queue

Command Mode

Privileged, exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear mls qos cosq-stats eth3 all
```

ip-access-list (extended named)

Use this command to create an extended named IPv4 access-control list (ACL).

Note: Enable QoS globally before giving this command (see mls qos enable).

Use the `no` parameter with this command to delete an ACL.

Command Syntax

```
ip-access-list extended NAME (deny|permit) (ip-in-
  ip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) A.B.C.D
  A.B.C.D A.B.C.D A.B.C.D ip-access-list extended NAME (deny|permit) (ip-
inip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) A.B.C.D A.B.C.D any

ip-access-list extended NAME (deny|permit) (ip-
  inip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) any A.B.C.D A.B.C.D

ip-access-list extended NAME (deny|permit) (ip-
  inip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) any any

ip-access-list extended NAME (deny|permit) (ip-in-
  ip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) A.B.C.D A.B.C.D
  host A.B.C.D ip-access-list extended NAME (deny|permit)
(ip-in-

  ip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) host A.B.C.D
  A.B.C.D A.B.C.D ip-access-list extended NAME (deny|permit)
(ip-in-

  ip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) host A.B.C.D host
```

A.B.C.D ip-access-list extended NAME (deny|permit) (ip-inip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) any host A.B.C.D

ip-access-list extended NAME (deny|permit) (ip-in-ip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) host A.B.C.D any

no ip-access-list extended NAME (deny|permit) (ip-in-ip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) A.B.C.D A.B.C.D A.B.C.D A.B.C.D no ip-access-list extended NAME (deny|permit) (ip-inip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) A.B.C.D A.B.C.D any

no ip-access-list extended NAME (deny|permit) (ip-inip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) any A.B.C.D A.B.C.D

no ip-access-list extended NAME (deny|permit) (ip-inip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) any any

no ip-access-list extended NAME (deny|permit) (ip-in-ip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) A.B.C.D A.B.C.D host A.B.C.D no ip-access-list extended NAME (deny|permit) (ip-in-

ip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) host A.B.C.D A.B.C.D A.B.C.D

no ip-access-list extended NAME (deny|permit) (ip-in-ip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) host A.B.C.D host A.B.C.D no ip-access-list extended NAME (deny|permit) (ip-inip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) any host A.B.C.D

no ip-access-list extended NAME (deny|permit) (ip-inip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) host A.B.C.D any

no ip-access-list extended NAME (deny|permit) (ip-in-ip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) A.B.C.D A.B.C.D A.B.C.D A.B.C.D no ip-access-list extended NAME (deny|permit) (ip-inip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) A.B.C.D A.B.C.D any

no ip-access-list extended NAME (deny|permit) (ip-inip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) any A.B.C.D A.B.C.D

no ip-access-list extended NAME (deny|permit) (ip-inip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) any any

no ip-access-list extended NAME (deny|permit) (ip-in-ip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) A.B.C.D A.B.C.D host A.B.C.D no ip-access-list extended NAME (deny|permit) (ip-in-

ip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) host A.B.C.D A.B.C.D A.B.C.D

Parameters

NAME	ACL name
deny	Deny traffic if conditions match.
permit	Permit traffic if conditions match.
ip-in-ip	Any IPv4 encapsulation packet
udp	UDP packet

tcp	TCP packet
gre	GRE packet
igmp	IGMP packet
pim	PIM packet
rsvp	RSVP packet
ospf	OSPF packet
vrrp	VRRP packet
ipcomp	IPPayload Compression packet
any	Any protocol packet
<0-255>	IANA-assigned protocol number
A.B.C.D	Source address.
A.B.C.D	Source wildcard mask.
A.B.C.D	Destination address.
A.B.C.D	Destination wildcard mask.
any	Any source or destination host.
host	A single source or destination host.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following shows allowing access only for hosts on a specified network.

```
#configure terminal
(config)#ip-access-list extended ACL2 permit ip-in-ip 192.5.255.0 0.0.0.255 any
```

ip-access-list (extended numbered)

Use this command to create an extended numbered IPv4 access-control list (ACL).

Note: Enable QoS globally before giving this command (see mls qos enable).

Use the `no` parameter with this command to delete an ACL.

Command Syntax

```
ip-access-list (<100-199>|<2000-2699>) (deny|permit) (ip-
  inip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) A.B.C.D A.B.C.D any

ip-access-list (<100-199>|<2000-2699>) (deny|permit) (ip-in-
  ip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) A.B.C.D A.B.C.D
  A.B.C.D A.B.C.D ip-access-list (<100-199>|<2000-2699>) (deny|permit) (ip-
inip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) any host A.B.C.D

ip-access-list (<100-199>|<2000-2699>) (deny|permit) (ip-
  inip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) any any

ip-access-list (<100-199>|<2000-2699>) (deny|permit) (ip-
  inip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) any A.B.C.D A.B.C.D

ip-access-list (<100-199>|<2000-2699>) (deny|permit) (ip-in-
  ip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) host A.B.C.D
  A.B.C.D A.B.C.D ip-access-list (<100-199>|<2000-2699>) (deny|permit)
(ip-in-

  ip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) host A.B.C.D
  host A.B.C.D ip-access-list (<100-199>|<2000-2699>) (deny|permit) (ip-
inip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) host A.B.C.D any

ip-access-list (<100-199>|<2000-2699>) (deny|permit) (ip-in-
  ip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) A.B.C.D A.B.C.D
  host A.B.C.D no ip-access-list (<100-199>|<2000-2699>) (deny|permit) (ip-
inip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) A.B.C.D A.B.C.D any

no ip-access-list (<100-199>|<2000-2699>) (deny|permit) (ip-in-
  ip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) A.B.C.D
  A.B.C.D A.B.C.D A.B.C.D no ip-access-list (<100-199>|<2000-2699>)
(deny|permit) (ip-in-

  ip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) A.B.C.D A.B.C.D
  host A.B.C.D no ip-access-list (<100-199>|<2000-2699>) (deny|permit) (ip-
inip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) any any

no ip-access-list (<100-199>|<2000-2699>) (deny|permit) (ip-
  inip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) any host A.B.C.D

no ip-access-list (<100-199>|<2000-2699>) (deny|permit) (ip-in-
  ip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) any A.B.C.D A.B.C.D
no ip-access-list (<100-199>|<2000-2699>) (deny|permit) (ip-in-
      ip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) host A.B.C.D A.B.C.D
  A.B.C.D  no  ip-access-list  (<100-199>|<2000-2699>)  (deny|permit)
(ip-in-
```

```
  ip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) host A.B.C.D
  host A.B.C.D no ip-access-list (<100-199>|<2000-2699>) (deny|permit)
(ip-in-
  ip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>)   host   A.B.C.D   any
```

Parameters

<100-199>	ACL number.
<2000-2699>	ACL number.
deny	Deny traffic if conditions match.
permit	Permit traffic if conditions match.
ip-in-ip	Any IPv4 encapsulation packet
udp	UDP packet
tcp	TCP packet
gre	GRE packet
igmp	IGMP packet
pim	PIM packet
rsvp	RSVP packet
ospf	OSPF packet
vrrp	VRRP packet
ipcomp	IP Payload Compression packet
any	Any protocol packet
<0-255>	IANA-assigned protocol number
A.B.C.D	Source address.
A.B.C.D	Source wildcard mask.
A.B.C.D	Destination address.
A.B.C.D	Destination wildcard mask.
any	Any source or destination host.
host	A single source or destination host.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
            (config)#ip-access-list 100 permit ip-in-ip 192.5.255.0 0.0.0.255 any
```

ip-access-list (standard named)

Use this command to create a standard named IPv4 access-control list (ACL).

Note: Enable QoS globally before giving this command (see mls qos enable).

Use the `no` parameter with this command to delete an ACL.

Command Syntax

The following syntax creates an IP ACL based on the source address:

```
ip-access-list standard NAME (deny|permit) A.B.C.D ip-access-list
standard NAME (deny|permit) A.B.C.D A.B.C.D ip-access-list standard
NAME (deny|permit) any no ip-access-list standard NAME (deny|permit)
A.B.C.D no ip-access-list standard NAME (deny|permit) A.B.C.D A.B.C.D
no ip-access-list standard NAME (deny|permit) any
```

Parameters

`NAME`	ACL name
`deny`	Deny traffic if conditions match.
`permit`	Permit traffic if conditions match.
`A.B.C.D`	Source address.
`A.B.C.D`	Source wildcard mask.
`any`	Any source host.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip-access-list standard ACL1 permit 192.5.255.0 0.0.0.255
(config)#ip-access-list standard ACL1 permit 128.88.0.0 0.0.255.255
(config)#ip-access-list standard ACL1 permit 36.0.0.0 0.0.0.255
```

ip-access-list (standard numbered)

Use this command to create a standard numbered IPv4 access-control list (ACL).

Note: Enable QoS globally before giving this command (see mls qos enable).

Use the `no` parameter with this command to delete an ACL.

Command Syntax `ip-access-list (<1-99>|<1300-1999>) (deny|permit) A.B.C.D ip-access-list (<1-99>|<1300-1999>) (deny|permit) A.B.C.D A.B.C.D ip-access-list (<1-99>|<1300-1999>) (deny|permit) any no ip-access-list (<1-99>|<1300-1999>) (deny|permit) A.B.C.D no ip-access-list (<1-99>|<1300-1999>) (deny|permit) A.B.C.D A.B.C.D no ip-access-list (<1-99>|<1300-1999>) (deny|permit) any`

Parameters

`<1-99>`	ACL number.
`<1300-1999>`	ACL number.
`deny`	Deny traffic if conditions match.
`permit`	Permit traffic if conditions match.
`A.B.C.D`	Source address.
`A.B.C.D`	Source wildcard mask.
`any`	Any source host.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip-access-list 1 permit 192.5.255.0 0.0.0.255
(config)#ip-access-list 1 permit 128.88.0.0 0.0.255.255
(config)#ip-access-list 1 permit 36.0.0.0 0.0.0.255
```

ip6-access-list (extended named)

Use this command to create an extended named IPv6 access-control list (ACL).

Note: Enable QoS globally before giving this command (see mls qos enable).

Use the `no` parameter with this command to delete an ACL.

Command Syntax

```
ip6-access-list extended (NAME) (deny|permit) (ip-in-
      ip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) (X:X::X:X/M|host
  X:X::X:X|any) (X:X::X:X/M|host X:X::X:X|any) no ip6-
access-list extended (NAME) (deny|permit) (ip-in-
  ip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) (X:X::X:X/M|host
  X:X::X:X|any) (X:X::X:X/M|host X:X::X:X|any)
```

Parameters

NAME	ACL name
deny	Deny traffic if conditions match.
permit	Permit traffic if conditions match.
ip-in-ip	Any IPv4 encapsulation packet
udp	UDP packet
tcp	TCP packet
gre	GRE packet
igmp	IGMP packet
pim	PIM packet
rsvp	RSVP packet
ospf	OSPF packet
vrrp	VRRP packet
ipcomp	IP Payload Compression packet
any	Any protocol packet
<0-255>	IANA-assigned protocol number
X:X::X:X/M	Source or destination address and mask.
host	A single source or destination host.
X:X::X:X	Host address.
any	Any source or destination host.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
                        (config)#ip6-access-list extended ACL4 permit ip-in-ip
2001:db8:1::ab9:C0A8:102/92
```

ip6-access-list (extended numbered)

Use this command to create an extended numbered IPv6 access-control list (ACL).

Note: Enable QoS globally before giving this command (see mls qos enable).

Use the `no` parameter with this command to delete an ACL.

Command Syntax

```
ip6-access-list (<100-199>|<2000-2699>) (deny|permit) (ip-in-
      ip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) (X:X::X:X/M|host
  X:X::X:X|any) (X:X::X:X/M|host X:X::X:X|any) no ip6-access-list
(<100-199>|<2000-2699>) (deny|permit) (ip-in-

  ip|udp|tcp|gre|igmp|pim|rsvp|ospf|vrrp|ipcomp|any|<0-255>) (X:X::X:X/M|host
  X:X::X:X|any) (X:X::X:X/M|host X:X::X:X|any)
```

Parameters

`<100-199>`	ACL number.
`<2000-2699>`	ACL number.
`deny`	Deny traffic if conditions match.
`permit`	Permit traffic if conditions match.
`ip`	Any IPv6 encapsulation packet
`udp`	UDP packet
`tcp`	TCP packet
`gre`	GRE packet
`igmp`	IGMP packet
`pim`	PIM packet
`rsvp`	RSVP packet
`ospf`	OSPF packet
`vrrp`	VRRP packet
`ipcomp`	IP Payload Compression packet
`any`	Any protocol packet
`<0-255>`	IANA-assigned protocol number
`X:X::X:X/M`	Source or destination address and mask.
`host`	A single source or destination host.
`X:X::X:X`	Host address.
`any`	Any source or destination host.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip6-access-list 122 permit
2001:0db8:85a3::8a2e:0370:7334/124 2001:db8:1::ab9:C0A8:102/124
```

ip6-access-list (standard named)

Use this command to create a standard named IPv6 access-control list (ACL).

Note: Enable QoS globally before giving this command (see mls qos enable).

Use the `no` parameter with this command to delete an ACL.

Command Syntax `ip6-access-list standard (NAME) (deny|permit) (X:X::X:X/M|host X:X::X:X|any)` `no ip6-access-list standard (NAME) (deny|permit) (X:X::X:X/M|host X:X::X:X|any)` **Parameters**

`NAME`	ACL name
`deny`	Deny traffic if conditions match.
`permit`	Permit traffic if conditions match.
`X:X::X:X/M`	Source address and mask.
`host`	A single source host.
`X:X::X:X`	Host address.
`any`	Any source host.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
  (config)#ip6-access-list standard ACL3 permit 2001:db8:1::ab9:C0A8:102/92
```

ip6-access-list (standard numbered)

Use this command to create a standard numbered IPv6 access-control list (ACL).

Note: Enable QoS globally before giving this command (see mls qos enable).

Use the `no` parameter with this command to delete an ACL.

Command Syntax `ip6-access-list (<1-99>|<1300-1999>) (deny|permit) (X:X::X:X/M|host X:X::X:X|any)`

`no ip6-access-list (<1-99>|<1300-1999>) (deny|permit) (X:X::X:X/M|host X:X::X:X|any)`

Parameters

`<1-99>`	ACL number.
`<1300-1999>`	ACL number.

deny	Deny traffic if conditions match.
permit	Permit traffic if conditions match.
X:X::X:X/M	Source address and mask.
host	A single source host.
X:X::X:X	Host address.
any	Any source host.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip6-access-list 57 permit 2001:0db8:85a3::8a2e:0370:7334/64
```

mac-access-list

Use this command to create an access-control list (ACL) based on a media access control (MAC) address.

Note: Enable QoS globally before giving this command (see mls qos enable).

Use the no parameter with this command to delete a MAC ACL.

Command Syntax

This form creates a MAC ACL for any source and a destination specified by the MAC and MASK parameters: mac-

```
access-list <2000-2699> (deny|permit) any MAC MASK <1-8>
```

This form creates a MAC ACL for a source specified by the MAC and MASK parameters and any destination: mac-

```
access-list <2000-2699> (deny|permit) MAC MASK any <1-8>
```

This form creates a MAC ACL for a source specified by the first MAC and MASK parameters and a destination specified by the second MAC and MASK parameters:

```
mac-access-list <2000-2699> (deny|permit) MAC MASK MAC MASK <1-8>
```

The no forms below correspond to the forms above:

```
    no mac-access-list <2000-2699> (deny|permit) any MAC MASK <1-8>
no mac-access-list <2000-2699> (deny|permit) MAC MASK any <1-8> no
mac-access-list <2000-2699> (deny|permit) MAC MASK MAC MASK <1-8>
```

Parameters

<2000-2699>	ACL number.
deny	Deny certain traffic if conditions match.
permit	Permit certain traffic if conditions match.
any	Any source or destination.

MAC	MAC address in HHHH.HHHH.HHHH format.
MASK	Part of the MAC address to ignore in hexadecimal format.
<1-8>	Packet format:
1	Ethernet II
2	802.3
4	SNAP
8	LLC

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
                    (config)#mac-access-list 2002 permit 2222.2222.2222 8 any 2
```

match access-group

Use this command to define a match criterion based on an access control list (ACL).

Use the `no` parameter with this command to remove an ACL match criterion.

Command Syntax `match access-group (<1-199>|<1300-2699>|WORD) no match access-group NAME`

Parameters

`<1-199>`	ACL number
`<1300-2699>`	ACL number
`WORD`	ACL name

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows configuring a class map named cmap1 with one match criterion: access list 103, which allows traffic from any source to any destination.

```
#configure terminal
(config)#ip-access-list 103 permit ip-in-ip any any
(config)#class-map cmap1
(config-cmap)#match access-group 103
```

match cos

Use this command to define a match criterion based on class of service (CoS) values.

Use the `no` parameter with this command to remove a CoS match criterion.

Command Syntax

```
match cos (<0-7>|<0-7> <0-7>|<0-7> <0-7> <0-7>|<0-7> <0-7> <0-7> <0-7>|<0-7> <0-7>
  <0-7> <0-7> <0-7>|<0-7> <0-7> <0-7> <0-7> <0-7> <0-7>| <0-7> <0-7> <0-7> <0-7>
  <0-7> <0-7> <0-7>|<0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7>) no match cos

((<0-7>|<0-7> <0-7>|<0-7> <0-7> <0-7>|<0-7> <0-7> <0-7> <0-7>|<0-7>

  <0-7> <0-7> <0-7> <0-7>|<0-7> <0-7> <0-7> <0-7> <0-7> <0-7>| <0-7> <0-7> <0-7>
  <07> <0-7> <0-7> <0-7>|<0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7>)|all)
```

Parameters

`<0-7>`	CoS values
`all`	Delete all matched cos values.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip-access-list 103 permit ip-in-ip any any
(config)#class-map cmap1
(config-cmap)#match cos 3 5 6
```

match cos inner

Use this command to define a match criterion based on class of service (CoS) values in the inner VLAN tag of a 802.1Q frame.

Use the `no` parameter with this command to remove a CoS match criterion.

Command Syntax

```
match cos inner (<0-7>|<0-7> <0-7>|<0-7> <0-7> <0-7>|<0-7> <0-7> <0-7>
<0-7>|<0-7> <0-7> <0-7> <0-7> <0-7>|<0-7> <0-7> <0-7> <0-7> <0-7> <0-7>|
<0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7>|<0-7> <0-7> <0-7> <0-7> <0-7>
<0-7> <0-7> <0-7>) no match cos inner ((<0-7>|<0-7> <0-7>|<0-7> <0-7> <0-
7>|<0-7> <0-7> <0-7> <07>|<0-7> <0-7>
<0-7> <0-7> <0-7>|<0-7> <0-7> <0-7> <0-7> <0-7> <0-7>| <0-7> <0-7> <0-7> <0-
  7> <0-7> <0-7> <0-7>|<0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-
```

7>)|all)

Parameters

<0-7>	CoS values
All	Delete all matched inner cos values

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#ip-access-list 103 permit ip-in-ip any any
(config)#class-map cmap1
(config-cmap)#match cos inner 2 6 7
```

match ethertype

Use this command to define a match criterion based on the EtherType.

Use the no parameter with this command to remove an EtherType match criterion.

Command Syntax match ethertype VALUE no match ethertype (VALUE|all)

Parameters

VALUE	EtherType in hexadecimal (range 0x0-0xffff)
all	Delete all matched EtherType

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal (config)#class-map cmap1
(config-cmap)#match ethertype 0x8100
```

match ip-dscp

Use this command to define a match criterion based on IPv4 differentiated service code point (DSCP) values.

Use the `no` parameter with this command to remove a DSCP match criterion.

Command Syntax

```
match ip-dscp (<0-63>|<0-63> <0-63>|<0-63> <0-63> <0-63>|<0-63> <0-63> <0-63> <0-
  63>|<0-63> <0-63> <0-63> <0-63> <0-63>|<0-63> <0-63><0-63> <0-63> <0-63> <063>|<0-63>
  <0-63> <0-63> <0-63> <0-63> <0-63> <0-63>|<0-63> <0-63> <0-63> <0-63> <0-63> <0-63>
  <0-63> <0-63>) no match ip-dscp ((<0-63>|<0-63> <0-63>|<0-63> <0-
63> <0-63>|<0-63> <0-63> <0-63>
  <0-63>|<0-63> <0-63> <0-63> <0-63> <0-63>|<0-63> <0-63> <0-63> <0-63> <0-63>
  <063>|<0-63> <0-63> <0-63> <0-63> <0-63> <0-63> <0-63>|<0-63> <0-63> <0-63>
  <0-63> <0-63> <0-63> <0-63> <0-63>)|all)
```

Parameter

`<0-63>`	One to eight DSCP values.
`all`	Delete all matched DSCP values.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following example shows configuring a class map named cmap1 with criterion that matches DSCP 56.

```
#configure terminal
(config)#class-map cmap1
(config-cmap)#match ip-dscp 56
```

match ip6-dscp

Use this command to define a match criterion based on IPv6 differentiated service code point (DSCP) values.

Use the `no` parameter with this command to remove a DSCP match criterion.

Command Syntax

```
match ip6-dscp (<0-63>|<0-63> <0-63>|<0-63> <0-63> <0-63>|<0-63> <0-63> <0-63> <0-
  63>|<0-63> <0-63> <0-63>    <0-63> <0-63>|<0-63> <0-63> <0-63> <0-63> <0-63> <0-
  <063>|<0-63> <0-63> <0-63>  63> <0-63> <0-63> <0-63>|<0-63> <0-63> <0-63> <0-
  63>
```

```
  <0-63> <0-63> <0-63> <0-63>) no match ip6-dscp ((<0-63>|<0-63> <0-63>|<0-63>
<0-63> <0-63>|<0-63> <0-63> <0-63> <0-63>|<0-63> <0-63> <0-63> <0-63> <0-
63>|<0-63> <0-63> <0-63> <0-63> <0-63> <063>|<0-63> <0-63> <0-63> <0-63> <0-63>
<0-63> <0-63>|<0-63> <0-63> <0-63> <0-63> <0-63> <0-63> <0-63> <0-63>)|all)
```

Parameter

<0-63>	One to eight DSCP values
all	Delete all matched IPv6 DSCP values

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following example shows configuring a class map named cmap1 with criterion that matches DSCP 43.

```
#configure terminal
(config)#class-map cmap1
(config-cmap)#match ip6-dscp 43
```

match ip-precedence

Use this command to define a match criterion based on IPv4 precedence values.

Use the no parameter with this command to remove precedence match criterion.

Command Syntax

```
match ip-precedence (<0-7>|<0-7> <0-7>|<0-7> <0-7> <0-7>|<0-7> <0-7> <0-7> <0-7>|<0-
  7> <0-7> <0-7> <0-7> <0-7>|<0-7> <0-7> <0-7> <0-7><0-7> <0-7>|<0-7> <0-7> <0-7> <0-
  7> <0-7> <0-7> <0-7>|<0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7>)
no match ip-precedence ((<0-7>|<0-7> <0-7>|<0-7> <0-7> <0-7>|<0-7> <0-7> <0-7>
<07>|<0-7> <0-7> <0-7> <0-7> <0-7>|<0-7> <0-7> <0-7> <0-7> <0-7> <0-7>|<0-7>
<0-7>
  <0-7> <0-7> <0-7> <0-7> <0-7>|<0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <07>)|all)
```

Parameter

<0-7>	One to eight precedence values
all	Delete all matched IP precedence values.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following example shows configuring a class-map named cmap1 to evaluate IPv4 packets for precedence values 5, 6, 4, and 3.

```
#configure terminal
(config)#class-map cmap1
(config-cmap)#match ip-precedence 5 6 4 3
```

match ip6-precedence

Use this command to define a match criterion based on IPv6 precedence values.

Use the `no` parameter with this command to remove precedence match criterion.

Command Syntax

```
match ip6-precedence (<0-7>|<0-7> <0-7>|<0-7> <0-7> <0-7>|<0-7> <0-7> <0-7> <07>|<0-7>
  <0-7> <0-7> <0-7> <0-7>|<0-7> <0-7> <0-7> <0-7> <0-7> <0-7>|<0-7> <0-7> <0-7> <0-7>
  <0-7> <0-7> <0-7>|<0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7>) no
          match  ip6-precedence  ((<0-7>|<0-7>  <0-7>|<0-7>  <0-7>  <0-7>|<0-7>  <0-7>
           <0-7> <07>|<0-7> <0-7> <0-7> <0-7> <0-7>|<0-7> <0-7> <0-7> <0-7> <0-7> <0-
           7>|<0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7>|<0-7> <0-7> <0-7> <0-7> <0-7>
                                  <0-7> <0-7> <07>)|all)
```

Parameter

`<0-7>`	One to eight precedence values.
`all`	Delete all matched IPv6 precedence values.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following example shows configuring a class-map named cmap1 to evaluate IPv6 packets for precedence values of 5, 6, 4, and 3.

```
#configure terminal
(config)#class-map cmap1
(config-cmap)#match ip6-precedence 5 6 4 3
```

match layer4

Use this command to define a UDP or TCP port as a match criterion.

Use the `no` parameter with this command to remove a UDP or TCP port match criterion.

Command Syntax `match layer4 (tcp|udp|any) (source-port|destination-port) <1-65535> no match layer4 (((tcp|udp|any) (source-port|destination-port) <1-65535>)|all)`

Parameters

`tcp` TCP port. `udp` UDP port. `any` TCP or UDP port. `source-port` Source port. `destination-port` Destination port.

`<1-65535>` Port number. `all` Delete all matched Layer 4 entries.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#class-map cmap1
(config-cmap)#match layer4 any source-port 20
```

match layer4-range

Use this command to define a range of UDP or TCP port numbers as a match criterion.

Use the `no` parameter with this command to remove UDP or TCP port match criterion.

Command Syntax

```
match layer4-range (tcp|udp|any) (source-port|destination-port) <1-65535> to <1-65535> no match layer4-range (((tcp|udp|any) (source-port|destination-port) <1-65535> to <1-65535>)|all)
```

Parameters

`tcp` TCP port. `udp` UDP port. `any` TCP or UDP port. `source-port` Source port. `destination-port` Destination port. `<1-65535>` Starting and ending port number. `all` Delete all matched Layer 4 range values.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#class-map cmap1
(config-cmap)#match layer4 any source-port 20 to 50
```

match vlan

Use this command to define a VLAN identifier as a match criterion.

Use the `no` parameter with this command to remove a VLAN identifier as a match criterion.

Command Syntax `match vlan <1-3999> no match vlan (<1-3999>|all)`

Parameter

`<1-3999>` VLAN identifier. `all` Delete all matched VLAN-ids.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following example shows configuring a class-map named cmap1 to include traffic from VLAN 3.

```
#configure terminal
(config)#class-map cmap1
(config-cmap)#match vlan 3
```

match vlan inner

Use this command to define an VLAN identifier in the inner tag of a 802.1Q frame as a match criterion.

Use the `no` parameter with this command to remove a VLAN identifier as a match criterion.

Command Syntax `match vlan inner <1-3999> no match vlan inner (<1-3999>|all)`

Parameter

`<1-3999>` VLAN identifier. `all` Delete all matched inner VLAN-ids.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following example shows configuring a class-map named cmap1 to include traffic from VLAN 3.

```
#configure terminal
(config)#class-map cmap1
(config-cmap)#match vlan inner 3
```

match vlan-range

Use this command to specify a range of VLAN identifiers as a match criterion.

Use the `no` parameter with this command to remove a VLAN range as match criterion.

Command Syntax `match vlan-range <1-3999> to <1-3999> no match vlan-range ((<1-3999> to <1-3999>)|all)`

Parameters

`<1-3999>` Starting and ending VLAN identifier. `all`

Delete all VLAN range values.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows configuring a class map named cmap1 with criterion that matches IP DSCP 56, with a VLAN range of 20 to 30.

```
#configure terminal
(config)#class-map cmap1
(config-cmap)#match ip-dscp 56
(config-cmap)#match vlan-range 20 to 30
```

mls qos aggregate-police

Use this command to define policer parameters to apply to multiple traffic classes in a policy map.

Note: Enable QoS globally before giving this command (see mls qos enable).

Use the `no` parameter with this command to delete an aggregate policer.

Command Syntax `mls qos aggregate-police NAME <1-10000000>`

`<1-200000> no mls qos aggregate-police NAME`

Parameters

`NAME` Name of the aggregate policer.

`<1-10000000>` Average traffic rate in kilobits/second.

`<1-200000>` Normal burst size in kilobytes.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example designates a policer with parameters of a traffic rate of 48000 bps and a burst size of 8000 kbps.

```
#configure terminal
(config)#mls qos aggregate-police transmit1 48000 8000
(config)#no mls qos aggregate-police transmit1
```

mls qos cos

Use this command to set a default Class-of-Service (CoS) value for an interface with override for both tagged and untagged packets or without override for un-tagged packets only.

Note: Enable QoS globally before giving this command (see mls qos enable).

Use the `no` parameter with this command to un-set the default CoS value.

Command Syntax `mls qos cos <1-7>`

`(override | ) no mls qos cos <1-7>`

`(override | )`

Parameters

`<1-7>`	CoS value.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#mls qos cos 7 override
(config-if)#no mls qos cos 7 override
```

mls qos cos-cos

Use this command to map an incoming Class-of-Service (CoS) value to an outgoing CoS value.

Note: Enable QoS globally before giving this command (see mls qos enable).

Use the `no` parameter with this command to unmap an incoming CoS value.

Command Syntax `mls qos cos-cos <0-7> <0-7> no mls qos cos-cos <0-7>`

Parameters

<0-7>	Incoming CoS value.
<0-7>	Outgoing CoS value.

Default

No default value is specified

Command Mode

Configure, Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
        Enter configuration commands, one per line. End with CNTL/Z.

(config)#mls qos cos-cos 2 5
```

mls qos cos-queue

Use this command to set the Class of Service (CoS) value for a queue.

Note: Enable QoS globally before giving this command (see mls qos enable).

Use the `no` parameter with this command to set the CoS for a queue to its default value (the same as the queue identifier).

Command Syntax `mls qos cos-queue <0-7> <0-7> no mls qos cos-queue <0-7>`

Parameters

<0-7>	CoS value.
<0-7>	Queue identifier.

Default

No default value is specified

Command Mode

Configure, Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#mls qos cos-queue 2 4
```

mls qos dscp

Use this command to set a default differentiated services code point (DSCP) value.

Note: Enable QoS globally before giving this command (see mls qos enable).

Use the `no` parameter with this command to reset the default DSCP value to zero.

Command Syntax `mls qos dscp <0-63> no mls qos dscp`

Parameters

`<0-63>`	DSCP value.

Default

By default, DSCP value is 0

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#interface eth1
(config-if)#mls qos dscp 52
```

mls qos dscp-dscp

Use this command to map an incoming differentiated services code point (DSCP) value to an outgoing DSCP value.

Note: Enable QoS globally before giving this command (see mls qos enable).

Use the `no` parameter with this command to unmap an incoming DSCP value.

Command Syntax `mls qos dscp-dscp <0-63> <0-63> no mls qos dscp-dscp <0-63>`

Parameters

`<0-63>`	Incoming DSCP value.
`<0-63>`	Outgoing DSCP value.

Default

No default value is specified

Command Mode

Configure, Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
(config)#interface xe2
(config-if)#mls qos dscp-dscp 46 54
(config-if)#
```

mls qos dscp-queue

Use this command to set the DSCP value for a queue.

Note: Enable QoS globally before giving this command (see mls qos enable).

Use the `no` parameter with this command to set the DSCP value for a queue to its default.

Command Syntax `mls qos dscp-queue <0-63> <0-7> no mls qos dscp-queue <0-63>`

Parameters

`<0-63>`	DSCP value.
`<0-7>`	Queue identifier.

Default

No default value is specified

Command Mode

Configure and Interface modes

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#mls qos dscp-queue 55 2

(config)#interface eth1
(config-if)#mls qos dscp-queue 55 2
```

mls qos enable

Use this command to enable Quality-of-Service (QoS).

Command Syntax `mls qos enable no mls qos`

Parameters

None

Default

By default, the QoS is disabled

Command Mode

Configure

Applicability

This command was introduced before SWMRE version 1.3

Examples

```
#configure terminal
(config)#mls qos enable

(config)#no mls qos
```

mls qos strict-queue

Use this command to set queue in strict priority Use the no command to un-set strict priority.

Command Syntax `mls qos strict-queue <0-7> no mls qos strict-queue <0-7>`

Parameters

`<0-7>`	queue-id

Default

By default, strict priority is set for default queues.

Command Mode

Configure Mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#mls qos strict-queue 3
                        (config)#no mls qos strict-queue 3
```

```
(config)#
```

mls qos trust

Use this command to configure the trust state of a port and classify incoming packets with a DSCP or CoS value.

Note: Enable QoS globally before giving this command (see mls qos enable).

Use the `no` parameter with this command to make the port untrusted.

Command Syntax `mls qos trust (dscp | cos ) no mls qos trust (dscp | cos )`

Parameters

`dscp`	Classify incoming packets with DSCP values
`cos`	Classify incoming packets with CoS values.

Default

By default, QoS trust for Layer2 interface is trust CoS and for Layer3 interface is trust DSCP.

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface eth1
(config-if)#mls qos trust dscp
```

mls qos wrr-weight

Use this command to set the Weighted Round-Robin (WRR) value for a queue.

Note: Enable QoS globally before giving this command (see mls qos enable).

Use the `no` parameter with this command to reset the WRR value for a queue to its default.

Command Syntax `mls qos wrr-weight <0-7> <1-127> no mls qos wrr-weight <0-7>`

Parameters

`<0-7>`	Queue identifier.
`<1-127>`	Weighted round-robin value.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#mls qos wrr-weight 1 5
```

mode

Use this command to set the policy operating mode.

Note: Enable QoS globally before giving this command (see mls qos enable).

Use the `no` parameter with this command to reset the mode to its default. (allow).

Command Syntax `mode (allow | deny ) no mode (allow | deny )`

Parameters

`allow`	Accept flow traffic (default).
`deny`	Deny flow traffic.

Default

By default, policy operating mode is allow.

Command Mode

Policy-class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#policy-map pmap1
(config-pmap)#class cmap1
(config-pmap-c)#mode deny
```

police

Use this command to configure traffic policing.

Use the `no` parameter with this command to remove a traffic policing configuration.

Command Syntax

```
police (srtcm |(trtcm <1-10000000>)) <1-10000000> <1-200000> <1-200000>
  exceedaction (drop | (transmit violate-action (drop|remark-down|transmit)) |
```

```
((set-costransmit <0-7> | set-dscp-transmit <0-63> |  set-tos-transmit <0-7>)
violateaction (drop)))

no police (srtcm |(trtcm <1-10000000>)) <1-10000000> <1-200000> <1-200000>
(exceedaction (drop | (transmit violate-action (drop|remark-down)) | ((set-cos-
transmit
<0-7> | set-dscp-transmit <0-63> | set-tos-transmit <0-7>) violate-action
(drop))))
```

Parameters `srtcm` Single Rate Three Color Marker: classifies traffic into a group that conforms to the specified committed information rate (CIR) and burst sizes, and a group that exceeds either the CIR or the burst sizes.

`trtcm` Two-Rate Three-Color Marker: adds the ability to classify nonconforming traffic into a third group that *continually* violates the CIR.

`<1-10000000>` Peak information rate (PIR) in kilobits/second. `<1-10000000>` Committed information rate (CIR) in kilobits/second. `<1-200000>` Committed burst size (CBS) in kilobits. `<1-200000>`

Exceed or peak burst size (EBS/PBS) in kilobits.

`exceed-action` Action taken on packets that conform to the PIR but not the CIR.

`drop` Drop the frame. `set-cos-transmit`

Remark the frame to new COS value.

`<0-7>` New cos value. `set-dscp-transmit`

Remark the frame to a new differentiated services code point (DSCP) value.

`<0-63>` New DSCP value.

`set-tos-transmit`

Remark the frame to a new ToS value.

`<0-7>` New ToS value. `violate-action` Action taken on packets that continuously exceed the PIR. `drop` Drop the frame. `remark-down` Remark down the frame to DSCP value 0. `transmit` Specifies the action of transmitting packets.

Default

Exceed Sets the action to take when the data rate is exceeded. The default value is drop.

Violate Sets the action to take when the data rate violates the configured rate values. The default value is drop.

Command Mode

Policy-class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#policy-map pmap1
(config-pmap)#class cmap1
(config-pmap-c)#police srtcm 48000 45000 8000 exceed-action drop
```


© Symanitron Proprietary

police-aggregate

Use this command to apply an aggregate policer named in the mls qos aggregate-police command in a policy map.

Use the `no` parameter with this command to delete an aggregate policer from a policy map.

Command Syntax `police-aggregate NAME` `no police-aggregate NAME`

Parameter

`NAME`	Aggregate-policer name

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example creates an aggregate policer and attaches it to multiple classes in a policy map. The ACLs allow traffic from network 10.1.0.0 and host 11.3.1.1. The traffic rate from network 10.1.0.0 and host 11.3.1.1 is policed. If the traffic exceeds a 48,000-bps average traffic rate and a 8,000-byte normal burst size, it is considered out of profile and is dropped. The policy map is attached to an incoming interface.

```
#configure terminal
(config)#ip-access-list 1 permit 10.1.0.0 0.0.255.255
(config)#ip-access-list 2 permit 11.3.1.1
(config)#mls qos aggregate-police transmit1 48000 8000
(config)#class-map cmap1
(config-cmap)#match access-group 1
(config-cmap)#exit
(config)#class-map cmap2
(config-cmap)#match access-group 2
(config-cmap)#exit
(config)#policy-map pmap1
(config-pmap)#class cmap1
(config-pmap-c)#police-aggregate transmit1
(config-pmap-c)#exit
(config-pmap)#class cmap2
(config-pmap-c)#set ip-dscp 56
(config-pmap-c)#police-aggregate transmit1
```

```
(config-pmap-c)#exit
(config-pmap)#exit
(config)#interface fe0
(config-if)#service-policy input pmap1
```

policy-map

Use this command to create a policy map and enter Policy-map mode.

Note: Enable QoS globally before giving this command (see mls qos enable).

Use the `no` parameter with this command to delete a policy map.

Command Syntax `policy-map NAME no policy-map NAME`

Parameter

`NAME`	Name of the policy-map.

Default

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#policy-map pmap1
(config-pmap)#
```

service-policy input

Use this command to apply a policy map to the input of an interface.

Note: Enable QoS globally before giving this command (see mls qos enable).

Use the `no` parameter with this command to remove a policy map from an interface.

Command Syntax `service-policy input NAME no service-policy input NAME`

Parameters

`NAME`	Policy-map name.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface fe0
(config-if)#service-policy input pmap1
```

set cos

Use this command to set the Class-of-Service (CoS) value of outgoing packets.

Use the `no` parameter with this command to not set a CoS value.

Command Syntax `set cos(<0-7>) no set cos`

Parameters

`<0-7>`	CoS value.

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#policy-map pmap1
(config-pmap)#class cmap1 (config-pmap-c)#set cos 2
```

set ip-dscp

Use this command to set a differentiated services code point (DSCP) value to classify traffic.

Use the `no` parameter with this command to not set a DSCP value.

Command Syntax `set ip-dscp <0-63> no set ip-dscp`

Parameter

`<0-63>`	DSCP value.

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#policy-map pmap1
(config-pmap)#class cmap1
(config-pmap-c)#set ip-dscp 40
```

set ip6-dscp

Use this command to set a differentiated services code point (DSCP) value to classify traffic.

Use the `no` parameter with this command to not set a DSCP value.

Command Syntax `set ip6-dscp <0-63> no set ip6-dscp`

Parameter

`<0-63>`	DSCP value.

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#policy-map pmap1
(config-pmap)#class cmap1
(config-pmap-c)#set ip6-dscp 37
```

set ip-precedence

Use this command to set an IP precedence value to classify traffic.

Use the `no` parameter with this command to remove an IP precedence value.

Command Syntax `set ip-precedence <0-7> no set ip-precedence`

Parameter

`<0-7>` IP precedence value.

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#policy-map pmap1
(config-pmap)#class cmap1
(config-pmap-c)#set ip-precedence 2
(config-pmap-c)#no set ip-precedence
```

set ip6-precedence

Use this command to set an IP precedence value to classify traffic.

Use the `no` parameter with this command to remove an IP-precedence value.

Command Syntax `set ip6-precedence <0-7> no set ip6-precedence`

Parameter

`<0-7>` IP precedence value.

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
```

```
(config)#policy-map pmap1
(config-pmap)#class cmap1
(config-pmap-c)#set ip6-precedence 3
(config-pmap-c)#no set ip6-precedence
```

set mirror-to-port

Use this command to copy a packet to a different interface.

Use the `no` parameter with this command to not copy a packet to a different interface.

Command Syntax `set mirror-to-port IFNAME no set mirror-to-port`

Parameter

`IFNAME`	Interface name

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#policy-map pmap1
(config-pmap)#class cmap1
(config-pmap-c)#set mirror-to-port fe1
```

set redirect-to-port

Use this command to direct a packet to a different interface.

Use the `no` parameter with this command to not direct a packet to a different interface.

Command Syntax `set redirect-to-port IFNAME no set redirect-to-port`

Parameter

`IFNAME`	Interface name

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#policy-map pmap1
(config-pmap)#class cmap1
(config-pmap-c)#set redirect-to-port fe0
```

set vlan

Use this command to set a different VLAN identifier and optionally a Class-of-Service (CoS) value.

Use the `no` parameter with this command to not set a different VLAN identifier and CoS value.

Command Syntax `set vlan (<1-3999>|<1-3999> <0-7>) no`

```
set vlan
```

Parameter

`<1-3999>`	VLAN identifier
`<0-7>`	CoS value

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#policy-map pmap1
(config-pmap)#class cmap1
(config-pmap-c)#set vlan 2031 5
```

show class-map name

Use this command to display the Quality-of-Service (QoS) class maps that define the match criteria for classifying traffic.

Note: Enable QoS globally before giving this command (see mls qos enable).

Command Syntax `show class-map`

`( NAME |)`

Parameter

`NAME`	Name of the class-map.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show class-map cmap1
 CLASS-MAP-NAME: cmap1
      Set IP DSCP: 56
      Match IP DSCP: 7
#
```

show mls qos

Use this command to display whether Quality-of-Service (QoS) is enabled.

Command Syntax `show mls qos`

Parameter

None

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
>show mls qos
  Disable
>
```

show mls qos aggregate-policer

Use this command to display the aggregate policer configuration.

Note: Enable QoS globally before giving this command (see mls qos enable).

Command Syntax `show mls qos aggregate-policer NAME`

Parameter

NAME	Name of the aggregate policer.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show mls qos aggregator-policer agp1
 AGGREGATOR-POLICER-NAME: agp1
    Police:    Average rate(1 kbps), burst size(1 bytes)    Exceed-action drop
#
```

show mls qos cosq-stat

Use this command to display CoS queue statistics.

Note: Enable QoS globally before giving this command (see mls qos enable).

Command Syntax `show mls qos cosq-stats IFNAME ((mcqueue <0-7>)| <0-7> | all)`

Parameter

`IFNAME`	Interface name.
`<0-7>`	Queue identifier.
`all`	Show cosq-stats of all queues

Command Mode

Privileged exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show mls qos cosq-stats eth3 all
```

show mls qos interface

Use this command to display queueing and scheduling information for an interface.

Note: Enable QoS globally before giving this command (see mls qos enable).

Command Syntax `show mls qos interface IFNAME`

Parameter

`IFNAME`	Interface name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show mls qos interface fe0
```

show policy-map name

Use this command to display Quality-of-Service (QoS) policy mappings.

Note: Enable QoS globally before giving this command (see mls qos enable).

Command Syntax `show policy-map show policy-map`

`NAME`

Parameter

`NAME`	Name of the policy map.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show policy-map pmap1
  POLICY-MAP-NAME: pmap1     State: detached

    CLASS-MAP-NAME: cmap1
      Set IP DSCP: 56
      Match IP DSCP: 7
#
```

show qos-access-list

Use this command to display IP and MAC access-control lists (ACLs). Note:

Enable QoS globally before giving this command (see

Command Syntax `show qos-access-list`

```
show qos-access-list (<1-99>|<100-199>|<1300-1999>|<2000-2699>|WORD)
```

Parameters

`<1-99>`	ACL number
`<100-199>`	ACL number
`<1300-1999>`	ACL number
`<2000-2699>`	ACL number
`WORD`	ACL name.

Command Mode

Exec mode and Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show qos-access-list 1
Standard IP-QOS-ACCESS-LIST: 1
permit 11.11.11.50
```

strict-queue

Use this command to set queue in strict priority Use the no command to un-set strict priority.

Command Syntax `strict-queue <0-7> no strict-queue <0-7>`

Parameters

`<0-7>`	queue-id

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#interface ge1
(config-if)#strict-queue 3
(config-if)#no strict-queue 3
(config-if)#
```

tail-drop threshold

Use this command to set the tail-drop threshold percentages for a queue.

Note: Enable QoS globally before giving this command (see

Use the `no` parameter with this command to reset the tail-drop threshold percentages to their default.

Command Syntax `tail-drop queue-id <0-7> threshold <1-100> no tail-drop queue-id <0-7>`

Parameters

`<0-7>`	Queue identifier.
`<1-100>`	Maximum threshold percentage.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface fe0
(config-if)#tail-drop queue-id 5 threshold 50
(config-if)#no tail-drop queue-id 5
```

traffic-shape rate

Use this command to set the outbound traffic rate limit.

Note: Enable QoS globally before giving this command (see mls qos enable).

Use the `no` parameter with this command to remove the outbound traffic rate limit.

Command Syntax `traffic-shape rate <8-1000000> kbps burst <2-2000> no traffic-shape rate`

Parameters

`<8-1000000>`	Rate limit in kilobit/second
`<2-2000>`	Burst size in kilobits

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface fe0
```

```
(config-if)#traffic-shape rate 400 kbps burst 500
```

wrr-queue queue-id

Use this command to set the weight of outgoing queues.

Note: Enable QoS globally before giving this command (see

Use the `no` parameter with this command to reset a queue to its default weight.

Command Syntax `wrr-queue queue-id <0-7> weight <1-127> no wrr-queue queue-id <0-7>`

Parameters

`<1-127>`	Weight of queues 0-7.
`<0-7>`	Outgoing queue identifier.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface fe0
(config-if)#wrr-queue queue-id 5 weight 99
(config-if)#no wrr-queue queue-id 5
```

wrr-queue random-detect

Use this command to set the Weighted Random Early Detection (WRED) drop threshold percentages for an outgoing queue. WRED drop threshold values are a percentage of queue capacity.

Note: Enable QoS globally before giving this command (see mls qos enable).

Use the `no` parameter with this command to reset the drop threshold percentages for a queue to their default.

Command Syntax

```
wrr-queue random-detect queue-id <0-7> min-threshold <1-100> max-
threshold <1-100>
  exp-weight <1-15>
no wrr-queue random-detect queue-id <0-7>
```

Parameters

`<0-7>`	Specify the Queue identifier.
`<1-100>`	Minimum threshold percentage.
`<1-100>`	Maximum threshold percentage.
`<1-15>`	Exponential weight value.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

The following example shows configuring threshold percentage weights of 60 and 100 on queue 1.

```
#configure terminal
(config)#interface fe0
(config-if)#wrr-queue random-detect queue-id 1 mim-threshold 45 max-
threshold 60 exp-weight 14
(config-if)#no wrr-queue random-detect queue-id 1
```

© Symanitron Proprietary

Quality of Service Configuration Guide

Contents

This document contains these chapters.

- Chapter 1, *QoS Introduction*
- Chapter 2, *Enable/Disable Configuration*
- Chapter 3, *QoS Statistics Configuration*
- Chapter 4, *DSCP to Queue Map Configuration*
- Chapter 5, *CoS to Queue Map Configuration*
- Chapter 6, *Trust DSCP on Layer 2 Interface Configuration*
- Chapter 7, *Weights for Queues Configuration*
- Chapter 8, *Marking/Remarking Configuration*
- Chapter 9, *Policing Configuration*
- Chapter 10, *Bandwidth Configuration*
- Chapter 11, *Shaping Configuration*
- Chapter 12, *Priority Configuration*
- Chapter 13, *WRED Configuration*
- Chapter 14, *Tail-Drop Configuration*
- Chapter 15, *Hierarchical Queuing Configuration*

CHAPTER 1 QoS Introduction

This chapter contains a general overview of QoS functionality and terminology.

QoS Functionality

Quality of Service (QoS) can be used to give certain traffic priority over other traffic. Without QoS, all traffic in a network has the same priority and chance of being delivered on time. If congestion occurs, all traffic has the same chance of being dropped. With QoS, specific network traffic can be prioritized to receive preferential treatment. In turn, a network performs more predictably, and utilizes bandwidth more effectively.

QoS is based on DiffServ architecture, which stipulates that individual packets be classified upon entry into a network. Classification information can be carried in the Layer-3 IP packet header or the Layer-2 frame. IP packet headers carry the information using 6-bits from the deprecated IP type of service (TOS) field. Layer-2 802.1Q frames carry the information using a 2-byte Tag Control Information field. All switches and routers accessing the Internet depend on class information to give the same forwarding treatment to packets with the same class information, and give different treatment to packets with different class information. A packet can be assigned class information, as follows:

- End hosts or switches along a path, based on a configured policy
- Detailed packet examination, expected to occur nearer to the network edge, to prevent overloading core switches and routers
- A combination of the above two techniques

Class information can be used by switches and routers along a path to limit the amount of allotted resources per traffic class. Per-hop behavior is an individual device's behavior when handling traffic in the DiffServ architecture. An end-toend QoS solution can be created if all devices along a path have consistent per-hop behavior.

Terminology

Following is a brief description of terms and concepts used to describe QoS.

ACL

Access control lists (ACLs) classify traffic with the same characteristics. IP traffic is classified using IP standard or IP extended ACLs. The ACL can have multiple access control entries (ACEs), which are commands that match fields against the contents of the packet. It is not possible to match IP fragments against configured IP extended ACLs to enforce QoS, but it is possible to match IP options against configured IP extended ACLs to enforce QoS.

CoS Value

Class of Service (CoS) is a 3-bit value used to classify the priority of Layer-2 frames upon entry into a network. QoS classifies frames by assigning priority-indexed CoS values to them, and gives preference to higher-priority traffic. Layer-2 802.1Q frame headers have a 2-byte Tag Control Information field that carries the CoS value in the three mostsignificant bits, called the User Priority bits. On interfaces configured as Layer-2 802.1Q trunks, all traffic is in

802.1Q frames, except for traffic in the native VLAN. Other frame types cannot carry Layer-2 CoS values. CoS values range from zero to seven, seven being the highest priority.

QoS Introduction

DSCP Value

Differentiated Services Code Point (DSCP) is a 6-bit value used to classify the priority of Layer-3 packets upon entry into a network. DSCP values range from 0 to 63, 63 being the highest priority, 0 being best-effort traffic.

Classification

Classification distinguishes one kind of traffic from another by examining the fields in the packet. The process generates an internal DSCP for a packet, which identifies all future QoS actions to be taken on the packet. Each packet is classified upon entry into the network. At the ingress, the packet is inspected, and the DSCP is determined based on ACLs or the configuration. The Layer-2 CoS value is then mapped to a DSCP value. The classification is carried in the IP packet header using 6 bits from the deprecated IP TOS field to carry the classification information. Classification can also occur in the Layer-2 frame. Classification is enabled only if QoS is globally enabled on the switch. By default, QoS is globally disabled, thus, no classification occurs. Classification occurs on an ingress physical port, but not at the switch virtual interface level. Classification can be based on QoS ACLs, or class maps and policy maps.

Policing

Policing determines whether a packet is in or out of profile by comparing the internal DSCP to the configured policer. Policer limits the bandwidth consumed by a traffic flow with the results given to the marker. The two types of policers:

- Individual: QoS applies the bandwidth limits specified in the policer, separately, to each matched traffic class. An individual policer is configured within a policy map.
- Aggregate: QoS applies the bandwidth limits specified in an aggregate policer, cumulatively, to all matched traffic flows. An aggregate policer is configured by specifying the policer name within a policy map. The bandwidth limits of the policer are specified. In this way, multiple classes of traffic across policy map share the aggregate policer.

Policing and policers have the following attributes:

- Policers can occur only on a physical port basis.
- Policing can occur on ingress interfaces.
- Only one policer can be applied to a packet per direction.

Marking

Marking determines how to handle a packet when it is out of profile. It assesses the policer and the configuration data to determine the action required for the packet, and then handles the packet using one of the following methods: • Let the packet through without modification

•Drop the packet

Marking can occur on ingress and egress interfaces.

Queuing

Queuing maps packets to a CoS queue. Each egress port can accommodate up 8 CoS queues, prioritized as 0 lowest and 7 highest. The tagged packet incoming priority can be mapped to one of the 8 queues obtained from the filtering mechanism result. The untagged packet CoS priority is also obtained from the filtering mechanism result. After the packets are mapped to a CoS queue, they are scheduled.

Bandwidth Reservation

Bandwidth reservation is the minimum guaranteed bandwidth allocated per queue. Total guaranteed bandwidth of all the queues belonging to a particular port should not exceed the interface Bandwidth. In case if no Bandwidth reservation is done for the queue, minimum guaranteed per each queue will be 1% of the parent node [scheduling node or interface]

Scheduling

Scheduling forwards or conditions packets using one of the following methods:

- Strict Priority-Based (SP), in which any high-priority packets are first transmitted. Lower-priority packets are transmitted only when the higher-priority queues are empty. A problem may occur when too many lower-priority packets are not transmitted. Strict Priority will be operating on the remaining bandwith available for the Port
- Weighted Round Robin (WRR), in which each queue is assigned a weight to control the number of packets relatively sent from each queue.The weights assigned for the queues will be in the ratio of bandwidth reservation of those queues
- Combination of WRR and SP, the Remaining Bandwidth will be scheduled in the strict order for the SP Queues. The Remaining Bandwidth will be scheduled in the WRR mode for WRR Queues.

Class Map

A class map names and isolates specific traffic from other traffic. The class map defines the criteria used to match against a specific traffic flow to classify it further. The criteria can include:

- Matching the access group defined by the ACL
- Matching a specific list of DSCP values

If there is more than one type of traffic to be classified, another class map can be created under a different name. After a packet is matched against the class-map criteria, it is further classified using a policy map.

Policy Map

A policy map specifies on which traffic class to act. This can be implemented as follows:

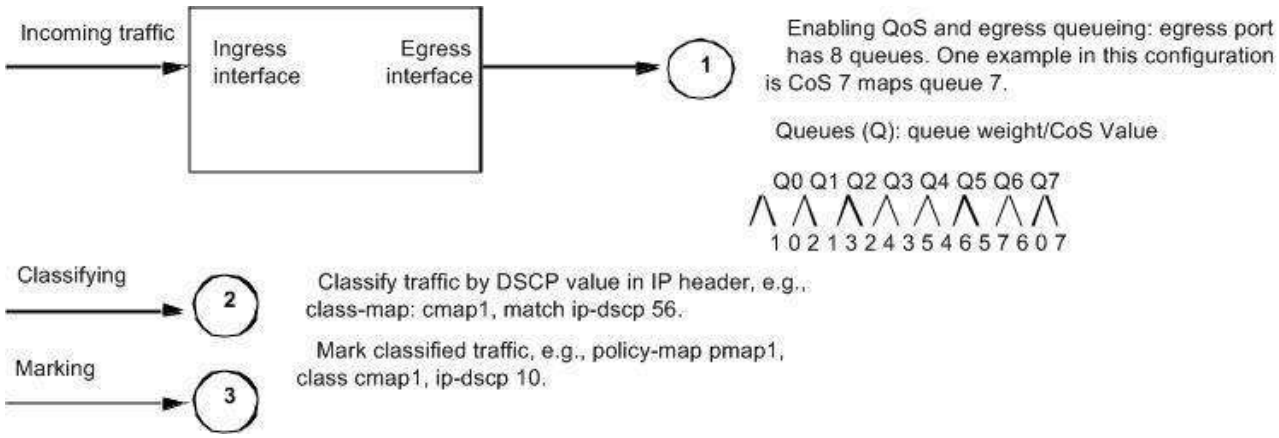
- Set a specific CoS or DSCP value in the traffic class.
- Specify the traffic bandwidth limitations for each matched traffic class (policer) and the action to take (marking) when the traffic is out of profile.

Policy maps have the following attributes:

- A policy map can contain multiple class statements, each with different match criteria and policers.

- A separate policy-map class can exist for each type of traffic received through an interface.
- There can be only one policy map per interface per direction. The same policy map can be applied to multiple interfaces and directions.
- Before a policy map can be effective, it must be attached to an interface.

QoS Introduction



CHAPTER 2 Enable/Disable Configuration

Topology

Figure 2-219: Simple configuration of QoS

Enabling QoS

The following steps describe how to enable QoS.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable (H)QoS on configuration mode.
`(config)#exit`	Exit configure mode.

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
qos enable !
```

Disabling QoS

The following steps disable QoS.

`#configure terminal`	Enter configure mode.
`(config)#qos disable`	Disable (H)QoS on configuration mode.
`(config)#exit`	Exit configure mode.

Validation

Enter the commands below to confirm the configurations.

```
    #show running-config qos
```
Enable/Disable Configuration

```
                                                % QoS is not enabled globally
```

CHAPTER 3 QoS Statistics Configuration

This chapter contains a complete sample of enabling QoS statistics.

Topology

Figure 3-220: Simple configuration of QoS

Enabling QoS Statistics on configuration mode

The following steps describe how to enable QoS Statistics.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics on configuration mode.
`(config)#exit`	Exit configure mode.

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
qos enable qos
statistics !
```

QoS Statistics Configuration

CHAPTER 4 DSCP to Queue Map Configuration

This chapter contains a complete sample of configuring DSCP to queue map.

Topology

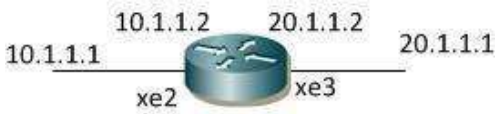


Figure 4-221: Simple configuration of DSCP to queue map

Configuration of DSCP to Queue Map on configuration mode

The following steps describe how to configure DSCP to queue map on configuration mode.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#qos map dscp 10 queue 5`	Map DSCP 10 to queue 5 on global mode.
`(config)#exit`	Exit configure mode.

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
qos enable qos
statistics qos map dscp
10 queue 5 !
```

Configuration of DSCP to Queue Map on Interface mode

The following steps describe how to configure DSCP to queue map on interface mode.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#qos map dscp 10 queue 6`	Map DSCP 10 to queue 6 for all the unicast frames/ packets received on this interface.

(config-if)#exit	Exit interface mode.
(config)#exit	Exit configure mode.

DSCP to Queue Map Configuration

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos qos enable qos statistics
!
interface xe2  qos map dscp 10 queue 6 !
```

CHAPTER 5 CoS to Queue Map Configuration

This chapter contains a complete sample of configuring CoS to queue map.

Topology

Figure 5-222: Simple configuration of CoS

Configuration of CoS to Queue Map on configuration mode

The following steps describe how to configure CoS to queue map on configuration mode.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#qos map cos 2 queue 4`	Map CoS 2 to queue 4 on global mode.
`(config)#exit`	Exit configure mode.

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
qos enable qos
statistics qos map cos 2
queue 4 !
```

Configuration of CoS to Queue Map on Interface mode

The following steps describe how to configure CoS to queue map on interface mode.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#qos map cos 2 queue 4`	Map Cos 2 to queue 4 for all the unicast frames/packets received on this interface.
`(config-if)#exit`	Exit interface mode.

`(config)#exit`	Exit configure mode.

CoS to Queue Map Configuration

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos qos enable qos statistics
!
interface xe2  qos map cos 2 queue 4 !
```

CHAPTER 6 Trust DSCP on Layer 2 Interface Configuration

This chapter contains a complete sample of configuring trust DSCP on Layer 2 interface.

Topology

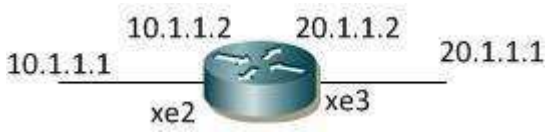


Figure 6-223: Simple configuration of trust DSCP

Configuration Trust DSCP on Interface mode

The following steps describe how to configure trust DSCP on Layer 2 interface.By default, Layer 2 interface will be trust CoS and layer3 interface will be trust DSCP.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#trust dscp`	Configure trust DSCP on the interface xe2.
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit configure mode.

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
qos enable qos
statistics
! ! interface
xe2 trust
dscp
```

Trust DSCP on Layer 2 Interface Configuration

CHAPTER 7 Weights for Queues Configuration

This chapter contains a complete sample of configuring WRR weights for queues.

Topology

Figure 7-224: Simple configuration of QoS

Configuring WRR Weights for Queues

Do the following to configure WRR weights for queues.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#class-map cmap1`	Enter class-map mode
`(config-cmap-qos)#match cos 2`	Configure match criteria as cos 2
`(config-cmap-qos)#exit`	Exit out of class-map mode
`(config)#class-map cmap2`	Enter class-map mode
`(config-cmap-qos)#match cos 3`	Configure match criteria as cos 3
`(config-cmap-qos)#exit`	Exit out of class-map mode
`(config)#policy-map pmap1`	Enter policy-map mode.
`(config-pmap-qos)#class cmap1`	Assign class cmap1.
`(config-pmap-c-qos)#set qos-group 1`	Remark matched traffic to qos-group 1
`(config-pmap-c-qos)#exit`	Exit out of pmap-c mode
`(config-pmap-qos)#exit`	Exit pmap mode.
`(config)#policy-map pmap1`	Enter policy-map mode.
`(config-pmap-qos)#class cmap2`	Assign class cmap2.
`(config-pmap-c-qos)#set qos-group 2`	Remark matched traffic to qos-group 2
`(config-pmap-c-qos)#exit`	Exit out of pmap-c mode
`(config-pmap-qos)#exit`	Exit pmap mode.
`(config)#class-map type queuing cq1`	Configure class-map of type queuing with name cq1, and enter into class-map mode
`(config-cmap-que)#match qos-group 1`	Configure match criteria as qos-group 1

(config-cmap-que)#exit	Exit out of class-map mode.
(config)#class-map type queuing cq2	Configure class-map of type queuing with name cq2, and enter into class-map mode.
(config-cmap-que)#match qos-group 2	Configure match criteria as qos-group 2.
(config-cmap-que)#exit	Exit out of class-map mode.

Weights for Queues Configuration

(config)#policy-map type queuing pq1	Configure policy-map of type queuing with name pq1, and enter into policy-map mode.
(config-pmap-que)#class cq1	Attach class cq1 to Policy-map pq1.
(config-pmap-c-que)#wrr-queue weight 2	Configure WRR Weight of 2.
(config-pmap-c-que)#exit	Exit from pmap-c mode.
(config-pmap-que)#class cq2	Assign class (queue) cq2 to pq1.
(config-pmap-c-que)#wrr-queue weight 4	Configure WRR weight of 4.
(config-pmap-c-que)#exit	Exit from pmap-c mode.
(config-pmap-que)#exit	Exit from pmap mode.
(config)#interface xe2	Enter into interface xe2.
(config-if)#service-policy type queuing output pq1	Assign service policy pq1 of type queueing on out direction.
(config-if)#exit	Exit interface mode
(config)#exit	Exit configure mode.

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
#show running-config qos qos
enable qos statistics
! class-map cmap2
match cos 3
! class-map cmap1
match cos 2
! class-map type queuing match-any
cq1 match qos-group 1
! class-map type queuing match-any
cq2 match qos-group 2
! policy-map pmap1
class cmap1   set qos-
group 1    exit  class
cmap2    set qos-group 2
exit
policy-map type queuing pq1  class
type queuing cq1   wrr-queue
weight 2   exit
```

```
     class type queuing cq2   wrr-
    queue weight 4   exit
    ! interface xe2
```



```
 service-policy type queuing output pq1

#show policy-map

Type qos policy-maps ====================

policy-map pmap1
class cmap1   set
qos-group 1   exit
class cmap2   set
qos-group 2   exit


Type queuing policy-maps ========================

policy-map type queuing pq1
class type queuing cq1   wrr-
queue weight 2   exit
 class type queuing cq2
wrr-queue weight 4   exit

#show class-map

  Type qos class-maps
===================       class-
map cmap2                  match
cos 3

      class-map cmap1
match cos 2


  Type queuing class-maps   ======================
      class-map type queuing match-any cq1
match qos-group 1

      class-map type queuing match-any cq2
match qos-group 2


#show policy-map interface xe2

Interface xe2
Global statistics status : enabled

Service-policy (queuing) output: pq1
```

```
--------------------------------
Class-map (queuing): cq1   match qos-
group 1
      output     : 0 packets, 0 bytes
```

Weights for Queues Configuration

```
          dropped    : 0 packets, 0 bytes

     Class-map (queuing): cq2  match qos-group 2       output     : 0 packets, 0
    bytes        dropped   : 0 packets, 0 bytes

    Class-map (queuing): mc-q0       output     : 0 packets, 0 bytes       dropped
    : 0 packets, 0 bytes

    Class-map (queuing): mc-q1       output     : 0 packets, 0 bytes       dropped
    : 0 packets, 0 bytes

    Class-map (queuing): mc-q2       output     : 0 packets, 0 bytes       dropped
    : 0 packets, 0 bytes

    Class-map (queuing): mc-q3       output     : 0 packets, 0 bytes       dropped
    : 0 packets, 0 bytes

    Class-map (queuing): mc-q4       output     : 0 packets, 0 bytes       dropped
    : 0 packets, 0 bytes

    Class-map (queuing): mc-q5       output     : 0 packets, 0 bytes       dropped
    : 0 packets, 0 bytes

    Class-map (queuing): mc-q6       output     : 0 packets, 0 bytes       dropped
    : 0 packets, 0 bytes

    Class-map (queuing): mc-q7       output     : 0 packets, 0 bytes       dropped
    : 0 packets, 0 bytes

    Wred Drop Statistics : ---------------------- green  : 0 packets
    yellow : 0 packets  red    : 0 packets
```

CHAPTER 8 Marking/Remarking Configuration

This chapter contains a complete sample of configuring Marking/Remarking.

Topology

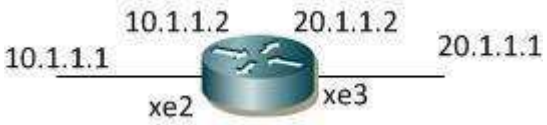


Figure 8-225: Simple configuration of Marking/Remarking

L2 Interface

The following steps describe how to configure Marking/Remarking.

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol rstp vlan-bridge`	Configure bridge 1 as RSTP-VLAN aware.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#switchport`	Configure xe2 as a Layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.
`(config-if)#switchport mode trunk`	Configure port as a trunk.
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe2 interface.
`(config-if)#exit`	Exit the xe2 interface mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#class-map type qos cmap1`	Enter Class-map mode
`(config-cmap-qos)#match cos 2`	Configure match criteria as CoS with Value 2
`(config-cmap-qos)#exit`	Exit Class-map mode
`(config)#policy-map type qos pmap1`	Enter policy-map mode
`(config-pmap-qos)#class type qos cmap1`	Assign Class cmap1 to Policy-map pmap1
`(config-pmap-c-qos)#set cos 5`	Remark cos from cos 2 to cos 5
`(config-pmap-c-qos)#exit`	Exit out of policy-class-map mode
`(config-pmap-qos)#exit`	Exit out of Policy-map mode

(config)#interface xe2	Enter xe2 interface
(config-if)#service-policy type qos input pmap1	Assign service-policy to interface on in-direction
(config-if)#exit	Exit the xe2 interface mode.
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure xe3 as a Layer 2 port.
(config-if)#bridge-group 1	Associate bridge to an interface.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the xe3 interface mode.
(config)#class-map type qos cmap2	Enter Class-map mode
(config-cmap-qos)#match protocol arp	Configure match criteria as protocol with arp
(config-cmap-qos)#exit	Exit Class-map mode
(config)#policy-map type qos pmap2	Enter policy-map mode
(config-pmap-qos)#class type qos cmap2	Assign Class cmap2 to Policy-map pmap2
(config-pmap-c-qos)#set cos 6	Remark all frame with ethertype as arp to cos 6
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#exit	Exit out of Policy-map mode
(config)#interface xe3	Enter xe3 interface
(config-if)#service-policy type qos input pmap2	Assign service-policy to interface on in-direction
(config-if)#exit	Exit out of interface mode

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
#show class-map cmap1   Type qos
class-maps   ===================
class-map type qos cmap1
match cos 2 #show policy-map

Type qos policy-maps
==================== policy-map
type qos pmap1  class type qos
cmap1   set cos 5 policy-map type
qos pmap2  class type qos cmap2
set cos 6

Type queuing policy-maps
```

```
========================
#show policy-map type qos
Type qos policy-maps
====================
policy-map type qos pmap1  class type
qos cmap1   set cos 5 policy-map type
qos pmap2  class type qos cmap2   set
cos 6


 #show policy-map interface xe2


 Interface xe2
 Global statistics status : enabled


 Service-policy (qos) input     : pmap1
 ------------------------------- Class-map (qos): cmap1 (match
 all)  match cos 2  set cos 5       matched    : 36926060
 packets, 2510973304 bytes


 Service-policy (queuing) output: default-out-policy
 ------------------------------- Class-map
 (queuing): q0  priority level 1       output
 : 0 packets, 0 bytes       dropped    : 0
 packets, 0 bytes


  Class-map (queuing): q1  priority level 1
 output     : 0 packets, 0 bytes       dropped
 : 0 packets, 0 bytes


  Class-map (queuing): q2  priority level 1
 output     : 0 packets, 0 bytes       dropped
 : 0 packets, 0 bytes


  Class-map (queuing): q3  priority level 1
 output     :  0 packets, 0 bytes       dropped
 : 0 packets,  0 bytes  Class-map (queuing): q4
 priority level 1       output      : 0 packets, 0
 bytes       dropped     : 0 packets, 0 bytes
```

```
 Class-map (queuing): q5  priority level 1
output     : 0 packets, 0 bytes        dropped    :
0 packets, 0 bytes


 Class-map (queuing): q6  priority level 1
      output     : 35204021 packets, 2393872952 bytes       dropped
: 0 packets, 0 bytes


 Class-map (queuing): q7  priority level 1
      output     : 12 packets, 768 bytes         dropped    :
0 packets, 0 bytes


Class-map (queuing): mc-q0       output      : 0
packets, 0 bytes       dropped     : 0 packets, 0
bytes


Class-map (queuing): mc-q1       output      : 0
packets, 0 bytes       dropped     : 0 packets, 0
bytes


Class-map (queuing): mc-q2       output      : 0
packets, 0 bytes       dropped     : 0 packets, 0
bytes


Class-map (queuing): mc-q3       output      : 0
packets, 0 bytes       dropped     : 0 packets, 0
bytes


Class-map (queuing): mc-q4       output      : 0
packets, 0 bytes       dropped     : 0 packets, 0
bytes Class-map (queuing): mc-q5        output
: 0 packets, 0 bytes       dropped     : 0 packets,
0 bytes


Class-map (queuing): mc-q6       output      : 0
packets, 0 bytes       dropped     : 0 packets, 0
bytes
```

```
Class-map (queuing): mc-q7       output     : 0
packets, 0 bytes       dropped    : 0 packets, 0
bytes


Wred Drop Statistics : ------------
--------- green  : 0 packets
yellow : 0 packets  red    : 0
packets


#show policy-map interface xe3


Interface xe3
Global statistics status : enabled


Service-policy (qos) input     : pmap2
------------------------------ Class-map (qos): cmap2 (match all)
match protocol arp  set cos 6       matched    : 45667711 packets,
3105405640 bytes




Service-policy (queuing) output: default-out-policy
------------------------------- Class-map
(queuing): q0  priority level 1       output      :
0 packets, 0 bytes       dropped     : 0 packets, 0
bytes


 Class-map (queuing): q1  priority level 1
      output      : 0 packets, 0 bytes         dropped    :
0 packets, 0 bytes


 Class-map (queuing): q2  priority level 1
output     : 0 packets, 0 bytes       dropped     :
0 packets, 0 bytes


 Class-map (queuing): q3  priority level 1
output     : 0 packets, 0 bytes       dropped     :
0 packets, 0 bytes
```

```
 Class-map (queuing): q4  priority level 1
output     : 0 packets, 0 bytes       dropped    :
0 packets, 0 bytes


 Class-map (queuing): q5  priority level 1
      output     : 43945672 packets, 2988305220 bytes       dropped
: 0 packets, 0 bytes


 Class-map (queuing): q6  priority level 1
output     : 0 packets, 0 bytes       dropped    :
0 packets, 0 bytes


 Class-map (queuing): q7  priority level 1
      output      : 15 packets, 960 bytes        dropped    :
0 packets, 0 bytes


Class-map (queuing): mc-q0       output      : 0
packets, 0 bytes       dropped    : 0 packets, 0
bytes


Class-map (queuing): mc-q1       output      : 0
packets, 0 bytes       dropped    : 0 packets, 0
bytes Class-map (queuing): mc-q2       output
: 0 packets, 0 bytes       dropped    : 0 packets,
0 bytes


 Class-map (queuing): mc-q3       output     : 0 packets, 0 bytes
 dropped    : 0 packets, 0 bytes


 Class-map (queuing): mc-q4       output     : 0 packets, 0 bytes
 dropped    : 0 packets, 0 bytes


 Class-map (queuing): mc-q5       output     : 0 packets, 0 bytes
 dropped    : 0 packets, 0 bytes


 Class-map (queuing): mc-q6       output     : 0 packets, 0 bytes
 dropped    : 0 packets, 0 bytes
```

```
Class-map (queuing): mc-q7       output      : 0 packets, 0 bytes
dropped     : 0 packets,0 bytes


Wred Drop Statistics : --------------------                green
: 0 packets    yellow : 0packets  red     : 0
packets
```

L3 Interface

#configure terminal	Enter configure mode.
(config)#interface xe3	Enter interface mode.
(config-if)#ip address 10.1.1.2/24	Assign IP Address on interface to 10.1.1.2 with mask 255.255.255.0
(config-if)#exit	Exit out of interface mode

(config)#qos enable	Enable QoS globally.
(config)#qos statistics	Enable QoS statistics.
(config)#class-map type qos cmap3	Configure class-map of type qos with name cmap3 and enter into Class-map mode
(config-cmap-qos)#match dscp 10	Configure match criteria as dscp with a value of 10.
(config-cmap-qos)#exit	Exit Class-map mode
(config)#policy-map type qos pmap3	Enter policy-map mode
(config-pmap-qos)#class type qos cmap3	Assign Class cmap3 to Policy-map pmap3
(config-pmap-c-qos)#set dscp ef	Remark frames with dscp value 10 to dscp 46
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#exit	Exit out of Policy-map mode
(config)#interface xe3	Enter xe3 interface
(config-if)#service-policy type qos input pmap3	Assign service-policy pmap3 to interface xe3 on in-direction
(config-if)#exit	Exit out of interface mode
(config)#access-list 101	Configure access-list 101 with action as permit for tcp traffic with destination port as ftp port
(config)#permit tcp any any eq ftp	Permit for tcp traffic with destination port as ftp port.
(config)#class-map type qos match-any cmap4	Enter Class-map mode

(config-cmap-qos)#match access-group 101	Configure access-group 101 as match criteria
(config-cmap-qos)#exit	Exit class-map mode
(config)#policy-map type qos pmap4	Enter policy map mode
(config-pmap-qos)#class cmap4	Assign Class cmap4 to Policy-map pmap4
(config-pmap-c-qos)#set precedence 7	Remark frames matching access-group 101 to precedence 7
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#exit	Exit out of Policy-map mode
(config)#interface xe2	Enter interface mode.
(config-if)#ip address 20.1.1.2/24	Assign IP Address on interface to 20.1.1.2 with mask 255.255.255.0
(config-if)#service-policy type qos input pmap4	Assign service-policy to interface on in-direction

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
#show running-config qos qos
enable !
qos statistics ! class-map type qos cmap3
match dscp af11 ! class-map type qos
match-any cmap4  match access-group 101 !
policy-map type qos pmap3  class
type qos cmap3   set dscp ef
exit policy-map type qos pmap4
class type qos cmap4   set
precedence network   exit !
interface xe2
 service-policy type qos input pmap4 !
interface xe3
 service-policy type qos input pmap3


#show class-map type qos

  Type qos class-maps   ====================
      class-map type qos match-any class-default

      class-map type qos cmap3        match
dscp af11
```

```
      class-map type qos match-any cmap4         match
access-group 101



#show policy-map

Type qos policy-maps

==================== policy-map type

qos pmap3  class type qos cmap3   set

dscp ef   exit


policy-map type qos pmap4  class
type qos cmap4   set precedence
network   exit



#show policy-map interface xe2


Interface xe2
Global statistics status : enabled




Service-policy (qos) input     : pmap4
------------------------------- Class-map (qos): cmap4 (match any)
match access-group 101  set precedence 7       matched    :
375594046 packets, 25540397168 bytes




Service-policy (queuing) output: default-out-policy
------------------------------- Class-map
(queuing): q0  priority level 1
      output     : 0 packets, 0 bytes       dropped    :
0 packets, 0 bytes


 Class-map (queuing): q1  priority level 1
      output     : 0 packets, 0 bytes       dropped    :
0 packets, 0 bytes


 Class-map (queuing): q2  priority level 1
```

```
      output     : 0 packets, 0 bytes       dropped
: 0 packets, 0 bytes Class-map (queuing): q3 priority
level 1
      output     : 0 packets, 0 bytes       dropped    :
0 packets, 0 bytes


 Class-map (queuing): q4   priority level 1
      output     : 0 packets, 0 bytes       dropped    :
0 packets, 0 bytes


 Class-map (queuing): q5   priority level 1
      output     : 391282612 packets, 25042086656 bytes     dropped
: 0 packets, 0 bytes


 Class-map (queuing): q6   priority level 1
      output     : 0 packets, 0 bytes       dropped    :
0 packets, 0 bytes


 Class-map (queuing): q7   priority level 1
      output     : 4 packets, 256 bytes       dropped    :
0 packets, 0 bytes


Class-map (queuing): mc-q0       output      : 0
packets, 0 bytes       dropped     : 0 packets, 0
bytes


Class-map (queuing): mc-q1       output      : 0
packets, 0 bytes       dropped     : 0 packets, 0
bytes


Class-map (queuing): mc-q2       output      : 0
packets, 0 bytes       dropped     : 0 packets, 0
bytes


Class-map (queuing): mc-q3       output      : 0
packets, 0 bytes       dropped     : 0 packets, 0
bytes Class-map (queuing): mc-q4        output
: 0 packets, 0 bytes       dropped     : 0
packets, 0 bytes
```

```
Class-map (queuing): mc-q5       output      : 0
packets, 0 bytes        dropped    : 0 packets, 0
bytes


Class-map (queuing): mc-q6       output      : 0
packets, 0 bytes        dropped    : 0 packets, 0
bytes


Class-map (queuing): mc-q7       output      : 0
packets, 0 bytes        dropped    : 0 packets, 0
bytes


Wred Drop Statistics : ----------
----------- green   : 0 packets
yellow : 0 packets  red     : 0
packets

#show policy-map interface xe3


Interface xe3
Global statistics status : enabled


Service-policy (qos) input     : pmap3
---------------------------              Class-map (qos): cmap3 (match all)
match dscp af11  set dscp 46        matched    : 401497149 packets,
25695819008 bytes


Service-policy (queuing) output: default-out-policy
------------------------------- Class-map
(queuing): q0  priority level 1
     output      : 0 packets, 0 bytes       dropped    :
0 packets, 0 bytes


 Class-map (queuing): q1
 priority level 1
     output      : 0 packets, 0 bytes       dropped    :
0 packets, 0 bytes


 Class-map (queuing): q2   priority level 1
     output      : 0 packets, 0 bytes       dropped    :
0 packets, 0 bytes
```

```
 Class-map (queuing): q3  priority level 1
      output     : 0 packets, 0 bytes       dropped     :
0 packets, 0 bytes


 Class-map (queuing): q4  priority level 1
      output     : 0 packets, 0 bytes       dropped     :
0 packets, 0 bytes


 Class-map (queuing): q5  priority level 1
      output     : 0 packets, 0 bytes       dropped     :
0 packets, 0 bytes


 Class-map (queuing): q6  priority level 1
      output     : 0 packets, 0 bytes       dropped     :
0 packets, 0 bytes


 Class-map (queuing): q7  priority level 1
      output    : 382211720 packets, 25990396484 bytes      dropped
: 0 packets, 0 bytes


Class-map (queuing): mc-q0       output     : 0
packets, 0 bytes       dropped    : 0 packets, 0
bytes


Class-map (queuing): mc-q1       output     : 0
packets, 0 bytes       dropped    : 0 packets, 0
bytes Class-map (queuing): mc-q2       output
: 0 packets, 0 bytes       dropped     : 0
packets, 0 bytes


Class-map (queuing): mc-q3       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q4       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q5       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes
```

```
Class-map (queuing): mc-q6       output     : 0  packets, 0 bytes
dropped     : 0 packets,0 bytes


Class-map (queuing): mc-q7       output     : 0  packets, 0 bytes
dropped     : 0 packets,0 bytes


Wred Drop Statistics : --------------------                        green
: 0 packets    yellow : 0packets   red     : 0 packets
```

CHAPTER 9 Policing Configuration

This chapter contains a complete sample of configuring Marking/Remarking.

Topology

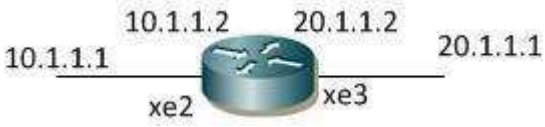


Figure 9-226: Simple configuration of Policing

L2 Interface

Do the following to configure policing on an L2 interface.

`#configure terminal`	Enter configure mode.
`(config)#bridge 1 protocol mstp`	Configure bridge 1 as mstp aware.
`(config)#interface xe2`	Enter interface mode.
`(config-if)#switchport`	Configure xe2 as a Layer 2 port.
`(config-if)#bridge-group 1`	Associate bridge to an interface.
`(config-if)#switchport mode trunk`	Configure port as a trunk.
`(config-if)#switchport trunk allowed vlan all`	Allow all the VLANs on the xe2 interface.
`(config-if)#exit`	Exit the xe2 interface mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#class-map type qos 1234`	Enter Class-map mode
`(config-cmap-qos)#match cos 3`	Configure match criteria as CoS with Value 3
`(config-cmap-qos)#exit`	Exit Class-map mode
`(config)#policy-map type qos 1234`	Enter policy-map mode
`(config-pmap-qos)#class type qos 1234`	Assign Class 1234 to Policy-map 1234
`(config-pmap-c-qos))# police cir 2 mbps pir 3 mbps bc 2 mbytes be 2 mbytes conform transmit exceed set-cos-transmit 1 violate drop`	Police access-list 102 frames @ Committed information rate 2 mbps, committed bust 2 mbyte, peak information rate 3 mbps, peak burst 2 mbytes when traffic is > CIR and <= PIR then Set the class of service (CoS) field to 1, if traffic violate the action then drop the frames.
`(config-pmap-c-qos)#exit`	Exit out of policy-class-map mode
`(config-pmap-qos)#exit`	Exit out of Policy-map mode
`(config)#interface xe2`	Enter xe2 interface

(config-if)#service-policy type qos input 1234	Assign service-policy to interface on in-direction
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure xe3 as a Layer 2 port.
(config-if)#bridge-group 1	Associate bridge to an interface.
(config-if)#switchport mode trunk	Configure port as a trunk.
(config-if)#switchport trunk allowed vlan all	Allow all the VLANs on the xe3 interface.
(config-if)#exit	Exit the xe3 interface mode.
(config)#mac access-list 102	Configure mac access-list with action
(config)#permit mac host 0000.0101.1010 host 0000.0202.2020	Permit when frames matches Source mac address 00:00:01:01:10:10 and destination mac address 00:00:02:02:20:20
(config)#class-map type match-any 2345	Enter Class-map mode
(config-cmap-qos)#match access-group name 102	Configure match criteria as access-group 102
(config-cmap-qos)#exit	Exit Class-map mode
(config)#policy-map type qos 2345	Enter policy-map mode
(config-pmap-qos)#class type qos 2345	Assign Class 2345 to Policy-map 2345
(config-pmap-c-qos))# police cir 2 mbps pir 3 mbps bc 2 mbytes be 2 mbytes conform transmit exceed set-cos-transmit 1 violate drop	Police access-list 102 frames @ Committed information rate 2 mbps, committed bust 2 mbytes, peak information rate 3 mbps, peak burst 2 mbytes when traffic is > CIR and <= PIR, then set the class of service (CoS) field to 1, if traffic violate the action, then drop the frames.
(config-pmap-qos)#exit	Exit Policy-map mode
(config)#interface xe3	Enter interface mode.
(config-if)#service-policy type qos input 2345	Assign service-policy 2345 to interface on in-direction
(config-if)#exit	Exit interface mode

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos
qos enable !
qos statistics ! class-
map type qos 1234
match cos 2 !
class-map type qos match-any 2345
match access-group 102 !
policy-map  type  qos  1234
class type qos 1234
  police colour-aware cir 1 mbps bc 1 mbytes conform set-cos-transmit 5
violate drop exit
policy-map  type  qos  2345
class type qos 2345
```

```
  police colour-aware cir 2 mbps pir 3 mbps bc 2 mbytes be 2 mbytes conform
tran smit exceed set-cos-transmit 1 violate drop
  exit !
interface xe2
 service-policy type qos input 1234
! interface xe3
 service-policy type qos input 2345 #show
class-map type qos

  Type qos class-maps
==================
class-map type qos 1234
match cos 2

      class-map type qos match-any 2345

match access-group 102       class-map type qos

match-any class-default

#show policy-map type qos

Type           qos           policy-maps
====================

policy-map   type   qos   1234
class type qos 1234
  police colour-aware cir 1 mbps bc 1 mbytes conform set-cos-transmit 5
violate drop exit

policy-map   type   qos   2345
class type qos 2345
  police colour-aware cir 2 mbps pir 3 mbps bc 2 mbytes be 2 mbytes conform
tran smit exceed set-cos-transmit 1 violate drop
exit
#
#show policy-map interface xe2


Interface xe2
Global statistics status : enabled


Service-policy (qos) input     : 1234
------------------------------ Class-
map (qos): 1234 (match all)  match cos
2
 police colour-aware cir 1 mbps bc 1 mbytes conform set-cos-transmit 5 violate
d rop
      matched    : 7419394 packets, 504519132 bytes
```

```
      dropped     : 7409793 packets, 503866264 bytes


Service-policy (queuing) output: default-out-policy
------------------------------ Class-map (queuing): q0  priority
level 1       output     : 0 packets, 0 bytes       dropped     :
0 packets, 0 bytes


 Class-map (queuing): q1  priority level 1
      output      : 7222 packets,  491096 bytes        dropped     : 0 packets, 0
bytes


 Class-map (queuing): q2  priority level 1
      output      : 14444 packets, 982192 bytes        dropped     : 0 packets, 0
bytes


 Class-map (queuing): q3  priority level 1       output     : 0
packets, 0 bytes       dropped    : 0 packets, 0 bytes


 Class-map (queuing): q4  priority level 1       output     : 0
packets, 0 bytes       dropped    : 0 packets, 0 bytes


 Class-map (queuing): q5  priority level 1       output     : 0
packets, 0 bytes       dropped    : 0 packets, 0 bytes


 Class-map (queuing): q6  priority level 1       output     : 0
packets, 0 bytes       dropped    : 0 packets, 0 bytes


 Class-map (queuing): q7  priority level 1
      output     : 2 packets, 246 bytes
      dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q0       output     : 0 packets, 0 bytes        dropped
: 0 packets, 0 bytes


Class-map (queuing): mc-q1       output     : 0 packets, 0 bytes        dropped
: 0 packets, 0 bytes
```

```
Class-map (queuing): mc-q2       output     : 0 packets, 0 bytes       dropped
: 0 packets, 0 bytes

Class-map (queuing): mc-q3       output     : 0 packets, 0 bytes       dropped
: 0 packets, 0 bytes

Class-map (queuing): mc-q4       output     : 0 packets, 0 bytes       dropped
: 0 packets, 0 bytes

Class-map (queuing): mc-q5       output     : 0 packets, 0 bytes       dropped
: 0 packets, 0 bytes

Class-map (queuing): mc-q6       output     : 0 packets, 0 bytes       dropped
: 0 packets, 0 bytes

Class-map (queuing): mc-q7       output     : 0 packets, 0 bytes       dropped
: 0 packets, 0 bytes

Wred Drop Statistics : ---------------------- green  : 0 packets
yellow : 0 packets  red    : 0 packets #show policy-map
interface xe3

Interface xe3
Global statistics status : enabled

Service-policy (qos) input     : 2345
------------------------------- Class-
map (qos): 2345 (match any)  match
access-group 102
 police colour-aware cir 2 mbps pir 3 mbps bc 2 mbytes be 2 mbytes conform
trans mit exceed set-cos-transmit 1 violate drop       matched    : 16218780
packets, 1102879420 bytes

Service-policy (queuing) output: default-out-policy
-------------------------------
Class-map (queuing): q0
priority level 1
      output         :  0  packets,  0  bytes
dropped    : 0 packets, 0 bytes
```

```
 Class-map     (queuing):     q1
priority level 1
      output          :  0 packets,   0 bytes
dropped    : 0 packets, 0 bytes


 Class-map     (queuing):     q2
priority level 1
      output          :  0 packets,   0 bytes
dropped    : 0 packets, 0 bytes


 Class-map     (queuing):     q3
priority level 1
      output          :  0 packets,   0 bytes
dropped    : 0 packets, 0 bytes


 Class-map     (queuing):     q4
priority level 1
      output          :  0 packets,   0 bytes
dropped    : 0 packets, 0 bytes


 Class-map     (queuing):     q5
priority level 1
      output     : 18527 packets, 1259836 bytes        dropped    : 0 packets, 0
bytes


 Class-map (queuing): q6  priority level 1       output     : 0
packets, 0 bytes       dropped    : 0 packets, 0 bytes


 Class-map (queuing): q7  priority level 1       output     : 5 packets,
615 bytes       dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q0       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q1       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q2       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes
```

```
Class-map (queuing): mc-q3       output      : 0 packets, 0 bytes
dropped     : 0 packets, 0 bytes


Class-map (queuing): mc-q4       output      : 0 packets, 0 bytes
dropped     : 0 packets, 0 bytes


Class-map (queuing): mc-q5       output      : 0 packets, 0 bytes
dropped     : 0 packets, 0 bytes


Class-map (queuing): mc-q6       output      : 0 packets, 0 bytes
dropped     : 0 packets, 0 bytes Class-map (queuing): mc-q7
output     : 0 packets, 0 bytes       dropped    : 0 packets, 0 bytes


Wred Drop Statistics : ---------------------- green  : 0 packets
yellow : 0 packets  red    : 0 packets
```

CHAPTER 10 Bandwidth Configuration

This chapter contains a complete sample of configuring Bandwidth.

Topology

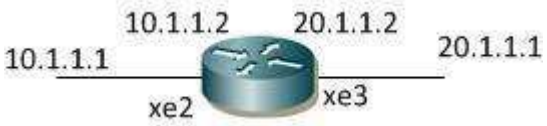


Figure 10-227: Simple configuration of Bandwidth

L2/L3 Interface

The following steps describe how to configure bandwidth.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos tsatistics`	Enable QoS statistics.
`(config)#class-map type queuing match-any cq1`	Configure class-map of type queuing with name cq1, and enter into class-map mode
`(config-cmap-que)#match qos-group 1`	Configure match criteria as qos-group 1
`(config-cmap-que)#exit`	Exit out of class-map mode
`(config)#class-map type queuing match-any cq2`	Configure class-map of type queuing with name cq2, and enter into class-map mode
`(config-cmap-que)#match qos-group 2`	Configure match criteria as qos-group 2
`(config-cmap-que)#exit`	Exit out of class-map mode
`(config)#policy-map type queuing P1`	Configure policy-map of type queuing with name P1, and enter into policy-map mode
`(config-pmap-que)#class type queuing cq1`	Attach class cq1 to Policy-map P1
`(config-pmap-c-que)#bandwidth percent 70`	Configure minimum bandwidth as 70 percent of total bandwidth available on interface
`(config-pmap-c-que)#exit`	Exit out of policy-class mode
`(config-pmap-que)#class type queuing cq2`	Attach class cq2 to Policy-map P1
`(config-pmap-c-que)#bandwidth remaining percent 30`	Configure minimum bandwidth as 30 percent of remaining bandwidth available on interface after all allocations are done.
`(config-pmap-c-que)#exit`	Exit out of policy-class mode
`(config-pmap-que)#exit`	Exit out of Policy-map mode
`(config)#class-map type qos c1`	Enter Class-map mode
`(config-cmap-qos)#match dscp 10`	Configure match criteria as dscp 10

(config-cmap-qos)#match cos 3	Configure match criteria as cos 3
(config-cmap-qos)#exit	Exit out of class-map mode
(config)#class-map type qos c2	Enter Class-map mode
(config-cmap-qos)#match dscp 22	Configure match criteria as dscp 22
(config-cmap-qos)#match cos 4	Configure match criteria as cos 4
(config-cmap-qos)#exit	Exit out of class-map mode
(config)#policy-map type qos pmap1	Configure policy-map with name pmap1 and enter policymap mode
(config-pmap-qos)#class type qos c1	Assign Class c1 to Policy-map pmap1
(config-pmap-c-qos)#set qos-group 1	Remark frames with either cos 3 or dscp 10 to qos-group 1
(config-pmap-c-qos)#exit	Exit out of pmap-c mode
(config-pmap-qos)#class type qos c2	Assign Class c2 to Policy-map pmap1
(config-pmap-c-qos)#set qos-group 2	Remark frames with either cos 4 or dscp 22 to qos-group 1
(config-pmap-c-qos)#exit	Exit out of pmap-c mode
(config)#interface xe2	Enter interface mode
(config-if)#service-policy type queuing output P1	Attach service-policy P1 of type queuing on out direction
(config-if)#exit	Exit out of interface mode
(config)#interface xe3	Enter interface mode
(config-if)#service-policy type qos input pmap1	Attach service-policy pmap1 of type qos on in direction
(config-if)#exit	Exit out of interface mode

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
#show running-config qos qos
enable !
qos statistics ! class-map type qos
match-any c1  match dscp af11  match
cos 3 !
class-map type qos match-any c2
match cos 4 !
class-map type queuing match-any cq1
match qos-group 1 !
class-map type queuing match-any cq2
match qos-group 2 ! policy-map type qos
pmap1  class type qos c1   set qos-group
1
  exit  class type qos c2   set qos-group 2
exit policy-map type queuing p1  class type
queuing cq1   bandwidth percent 70   exit
```

```
class type queuing cq2   bandwidth remaining
percent 30   exit ! interface xe2
 service-policy type queuing output p1 !
interface  xe3   service-policy  type  qos  input
pmap1
```

Bandwidth Configuration

```
#show policy-map interface xe2

Interface xe2
Global statistics status : enabled

Service-policy (queuing) output: p1
------------------------------ Class-map
(queuing): cq1  match qos-group 1   bandwidth
percent 70
      output     : 4385296 packets, 298199584 bytes     dropped
: 0 packets, 0 bytes

 Class-map (queuing): cq2  match qos-group 2
bandwidth remaining percent 30        output     :
0 packets, 0 bytes       dropped     : 0 packets,
0 bytes Class-map (queuing): mc-q0        output
: 0 packets, 0 bytes       dropped     : 0
packets, 0 bytes

Class-map (queuing): mc-q1        output    : 0 packets, 0
bytes       dropped     : 0 packets, 0 bytes

Class-map (queuing): mc-q2        output    : 0 packets, 0
bytes       dropped     : 0 packets, 0 bytes

Class-map (queuing): mc-q3        output    : 0 packets, 0
bytes       dropped     : 0 packets, 0 bytes
```

```
Class-map (queuing): mc-q4       output     : 0 packets, 0
bytes       dropped     : 0 packets, 0 bytes


Class-map (queuing): mc-q5       output     : 0 packets, 0
bytes       dropped     : 0 packets, 0  bytes


Class-map (queuing): mc-q6       output     : 0 packets, 0
bytes       dropped     : 0 packets, 0  bytes


Class-map (queuing): mc-q7       output     : 0 packets, 0
bytes       dropped     : 0 packets, 0  bytes


Wred Drop Statistics : ---------------------
green  : 0 packets   yellow : 0 packets   red   :
0 packets




D-6K#show policy-map interface xe3 Interface
xe3 Global statistics status : enabled




Service-policy (qos) input     : pmap1
------------------------------- Class-map (qos): c1 (match any)
match dscp af11  match cos 3  set qos-group 1       matched
: 11469844 packets, 779950684 bytes


 Class-map (qos): c2 (match any)  match cos 4
set qos-group 2       matched    : 0 packets, 0
bytes




Service-policy (queuing) output: default-out-policy
------------------------------- Class-map
(queuing): q0  priority level 1       output
: 0 packets, 0 bytes       dropped    : 0
packets, 0 bytes


 Class-map (queuing): q1  priority level 1
```

```
      output    : 9753858 packets, 702277272 bytes      dropped
: 0 packets, 0 bytes


 Class-map (queuing): q2  priority level 1
output     : 0 packets, 0 bytes       dropped
: 0 packets, 0 bytes


 Class-map (queuing): q3  priority level 1
output     : 0 packets, 0 bytes        dropped
: 0 packets, 0 bytes   Class-map (queuing): q4
priority level 1       output     : 0 packets, 0
bytes       dropped    : 0 packets, 0 bytes


 Class-map (queuing): q5  priority level 1       output     : 0
packets, 0 bytes       dropped    : 0 packets, 0 bytes


 Class-map (queuing): q6  priority level 1       output     : 0
packets, 0 bytes       dropped    : 0 packets, 0 bytes


 Class-map (queuing): q7  priority level 1       output     : 0
packets, 0 bytes       dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q0       output     : 0 packets, 0
bytes       dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q1       output     : 0 packets, 0
bytes       dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q2       output     : 0 packets, 0
bytes       dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q3       output     : 0 packets, 0
bytes       dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q4       output     : 0 packets, 0
bytes       dropped    : 0 packets, 0 bytes Class-map
(queuing): mc-q5       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes
```

```
Class-map (queuing): mc-q6       output     : 0 packets, 0
bytes       dropped     : 0packets, 0  bytes


Class-map (queuing): mc-q7       output     : 0 packets, 0
bytes       dropped     : 0packets, 0  bytes


Wred Drop Statistics : ---------------------
green  : 0 packets   yellow: 0 packets   red     :
0 packets
```

CHAPTER 11 Shaping Configuration

This chapter contains a complete sample of configuring Shaping.

Topology

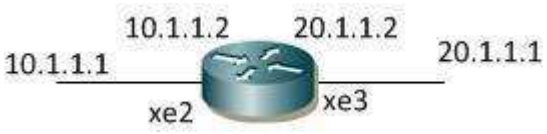


Figure 11-228: Simple configuration of Shaping

L2/L3 Interface

The following steps describe how to configure Shaping.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#class-map type queuing match-any cq1`	Configure class-map of type queuing with name cq1, and enter into class-map mode
`(config-cmap-que)#match qos-group 1`	Configure match criteria as qos-group 1
`(config-cmap-que)#exit`	Exit out of class-map mode
`(config)#class-map type queuing match-any cq2`	Configure class-map of type queuing with name cq2, and enter into class-map mode
`(config-cmap-que)#match qos-group 2`	Configure match criteria as qos-group 2
`(config-cmap-que)#exit`	Exit out of class-map mode
`(config)#policy-map type queuing P1`	Configure policy-map of type queuing with name P1, and enter into policy-map mode
`(config-pmap-que)#class type queuing cq1`	Attach class cq1 to Policy-map P1
`(config-pmap-c-que)#shape average 200 mbps`	Configure shaping to 200 mbps
`(config-pmap-c-que)#exit`	Exit out of policy-class mode
`(config-pmap-que)#class type queuing cq2`	Attach class cq2 to Policy-map P1
`(config-pmap-c-que)#shape average 150 mbps`	Configure shaping to 150 mbps
`(config-pmap-c-que)#exit`	Exit out of policy-class mode
`(config-pmap-que)#exit`	Exit out of Policy-map mode
`(config)#class-map type qos c1`	Enter Class-map mode
`(config-cmap-qos)#match dscp 10`	Configure match criteria as dscp 10
`(config-cmap-qos)#match cos 3`	Configure match criteria as cos 3

(config-cmap-qos)#exit	Exit out of class-map mode
(config)#class-map type qos c2	Enter Class-map mode
(config-cmap-qos)#match dscp 22	Configure match criteria as dscp 22
(config-cmap-qos)#match cos 4	Configure match criteria as cos 4
(config-cmap-qos)#exit	Exit out of class-map mode
(config)#policy-map type qos pmap1	Configure policy-map with name pmap1 and enter policymap mode
(config-pmap-qos)#class type qos c1	Assign Class c1 to Policy-map pmap1
(config-pmap-c-qos)#set qos-group 1	Remark frames with either cos 3 or dscp 10 to qos-group 1
(config-pmap-c-qos)#exit	Exit out of pmap-c mode
(config-pmap-qos)#class type qos c2	Assign Class c2 to Policy-map pmap1
(config-pmap-c-qos)#set qos-group 2	Remark frames with either cos 4 or dscp 22 to qos-group 1
(config-pmap-c-qos)#exit	Exit out of pmap-c mode
(config)#interface xe2	Enter interface mode
(config-if)#service-policy type queuing output P1	Attach service-policy P1 of type queuing on out direction
(config-if)#exit	Exit out of interface mode
(config)#interface xe3	Enter interface mode
(config-if)#service-policy type qos input pmap1	Attach service-policy pmap1 of type qos on in direction
(config-if)#exit	Exit out of interface mode

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
#show policy-map type queuing

Type queuing policy-maps ========================

policy-map type queuing P1  class type queuing cq1
shape average  200 mbps   exit  class type queuing cq2
shape average  150 mbps   exit

#show policy-map type qos

Type qos policy-maps ====================

policy-map type qos pmap1  class type qos c1   set
qos-group 1   exit  class type qos c2
  set   qos-group   2
exit
```

```
#show class-map type queuing

  Type            queuing             class-maps
=======================
      class-map type queuing match-any cq2
match qos-group 2

      class-map type queuing match-any cq1          match

qos-group 1       class-map type queuing match-any cqueuing-

class-default


#show class-map type qos

  Type qos class-maps
  ===================

      class-map type qos c2
match cos 4          match dscp
22

      class-map type qos c1
match cos 3          match dscp
10




#show queuing interface xe2

Egress Queuing for Ethernet xe2[System]
------------------------------------------------------------------------------------------
L0              L1              L2              Group  PrioLevel   Shape
Bandwidth ------------------------------------------------------------------
----------cq1                                                 1      -           200 mbps
cq2                                             2      -           150 mbps        #


#show policy-map interface xe3


Interface xe3
Global statistics status : enabled
```

```
Service-policy (qos) input     : pmap1
------------------------------ Class-map (qos): c1 (match all)
match dscp af11  match cos 3  set qos-group 1       matched    : 0
packets, 0 bytes


 Class-map (qos): c2 (match all)  match dscp af23  match cos 4  set
qos-group 2       matched    : 0 packets, 0 bytes




Service-policy (queuing) output: default-out-policy
------------------------------- Class-map (queuing): q0
priority level 1
      output     : 0 packets, 0 bytes       dropped    : 0 packets, 0 bytes


 Class-map (queuing): q1  priority level 1
      output     : 810205010 packets, 58334760216 bytes        dropped    : 0 packets, 0
bytes


 Class-map (queuing): q2  priority level 1
      output     : 0 packets, 0 bytes       dropped    : 0 packets, 0 bytes


 Class-map (queuing): q3  priority level 1
      output     : 0 packets, 0 bytes       dropped    : 0 packets, 0 bytes


 Class-map (queuing): q4
 priority level 1       output     : 0 packets, 0 bytes       dropped     : 0 packets,
0 bytes


 Class-map (queuing): q5  priority level 1       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes


 Class-map (queuing): q6  priority level 1       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes


 Class-map (queuing): q7  priority level 1       output     : 4 packets, 256 bytes
dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q0       output     : 0 packets, 0 bytes       dropped     : 0
packets, 0 bytes
```

```
Class-map (queuing): mc-q1       output     : 0 packets, 0 bytes       dropped    : 0
packets, 0 bytes

Class-map (queuing): mc-q2       output     : 0 packets, 0 bytes       dropped    : 0
packets, 0 bytes

Class-map (queuing): mc-q3       output     : 0 packets, 0 bytes       dropped    : 0
packets, 0 bytes

Class-map (queuing): mc-q4       output     : 0 packets, 0 bytes       dropped    : 0
packets, 0 bytes

Class-map (queuing): mc-q5       output     : 0 packets, 0 bytes       dropped    : 0
packets, 0 bytes

Class-map (queuing): mc-q6       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes

Class-map (queuing): mc-q7       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes

Wred Drop Statistics : ---------------------- green  :
0 packets  yellow : 0 packets  red    : 0 packets



D-6K#show policy-map interface xe2


Interface xe2
Global statistics status : enabled



Service-policy (queuing) output: p1
------------------------------- Class-map (queuing): cq1  match
qos-group 1  shape average 200 mbps
      output     : 194567830 packets, 13230611896 bytes       dropped    : 3175 packets,
215900 bytes
```

```
 Class-map (queuing): cq2  match qos-group 2  shape average 150 mbps
output      : 0 packets, 0 bytes       dropped     : 0 packets, 0 bytes


Class-map (queuing): mc-q0       output     : 0 packets, 0 bytes
dropped     : 0 packets,  0 bytes Class-map (queuing): mc-q1
output      : 0 packets,  0 bytes       dropped     : 0 packets, 0 bytes


Class-map (queuing): mc-q2       output     : 0 packets, 0 bytes       dropped     : 0
packets, 0 bytes


Class-map (queuing): mc-q3       output     : 0 packets, 0 bytes       dropped     : 0
packets, 0 bytes


Class-map (queuing): mc-q4       output     : 0 packets, 0 bytes       dropped     : 0
packets, 0 bytes


Class-map (queuing): mc-q5       output     : 0 packets, 0 bytes       dropped     : 0
packets, 0  bytes


Class-map (queuing): mc-q6       output     : 0 packets, 0 bytes       dropped     : 0
packets, 0  bytes


Class-map (queuing): mc-q7       output     : 0 packets, 0 bytes       dropped     : 0
packets, 0  bytes


Wred Drop Statistics : ---------------------- green  : 0 packets  yellow
: 0 packets   red   : 0 packets
```

CHAPTER 12 Priority Configuration

This chapter contains a complete sample of configuring Priority

Topology

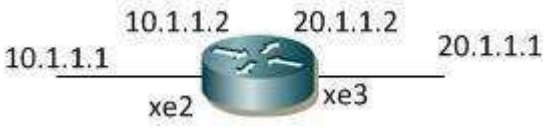


Figure 12-229: Simple configuration of Priority

Configuration of L2 /L3 Interface

The following steps describe how to configure priority level.By default all the system defined queues will be configured with priority level.We cannot configure Priority-level on user-defined queues.We can modify default queues from strictpriority to WRR, but cannot unconfigure it.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#policy-map type queuing default default-out-policy`	Enter policy-map type queueing default.
`(config-pmap-que-def)#class type queuing default q0`	Enter policy-class-map mode.
`(config-pmap-c-que-def)#wrr-queue weight 2`	Modify strict queue to wrr-queue with weight 2.
`(config-pmap-c-que-def)#exit`	Exit from policy-class-map mode.
`(config-pmap-que-def)#exit`	Exit from policy-map mode.
`(config)#exit`	Exit configure mode.

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
#show policy-map type queuing default default-out-policy
Type queuing policy-maps ========================

policy-map type queuing default default-out-policy
class type queuing default q0   wrr-queue weight 2
bandwidth percent 1   exit
 class type queuing default q1
priority level 1   bandwidth
percent 1   exit
 class type queuing default q2
```

Priority Configuration

```
  priority level 1
bandwidth percent 1   exit
 class type queuing default q3
priority level 1   bandwidth
percent 1   exit
 class type queuing default q4
priority level 1   bandwidth
percent 1   exit
 class type queuing default q5
priority level 1   bandwidth
percent 1   exit
 class type queuing default q6
priority level 1   bandwidth
percent 1   exit
 class type queuing default q7
priority level 1   bandwidth
percent 1   exit


#show queuing interface xe2

Egress Queuing for Ethernet xe2 [System]
-------------------------------------------------------------------------------------------
L0              L1             L2             Group  PrioLevel   Shape          Bandwidth ---
                                                                                     q0
-      -           -             q1                                              -      High
-              q2                                              -     High        -
q3                                             -      High        -              q4
-      High        -             q5                                              -      High
-              q6                                              -     High        -
q7                                             -      High        -              #
```

CHAPTER 13 WRED Configuration

This chapter contains a complete sample of configuring WRED.

Topology

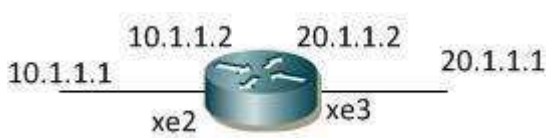


Figure 13-230: Simple configuration of WRED

L2/L3 Interface

The following steps describe how to configure WRED

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.

(config)#qos statistics	Enable QoS statistics.
(config)#class-map type queuing match-any cq1	Configure class-map of type queuing with name cq1, and enter into class-map mode
(config-cmap-que)#match qos-group 1	Configure match criteria as qos-group 1
(config-cmap-que)#exit	Exit out of class-map mode
(config)#class-map type queuing match-any cq2	Configure class-map of type queuing with name cq2, and enter into class-map mode
(config-cmap-que)#match qos-group 2	Configure match criteria as qos-group 2
(config-cmap-que)#exit	Exit out of class-map mode
(config)#class-map type queuing match-any cq3	Configure class-map of type queuing with name cq3, and enter into class-map mode
(config-cmap-que)#match qos-group 3	Configure match criteria as qos-group 3
(config-cmap-que)#exit	Exit out of class-map mode
(config)#policy-map type queuing P1	Configure policy-map of type queuing with name P1, and enter into policy-map mode
(config-pmap-que)#class type queuing cq1	Attach class cq1 to policy-map P1
(config-pmap-c-que)#shape percent 20	Configure shaping to 20 percent of bandwidth available on interface
(config-pmap-c-que)#random-detect minimumthreshold 50 maximum-threshold 80 kbytes	Configure WRED for minimum threshold of 50 kbytest and maximum threshold of 80 kbytes of queue size.
(config-pmap-c-que)#exit	Exit out of policy-class mode
(config-pmap-que)#class type queuing cq2	Attach class cq2 to policy-map P1
(config-pmap-c-que)#bandwidth 25000 kbps	Configure bandwidth to 25000 kbps
(config-pmap-c-que)#random-detect minimumthreshold 30 maximum-threshold 70 kbytes	Configure WRED for minimum threshold of 30 kbytes and maximum threshold of 70 kbytes .
(config-pmap-c-que)#exit	Exit out of policy-class mode

(config-pmap-que)#class type queuing cq3	Attach class cq3 to policy-map P1
(config-pmap-c-que)#)# random-detect minimumthreshold 20 maximum-threshold 50 kbytes	Configure WRED for minimum threshold of 20 and maximum threshold of 50 kbytes.
(config-pmap-c-que)#bandwidth rem per 20	Configure bandwidth remaining for 20%
(config-pmap-que)#exit	Exit out of policy-map mode
(config)#class-map type qos c1	Enter Class-map mode
(config-cmap-qos)#match precedence 2	Configure match criteria as precedence 2
(config-cmap-qos)#match cos 2	Configure match criteria as cos 2
(config-cmap-qos)#exit	Exit out of class-map mode
(config)#class-map type qos c2	Enter class-map mode
(config-cmap-qos)#match precedence 3	Configure match criteria as precedence 3
(config-cmap-qos)#match cos 3	Configure match criteria as cos 3
(config-cmap-qos)#exit	Exit out of class-map mode
(config)#class-map type qos c3	Enter Class-map mode
(config-cmap-qos)#match precedence 4	Configure match criteria as precedence 4
(config-cmap-qos)#match cos 4	Configure match criteria as cos 4
(config-cmap-qos)#exit	Exit out of class-map mode
(config)#policy-map type qos pmap1	Configure policy-map with name pmap1 and enter policymap mode
(config-pmap-qos)#class type qos c1	Assign Class c1 to policy-map pmap1
(config-pmap-c-qos)#set qos-group 1	Remark frames with either cos 2 or precedence 2 to qosgroup 1
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#class type qos c2	Assign Class c2 to policy-map pmap1
(config-pmap-c-qos)#set qos-group 2	Remark frames with either cos 3 or precedence 3 to qosgroup 2
(config-pmap-c-qos)#exit	Exit policy-class-map mode
(config-pmap-qos)#class type qos c3	Assign Class c3 to policy-map pmap1
(config-pmap-c-qos)#set qos-group 3	Remark frames with either cos 4 or precedence 4 to qosgroup 3
(config-pmap-c-qos)#exit	Exit policy-class-map mode
(config-pmap-qos)#exit	Exit policy-map mode
(config)#interface xe2	Enter interface mode
(config-if)#service-policy type queuing output P1	Attach service-policy P1 of type queuing on out direction
(config-if)#exit	Exit out of interface mode
(config)#interface xe3	Enter interface mode

(config-if)#service-policy type qos input pmap1	Attach service-policy pmap1 of type qos on in direction
(config-if)#exit	Exit out of interface mode

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos qos enable !
qos statistics ! class-map type qos c1 match precedence
immediate match cos 2 ! class-map type qos c2 match
precedence flash match cos 3 !

class-map type qos c3  match precedence flashoverride  match cos 4 !
class-map type queuing match-any cq1
 match qos-group 1
!class-map type queuing match-any cq2
 match qos-group 2
! class-map type queuing match-any cq3
 match qos-group 3 ! policy-map type qos pmap1  class
type qos c1   set qos-group 1   exit  class type qos c2
set qos-group 2   exit  class type qos c3   set qos-
group 3   exit
policy-map type queuing p1  class type queuing cq1   shape
average percent 20
  random-detect minimum-threshold 50 maximum-threshold 80 kbytes   exit  class type queuing cq2
  random-detect minimum-threshold 30 maximum-threshold 70 kbytes   bandwidth 25000 kbps   exit
class type queuing cq3
  random-detect minimum-threshold 20 maximum-threshold 50 kbytes
  bandwidth remaining percent 20   exit ! interface xe2
 service-policy type queuing output p1 !
interface xe3
 service-policy type qos input pmap1

#show policy-map interface xe2


Interface xe2
Global statistics status : enabled




Service-policy (queuing) output: p1
------------------------------- Class-map (queuing): cq1  match
qos-group 1  shape average percent 20
 random-detect minimum-threshold 50 maximum-threshold 80 kbytes percent
      output     : 0 packets, 0 bytes       dropped    : 0 packets, 0 bytes


 Class-map (queuing): cq2  match qos-group 2
 random-detect minimum-threshold 30 maximum-threshold 70 kbytes percent  bandwidth 25000 kbps
      output     : 194567830 packets, 13230611896 bytes       dropped    : 3175 packets,
215900 bytes


 Class-map (queuing): cq3 match qos-group 3 random-detect minimum-
 threshold 20 maximum-threshold 50 kbytes percent
```

```
 bandwidth remaining percent 20       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q0       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q1       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q2       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q3       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes Class-map (queuing): mc-q4
output     : 0 packets, 0 bytes       dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q5       output     : 0 packets, 0 bytes       dropped    : 0 packets,
0 bytes


Class-map (queuing): mc-q6       output     : 0 packets, 0 bytes       dropped    : 0 packets,
0 bytes


Class-map (queuing): mc-q7       output     : 0 packets, 0 bytes       dropped    : 0 packets,
0 bytes


Wred Drop Statistics : ---------------------- green  : 0 packets  yellow : 0
packets  red    : 0 packets



#show policy-map interface xe3


Interface xe3
Global statistics status : enabled



Service-policy (qos) input     : pmap1
------------------------------ Class-map (qos): c1 (match all)  match precedence immediate
match cos 2  set qos-group 1       matched    : 0 packets, 0 bytes


 Class-map (qos): c2 (match all)  match precedence flash  match cos 3  set qos-group 2
matched    : 0 packets, 0 bytes


 Class-map (qos): c3 (match all) match precedence flashoverride match cos 4 set qos-
group 3
```

```
    matched    : 0 packets, 0 bytes



Service-policy (queuing) output: default-out-policy
---------------------------------
  Class-map (queuing): q0  priority level 1        output    : 0 packets, 0
bytes       dropped    : 0 packets, 0 bytes


  Class-map (queuing): q1  priority level 1
      output      : 951907535 packets, 68537342016 bytes      dropped    : 0 packets, 0 bytes


  Class-map (queuing): q2  priority level 1        output    : 0 packets, 0
bytes       dropped    : 0 packets, 0 bytes


  Class-map (queuing): q3  priority level 1        output    : 0 packets, 0
bytes       dropped    : 0 packets, 0 bytes


  Class-map (queuing): q4  priority level 1        output    : 0 packets, 0
bytes       dropped    : 0 packets, 0 bytes


  Class-map (queuing): q5  priority level 1        output    : 0 packets, 0
bytes       dropped    : 0 packets, 0 bytes


  Class-map (queuing): q6  priority level 1        output    : 0 packets, 0
bytes       dropped    : 0 packets, 0 bytes


  Class-map (queuing): q7  priority level 1        output    : 0 packets, 0
bytes       dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q0       output     : 0 packets, 0 bytes       dropped
: 0 packets, 0 bytes Class-map (queuing): mc-q1       output     : 0 packets,
0 bytes       dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q2
output     : 0  packets, 0 bytes
dropped    : 0  packets, 0 bytes


Class-map (queuing): mc-q3
output     : 0  packets, 0 bytes
dropped    : 0  packets, 0 bytes


Class-map (queuing): mc-q4
output     : 0  packets, 0 bytes
dropped    : 0  packets, 0 bytes
```

```
Class-map (queuing): mc-q5
output     : 0 packets,  0bytes
dropped    : 0 packets,  0bytes


Class-map (queuing): mc-q6
output     : 0 packets,  0bytes
dropped    : 0 packets,  0bytes


Class-map (queuing): mc-q7
output     : 0 packets,  0bytes
dropped    : 0 packets,  0bytes


Wred Drop Statistics :
---------------------
green   : 0 packets
yellow : 0 packets
red     : 0 packets




#show queuing interface xe2

Egress Queuing for Ethernet xe2 [System]
-----------------------------------------------------------------------------------------------
-
L0              L1              L2              Group  PrioLevel   Shape          Bandwidth ---
                                                                                            cq1
1      -          20 percent     cq2                                                2      -
-              25000 kbps cq3                                              3      -            -
20 percent of remaining

#show queuing interface xe3

Egress Queuing for Ethernet xe3 [System] ------------------------------------------------
-------------------------------------------
L0              L1              L2              Group  PrioLevel   Shape          Bandwidth ---
                                                                                             q0
-      High        -              q1                                                -      High
-              q2                                                  -      High        -
q3                                                  -      High        -              q4
-      High        -              q5                                                -      High
-              q6                                                  -      High        -
q7                                                  -      High        -              #
```

CHAPTER 14 Tail-Drop Configuration

Topology

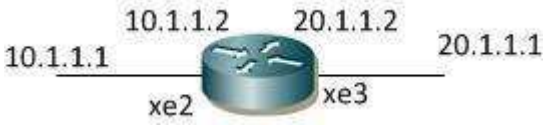


Figure 14-231: Simple configuration of Tail-Drop

Configuring Tail-Drop

The following steps describe how to configure Tail-Drop.

Configuration on L2/L3 Interfaces

Do the following to configure Tail-Drop on a queue.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos tsatistics`	Enable QoS statistics.
`(config)#class-map type queuing match-any cq1`	Configure class-map of type queuing with name cq1, and enter into class-map mode
`(config-cmap-que)#match qos-group 1`	Configure match criteria as qos-group 1
`(config-cmap-que)#exit`	Exit out of class-map mode
`(config)#class-map type queuing match-any cq2`	Configure class-map of type queuing with name cq2, and enter into class-map mode
`(config-cmap-que)#match qos-group 2`	Configure match criteria as qos-group 2
`(config-cmap-que)#exit`	Exit out of class-map mode
`(config)#class-map type queuing match-any cq3`	Configure class-map of type queuing with name cq3, and enter into class-map mode
`(config-cmap-que)#match qos-group 3`	Configure match criteria as qos-group 3
`(config-cmap-que)#exit`	Exit out of class-map mode
`(config)#policy-map type queuing P1`	Configure policy-map of type queuing with name P1, and enter into policy-map mode
`(config-pmap-que)#class type queuing cq1`	Attach class cq1 to policy-map P1
`(config-pmap-c-que)#shape percent 20`	Configure shaping to 20 percent of bandwidth available on interface
`(config-pmap-c-que)#queue-limit 100 packets`	Configure tail-drop for 100 packets
`(config-pmap-c-que)#exit`	Exit out of policy-class mode

(config-pmap-que)#class type queuing cq2	Attach class cq2 to policy-map P1
(config-pmap-c-que)#bandwidth 25000 kbps	Configure bandwidth to 25000 kbps
(config-pmap-c-que)#queue-limit 99 packets	Configure tail-drop to 99 packets
(config-pmap-c-que)#exit	Exit out of policy-class mode
(config-pmap-que)#class type queuing cq3	Attach class cq3 to policy-map P1
(config-pmap-c-que)#queue-limit 101 packets	Configure tail-drop to 101 packets
(config-pmap-que)#exit	Exit out of policy-map mode
(config)#class-map type qos c1	Enter Class-map mode
(config-cmap-qos)#match precedence 2	Configure match criteria as precedence 2
(config-cmap-qos)#match cos 2	Configure match criteria as cos 2
(config-cmap-qos)#exit	Exit out of class-map mode
(config)#class-map type qos c2	Enter Class-map mode
(config-cmap-qos)#match precedence 3	Configure match criteria as precedence 3
(config-cmap-qos)#match cos 3	Configure match criteria as cos 3
(config-cmap-qos)#exit	Exit out of class-map mode
(config)#class-map type qos c3	Enter Class-map mode
(config-cmap-qos)#match precedence 4	Configure match criteria as precedence 4
(config-cmap-qos)#match cos 4	Configure match criteria as cos 4
(config-cmap-qos)#exit	Exit out of class-map mode
(config)#policy-map type qos pmap1	Configure policy-map with name pmap1 and enter policymap mode
(config-pmap-qos)#class type qos c1	Assign Class c1 to policy-map pmap1
(config-pmap-c-qos)#set qos-group 1	Remark frames with either cos 2 or precedence 2 to qosgroup 1
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#class type qos c2	Assign Class c2 to policy-map pmap1
(config-pmap-c-qos)#set qos-group 2	Remark frames with either cos 3 or precedence 3 to qosgroup 2
(config-pmap-c-qos)#exit	Exit policy-class-map mode
(config-pmap-qos)#class type qos c3	Assign Class c3 to policy-map pmap1
(config-pmap-c-qos)#set qos-group 3	Remark frames with either cos 4 or precedence 4 to qosgroup 3
(config-pmap-c-qos)#exit	Exit policy-class-map mode
(config-pmap-qos)#exit	Exit pmap mode
(config)#interface xe2	Enter interface mode
(config-if)#service-policy type queuing output P1	Attach service-policy P1 of type queuing on out direction

(config-if)#exit	Exit out of interface mode
(config)#interface xe3	Enter interface mode
(config-if)#service-policy type qos input pmap1	Attach service-policy pmap1 of type qos on in direction
(config-if)#exit	Exit out of interface mode

Validation

Enter the commands below to confirm the configurations.

```
#show running-config qos qos enable !
qos statistics ! class-map type qos c1 match precedence immediate match
cos 2 ! class-map type qos c2 match precedence flash match cos 3 !
class-map type qos c3 match precedence flashoverride match cos 4 ! class-map type
queuing match-any cq1 match qos-group 1
! class-map type queuing match-any cq2  match qos-group 2
! class-map type queuing match-any cq3  match qos-group 3 ! policy-map type qos
pmap1  class type qos c1   set qos-group 1   exit  class type qos c2   set qos-group
2   exit  class type qos c3   set qos-group 3   exit policy-map type queuing p1
class type queuing cq1   shape average percent 20   queue-limit 100 packets   exit
class type queuing cq2   queue-limit 99 packets   bandwidth 25000 kbps   exit  class
type queuing cq3   queue-limit 101 packets   exit !
interface xe2  service-policy type queuing output p1 !
interface xe3  service-policy type qos input pmap1 show class-map

  Type qos class-maps   ===================       class-map type qos c1
match cos 2          match precedence immediate

      class-map type qos c2          match cos 3          match precedence
flash

      class-map type qos c3          match cos 4          match precedence flashoverride
class-map type qos match-any class-default


  Type queuing class-maps   ======================       class-map type queuing match-
any cq1          match qos-group 1

      class-map type queuing match-any cq2          match qos-group 2

      class-map type queuing match-any cq3          match qos-group 3       class-map

match-any q0       class-map match-any q1       class-map match-any q2       class-map

match-any q3       class-map match-any q4       class-map match-any q5       class-map

match-any q6       class-map match-any q7

show policy-map

Type qos policy-maps ====================

policy-map type qos pmap1 class type qos c1 set qos-group 1 exit class type qos
c2 set qos-group 2 exit class type qos c3 set qos-group 3 exit
```

```
Type queuing policy-maps ========================

policy-map type queuing p1   class type queuing cq1    shape average percent 20
queue-limit 100 packets    exit   class type queuing cq2    queue-limit 99 packets
bandwidth 25000 kbps    exit   class type queuing cq3    queue-limit 101 packets    exit



show policy-map interface xe2


Interface xe2
Global statistics status : enabled



Service-policy (queuing) output: p1
------------------------------- Class-map (queuing): cq1  match qos-group 1  shape average
percent 20  queue-limit 100 packets       output     : 0 packets, 0 bytes       dropped     : 0
packets, 0 bytes  Class-map (queuing): cq2  match qos-group 2  queue-limit 99 packets
bandwidth 25000 kbps
      output     : 194567830 packets, 13230611896 bytes       dropped    : 3175 packets, 215900
bytes


 Class-map (queuing): cq3  match qos-group 3  queue-limit 101 packets
output     : 0 packets, 0 bytes       dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q0       output     : 0 packets, 0 bytes       dropped
: 0 packets,  0 bytes


Class-map (queuing): mc-q1       output     : 0 packets, 0 bytes       dropped
: 0 packets,  0 bytes


Class-map (queuing): mc-q2       output     : 0 packets, 0 bytes       dropped
: 0 packets,  0 bytes


Class-map (queuing): mc-q3       output     : 0 packets, 0 bytes       dropped
: 0 packets,  0 bytes


Class-map (queuing): mc-q4       output     : 0 packets, 0 bytes       dropped
: 0 packets,  0 bytes


Class-map (queuing): mc-q5       output     : 0 packets, 0 bytes       dropped
: 0 packets,  0 bytes


Class-map (queuing): mc-q6       output     : 0 packets, 0 bytes       dropped
: 0 packets,  0 bytes
```

```
Class-map (queuing): mc-q7       output      : 0 packets, 0 bytes       dropped
: 0 packets, 0 bytes


Wred Drop Statistics : ---------------------     green  : 0 packets
yellow : 0 packets  red    : 0 packets



show policy-map interface xe3


Interface xe3
Global statistics status : enabled



Service-policy (qos) input     : pmap1
------------------------------- Class-map (qos): c1 (match all)  match
precedence immediate  match cos 2  set qos-group 1       matched    : 0
packets, 0 bytes


 Class-map (qos): c2 (match all)  match precedence flash  match cos 3  set
qos-group 2       matched    : 0 packets, 0 bytes


 Class-map (qos): c3 (match all)  match precedence flashoverride  match cos 4
set qos-group 3       matched    : 0 packets, 0 bytes



Service-policy (queuing) output: default-out-policy
--------------------------------
 Class-map (queuing): q0  priority level 1        output     : 0 packets,  0
bytes       dropped    : 0 packets, 0 bytes


 Class-map (queuing): q1  priority level 1
      output      : 547547300 packets, 39423405024 bytes       dropped    : 0 packets, 0 bytes


 Class-map (queuing): q2  priority level 1        output     : 0 packets,  0
bytes       dropped    : 0 packets, 0 bytes   Class-map (queuing): q3
priority level 1       output     : 0 packets, 0 bytes        dropped    : 0
packets, 0 bytes


 Class-map (queuing): q4  priority level 1        output     : 0 packets,  0 bytes       dropped
: 0 packets, 0 bytes


 Class-map (queuing): q5  priority level 1        output     : 0 packets,  0 bytes       dropped
: 0 packets, 0 bytes
```

```
 Class-map (queuing): q6  priority level 1       output     : 0 packets, 0 bytes       dropped
: 0 packets, 0 bytes


 Class-map (queuing): q7  priority level 1       output     : 0 packets, 0 bytes       dropped
: 0 packets, 0 bytes


Class-map (queuing): mc-q0       output     : 0 packets, 0 bytes       dropped    : 0 packets,
0 bytes


Class-map (queuing): mc-q1       output     : 0 packets, 0 bytes       dropped    : 0 packets,
0 bytes


Class-map (queuing): mc-q2       output     : 0 packets, 0 bytes       dropped    : 0 packets,
0 bytes


Class-map (queuing): mc-q3       output     : 0 packets, 0 bytes       dropped    : 0 packets,
0 bytes


Class-map (queuing): mc-q4       output     : 0 packets, 0 bytes       dropped    : 0 packets,
0 bytes


Class-map (queuing): mc-q5       output     : 0 packets, 0 bytes       dropped    : 0 packets,
0 bytes Class-map (queuing): mc-q6       output     : 0 packets, 0 bytes       dropped     : 0
packets, 0 bytes


Class-map (queuing): mc-q7
output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes


Wred Drop Statistics :
---------------------
green   : 0 packets
yellow : 0 packets
red     : 0 packets




show queuing interface xe2

Egress Queuing for Ethernet xe2 [System]
------------------------------------------------------------------------------------------------
-
----
L0              L1              L2              Group  PrioLevel   Shape          Bandwidth ---
------------------------------------------------------------------------------------------------
----
```

```
cq1                                                1      -          20 percent     cq2
2       -           -             25000 kbps cq3
3       -           -             -


show queuing interface xe3

Egress Queuing for Ethernet xe3 [System]
-------------------------------------------------------------------------------------
L0               L1              L2              Group  PrioLevel    Shape

Bandwidth ------------------------------------------------------------------------
------q0                                                -      High         -             q1
-      High         -             q2                                                -
High         -             q3                                                -     High
-               q4                                                -      High        -
q5                                                -      High         -             q6
-      High         -             q7                                                -
High         -             -
```

CHAPTER 15 Hierarchical Queuing Configuration

This chapter contains a complete sample of configuring hierarchical queuing.

Topology

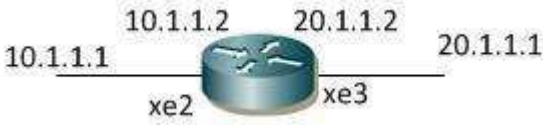


Figure 15-232: Simple configuration of Hierarchical Queuing

Configuring Hierarchical Queuing

Do the following to configure 3-level hierarchical queuing on an interface.

`#configure terminal`	Enter configure mode.
`(config)#qos enable`	Enable QoS globally.
`(config)#qos statistics`	Enable QoS statistics.
`(config)#class-map type qos match-any C_QOS1`	Configure class-map C_QOS1 of type qos and enter into class-map mode
`(config-cmap-qos)#match cos 0`	Configure match criteria as cos 0
`(config-cmap-qos)#match dscp 0-7`	Configure match criteria as dscp 0-7
`(config-cmap-qos)#exit`	Exit out of cmap mode
`(config)#class-map type qos match-any C_QOS2`	Configure class-map C_QOS2 of type qos and enter into class-map mode
`(config-cmap-qos)#match cos 1`	Configure match criteria as cos 1
`(config-cmap-qos)#match dscp 8-15`	Configure match criteria as dscp 8-15
`(config-cmap-qos)#exit`	Exit out of cmap mode
`(config)#class-map type qos match-any C_QOS3`	Configure class-map C_QOS3 of type qos and enter into class-map mode
`(config-cmap-qos)#match cos 2`	Configure match criteria as cos 2
`(config-cmap-qos)#match dscp 16-23`	Configure match criteria as dscp 16-23
`(config-cmap-qos)#exit`	Exit out of cmap mode
`(config)#class-map type qos match-any C_QOS4`	Configure class-map C_QOS4 of type qos and enter into class-map mode
`(config-cmap-qos)#match cos 3`	Configure match criteria as cos 3
`(config-cmap-qos)#match dscp 24-31`	Configure match criteria as dscp 24-31
`(config-cmap-qos)#exit`	Exit out of cmap mode
`(config)#class-map type qos match-any C_QOS5`	Configure class-map C_QOS5 of type qos and enter into class-map mode

(config-cmap-qos)#match cos 4	Configure match criteria as cos 4
(config-cmap-qos)#match dscp 32-39	Configure match criteria as dscp 32-39

(config-cmap-qos)#exit	Exit out of cmap mode
(config)#class-map type qos match-any C_QOS6	Configure class-map C_QOS6 of type qos and enter into class-map mode
(config-cmap-qos)#match cos 5	Configure match criteria as cos 5
(config-cmap-qos)#match dscp 40-47	Configure match criteria as dscp 40-47
(config-cmap-qos)#exit	Exit out of cmap mode
(config)#class-map type qos match-any C_QOS7	Configure class-map C_QOS7 of type qos and enter into class-map mode
(config-cmap-qos)#match cos 6	Configure match criteria as cos 6
(config-cmap-qos)#match dscp 48-55	Configure match criteria as dscp 48-55
(config-cmap-qos)#exit	Exit out of cmap mode
(config)#class-map type qos match-any C_QOS8	Configure class-map C_QOS8 of type qos and enter into class-map mode
(config-cmap-qos)#match cos 7	Configure match criteria as cos 7
(config-cmap-qos)#match dscp 56-63	Configure match criteria as dscp 56-63
(config-cmap-qos)#exit	Exit out of cmap mode
(config)#class-map type queuing match-any cq1	Configure class-map cq1 of type queuing and enter into class-map mode.
(config-cmap-que)#match qos-group 1	Configure match criteria as qos-group 1
(config-cmap-que)#exit	Exit out of cmap mode.
(config)#class-map type queuing match-any cq2	Configure class-map cq2 of type queuing and enter into class-map mode.
(config-cmap-que)#match qos-group 2	Configure match criteria as qos-group 2
(config-cmap-que)#exit	Exit out of cmap mode.
(config)#class-map type queuing match-any cq3	Configure class-map cq3 of type queuing and enter into class-map mode.
(config-cmap-que)#match qos-group 3	Configure match criteria as qos-group 3
(config-cmap-que)#exit	Exit out of cmap mode.
(config)#class-map type queuing match-any cq4	Configure class-map cq4 of type queuing and enter into class-map mode.
(config-cmap-que)#match qos-group 4	Configure match criteria as qos-group 4
(config-cmap-que)#exit	Exit out of cmap mode.
(config)#class-map type queuing match-any cq5	Configure class-map cq5 of type queuing and enter into class-map mode.
(config-cmap-que)#match qos-group 5	Configure match criteria as qos-group 5
(config-cmap-que)#exit	Exit out of cmap mode.

(config)#class-map type queuing match-any cq6	Configure class-map cq6 of type queuing and enter into class-map mode.
(config-cmap-que)#match qos-group 6	Configure match criteria as qos-group 6
(config-cmap-que)#exit	Exit out of cmap mode.
(config)#class-map type queuing match-any cq7	Configure class-map cq7 of type queuing and enter into class-map mode.
(config-cmap-que)#match qos-group 7	Configure match criteria as qos-group 7
(config-cmap-que)#exit	Exit out of cmap mode.

(config)#class-map type queuing match-any cq8	Configure class-map cq8 of type queuing and enter into class-map mode.
(config-cmap-que)#match qos-group 8	Configure match criteria as qos-group 8
(config-cmap-que)#exit	Exit out of cmap mode.
(config)#policy-map type qos pmap1	Configure policy-map pmap1 og type qos and enter into policy-map mode.
(config-pmap-qos)#class type qos C_QOS1	Assign class C-QOS1 to pmap1 and enter into policy-classmap mode.
(config-pmap-c-qos)#set qos-group 1	Remark matched traffic to qos-group 1
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#class type qos C_QOS2	Assign class C-QOS2 to pmap1 and enter into policy-classmap mode.
(config-pmap-c-qos)#set qos-group 2	Remark matched traffic to qos-group 2
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#class type qos C_QOS3	Assign class C-QOS3 to pmap1 and enter into policy-classmap mode.
(config-pmap-c-qos)#set qos-group 3	Remark matched traffic to qos-group 3
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#class type qos C_QOS4	Assign class C-QOS4 to pmap1 and enter into policy-classmap mode.
(config-pmap-c-qos)#set qos-group 4	Remark matched traffic to qos-group 4
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#class type qos C_QOS5	Assign class C-QOS5 to pmap1 and enter into policy-classmap mode.
(config-pmap-c-qos)#set qos-group 5	Remark matched traffic to qos-group 5
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#class type qos C_QOS6	Assign class C-QOS6 to pmap1 and enter into policy-classmap mode.
(config-pmap-c-qos)#set qos-group 6	Remark matched traffic to qos-group 6
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#class type qos C_QOS7	Assign class C-QOS7 to pmap1 and enter into policy-classmap mode.

(config-pmap-c-qos)#set qos-group 7	Remark matched traffic to qos-group 7
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#class type qos C_QOS8	Assign class C-QOS8 to pmap1 and enter into policy-classmap mode.
(config-pmap-c-qos)#set qos-group 8	Remark matched traffic to qos-group 8
(config-pmap-c-qos)#exit	Exit out of policy-class-map mode
(config-pmap-qos)#exit	Exit out of policy-map mode
(config)#policy-map type queuing P1P1	Configure policy-map of type queuing P1P1 and enter into policy-map mode.
(config-pmap-que)#class type queuing cq1	Assign class cq1 to policy-map P1 and enter into policyclass-map mode.
(config-pmap-c-que)#shape average percent 20	Shape the matched traffic to percent 20
(config-pmap-c-que)#queue-limit 70 packets	Configure tail-drop on q1 to 70 packets.

(config-pmap-c-que)#bandwidth percent 18	Configure minimum bandwidth to 18 percent on q1.
(config-pmap-c-que)#exit	Exit out of policy-class-map mode.
(config-pmap-que)#class type queuing cq2	Assign class cq2 to policy-map P1 and enter into policyclass-map mode.
(config-pmap-c-que)#shape average percent 80	Shape the matched traffic to percent 80
(config-pmap-c-que)#queue-limit 70 packets	Configure tail-drop on q2 to 70 packets.
(config-pmap-c-que)#bandwidth percent 75	Configure minimum bandwidth to 75 percent on q2.
(config-pmap-c-que)#exit	Exit out of policy-class-map mode.
(config-pmap-que)#exit	Exit out of policy-map mode.
(config)#policy-map type queuing P2	Configure policy-map of type queuing P2 and enter into policy-map mode.
(config-pmap-que)#class type queuing cq3	Assign class cq3 to policy-map P2 and enter into policyclass-map mode.
(config-pmap-c-que)#shape average percent 25	Shape the matched traffic to percent 25
(config-pmap-c-que)#random-detect minimumthreshold 50 maximum-threshold 75 kbytes	Configure WRED on q3 to minimum threshold 50 and maximum threshold 75 packets.
(config-pmap-c-que)#bandwidth percent 20	Configure minimum bandwidth to 20 percent on q3.
(config-pmap-c-que)#exit	Exit out of policy-class-map mode.
(config-pmap-que)#class type queuing cq4	Assign class cq4 to policy-map P2 and enter into policyclass-map mode.
(config-pmap-c-que)#shape average percent 75	Shape the matched traffic to percent 75
(config-pmap-c-que)#random-detect minimumthreshold 50 maximum-threshold 75 kbytes	Configure WRED on q4 to minimum threshold 50 and maximum threshold 75 kbytes.
(config-pmap-c-que)#bandwidth percent 65	Configure minimum bandwidth to 65 percent on q4.
(config-pmap-c-que)#exit	Exit out of policy-class-map mode.

(config-pmap-que)#exit	Exit out of policy-map mode.
(config)#policy-map type queuing P3	Configure policy-map of type queuing P3 and enter into policy-map mode.
(config-pmap-que)#class type queuing cq5	Assign class cq5 to policy-map P3 and enter into policyclass-map mode.
(config-pmap-c-que)#shape average percent 40	Shape the matched traffic to percent 40
(config-pmap-c-que)#queue-limit 100 packets	Configure Tail-Drop on q5 to 100 packets.
(config-pmap-c-que)#bandwidth percent 35	Configure minimum bandwidth to 35 percent on q5.
(config-pmap-c-que)#exit	Exit out of policy-class-map mode.
(config-pmap-que)#class type queuing cq6	Assign class cq6 to policy-map P3 and enter into policyclass-map mode.
(config-pmap-c-que)#shape average percent 60	Shape the matched traffic to percent 60
(config-pmap-c-que)#queue-limit 100 packets	Configure Tail-Drop on q6 to 100 packets.
(config-pmap-c-que)#bandwidth percent 55	Configure minimum bandwidth to 55 percent on q6.
(config-pmap-c-que)#exit	Exit out of policy-class-map mode.
(config-pmap-que)#exit	Exit out of policy-map mode.
(config)#policy-map type queuing P4	Configure policy-map of type queuing P4 and enter into policy-map mode.
(config-pmap-que)#class type queuing cq7	Assign class cq7 to policy-map P4 and enter into policyclass-map mode.

(config-pmap-c-que)#shape average percent 40	Shape the matched traffic to percent 40
(config-pmap-c-que)#random-detect minimumthreshold 80 packets maximum-threshold 100 packets	Configure WRED on q7 to maximum threshold of 80 packets and maximum threshold of 100 packets..
(config-pmap-c-que)#bandwidth percent 35	Configure minimum bandwidth to 35 percent on q7.
(config-pmap-c-que)#exit	Exit out of policy-class-map mode.
(config-pmap-que)#class type queuing cq8	Assign class cq8 to policy-map P4 and enter into policyclass-map mode.
(config-pmap-c-que)#shape average percent 60	Shape the matched traffic to percent 60
(config-pmap-c-que)#random-detect minimumthreshold 80 packets maximum-threshold 100 packets	Configure WRED on q8 to minimum threshold of 80 packets and maximum threshold of 100 packets..
(config-pmap-c-que)#bandwidth percent 55	Configure minimum bandwidth to 55 percent on q8.
(config-pmap-c-que)#exit	Exit out of policy-class-map mode.
(config-pmap-que)#exit	Exit out of policy-map mode.
(config)#class-map type queuing match-any empty1	Configure class-map of type queuing empty1
(config-cmap-que)#exit	Exit out of cmap mode
(config)#class-map type queuing match-any empty2	Configure class-map of type queuing empty2

(config-cmap-que)#exit	Exit out of cmap mode
(config)#class-map type queuing match-any empty3	Configure class-map of type queuing empty3
(config-cmap-que)#exit	Exit out of cmap mode
(config)#class-map type queuing match-any empty4	Configure class-map of type queuing empty4
(config-cmap-que)#exit	Exit out of cmap mode
(config)#class-map type queuing match-any empty5	Configure class-map of type queuing empty5
(config-cmap-que)#exit	Exit out of cmap mode
(config)#class-map type queuing match-any empty6	Configure class-map of type queuing empty6
(config-cmap-que)#exit	Exit out of cmap mode
(config)#policy-map type queuing P1P2	Configure policy-map of type queuing P1P2 and enter into policy-map mode.
(config-pmap-que)#class type queuing empty1	Assign class-map of type queuing empty1 to P1P2 and enter into policy-class-map mode.
(config-pmap-c-que)#shape average percent 40	Shape the matched traffic to 40 percent
(config-pmap-c-que)#bandwidth percent 30	Configure minimum bandwidth to 30 percent on empty1.
(config-pmap-c-que)#service-policy P1P1	Assign service-policy P1P1
(config-pmap-c-que)#exit	Exit out of policy-class-map mode.
(config-pmap-que)#class type queuing empty2	Assign class-map of type queuing empty2 to P1P2 and enter into policy-class-map mode.
(config-pmap-c-que)#shape average percent 60	Shape the matched traffic to 60 percent
(config-pmap-c-que)#bandwidth percent 55	Configure minimum bandwidth to 55 percent on empty2.
(config-pmap-c-que)#service-policy P2	Assign service-policy P2

(config-pmap-c-que)#exit	Exit out of policy-class-map mode.
(config-pmap-que)#exit	Exit out of policy-map mode.
(config)#policy-map type queuing P3P4	Configure policy-map of type queuing P3P4 and enter into policy-map mode.
(config-pmap-que)#class type queuing empty3	Assign class-map of type queuing empty3 to P3P4 and enter into policy-class-map mode.
(config-pmap-c-que)#shape average percent 40	Shape the matched traffic to 40 percent
(config-pmap-c-que)#bandwidth percent 35	Configure minimum bandwidth to 35 percent on empty3.
(config-pmap-c-que)#service-policy P3	Assign service-policy P3
(config-pmap-c-que)#exit	Exit out of policy-class-map mode.
(config-pmap-que)#class type queuing empty4	Assign class-map of type queuing empty4 to P3P4 and enter into policy-class-map mode.
(config-pmap-c-que)#shape average percent 60	Shape the matched traffic to 60 percent
(config-pmap-c-que)#bandwidth percent 50	Configure minimum bandwidth to 50 percent on empty4.

(config-pmap-c-que)#service-policy P4	Assign service-policy P4
(config-pmap-c-que)#exit	Exit out of policy-class-map mode.
(config-pmap-que)#exit	Exit out of policy-map mode.
(config)#policy-map type queuing Pend	Configure policy-map of type queuing Pend and enter into policy-map mode.
(config-pmap-que)#class type queuing empty5	Assign class-map of type queuing empty5 to Pend and enter into policy-class-map mode.
(config-pmap-c-que)#shape average 400 mbps	Shape the matched traffic to 400 mbps
(config-pmap-c-que)#bandwidth 350 mbps	Configure minimum bandwidth to 350 mbps.
(config-pmap-c-que)#service-policy P1P1	Assign service-policy P1P1
(config-pmap-c-que)#exit	Exit out of policy-class-map mode.
(config-pmap-que)#class type queuing empty6	Assign class-map of type queuing empty6 to Pend and enter into policy-class-map mode.
(config-pmap-c-que)#shape average 500 mbps	Shape the matched traffic to 500 mbps
(config-pmap-c-que)#bandwidth 450 mbps	Configure minimum bandwidth to 450 mbps.
(config-pmap-c-que)#service-policy P3P4	Assign service-policy P3P4
(config-pmap-c-que)#exit	Exit out of policy-class-map mode.
(config-pmap-que)#exit	Exit out of policy-map mode.
(config)#interface xe2	Enter into interface mode
(config-if)#service-policy type qos input pmap1	Assign service-policy of type qos policy-map1.
(config-if)#exit	Exit out of intf mode
(config)#interface xe3	Enter into interface mode
(config-if)#service-policy type queuing output Pend	Assign service-policy of type queing pend on out direction.
(config-if)#exit	Exit out of interface mode
(config)#set qos wrr uc 1 non-uc 2	Schedule unicast and multicast traffic in 1:2
(config)#set qos sp	Set strict priority between unicast and multicast traffic, with higher priority to multicast traffic
(config)#interface xe49/2	Enter interface mode
(config-if)#set qos wrr uc 1 non-uc 2	Schedule unicast and multicast traffic in 1:2 on particular interface
(config-if)#set qos sp	Set strict priority between unicast and multicast traffic, with higher priority to multicast traffic on particular interface
(config-if)#exit	Exit interface mode

Validation

Enter the commands listed in the sections below to confirm the configurations.

```
#show running-config qos qos enable
!
```

```
    qos statistics
    !
    class-map type qos match-any C_QOS1 match dscp 0-7 match
    cos 0

    ! class-map type qos match-any C_QOS2 match dscp 8-15
    match cos 1
    ! class-map type qos match-any C_QOS3 match dscp 16-23
    match cos 2
    ! class-map type qos match-any C_QOS4 match dscp 24-31
    match cos 3
    ! class-map type qos match-any C_QOS5 match dscp 32-39
    match cos 4
    ! class-map type qos match-any C_QOS6 match dscp 40-47
    match cos 5
!
    class-map type qos match-any C_QOS7 match dscp 48-55
    match cos 6
!
    class-map type qos match-any C_QOS8 match dscp 56-63
    match cos 7
    ! class-map type queuing match-any cq1  match qos-group 1
!
    class-map type queuing match-any cq2  match qos-group 2
    ! class-map type queuing match-any cq3  match qos-group 3
! class-map type queuing match-any cq4  match qos-group 4
! class-map type queuing match-any cq5  match qos-group 5
! class-map type queuing match-any cq6  match qos-group 6
! class-map type queuing match-any cq7  match qos-group 7
! class-map type queuing match-any cq8  match qos-group 8
!
class-map type queuing match-any empty1
!
class-map type queuing match-any empty2
!
class-map type queuing match-any empty3
!
class-map type queuing match-any empty4
!
class-map type queuing match-any empty5
!
class-map type queuing match-any empty6
! policy-map type qos pmap1  class type qos C_QOS1   set qos-group
1   exit   class type qos C_QOS2   set qos-group 2   exit   class
type qos C_QOS3   set qos-group 3    exit  class type qos C_QOS4
set qos-group 4    exit  class type qos C_QOS5   set qos-group 5
exit  class type qos C_QOS6    set qos-group 6  exit   class type
qos C_QOS7   set qos-group 7    exit  class type qos C_QOS8    set
qos-group 8   exit policy-map type queuing p1   class type queuing
```

```
cq1    shape average percent 20   queue-limit 70 packets
bandwidth percent 18   exit
 class type queuing cq2   shape average
percent 80   queue-limit 70 packets
bandwidth percent 75   exit
policy-map type queuing p1p1   class type
queuing empty1   shape average percent 40
bandwidth percent 30   service-policy p1
exit
 class type queuing empty2    shape
average percent 60    bandwidth percent
55   service-policy p2    exit
policy-map type queuing p2   class type
queuing cq3    shape average percent 25
  random-detect minimum-threshold 50 maximum-threshold 75 kbytes   bandwidth
percent 20   exit
 class type queuing cq4   shape average
percent 75
  random-detect minimum-threshold 50 maximum-threshold 75 kbytes   bandwidth
percent 65   exit
policy-map type queuing p3   class type
queuing cq5    shape average percent 40
queue-limit 100 packets   bandwidth
percent 35   exit
 class type queuing cq6   shape average
percent 60   queue-limit 100 packets
bandwidth percent 55   exit
policy-map type queuing p3p4   class type
queuing empty3   shape average percent 40
bandwidth percent 35   service-policy p3
exit
 class type queuing empty4    shape
average percent 60    bandwidth percent
50   service-policy p4    exit
policy-map type queuing p4   class type
queuing cq7    shape average percent 40
  random-detect minimum-threshold 80 maximum-threshold 100 packets   bandwidth
percent 35
  exit
 class type queuing cq8   shape average
percent 60
  random-detect minimum-threshold 80 maximum-threshold 100 packets   bandwidth
percent 55   exit
policy-map type queuing pend   class type
queuing empty5   shape average 400 mbps
bandwidth 350 kbps    service-policy p1p1
exit
 class type queuing empty6    shape
average 500 mbps    bandwidth 450 kbps
service-policy p3p4   exit
```

```
!
interface xe2
 service-policy type qos input pmap1
! interface xe3
 service-policy type queuing output pend


#show class-map

  Type qos class-maps   ===================
      class-map type qos match-any C_QOS1
match cos 0          match dscp 0-7

      class-map type qos match-any C_QOS2
match cos 1          match dscp 8-15

      class-map type qos match-any C_QOS3
match cos 2          match dscp 16-23

      class-map type qos match-any C_QOS4
match cos 3          match dscp 24-31

      class-map type qos match-any C_QOS5
match cos 4          match dscp 32-39

      class-map type qos match-any C_QOS6
match cos 5          match dscp 40-47

      class-map type qos match-any C_QOS7
match cos 6          match dscp 48-55
      class-map type qos match-any C_QOS8          match cos 7          match
dscp 56-63       class-map type qos match-any class-default


  Type queuing class-maps   ======================       class-map type
queuing match-any cq1          match qos-group 1

      class-map type queuing match-any cq2          match qos-group 2

      class-map type queuing match-any cq3          match qos-group 3

      class-map type queuing match-any cq4          match qos-group 4

      class-map type queuing match-any cq5          match qos-group 5

      class-map type queuing match-any cq6          match qos-group 6

      class-map type queuing match-any cq7          match qos-group 7

      class-map type queuing match-any cq8          match qos-group 8

class-map type queuing match-any empty1       class-map type queuing match-

any empty2       class-map type queuing match-any empty3       class-map
```

```
type queuing match-any empty4        class-map type queuing match-any empty5

class-map type queuing match-any empty6        class-map match-any q0

class-map match-any q1        class-map match-any q2        class-map match-

any q3        class-map match-any q4        class-map match-any q5

                  class-map match-any q6        class-map match-any q7


#show policy-map

Type qos policy-maps ====================

policy-map type qos pmap1  class type qos C_QOS1    set qos-group 1    exit
class type qos C_QOS2    set qos-group 2   exit    class type qos C_QOS3   set
qos-group 3   exit  class type qos C_QOS4   set qos-group 4   exit   class
type qos C_QOS5   set qos-group 5   exit  class type qos C_QOS6    set qos-
group 6   exit  class type qos C_QOS7   set qos-group 7   exit   class type
qos C_QOS8   set qos-group 8    exit


Type queuing policy-maps ========================

policy-map type queuing p1  class type queuing cq1    shape average percent 20
queue-limit 70 packets   bandwidth percent 18    exit  class type queuing cq2
shape average percent 80   queue-limit 70 packets    bandwidth percent 75
exit

policy-map type queuing p1p1  class type queuing empty1   shape average percent
40   bandwidth percent 30   service-policy p1
  exit
 class type queuing empty2    shape
average percent 60   bandwidth percent
55   service-policy p2   exit

policy-map type queuing p2   class type
queuing cq3   shape average percent 25
  random-detect minimum-threshold 50 maximum-threshold 75 kbytes    bandwidth
percent 20   exit
 class type queuing cq4   shape average
percent 75
  random-detect minimum-threshold 50 maximum-threshold 75 kbytes    bandwidth
percent 65   exit

policy-map type queuing p3   class type
queuing cq5   shape average percent 40
queue-limit 100 packets   bandwidth
percent 35   exit
 class type queuing cq6   shape average
percent 60   queue-limit 100 packets
bandwidth percent 55   exit
```

```
policy-map type queuing p3p4   class type
queuing empty3   shape average percent 40
bandwidth percent 35    service-policy p3
exit
 class type queuing empty4   shape
average percent 60    bandwidth percent
50   service-policy p4    exit

policy-map type queuing p4   class type
queuing cq7    shape average percent 40
  random-detect minimum-threshold 80 maximum-threshold 100 packets   bandwidth
percent 35   exit
 class type queuing cq8    shape average
percent 60
  random-detect minimum-threshold 80 maximum-threshold 100 packets   bandwidth
percent 55   exit

policy-map type queuing pend   class type
queuing empty5   shape average 400 mbps
bandwidth 350 kbps    service-policy p1p1
exit
 class type queuing empty6   shape average 500
mbps   bandwidth 450 kbps    service-policy p3p4
exit




#show policy-map interface xe2


Interface xe2
Global statistics status : enabled



Service-policy (qos) input     : pmap1
------------------------------ Class-map (qos): C_QOS1 (match any)  match dscp
0-7  match cos 0  set qos-group 1       matched    : 141900456 packets,
10216834992 bytes


 Class-map (qos): C_QOS2 (match any)  match dscp 8-15  match cos 1
set qos-group 2       matched    : 125 packets, 9000 bytes


 Class-map (qos): C_QOS3 (match any)  match dscp 16-23  match
cos 2  set qos-group 3       matched    : 0 packets, 0 bytes
```

```
 Class-map (qos): C_QOS4 (match any)  match dscp 24-31  match
cos 3  set qos-group 4       matched    : 0 packets, 0 bytes


 Class-map (qos): C_QOS5 (match any)  match dscp 32-39
match cos 4  set qos-group 5
      matched    : 0 packets, 0 bytes


 Class-map (qos): C_QOS6 (match any)  match dscp 40-47
match cos 5 set qos-group 6 matched : 0 packets, 0 bytes


 Class-map (qos): C_QOS7 (match any)  match dscp 48-55
match cos 6 set qos-group 7 matched : 0 packets, 0 bytes


 Class-map (qos): C_QOS8 (match any)  match dscp 56-63
match cos 7 set qos-group 8 matched : 0 packets, 0 bytes




Service-policy (queuing) output: default-out-policy
------------------------------ Class-map (queuing):
q0  priority level 1
      output     : 0 packets, 0 bytes       dropped     : 0
packets, 0 bytes


 Class-map (queuing): q1  priority level 1
      output     : 3017237090 packets, 205172121644 bytes       dropped    :
26231 packets, 1783708 bytes


 Class-map (queuing): q2  priority level 1
      output     : 0 packets, 0 bytes       dropped     : 0
packets, 0 bytes


 Class-map (queuing): q3  priority level 1
      output     : 0 packets, 0 bytes       dropped     : 0
packets, 0 bytes


 Class-map (queuing): q4  priority level 1
      output     : 0 packets, 0 bytes       dropped     : 0
packets, 0 bytes  Class-map (queuing): q5   priority level 1
output     : 0 packets, 0 bytes       dropped    : 0 packets, 0
bytes
```

```
 Class-map (queuing): q6  priority level 1       output     : 0 packets, 0
bytes       dropped    : 0 packets, 0 bytes

 Class-map (queuing): q7  priority level 1       output     : 0 packets, 0
bytes       dropped    : 0 packets, 0 bytes

Class-map (queuing): mc-q0       output     : 0 packets, 0 bytes       dropped
: 0 packets, 0 bytes

Class-map (queuing): mc-q1       output     : 0 packets, 0 bytes       dropped
: 0 packets, 0 bytes

Class-map (queuing): mc-q2       output     : 0 packets, 0 bytes       dropped
: 0 packets, 0 bytes

Class-map (queuing): mc-q3       output     : 0 packets, 0 bytes       dropped
: 0 packets, 0 bytes

Class-map (queuing): mc-q4       output     : 0 packets, 0 bytes       dropped
: 0 packets, 0 bytes

Class-map (queuing): mc-q5       output     : 0 packets, 0 bytes       dropped
: 0 packets, 0 bytes

Class-map (queuing): mc-q6       output     : 0 packets, 0 bytes       dropped
: 0 packets, 0 bytes

Class-map (queuing): mc-q7       output     : 0 packets, 0 bytes       dropped
: 0 packets, 0 bytes Wred Drop Statistics : ---------------------- green  : 0
packets  yellow : 0 packets  red    : 0 packets


show policy-map interface xe3

Interface xe3
Global statistics status : enabled



Service-policy (queuing) output: pend
------------------------------ Class-map (queuing):
empty5  shape average 400 mbps  bandwidth 350 kbps
```

```
Service-policy (queuing) output: p1p1
------------------------------ Class-map (queuing):
empty1  shape average percent 40  bandwidth percent 30


Service-policy (queuing) output: p1
------------------------------ Class-map (queuing): cq1
match qos-group 1 shape average percent 20 queue-limit
70 packets bandwidth percent 18
      output     : 5210667 packets, 375168024 bytes       dropped    :
122230964 packets, 8800629408 bytes


 Class-map (queuing): cq2 match qos-group 2 shape average
percent 80 queue-limit 70 packets bandwidth percent 75
output : 0 packets, 0 bytes dropped : 0 packets, 0 bytes



 Class-map (queuing): empty2  shape average percent 60
bandwidth percent 55 Service-policy (queuing) output: p2
------------------------------ Class-map
(queuing): cq3  match qos-group 3  shape average
percent 25
 random-detect minimum-threshold 50 maximum-threshold 75 kbytes percent
bandwidth percent 20       output     : 0 packets, 0 bytes       dropped    : 0
packets, 0 bytes


 Class-map (queuing): cq4  match qos-
group 4  shape average percent 75
 random-detect minimum-threshold 50 maximum-threshold 75 kbytes percent
bandwidth percent 65       output     : 0 packets, 0 bytes       dropped    : 0
packets, 0 bytes


 Class-map (queuing): empty6 shape average 500
mbps bandwidth 450 kbps


Service-policy (queuing) output: p3p4
------------------------------ Class-map
(queuing): empty3 shape average percent 40
bandwidth percent 35


Service-policy (queuing) output: p3
------------------------------ Class-map (queuing):
cq5 match qos-group 5 shape average percent 40
queue-limit 100 packets bandwidth percent 35
output     : 0 packets, 0 bytes       dropped    : 0
packets, 0 bytes
```

```
 Class-map (queuing): cq6 match qos-group 6 shape
average percent 60 queue-limit 100 packets
bandwidth percent 55       output     : 0 packets, 0
bytes       dropped    : 0 packets, 0 bytes


 Class-map (queuing): empty4 shape average
percent 60 bandwidth percent 50


Service-policy (queuing) output: p4
------------------------------ Class-map
(queuing): cq7  match qos-group 7  shape
average percent 40
 random-detect minimum-threshold 80 maximum-threshold 100 packets bytes kbytes
percent  bandwidth percent 35
      output     : 0 packets, 0 bytes       dropped    : 0
packets, 0 bytes


 Class-map (queuing): cq8  match qos-
group 8  shape average percent 60
 random-detect minimum-threshold 80 maximum-threshold 100 packets bytes kbytes
percent bandwidth percent 55
      output     : 0 packets, 0 bytes       dropped    : 0
packets, 0 bytes


Class-map (queuing): mc-q0       output     : 0
packets, 0 bytes       dropped    : 0 packets, 0
bytes


Class-map (queuing): mc-q1       output     : 0
packets, 0 bytes       dropped    : 0 packets, 0
bytes


Class-map (queuing): mc-q2       output     : 0
packets, 0 bytes       dropped    : 0 packets, 0
bytes


Class-map (queuing): mc-q3       output     : 0
packets, 0 bytes       dropped    : 0 packets, 0
bytes


Class-map (queuing): mc-q4       output     : 0
packets, 0 bytes       dropped    : 0 packets, 0
bytes
```

```
Class-map (queuing): mc-q5       output      : 0
packets, 0 bytes        dropped    : 0 packets, 0
bytes Class-map (queuing): mc-q6        output    :
0 packets, 0 bytes        dropped    : 0 packets, 0
bytes


Class-map (queuing): mc-q7
output     : 0  packets, 0 bytes
dropped    : 0  packets, 0 bytes


Wred Drop Statistics : ----
----------------- green  :
122230036 packets   yellow :
0 packets  red     : 0
packets



#show queuing interface xe2

Egress Queuing for Ethernet xe2 [System]
------------------------------------------------------------------------------
----------------
L0              L1              L2              Group  PrioLevel   Shape
Bandwidth
------------------------------------------------------------------------------
------------------
q0                                                -     High        -
-
q1                                                -     High        -
-
q2                                                -     High        -
-
q3                                                -     High        -
-
q4                                                -     High        -
-
q5                                                -     High        -
-
q6                                                -     High        -
-
q7                                                -     High        -
-


show queuing interface xe3

Egress Queuing for Ethernet xe3 [System]
```

```
-------------------------------------------------------------------------------
----------------
L0              L1              L2              Group  PrioLevel   Shape
Bandwidth
-------------------------------------------------------------------------------
------------------
empty5                                          -      -           400 mbps
350 kbps
                empty1                          -      -           40 percent
30 percent
                                cq1             1      -           20 percent
18 percent
                                cq2             2      -           80 percent
75 percent
                empty2                          -      -           60 percent
55 percent
                                cq3             3      -           25 percent
20 percent
                                cq4             4      -           75 percent
65 percent
empty6                                          -      -           500 mbps
450 kbps
                empty3                          -      -           40 percent
35 percent
                                cq5             5      -           40 percent
35 percent
                                cq6             6      -           60 percent
55 percent
                empty4                          -      -           60 percent
50 percent
                                cq7             7      -           40 percent
35 percent
                                cq8             8      -           60 percent
55 percent
(config)#set qos wrr uc 1 non-uc 127
(config)#exit
#show policy-map interface xe49/1

Interface xe49/1
Global statistics status : enabled



Service-policy (queuing) output: default-out-policy
-------------------------------
Class-map (queuing): q0
priority level 1
```

```
      output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes


 Class-map (queuing): q1
priority level 1
      output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes


 Class-map (queuing): q2
priority level 1
      output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes Class-map
(queuing): q3  priority level 1
      output     : 0 packets, 0 bytes       dropped    : 0 packets, 0
bytes

 Class-map (queuing): q4  priority level 1
      output     : 0 packets, 0 bytes       dropped    : 0 packets, 0
bytes


 Class-map (queuing): q5  priority level 1
      output     : 0 packets, 0 bytes       dropped    : 0 packets, 0
bytes


 Class-map (queuing): q6  priority level 1
      output     : 0 packets, 0 bytes       dropped    : 0 packets, 0
bytes


 Class-map (queuing): q7  priority level 1
      output     : 112144 packets, 7625792 bytes       dropped    : 14246424
packets, 968756472 bytes


Class-map (queuing): mc-q0       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q1       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q2       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q3       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes
```

```
Class-map (queuing): mc-q4       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes



Class-map (queuing): mc-q5
      output      : 0 packets, 0 bytes       dropped     : 0 packets, 0
bytes

Class-map (queuing): mc-q6       output      : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes

Class-map (queuing): mc-q7
      output : 14242202 packets, 968469396 bytes dropped : 112013 packets,
7616884 bytes


Wred Drop Statistics : ----------------------
green  : 0 packets  yellow : 0 packets  red    :
0 packets

(config)#set qos sp
#show policy-map interface xe49/2


Interface xe49/2
Global statistics status : enabled



Service-policy (queuing) output: default-out-policy
------------------------------- Class-map (queuing): q0
priority level 1
      output     : 0 packets, 0 bytes       dropped    : 0 packets, 0
bytes


 Class-map (queuing): q1  priority level 1
      output     : 0 packets, 0 bytes       dropped    : 0 packets, 0
bytes


 Class-map (queuing): q2  priority level 1
      output     : 0 packets, 0 bytes       dropped    : 0 packets, 0
bytes


 Class-map (queuing): q3  priority level 1
      output     : 0 packets, 0 bytes       dropped    : 0 packets, 0
bytes
```

```
 Class-map (queuing): q4  priority level 1
      output     : 0 packets, 0 bytes       dropped    : 0 packets, 0
bytes

 Class-map (queuing): q5  priority level 1
      output     : 0 packets, 0 bytes       dropped    : 0 packets, 0
bytes


 Class-map (queuing): q6  priority level 1
      output     : 0 packets, 0 bytes       dropped    : 0 packets, 0
bytes


 Class-map (queuing): q7  priority level 1
      output     : 239 packets, 16252 bytes       dropped     : 22486928
packets, 1529110732 bytes


Class-map (queuing): mc-q0       output     : 0 packets, 0
bytes       dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q1       output     : 0 packets, 0
bytes       dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q2       output     : 0 packets, 0
bytes       dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q3       output     : 0 packets, 0
bytes       dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q4       output     : 0 packets, 0
bytes       dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q5       output     : 0 packets, 0
bytes       dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q6       output     : 0 packets, 0
bytes       dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q7
      output : 22482826 packets, 1528831760 bytes dropped : 0 packets, 0
bytes
```

```
Wred Drop Statistics : ----------------------
green  : 0 packets  yellow : 0 packets  red    :
0 packets

(config-if)#set qos wrr uc 1 non-uc 2 (config-if)#end

#show policy-map interface xe49/1


Interface xe49/1
Global statistics status : enabled



Service-policy (queuing) output: default-out-policy
 ------------------------------- Class-map (queuing): q0
priority level 1
      output      : 0 packets, 0 bytes       dropped    : 0 packets, 0
bytes


 Class-map (queuing): q1  priority level 1
      output      : 0 packets, 0 bytes       dropped    : 0 packets, 0
bytes


 Class-map (queuing): q2  priority level 1
      output      : 0 packets, 0 bytes       dropped    : 0 packets, 0
bytes


 Class-map (queuing): q3  priority level 1
      output      : 0 packets, 0 bytes       dropped    : 0 packets, 0
bytes


 Class-map (queuing): q4  priority level 1
      output      : 0 packets, 0 bytes       dropped    : 0 packets, 0
bytes


 Class-map (queuing): q5  priority level 1
      output      : 0 packets, 0 bytes
      dropped     : 0 packets, 0 bytes


 Class-map (queuing): q6  priority level  1      output      : 0
packets, 0 bytes       dropped    : 0 packets, 0 bytes


 Class-map (queuing): q7  priority level  1
       output      : 1652752 packets, 112387000 bytes        dropped   : 3308396
                             packets, 224970580 bytes
```

```
Class-map (queuing): mc-q0       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes

Class-map (queuing): mc-q1       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes

Class-map (queuing): mc-q2       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes

Class-map (queuing): mc-q3       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes

Class-map (queuing): mc-q4       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes

Class-map (queuing): mc-q5       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes

Class-map (queuing): mc-q6       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes



Class-map (queuing): mc-q7
       output     : 3305521 packets, 224775224 bytes       dropped    : 1653583
 packets, 112443576 bytes Wred Drop Statistics : ---------------------- green  :
               0 packets  yellow : 0 packets  red    : 0 packets

(config)#interface xe49/2
(config-if)#set qos sp
(config-if)#end
#show policy-map interface xe49/2


Interface xe49/2
Global statistics status : enabled



Service-policy (queuing) output: default-out-policy
------------------------------- Class-map (queuing): q0  priority
level 1       output     : 0 packets, 0 bytes       dropped    :
0 packets, 0 bytes
```

```
 Class-map (queuing): q1  priority level 1       output      : 0
packets, 0 bytes       dropped     : 0 packets, 0 bytes

 Class-map (queuing): q2  priority level 1       output      : 0
packets, 0 bytes       dropped     : 0 packets, 0 bytes

 Class-map (queuing): q3  priority level 1       output      : 0
packets, 0 bytes       dropped     : 0 packets, 0 bytes

 Class-map (queuing): q4  priority level 1       output      : 0
packets, 0 bytes       dropped     : 0 packets, 0 bytes



 Class-map (queuing): q5  priority level 1
      output     : 0 packets, 0 bytes       dropped     : 0 packets, 0
bytes

 Class-map (queuing): q6  priority level 1       output     : 0
packets, 0 bytes       dropped    : 0 packets, 0 bytes

 Class-map (queuing): q7  priority level 1
      output     : 66 packets, 4488 bytes       dropped    : 6208329 packets,
422166024 bytes

Class-map (queuing): mc-q0       output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes

Class-map (queuing): mc-q1       output     : 0  packets, 0 bytes
dropped    : 0 packets, 0 bytes

Class-map (queuing): mc-q2       output     : 0  packets, 0 bytes
dropped    : 0 packets, 0 bytes

Class-map (queuing): mc-q3       output     : 0  packets, 0 bytes
dropped    : 0 packets, 0 bytes

Class-map (queuing): mc-q4       output     : 0  packets, 0 bytes
dropped    : 0 packets, 0 bytes
```

```
Class-map (queuing): mc-q5       output      : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q6       output      : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes


Class-map (queuing): mc-q7
      output      : 6203974 packets, 421869892 bytes       dropped     : 0
packets, 0 bytes
Wred Drop Statistics : ---------------------- green  : 0 packets   yellow : 0
packets  red    : 0 packets
```

Quality of Service Command Reference

Contents

This document contains this chapter:

- Chapter 1, *Quality of Service Commands*

© Symanitron

Quality of Service Command Reference

CHAPTER 1 Quality of Service Commands

This chapter is a reference for the ingress Quality of Service (QoS) and hierarchical QoS for the Trident II, Trident II+, Tomahawk, and Qumran platforms.

- bandwidth
- bandwidth remaining
- class-map type qos
- class-map type queuing
- class type qos
- class type queuing
- clear qos statistics
- match access-group
- match cos
- match cos inner
- match dscp
- match ip rtp
- match mac
- match precedence
- match protocol
- match qos-group
- match traffic-type
- match vlan
- match vlan inner
- police
- policy-map
- priority level
- qos (enable | disable)
- qos map
- qos remark dei
- qos statistics
- queue-limit
- random-detect
- shape
- service-policy
- service-policy type qostrust dscp
- service-policy type queuing
- set bridge cos
- set bridge dscp
- set cos

- set dscp
- set mpls class
- set precedence
- set qos-group
- set qos queue scheduler
- show class-map
- show policy-map
- show policy-map interface
- show queuing interface
- show running-config qos
- storm-control
- trust dscp
- wrr-queue weight

© Symanitron Proprietary

bandwidth

Use this command to allocate a minimum percentage of the interface bandwidth to a queue.

Use the `no` command to remove a bandwidth configuration.

Command Syntax `bandwidth (<1-1000000000> (kbps|mbps|gbps) | percent <1-100>) no bandwidth (<1-1000000000> (kbps|mbps|gbps) | percent <1-100>)`

Parameters

`<1-1000000000>` Bandwidth value `kbps` Units in kilobits/sec. `mbps` Units in megabits/sec. `gbps` Units in gigabits/sec. `percent` Specify the percentage from 1 to 100.

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
(config)# policy-map type queuing PQOS (config-pmap-
que)# class type queuing 1p7q4t-out-pq1 (config-
pmap-c-que)# bandwidth 10 mbps
```

bandwidth remaining

Use this command to configure the bandwidth remaining on the interface in a queue.

Use the `no command` to remove the remaining bandwidth allocation.

Command Syntax `bandwidth remaining percent <1-100> no bandwidth remaining percent <1-100>`

Parameters

`<1-100>` Specify the percentage of remaining bandwidth on the underlying link.

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
(config)# policy-map type queuing P1
(config-pmap-que)#class type queuing q1
 (config-pmap-c-que)# bandwidth percent 70
(config-pmap-c-que)#exit
(config-pmap-que)#class type queuing q2
(config-pmap-c-que)# bandwidth remaining percent 30
```

class-map type qos

Use this command to create a class-map of type qos.

Use the `no` command to remove a class-map.

Note: Class-map without any match qualification behaves similar to default class by matching all the packets on the interface it is attached via service policy.

In a class-map, adding or deleting match criteria with misconfiguration will have silent exit and will not proceed with operation.

Command Syntax `class-map (type qos|) (match-any|match-all|)`

```
NAME no class-map (type qos|) (match-any|match-all|)
NAME
```

Parameters

`NAME` Specify the class map name (Max Size 32) `match-any` Match any parameter (boolean OR) `match-all` Match all parameters (boolean AND)

Default

By default, match type is match-all for any class-map

Command Mode

Configuration Mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal

(config)# class-map type qos C_QOS1
```

class-map type queuing

Use this command to create a class-map of type queuing.

Use the `no` command to remove a class-map.

Note: Class-maps with no action are treated as incomplete configuration and don't take any effect until the action is added. Class-map deletion is not allowed if it is referenced by any policy-map.

Command Syntax `class-map type queuing (match-any|)`
`NAME no class-map type queuing (match-any|) NAME`

Parameters

`NAME` Specify the class map name (Max Size 32) `match-any` Match any parameter (boolean OR) `match-all` Match all parameters (boolean AND)

Default

By default, class-map type is match-any

Command Mode

Configuration Mode

Applicability

This command was introduced before SWMRE version 1.3.

This command applies only to the Trident II and Trident II+ platforms.

Examples

```
#configure terminal
(config)# class-map type queuing C_QOS1
```

class type qos

Use this command to add a QoS class-map to a qos policy map.

Use the `no command` to remove a QoS class-map from the policy map.

Note: Implicit priority of the classes in a policy-map will be calculated based number of matches with VLAN match given lower weight-age over other matches. In case of classes with conflicting match, it is not guarantied which class the traffic would hit. User is recommended to use priority in such cases.

Command Syntax `class (type qos|) (NAME|class-default) no class (type qos|) (NAME|class-default)`

Parameters

`NAME` Specify the class map name

Default

By default, class is type qos

Command Mode

Policy-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#
(config)#policy-map type qos PP
(config-pmap-que)#class type qos C_PP_1
```

class type queuing

Use this command to add a queuing class-map to a queuing policy map.

Use the `no` command to remove a queuing class-map from the policy map.

Command Syntax

```
class (type queuing ((default (q0|q1|q2|q3|q4|q5|q6|q7))|NAME) | NAME | queuing
  class-default)
no class (type queuing|) NAME
```

Parameters

`NAME`	Specify the class map name
`<q0-q7>`	Default queue name

Default

No default value is specified

Command Mode

Policy Map type queuing Mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#
```

```
(config)#policy-map type queuing PP
(config-pmap-que)#class type queuing C_PP_1
```

clear qos statistics

Use this command to clear the quality of service (QoS) statistics.

Command Syntax `clear qos statistics (interface NAME |)(input | output |) (type (qos | queuing)|)`

Parameters

`NAME`	Specify which interface to clear.

Default

By default, type QoS, type queuing class statistics on all interface's will be cleared, if no parameters configured

Command Mode

Privileged Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#clear qos statistics
#
```

match access-group

Use this command to classify the group based on the access group.

Use the `no command` remove access group match criteria from a class map

Command Syntax **`match access-group`** NAME

Parameters

NAME	Specify the access group name

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)# class-map class_acl (config-cmap-qos)#
match access-group name my_acl
```

match cos

Use this command to classify the traffic based on cos

Use the `no command` to remove the match configuration.

Note: The match commands which accept range has silent exit which makes removal of these match configuration easier. For example, classify the traffic based on cos using the command `match cos 2,4,6` and remove the match configuration using the command `no match cos 2-6.`

Command Syntax `match (not|) cos WORD`

`no match (not|) cos (WORD|all)`

Parameters

WORD	CoS value or list of specified CoS values. Valid values are from 0 to 7.
all	Delete all matched cos entries.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#class-map type qos C_QOS1
(config-cmap-qos)#match cos 1
```

match cos inner

Use this command to classify the traffic based on inner cos.

Use the `no` command to remove the match configuration.

Note: The match commands which accept range has silent exit which makes removal of these match configuration easier. For example, classify the traffic based on inner cos using the command `match cos inner 2,4,6` and remove the match configuration using the command `no match cos inner 2-6`.

Command Syntax `match (not|) cos inner WORD`

```
no match (not|) cos inner (WORD|all)
```

Parameters

`WORD`	Inner CoS value or list of specified CoS values. Valid values are from 0 to 7.
`all`	Delete all matched cos entries.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#class-map type qos C_QOS1
(config-cmap-qos)#match cos inner 1
```

match dscp

Use this command to classify the traffic based on dscp.

Use the `no` command to remove the configured dscp value.

Note: The match commands which accept range has silent exit which makes removal of these match configuration easier. For example, classify the traffic based on dscp using the command `match dscp 2,4,6` and remove the match configuration using the command `no match dscp 2-6`.

Command Syntax

```
match (not|) dscp [WORD | af11 | af12 | af13 | af21 | af22 | af23 | af31| af32 | af33 |
af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6| cs7 | default | ef] no match
```

```
(not|) dscp ([WORD | af11 | af12 | af13 |    af21 | af22 | af23 | af31 | af32 | af33 |
af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4    cs5 | cs6 | cs7 | default | ef]|all)
```

Parameters

WORD	<0-63> List of DSCP values.
af11	AF11 dscp (001010).
af12	AF12 dscp (001100)
af13	AF13 dscp (001110)
af21	AF21 dscp (010010)
af22	AF22 dscp (010100)
af23	AF23 dscp (010110)
af31	AF31 dscp (011010)
af32	AF32 dscp (011100)
af33	AF33 dscp (011110)
af41	AF41 dscp (100010)
af42	AF42 dscp (100100)
af43	AF43 dscp (100110)
cs1	CS1(precedence 1) dscp (001000)
cs2	CS2(precedence 2) dscp (010000)
cs3	CS3(precedence 3) dscp (011000)
cs4	CS4(precedence 4) dscp (100000)
cs5	CS5(precedence 5) dscp (101000)
cs6	CS6(precedence 6) dscp (110000)
cs7	CS7(precedence 7) dscp (111000)
default	Default dscp (000000)
ef	EF dscp (101110)
all	Delete all matched DSCP values.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#class-map type qos C_QOS7
(config-cmap-qos)#match dscp 48-55
```


© Symanitron Proprietary

match ip rtp

Use this command to configure a class map to use the Real-Time Protocol (RTP) port as a match criteria.

Use the `no command` to remove the RTP port as a match criteria.

Note: The match commands which accept range has silent exit which makes removal of these match configuration easier. For example, classify the traffic based on RTP port using the command `match ip rtp 5000,7000, 9000` and remove the match configuration using the command `no match ip rtp 5000-9000`.

Command Syntax `match (not|) ip rtp`

`WORD no match (not|) ip rtp`

`(WORD|all)`

Parameters

`WORD`	Specify User Datagram Protocol (UDP) or list of UDP ports that are using RTP. Valid values are from 2000 to 65535.
`all`	Delete all matched IP RTP values.

Default

No default value is specified

Command Mode

Class-map type qos

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)# class-map my_test
(config-cmap-qos)# match ip rtp 2300
```

match mac

Use this command to classify based on the mac address (can be source or destination or both)

Use the `no` command to remove the match configuration.

Command Syntax `match mac (src |dest ) (XX:XX:XX:XX:XX:XX| XX-XX-XX-XX-XX-XX |XXXX.XXXX.XXXX) no match mac (src |dest ) (XX:XX:XX:XX:XX:XX| XX-XX-XX-XX-XX-XX |XXXX.XXXX.XXXX)`

Parameters

`Mac`	Ethernet mac address
`Src`	specifies the source mac
`Dest`	specifies the destination mac
`XX:XX:XX:XX:XX:XX`	MAC address option 1

XX-XX-XX-XX-XX-XX MAC address option 2 XXXX.XXXX.XXXX

MAC address option 3

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#class-map type qos C_QOS1 (config-cmap-
qos)#match mac src 11:22:33:44:55:66 (config-
cmap-qos)#match mac dest 3344.5566.7788
```

match precedence

Use this command to traffic classification based on precedence.

Use the no command to remove the match configuration.

Note: The match commands which accept range has silent exit which makes removal of these match configuration easier. For example, classify the traffic based on precedence using the command match precedence 2,4,6 and remove the match configuration using the command no match precedence 2-6.

Command Syntax

```
match (not|) precedence [WORD | critical | flash | flash-override | immediate |
  internet | network | priority | routine]

          no match (not|) precedence ([WORD | critical | flash | flash-override|
                                                                    immediate |
  internet | network | priority | routine]|all)
```

Parameters

word IP precedence value critical

Critical precedence flash

Flash precedence

flash-override Flash override precedence immediate

Immediate precedence internet Internetwork

control precedence network Network control precedence

priority Priority precedence routine Routine

precedence all Delete all matched IP precedence

values.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)# class-map my_test
(config-cmap-qos)#  7
```

match protocol

Use this command to classify traffic based on protocol.

Use the `no command` to remove the specified protocol as a match criteria.

Command Syntax

```
        match (not|) protocol (arp | bridging |cdp | clns | clns-is |clns-es | dhcp
                                                                              | isis
  | ldp| netbios ) no match (not|) protocol (arp|bridging|cdp|clns|clns-es|
clns-is| dhcp |isis |ldp |netbios|all)
```

Parameters

`arp`	Address Resolution Protocol (ARP)
`bridging`	Bridging
`cdp`	Cisco Discovery Protocol (CDP)
`clns`	Connection-less Network Service (CLNS)
`clns-is`	CLNS Intermediate System
`clns-es`	CLNS end System
`dhcp`	Dynamic Host Configuration (DHCP)
`isis`	Intermediate system to intermediate system (IS-IS)
`ldp`	Label Distribution Protocol (LDP)
`netbios`	NetBIOS Extended User Interface (NetBEUI)
`all`	Delete all matched protocols.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)# class-map my_test
(config-cmap-qos)# match protocol ldp
```

match qos-group

Use this command to match a QoS group in a type queuing class map.

Use the `no` to remove a QoS match on a queue number from a type queuing class map.

Command Syntax `match qos-group <1-2000> no`

```
match qos-group <1-2000>
```

Parameters

`<1-2000>`	Specify qos group value or list of qos group values specified in bytes.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

This command applies only to Trident II and Trident II+ platforms.

Examples

```
(config)#
(config)#class-map type queuing match-any C_PP_1
(config-cmap-que)#match qos-group 1
```

match traffic-type

Use this command to classify based on traffic-type

Use the `no` command to remove the match configuration.

Note: Class with match traffic type default will have lower priority over class with other traffic type match.

Command Syntax `match (not|) traffic-type (l2-uc|l2-uc-unknown|default)`

```
no match (not|) traffic-type (l2-uc|l2-uc-unknown|default)
```

Parameters

`Traffic-type`	type of traffic to be matched
`l2-uc`	L2 Unicast traffic

l2-uc-unknown	Unknown L2 Unicast traffic	default	All other traffic-types

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
(config)#class-map type qos C_QOS1
(config-cmap-qos)#match traffic-type l2-uc
```

match vlan

Use this command to classify the traffic based on a VLAN.

Use the `no` command to remove the match configuration.

Note: The match commands which accept range has silent exit which makes removal of these match configuration easier. For example, classify the traffic based on VLAN using the command `match vlan 2,4,6` and remove the match configuration using the command `no match vlan 2-6`.

Command Syntax

`match (not|) vlan WORD`

`no match (not|) vlan (WORD|all)`

Parameters

`not`	Match all except this.
`WORD`	Enter VLAN ID <1-4094> or range of VLAN ID's separated by commas. For example, 2 or 2,4-5 or 50,51,52 or 100-120,122-130 etc.
`all`	Delete all VLAN ID entries.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#class-map type qos C_QOS1
(config-cmap-qos)#match vlan 1
```

match vlan inner

Use this command to classify the traffic based on the inner VLAN.

Use the `no` command to remove the match configuration.

Note: The match commands which accept range has silent exit which makes removal of these match configuration easier. For example, classify the traffic based on the inner VLAN using the command `match vlan inner 2,4,6` and remove the match configuration using the command `no match vlan inner 2-6`.

Command Syntax `match (not|) vlan inner WORD no match (not|) vlan inner (WORD|all)`

Parameters

`not`	Match all except this.
`WORD`	Enter VLAN ID <1-4094> or list of VLAN ID's separated by commas. For example, 2,4 etc.
`all`	Delete all VLAN ID entries.

Default

No default value is specified

Command Mode

Class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#class-map type qos C_QOS1
(config-cmap-qos)#match vlan inner 1
```

police

Use this command to configure policing of the data rates for a particular class of traffic.

Use the `no` command to remove a policing configuration.

Note: Committed Information Rate (CIR) and Peak Information Rate (PIR) can only be whole numbers.

Command Syntax

Trident II, Trident II+, and Tomahawk platforms:

```
police (colour-blind | colour-aware|)(cir) (<1-2000000000>
(kbps|mbps|gbps)) ((pir (<1-2000000000> (kbps|mbps|gbps))|)((bc) <1-256000>
(kbytes|mbytes|ms|us)|)((be)<1-256000> (kbytes|mbytes|ms|us)|)((conform
(transmit | set-prec-transmit <0-7> | set-dscp-transmit <0-63> | set-cos-
transmit
```

```
                                                                    <0-7>  |
    set-mpls-class <0-7> ))  |)((exceed (drop | set-dscp-transmit <0-63> | set-
    costransmit <0-7> | transmit | set-mpls-class <0-7> ))|) ((violate (drop | set-
    dscptransmit <0-63> | set-cos-transmit <0-7> | transmit | set-mpls-class <0-7>
    ))|))

  no police (cir) (<1-2000000000> (kbps|mbps|gbps)) ((pir (<1-2000000000>
    (kbps|mbps|gbps))|)((bc) <1-256000> (kbytes|mbytes|ms|us)|)((be)<1-256000>
(kbytes|mbytes|ms|us)|)((conform (transmit | set-prec-transmit <0-7> | set-
dscptransmit <0-63> | set-cos-transmit <0-7> | set-mpls-class <0-7> )) |)((exceed
(drop | set-dscp-transmit <0-63> | set-cos-transmit <0-7> | transmit | set-mplsclass
<0-7> ))|) ((violate (drop | set-dscp-transmit <0-63> | set-cos-transmit <0-7> |
transmit | set-mpls-class <0-7> ))|)) Qumran platform:

  police (cir) (<1-2000000000> (kbps|mbps|gbps)) ((pir (<1-2000000000>
    (kbps|mbps|gbps))|) ((bc) <1-256000> (kbytes|mbytes|ms|us)|)((be) <1-256000>
    (kbytes|mbytes|ms|us)|))  no  police  (cir)  (<1-2000000000>

  (kbps|mbps|gbps)) ((pir (<1-2000000000>

    (kbps|mbps|gbps))|) ((bc) <1-256000> (kbytes|mbytes|ms|us)|) ((be) <1-256000>
    (kbytes|mbytes|ms|us)|))
```

Parameters `colour-blind` Do not police on

color. `colour-aware` Do police on

color.

`cir <1-2000000000>`

Specify Committed information rate.

`pir <1-2000000000>`

Peak information rate.

`kbps` Specify the units of kbps per second. `mbps`

Specify the units of mbps per second. `gbps`

Specify the units of gbps per second.

`bc <1-256000>`

Burst rate committed.

`be <1-256000>` Burst rate extended.

`transmit`	Specify the action of transmitting packets.
`set-prec-transmit`	Sets the IP precedence field to the specified value and transmits the packet.
`set-dscp-transmit`	Sets the Differentiated Service Code Point (DSCP) field to the specified value and transmits the packet.
`set-cos-transmit`	Sets the class of service (CoS) field to the specified value and transmits the packet.
`set-mpls-class`	Set the mpls class filed to the give value and tx the packet
`drop`	Specify the action of dropping packets.
`conform`	Sets the action to take when the data rate is within bounds
`exceed`	Sets the action to take when the data rate is exceeded. Default is drop.
`violate`	Sets the action to take when the data rate violates the configured rate values. The default is drop.

Default

By default, policer type is colour-blind

Command Mode

Policy-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)# policy-map type qos 2345
(config-pmap-qos)#class type qos 2345
(config-pmap-c-qos)# police cir 2 mbps pir 4 mbps bc 2 mbytes be 4
mbytes conform transmit exceed set-cos-transmit 1 violate drop
```

policy-map

Use this command to create a policy map and enter policy-map mode.

Use the `no` command to remove a policy map.

Note: You cannot delete a policy map if it is attached to an interface.

Command Syntax `policy-map {NAME | (type (qos|queuing (|default)) NAME)} no policy-map {NAME |(type (qos|queuing (|default)) NAME)}`

Parameters

`NAME`	Policy map name (maximum 32 characters)
`qos`	QoS policy map
`queuing`	Queuing policy map

Default

© Symanitron Proprietary

No default value is specified

Command Mode

Configuration mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#
(config)#policy-map type qos PQOS
```

priority

Use this command to set the user priority for the class attached to this policy-map Use the `no` parameter with this command to unset the priority value

Note: The higher the priority number, higher the priority for the class in a policy-map. User configured priority takes effect over default priority.

Command Syntax

```
priority     <1-
1000> no priority
```

Parameters

`<1-1000>`	Priority value

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#policy-map pmap1
(config-pmap)#class cmap1
(config-pmap-c)#priority 20
```

priority level

Use this command to configure a single output queuing class as the priority queue.

Note: Priority can be set only on default queues (such as queues in the default queuing policy-map).

Command Syntax `priority`

`(level VALUE |)`

Parameters

`VALUE`	Specify the priority level for an output queuing class. Only one priority level is supported. The priority value can only be 1.

Default

No default value is specified

Command Mode

Policy map-class type queuing mode

Applicability

This command was introduced before SWMRE version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
#configure terminal
(config)#policy-map type queuing default default-out-policy
(config-pmap-que)#class type queuing default q0
(config-pmap-c-que)#priority level 1
```

qos (enable | disable)

Use this command to globally enable or disable Quality-of-Service (QoS).

Note: Enabling or disabling QoS is a disruptive operation, stopping all traffic on ports which causes traffic loss.

Command Syntax `qos (enable |`

`disable)`

Parameters

None

Default

By default, QoS is disabled

Command Mode

Configure

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
```

```
(config)# qos enable (config)#qos

disable
```

qos map

Use this command to map either a Differentiated Services Control Protocol (DSCP) value or a Class of Service (CoS) value to a particular queue.

Use the no form of this command to remove the mapping.

Command Syntax `qos map ((cos <0-7> | dscp <0-63> ) | queue <0-7>)) no qos map ((cos <0-7> | dscp <0-63> ) | queue <0-7>))`

Parameters

`<0-7>`	CoS value
`<0-63>`	DSCP value
`<0-7>`	Identifying queue number

Default

By default, CoS to queue mapping is one to one.

By default, 8 DSCP values are mapped to one queue. For example: DSCP 0-7 queue 0, DSCP 8-15 queue 1.

Command Mode

Configure, Interface modes

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
(config)#qos map cos 1 queue 7

(config)#qos map dscp 45 queue 1
```

Example for one to one CoS to queue mapping:

```
(config)#qos map cos 1 queue 1

(config)#qos map cos 2 queue 2
```

qos remark dei

Use this command to enable remarking of the Drop Eligible Indicator (DEI) bit.

Use the `no` command to disable remarking of the DEI bit.

Command Syntax `qos remark dei no qos remark dei`

Parameters

None

Default

By default, remarking of the DEI bit is disabled.

Command Mode

Configure Mode

Applicability

This command was introduced before SWMRE version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
(config)#qos remark dei
(config)#
```

qos statistics

Use this command to enable Quality of Service (QoS) statistics.

Use the `no` command to disable QoS statistics

Note: Class-map statistics is cleared whenever the match or action property of the class is modified dynamically.

Command Syntax `qos statistics` `no qos statistics`

Parameters

None

Default

By default, QoS statistics is disabled

Command Mode

Configure Mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#qos statistics
(config)#
```

queue-limit

Use this command to configure tail drop by setting queue limits on egress queues.

Use the `no command` to remove a queue limit.

Command Syntax `queue-limit (<1-524288>) (packets | bytes | kbytes) no queue-limit (<1-524288>) (packets | bytes | kbytes)`

Parameters

524288> Specify queue-limit in packets, bytes, or Kilobytes.

Max value for bytes is 524288

Max value for kilobytes is 512 Max value for packets is 600

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
(config)# policy-map type queuing P1
(config-pmap-que)#class type queuing q1
(config-pmap-c-que)# queue-limit percent 50
```

random-detect

Use this command to configure weighted random early detection (WRED).

Use the `no command` to remove a WRED configuration.

Command Syntax

```
random-detect (green (minimum-threshold|)<1-524288> (maximum-threshold|)<1-524288> yellow (minimum-threshold|)<1-524288> (maximum-threshold|)<1-524288> red (minimum-threshold|)<1-524288> (maximum-threshold|)<1-524288>)(packets | bytes | kbytes)

no random-detect (green (minimum-threshold|)<1-524288> (maximum-threshold|)<1524288> yellow (minimum-threshold|)<1-524288> (maximum-threshold|)<1-524288> red(minimum-threshold|)<1-524288> (maximum-threshold|)<1-524288>)(packets | bytes |kbytes)
```

Parameters `minimum-threshold`

Specify the minimum threshold. In the range of <1-524288>

`maximum-threshold`

Specify the maximum threshold. In the range of <1-524288>

`Packets, bytes, kbytes`

Specify the thresholds in Packets, Bytes, or Kilobytes.

Default

No default value is specified

Command Mode

Policy-class map mode

Applicability

This command was introduced before SWMRE version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
(config)# policy-map type queuing P1 (config-pmap-que)#class
type queuing q1 (config-pmap-c-que)# random-detect minimum-
threshold percent 50 maximumthreshold percent 80
```

service-policy

Use this command to attach a child policy onto a parent policy.

Use the `no` command detach child policy from the parent policy.

Command Syntax `service-policy NAME no service-policy`

`NAME`

Parameters

`NAME` Specify the policy map to attach to this interface.

Default

No default value is specified

Command Mode

Policy-class-map queuing mode

Applicability

This command was introduced before SWMRE version 1.3.

This command applies only to the Trident II and Trident II+ platforms.

Examples

```
(config)#policy-map type queuing P1
```

```
(config-pmap-que)#class type queuing empty5b
(config-pmap-c-que)#service-policy PQOS
```

service-policy type qos

Use this command to attach a service-policy of type qos to the interface.

Use the `no` command to remove a service-policy from an interface.

Command Syntax `service-policy type qos (input|output) NAME no service-policy type qos (input|output) NAME`

Parameters

`type`	Specify whether the policy map is of type qos.
`NAME`	Specify the policy map to attach to this interface.

Default

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#int xe3
                (config-if)#service-policy type qos input PQOS
```

service-policy type queuing

Use this command to attach a service-policy of type queuing to the interface.

Use the `no` command to remove a service-policy from an interface.

Command Syntax `service-policy type queuing output NAME no service-policy type queuing output NAME`

Parameters

`type`	Specify whether the policy map is of type queuing.
`NAME`	Specify the policy map to attach to this interface.

Default

By default, default-out-policy is attached on all interface

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)#int xe3
                                (config-if)#service-policy type queuing output PQOS
```

set bridge cos

Use this command to set the Class-of-Service (CoS) value for L2 packets only.

Use the `no` parameter with this command to unset a CoS value.

Command Syntax `set bridge cos (<0-7>) no set bridge cos <0-7>`

Parameters

`<0-7>`	CoS value.

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
#configure terminal
(config)#policy-map pmap1
(config-pmap)#class cmap1
(config-pmap-c)#set bridge cos 2
```

set bridge dscp

Use this command to set the DSCP value for L2 packets only.

Use the `no` parameter with this command to unset a DSCP value.

Command Syntax `set bridge dscp (<0-63>|af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef ) no set bridge dscp (<0-63>|af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef )`

Parameters

`<0-63>`	DSCP value
`af11`	DSCP (001011) decimal value 11

af12	DSCP (001100) decimal value 12
af13	DSCP (001101) decimal value 13
af21	DSCP (010101) decimal value 21
af22	DSCP (010110) decimal value 22
af23	DSCP (010111) decimal value 23
af31	DSCP (011111) decimal value 31
af32	DSCP (010000) decimal value 32
af33	DSCP (010001) decimal value 33
af41	DSCP (101001) decimal value 41
af42	DSCP (101010) decimal value 42
af43	DSCP (101011) decimal value 38
cs1	(Precedence 1) DSCP (001000) decimal value 8
cs2	(Precedence 2) DSCP (010000) decimal value 16
cs3	(Precedence 3) DSCP (011000) ecimal value 24
cs4	(Precedence 4) DSCP (100000) decimal value 32
cs5	(Precedence 5) DSCP (101000) decimal value 40
cs6	(Precedence 6) DSCP (110000) decimal value 48
cs7	(Precedence 7) DSCP (111000) decimal value 56
default	DSCP (000000) decimal value 0
ef	DSCP (101110) decimal value 46

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
#configure terminal
(config)#policy-map pmap1
(config-pmap)#class cmap1
(config-pmap-c)#set bridge dscp 25
```

set cos

Use this command for matching traffic classes set action as change cos in the egress packet to the prescribed value.

Use the `no command` to remove the assigned value from the class.

Command Syntax `set`

```
cos <0-7> no set
cos <0-7>
```

Parameters

`<0-7>`	Specify CoS value to assign for this class of traffic

Default

No default value is specified

Command Mode

Policy-map mode

Applicability

This command was introduced before SWMRE version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
(config)# policy-map my_policy1
(config-pmap-qos)# class traffic_class2
(config-pmap-c-qos)# no set cos 3
(config-pmap-c-qos)#
```

set dscp

Use this command for matching traffic classes set action as change DSCP in the egress packet to the prescribed value.

Use the `no` command to remove the assigned value from the class

Command Syntax `set dscp (<0-63>|af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef ) no set dscp (<0-63>|af11| af12| af13| af21| af22| af23| af31| af32| af33| af41| af42| af43| cs1| cs2| cs3| cs4| cs5| cs6| cs7| default| ef )`

Parameters

`<0-63>`	DSCP value
`af11`	DSCP (001011) decimal value 11
`af12`	DSCP (001100) decimal value 12

af13	DSCP (001101) decimal value 13
af21	DSCP (010101) decimal value 21
af22	DSCP (010110) decimal value 22
af23	DSCP (010111) decimal value 23
af31	DSCP (011111) decimal value 31
af32	DSCP (010000) decimal value 32
af33	DSCP (010001) decimal value 33
af41	DSCP (101001) decimal value 41
af42	DSCP (101010) decimal value 42
af43	DSCP (101011) decimal value 38
cs1	(Precedence 1) DSCP (001000) decimal value 8
cs2	(Precedence 2) DSCP (010000) decimal value 16
cs3	(Precedence 3) DSCP (011000) ecimal value 24
cs4	(Precedence 4) DSCP (100000) decimal value 32
cs5	(Precedence 5) DSCP (101000) decimal value 40
cs6	(Precedence 6) DSCP (110000) decimal value 48
cs7	(Precedence 7) DSCP (111000) decimal value 56
default	DSCP (000000) decimal value 0
ef	DSCP (101110) decimal value 46

Default

No default value is specified

Command Mode

Policy map class mode

Applicability

This command was introduced before SWMRE version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
#configure terminal
(config)#policy-map pmap1
(config-pmap)#class cmap1
(config-pmap-c)#set dscp af12
```


© Symanitron Proprietary

set mpls class

Use this command to set mpls class(queue) for the matched packet.

Use the no command to remove the assigned value from the class.

Command Syntax `set mpls class <0-7> no set mpls class <0-7>`

Parameters

`<0-7>` Specify class value to assign for this traffic.

Default

No default value is specified

Command Mode

Policy-map type qos

Applicability

This command was introduced before SWMRE version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
(config)# policy-map my_policy1
(config-pmap-qos)# class traffic_class2
(config-pmap-c-qos)# set mpls class 3
(config-pmap-c-qos)#
```

set precedence

Use this command for matching traffic classes set action as change precedence in the egress packet to the prescribed value.

Use the `no command` to leave the precedence value unchanged for the class

Command Syntax

```
set (precedence (<0-7>| critical| flash | flash-override|immediate|internet|
  network| priority| routine))
no set (precedence (<0-7>| critical| flash | flash-override|immediate|internet|
  network| priority| routine))
```

Parameters

`<0-7>` Specify IP precedence value to assign for this class of traffic `critical`

Critical precedence `flash` Flash precedence

`flash-override` Flash override precedence

`immediate` Immediate precedence `internet`

Internetwork control precedence `network`

Network control precedence `priority`

Priority precedence `routine` Routine precedence

Default

No default value is specified

Command Mode

Policy-map mode

Applicability

This command was introduced before SWMRE version 1.3.

This command applies only to the Trident II, Trident II+, and Tomahawk platforms.

Examples

```
(config)# policy-map policy1
(config-pmap-qos)# class class2
(config-pmap-c-qos)# set precedence 3
(config-pmap-c-qos)#
```

set qos-group

Use this command to match a QoS group in a type queuing class map.

Use the `no` command to remove a QoS group match on a queue number from a type queuing class map.

Command Syntax `set qos-group <1-2000>`

`no set qos-group <1-2000>`

Parameters

`<1-2000>` Specify the QoS group value to assign for this class of traffic.

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

This command applies only to the Trident II and Trident II+ platforms.

Examples

```
(config)#
(config)#policy-map type qos PQOS
(config-pmap-qos)#class type qos C_QOS1
```

```
(config-pmap-c-qos)#set qos-group 1
```

set qos queue scheduler

Use this command to change the scheduler mode of Unicast Queue and Non-Unicast queue groups to WRR or SP. Use the `no` command to disable the set mode, and to change to the default mode

Command Syntax `set qos ((wrr uc <1-127> non-uc <1-127>)|(sp uc <0-1> non-uc <0-1>)) no set qos ((wrr uc <1-127> non-uc <1-127>)|(sp uc <0-1> non-uc <0-1>))`

Parameters

wrr	Weighted Round Robin Mode
uc - <1-127>	Unicast Queues non-uc <1-127> Non-Unicast Queues
`sp`	Strict Priority Mode

Default

The default is WRR with 32:2.

Command Mode

Configure Mode

Applicability

This command was introduced before SWMRE version 1.3.

This command applies only to the Trident II and Trident II+ platforms.

Examples

```
(config)#set qos wrr uc 30 non-uc 40
(config)#
```

shape

Use this command to configure shaping on an egress queue to impose a maximum rate on it.

Command Syntax Use the `no command` to remove a shaping configuration.

```
shape (average|) (<1-1000000000> (kbps|mbps|gbps) | percent <1-100>) no shape (average|) (<1-1000000000> (kbps|mbps|gbps) | percent <1-100>)
```

Parameters

`average`	Specify an optional keyword. Shaping is based on an average rate. Average rate for shaping in the range of `<1-1000000000>`
`kbps`	Specify the units of kbps per second.
`mbps`	Specify the units of mbps per second.
`gbps`	Specify the units of gbps per second.
`percent`	Specify the percentage from 1 to 100.

Default

No default value is specified

Command Mode

Policy-class-map mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
(config)# policy-map type queuing my_queue
(config-pmap-que)# class type queuing PQOS
(config-pmap-c-que)# shape percent 25
(config-pmap-c-que)#
```

show class-map

Use this command to display qos/queuing class maps.

Command Syntax `show class-map (type (qos|queuing)|) (NAME|)`

Parameters

NAME	Specify the named class map

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show class-map type qos
Type qos class-maps ================== class-map type qos
1234 match cos 3 class-map type qos 2345 QOS-ACCESS-LIST-
NAME: 101



#show class-map 1234
Type qos class-maps ================== class-map type qos
1234 match cos 3
```

show policy-map

Use this command to display qos/queuing policy-map.

Command Syntax `show policy-map (type (qos (statistics |)|queuing|vlan-queuing|hybrid-queuing)|) show policy-map (type (qos (statistics |)|vlan-queuing|hybrid-queuing|queuing (default |))|) NAME`

Parameters

qos	Specify the policy maps of the type qos only.
statistics	Displays QoS statistics.
queuing	Specify the policy maps of the type queuing only.
default	Default queue of the port
NAME	Specify named policy map.

Command Mode

Exec and Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

Examples

```
#show policy-map type qos statistics
+------------- +------------------       +-----------------+-----------------+-----------------+-----------------     + |
Interface   |     Class-map      |    Match pkts     |  Match bytes    |  Dropped pkts   |  Dropped Bytes   | +-----
------------+--------------------+-------------------+-----------------+-----------------+-----------------               + Policy-
map: p5 (input)
xe3/1          c5                   213537882         14520578356       -                 Policy-map: q5
(input)
xe3/2          c5                   213538483         14520618816       -                 -

#show policy-map type qos statistics p5
+------------- +------------------       +-----------------+-----------------+-----------------+-----------------     + |
Interface   |     Class-map      |    Match pkts     |  Match bytes    |  Dropped pkts   |  Dropped Bytes   | +-----
------------+--------------------+-------------------+-----------------+-----------------+-----------------               + Policy-
map: p5 (input)
xe3/1          c5                   246954616         16792916200       -                 -
```

show policy-map interface

Use this command to display the statistics and the configurations of the input and output policies that are attached to an interface.

Command Syntax `show policy-map interface (NAME (input | output | ) (type (qos | queuing)|) | brief)` **Parameters**

NAME	Interface name.
brief	brief policy interface.

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show policy-map interface xe19/1


Interface xe19/1
Global statistics status : enabled
```

```
Service-policy (qos) input : p1
-------------------------------
Class-map (qos): c1 (match all)
match vlan 2  police cir 2 mbps
      matched    : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes


 Class-map (qos): c3 (match all)
police cir 2 mbps
      matched    : 2172408 packets, 2172408000 bytes
dropped    : 2128959 packets, 2128959000 bytes


Service-policy (queuing) output: default-out-policy
-------------------------------
Class-map (queuing): q0
priority level 1  bandwidth
percent 1
      output     : 0 packets, 0 bytes
dropped    : 0 packets, 0 bytes


 Class-map (queuing): q1
priority level 1
```

```
 bandwidth percent 1       output     : 0 packets, 0 bytes       dropped     :
0  packets, 0 bytes

 Class-map (queuing): q2  priority level 1  bandwidth percent 1       output
: 0 packets, 0 bytes       dropped    : 0 packets, 0 bytes

 Class-map (queuing): q3  priority level 1  bandwidth percent 1       output
: 0 packets, 0 bytes       dropped    : 0 packets, 0 bytes

 Class-map (queuing): q4  priority level 1  bandwidth percent 1       output
: 0 packets, 0 bytes       dropped    : 0 packets, 0 bytes

 Class-map (queuing): q5  priority level 1  bandwidth percent 1       output
: 0 packets, 0 bytes       dropped    : 0 packets, 0 bytes

 Class-map (queuing): q6   priority level 1  bandwidth percent 1        output
: 0 packets, 0 bytes       dropped    : 0 packets, 0 bytes

 Class-map (queuing): q7  priority level 1  bandwidth percent 1
      output     : 1445 packets, 92536 bytes       dropped     : 0 packets, 0 bytes

 Class-map (queuing): mc-q0       output     : 0 packets, 0 bytes
dropped     : 0 packets, 0 bytes

 Class-map (queuing): mc-q1       output     : 0 packets, 0 bytes
dropped     : 0 packets, 0 bytes  Class-map (queuing): mc-q2       output      :
0  packets, 0 bytes       dropped    : 0 packets, 0 bytes

 Class-map (queuing): mc-q3       output     : 0 packets, 0 bytes       dropped     :
0  packets, 0 bytes

 Class-map (queuing): mc-q4       output     : 0 packets, 0 bytes       dropped     :
0  packets, 0 bytes

 Class-map (queuing): mc-q5       output     : 0 packets, 0 bytes       dropped     :
0  packets, 0 bytes

 Class-map (queuing): mc-q6       output     : 0 packets, 0 bytes       dropped     :
0  packets, 0 bytes
```

```
 Class-map (queuing): mc-q7       output     : 0 packets, 0 bytes       dropped    :
0 packets, 0 bytes
```

show queuing interface

Use this command to see the configurations of queues that are attached to an interface.

Command Syntax `show queuing interface NAME`

Parameters

`NAME` Interface name.

Command Mode

Exec & config mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
# show queuing interface xe1/1
Egress Queuing for Ethernet xe1/1 [System]
------------------------------------------------------------------------------
------------------
L0              L1              L2              Group PrioLevel   Shape Bandwidth
------------------------------------------------------------------------------
----------------------
q0                                                    -     High        -
-
q1                                                    -     High        -
-
q2                                                    -     High        -
-
q3                                                    -     High        -
-
q4                                                    -     High        -
-
q5                                                    -     High        -
-
q6                                                    -     High        -
-
q7                                                    -     High        -
-
```

show running-config qos

Use this command to show the user configured QoS configurations.

Command Syntax `show running-config qos (all|)`

Parameters `all` Show all QoS related configuration information including all defaults.

Command Mode

Exec, config, interface, class-map, policy-map and policy-map-class

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#show running-config qos qos enable
!
!
#show running-config qos ? all diplay all qos info
including defaults

  |    Output modifiers
  >    Output redirection   <cr>

#show running-config qos  all qos enable
! qos map cos 0 queue 0 qos map cos 1
queue 1 qos map cos 2 queue 2 qos map
cos 3 queue 3 qos map cos 4 queue 4 qos
map cos 5 queue 5 qos map cos 6 queue 6
qos map cos 7 queue 7 qos map dscp 0
queue 0 qos map dscp 1 queue 0 qos map
dscp 2 queue 0 qos map dscp 3 queue 0
qos map dscp 4 queue 0 qos map dscp 5
queue 0 qos map dscp 6 queue 0 qos map
dscp 7 queue 0 qos map dscp 8 queue 1
qos map dscp 9 queue 1 qos map dscp 10
queue 1 qos map dscp 11 queue 1 qos map
dscp 12 queue 1 qos map dscp 13 queue 1
qos map dscp 14 queue 1 qos map dscp 15
queue 1 qos map dscp 16 queue 2 qos map
dscp 17 queue 2 qos map dscp 18 queue 2
qos map dscp 19 queue 2 qos map dscp 20
queue 2 qos map dscp 21 queue 2 qos map
dscp 22 queue 2 qos map dscp 23 queue 2
qos map dscp 24 queue 3 qos map dscp 25
queue 3 qos map dscp 26 queue 3 qos map
dscp 27 queue 3 qos map dscp 28 queue 3
qos map dscp 29 queue 3 qos map dscp 30
queue 3 qos map dscp 31 queue 3 qos map
dscp 32 queue 4 qos map dscp 33 queue 4
qos map dscp 34 queue 4 qos map dscp 35
queue 4 qos map dscp 36 queue 4 qos map
dscp 37 queue 4 qos map dscp 38 queue 4
qos map dscp 39 queue 4 qos map dscp 40
queue 5 qos map dscp 41 queue 5 qos map
dscp 42 queue 5 qos map dscp 43 queue 5
```

```
    qos map dscp 44 queue 5 qos map dscp 45
    queue 5 qos map dscp 46 queue 5 qos map
    dscp 47 queue 5 qos map dscp 48 queue 6
    qos map dscp 49 queue 6 qos map dscp 50
    queue 6 qos map dscp 51 queue 6 qos map
    dscp 52 queue 6 qos map dscp 53 queue 6
    qos map dscp 54 queue 6 qos map dscp 55
    queue 6 qos map dscp 56 queue 7 qos map
    dscp 57 queue 7 qos map dscp 58 queue 7
    qos map dscp 59 queue 7 qos map dscp 60
    queue 7 qos map dscp 61 queue 7 qos map
    dscp 62 queue 7 qos map dscp 63 queue 7
!
policy-map type queuing default default-out-policy  class type queuing default q0
priority level 1   exit
 class type queuing default q1   priority level 1
  exit
class type queuing default q2   priority level 1   exit
 class type queuing default q3   priority level 1   exit
 class type queuing default q4   priority level 1   exit
 class type queuing default q5   priority level 1   exit
 class type queuing default q6   priority level 1   exit
 class type queuing default q7   priority level 1   exit
! interface xe1/1
 service-policy type queuing default default-out-policy
! interface xe1/2
 service-policy type queuing default default-out-policy
! interface xe1/3
 service-policy type queuing default default-out-policy
! interface xe1/4
 service-policy type queuing default default-out-policy
! interface xe2/1
 service-policy type queuing default default-out-policy
```

storm-control

Use this command to set the rising threshold level for broadcast, multicast, or destination lookup failure traffic. The storm control action occurs when traffic utilization reaches this level.

Storm control is used to block the forwarding of unnecessary flooded traffic. A packet storm occurs when a large number of broadcast packets are received on a port. Forwarding these packets can cause the network to slow down or time out.

The minimum granularity for storm-control is 64kbps.

Use the `no` form of this command to disable storm control.

Command Syntax

```
storm-control (broadcast|multicast|dlf) (level LEVEL | <0-1000000000>
  (kbps|mbps|gbps))     no     storm-control

(broadcast|multicast|dlf)
```

Parameters `broadcast` Broadcast rate limiting.

`multicast` Multicast rate limiting. `dlf`

Destination lookup failure limiting.

`level` Sets the percentage of the threshold.

`LEVEL` The percentage of the threshold; percentage of the maximum speed (pps) of the interface <0.0000-1000.0000>.

`<0-1000000000>` Sets absolute threshold value <0-1000000000>

`kbps` specifies the units of Kilobits per second. `mbps`

specifies the units of Megabits per second. `gbps`

specifies the units of Gigabits per second.

Default

By default, storm control is disabled

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
    #configure terminal
    (config)#interface eth0
    (config-if)#storm-control broadcast level 30

    (config)#interface eth0 (config-if)#storm-
    control multicast level 30

    (config)#interface eth0 (config-
if)#storm-control multicast 300 mbps

(config)#interface eth0
(config-if)#no storm-control multicast
```

trust dscp

Use this command to use dscp value to decide queue mapping for packets in Layer 2 interfaces.

The no parameter with this command un-sets trust dscp.

Command Syntax `trust dscp  no  trust dscp`

Parameters

None

Default

By default, trust dscp is enabled on L2 interface

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

This command applies only to the Trident II and Trident II+ platforms.

Examples

```
#configure terminal
(config)#int xe1/1
(config-if)#trust dscp
```

wrr-queue weight

Use this command to set wrr-queue weight for a queue.

Use the priority level command to un-set configured wrr configuration.

Command Syntax `wrr-queue weight <1-127>`

Parameters

`<1-127>`	wrr queue weight to be configured.

Default

No default value is specified

Command Mode

Policy-class-map queuing Mode

Applicability

This command was introduced in version SWMRE version 1.3.

Examples

```
(config)#policy-map type queuing default default-out-policy
(config-pmap-que-def)# class type queuing default q0
(config-pmap-c-que-def)#wrr-queue weight (config-pmap-c-
que-def)#wrr-queue weight 2 (config-pmap-c-que-
def)#priority level 1
```

SECTION 14 Virtual eXtensible Local Area Network

Virtual eXtensible Local Area Network Configuration Guide

Contents

This guide contains the chapters:

- Chapter 1, *Overview*
- Chapter 2, *VXLAN Unicast Configuration*
- Chapter 3, *VXLAN Multicast Configuration*
- Chapter 4, *VXLAN-EVPN Configuration*
- Chapter 5, *VXLAN Quality of Service Configuration*
- Chapter 6, *VXLAN EVPN EVC Configuration*
- Chapter 7, *VXLAN Hybrid Access Port Configuration*

CHAPTER 1 Overview

This chapter provides an overview of Virtual eXtensible Local Area Network (VXLAN) and its implementation with SWMRE. VXLAN creates LAN segments using a MAC in IP encapsulation. The encapsulation carries the original L2 frame received from a host to the destination in another server using IP tunnels. The endpoints of the virtualized tunnel formed using VXLAN are called VTEPs (VXLAN Tunnel EndPoints). This technology allows the network to support several tenants with minimum changes in the network. The VTEPs carry tenant data in L3 tunnels over the network. The tenant data is not used in routing or switching. This aids in tenant machine movement and allows the tenants to have the same IP or MAC addresses on end devices, hosts/VM's.

SWMRE supports VxLAN IPv4 tunnels, but both IPv4 and IPv6 hosts are supported.

Terminology

Terms related to VXLAN configuration are defined in the table below.

IGMP	Internet Group Management Protocol
PIM	Protocol Independent Multicast
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNI	VXLAN Network Identifier (or VXLAN Segment ID)
VTEP	VXLAN Tunnel End Point. An entity that originates and/or terminates VXLAN tunnels
VXLAN	Virtual eXtensible Local Area Network
VXLAN Segment	VXLAN Layer 2 overlay network over which VMs communicate
VXLAN Gateway	An entity that forwards traffic between VXLANs

VXLAN Architecture

VXLAN runs over the existing networking infrastructure. It provides a means to "stretch" a Layer 2 network. In short, VXLAN is a Layer 2 overlay scheme on a Layer 3 network.

Each overlay is termed as a VXLAN segment. Only VMs within the same VXLAN segment can communicate with each other. Each VXLAN segment is identified through a 24-bit segment ID termed the "VXLAN Network Identifier (VNI)". This allows up to 16 million VXLAN segments to coexist within the same administrative domain.

VNI identifies the scope of the inner MAC frame originated by the individual VM. Hence, we can have overlapping MAC addresses across segments but never have traffic “cross over” since the traffic is isolated using the VNI. The VNI is in an outer header that encapsulates the inner MAC frame originated by the VM.

Overview

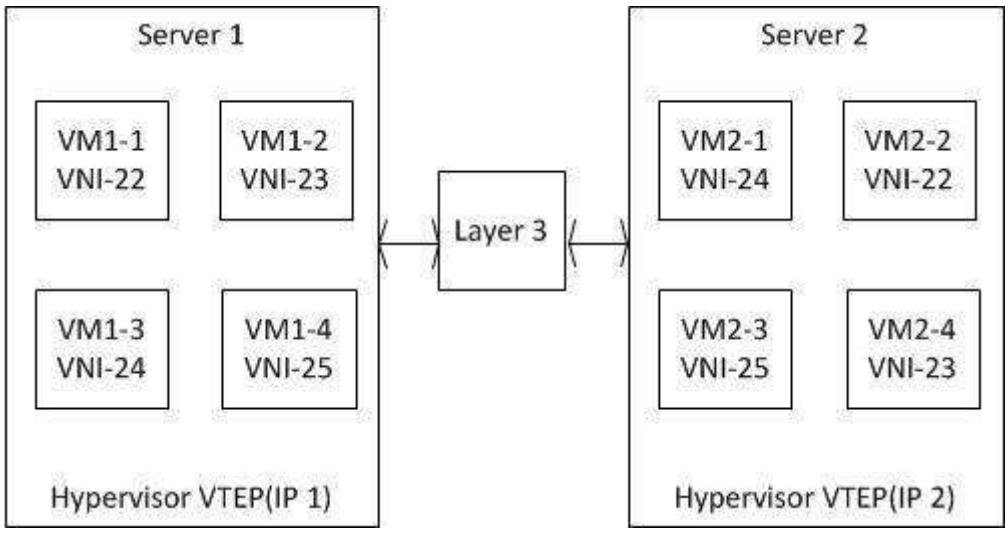


Figure 1-233: VXLAN Deployment - VTEPs across a Layer 3 Network

CHAPTER 2 VXLAN Unicast Configuration

This chapter contains basic VXLAN unicast configuration examples. To see details on the commands used in these examples or to see the outputs of the Validation commands, refer to the *VXLAN Command Reference*. The *NSM Command Reference* defines common commands.

Port Mapping

In this example each VTEP (VTEP1 and VTEP2) is a multilayer switch where xe2 is an access port while xe1 is network port.

After we start sending a packet (say untagged ipv4 packet) from VM1, it hits the VTEP1,VTEP1 does encapsulation based on the VNID configured and send it on xe1. Now the packet reaches VTEP2 and it does decapsulation of the packet.Now based on VNID packet is sent out on access port and it reaches destination VM, VM2.

Topology

The procedures in this section use the topology in Figure 2-234

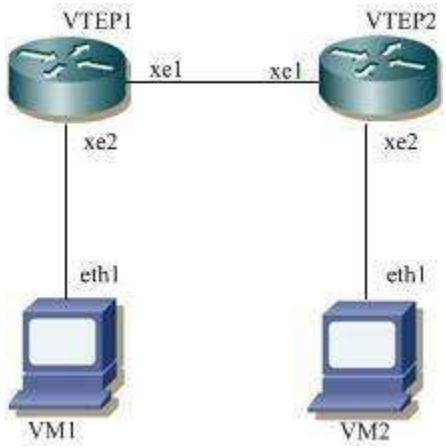


Figure 2-234: VXLAN unicast

VTEP1

`#configure terminal`	Enter the configure mode.
`(config)#interface xe2`	Enter the interface mode.
`(config-if)#switchport`	Configure the interface as switchport.
`(config-if)#no shutdown`	Bring the interface into operation with the no shutdown
`(config-if)#exit`	Exit interface mode.
`(config)#interface lo`	Enter the configure mode.
`(config-if)#ip address 1.1.1.1/32`	Configure IP address on the interface xe1.
`(config-if)#no shutdown`	Bring the interface into operation with the no shutdown

(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter the configure mode.
(config-if)#ip address 5.5.5.2/24	Configure IP address on the interface xe1.
(config-if)#no shutdown	Bring the interface into operation with the no shutdown
(config-if)#exit	Exit interface mode.
(config)#ip route 2.2.2.2/32 5.5.5.4	Configure static route
(config)#nvo vxlan enable	Enable VXLAN globally on this vtep.
(config)#interface tunnel 4	Specify the interface (Tunnel4)to be configured and enter the interface mode.
(config-if)#tunnel mode vxlan	Assign this tunnel mode as VXLAN.
(config-if)#tunnel source 1.1.1.1	Configure the source IP of this tunnel as an IP address which is configured on the interface xe1 of VTEP1.
(config-if)#tunnel destination 2.2.2.2	Configure the destination IP of this tunnel as an IP address which is configured on the interface xe1 of VTEP2.
(config-if)#exit	Exit the interface mode.
(config)#nvo vxlan id 2	Configure a VNID on this VTEP and enter the nvo mode.
(config-nvo)#vxlan map-network tunnel Tunnel4	Map the tunnel 4 with VNID 2
(config-nvo)#vxlan static-entry host-mac 0000.0000.aaaa remote-vtep-ip 2.2.2.2	Configure a static entry for remote VM with MAC address and IP address.
(config-nvo)#exit	Exit the nvo mode.
(config)#nvo vxlan access-if port xe2	Map the access port xe2 of this VTEP
(config-nvo-acc-if)#map vnid 2	Map the VNID 2 to access-port xe2
(config-nvo-acc-if)#exit	Exit the nvo access-if mode

VTEP2

#configure terminal	Enter the configure mode.
(config)#interface xe2	Enter the interface mode.
(config-if)#switchport	Configure the interface as switchport.
(config-if)#no shutdown	Bring the interface into operation with the no shutdown
(config-if)#exit	Exit interface mode.
(config)#interface lo	Enter the configure mode.
(config-if)#ip address 2.2.2.2/32	Configure IP address on the interface xe1.
(config-if)#no shutdown	Bring the interface into operation with the no shutdown
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter the configure mode.
(config-if)#ip address 5.5.5.4/24	Configure IP address on the interface xe1.
(config-if)#no shutdown	Bring the interface into operation with the no shutdown

(config-if)#exit	Exit interface mode.
(config)#ip route 1.1.1.1/32 5.5.5.2	Configure static route
(config)#nvo vxlan enable	Enable VXLAN globally on this vtep.
(config)#interface tunnel 4	Specify the interface (Tunnel4)to be configured and enter the interface mode.
(config-if)#tunnel mode vxlan	Assign this tunnel mode as VXLAN.
(config-if)#tunnel source 2.2.2.2	Configure the source IP of this tunnel as an IP address which is configured on the interface xe1 of VTEP1.
(config-if)#tunnel destination 1.1.1.1	Configure the destination IP of this tunnel as an IP address which is configured on the interface xe1 of VTEP2.
(config-if)#exit	Exit the interface mode.
(config)#nvo vxlan id 2	Configure a VNID on this VTEP and enter the nvo mode.
(config-nvo)#vxlan map-network tunnel Tunnel4	Map the tunnel 4 with VNID 2
(config-nvo)#vxlan static-entry host-mac 0000.0000.bbbb remote-vtep-ip 1.1.1.1	Configure a static entry for remote VM with MAC address and IP address.
(config-nvo)#exit	Exit the nvo mode.
(config)#nvo vxlan access-if port xe2	Map the access port xe2 of this VTEP
(config-nvo-acc-if)#map vnid 2	Map the VNID 2 to access-port xe2
(config-nvo-acc-if)#exit	Exit the nvo access-if mode

Validation

VTEP1

```
VTEP1#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source            Destination     Status
=====================================================
1.1.1.1           2.2.2.2          Installed Total  number
of entries are 1

VTEP1#show nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
VNID     Type Interface    Vlan  Src-addr        Dst-addr
_____________________________________________________________
2        NW     ----       ---- 1.1.1.1         2.2.2.2
2        AC   xe2          ALL    ----            ----
Total number of entries are 1

VTEP1#sh nvo vxlan mac-table
================================================================
                  VXLAN MAC Entries
```

```
=================================================================

VNID      Interface    Mac-Addr           VTEP-Ip         Type
_________________________________________________________________
2           ---        0000.0000.aaaa      2.2.2.2     Remote
2           xe2        0000.0000.bbbb      1.1.1.1     Dynamic Local
Total number of entries are 2
VTEP1#sh nvo vxlan mac-table vnid 2
=================================================================
                  VXLAN MAC Entries
=================================================================

VNID       Interface   Mac-Addr           VTEP-Ip          Type
_________________________________________________________________
2           ---        0000.0000.aaaa     2.2.2.2       Remote
2           xe2        0000.0000.bbbb     1.1.1.1       Dynamic Local Total
number of entries are 2
```

VTEP2

```
VTEP2#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status
=================================================
2.2.2.2           1.1.1.1         Installed
Total  number of entries are 1

VTEP2#show nvo vxlan vnid 2
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
VNID    Type Interface   Vlan  Src-addr        Dst-addr
_____________________________________________________________
2        NW     ----      ----  2.2.2.2        1.1.1.1
2        AC   xe2          ALL    ----            ----
Total number  of entries are 1

VTEP2#sh nvo vxlan mac-table
=================================================================
                  VXLAN MAC Entries
=================================================================

VNID      Interface    Mac-Addr           VTEP-Ip         Type
_________________________________________________________________
2          xe2         0000.0000.aaaa      2.2.2.2     Dynamic Local
2          ---         0000.0000.bbbb      1.1.1.1     Remote
Total number of entries are 2

VTEP2#sh nvo vxlan mac-table vnid 2
=================================================================
                  VXLAN MAC Entries
```

```
=============================================================

VNID      Interface    Mac-Addr           VTEP-Ip         Type
_____________________________________________________________
2          xe2         0000.0000.aaaa      2.2.2.2     Dynamic Local
2          ---         0000.0000.bbbb      1.1.1.1     Remote
Total number of entries are 2
```

Intermediate Non-VXLAN Router

This example is same as port mapping but we have an intermediate non VXLAN router. It does forwarding based on IP header.

Topology

The procedures in this section use the topology in Figure 2-235

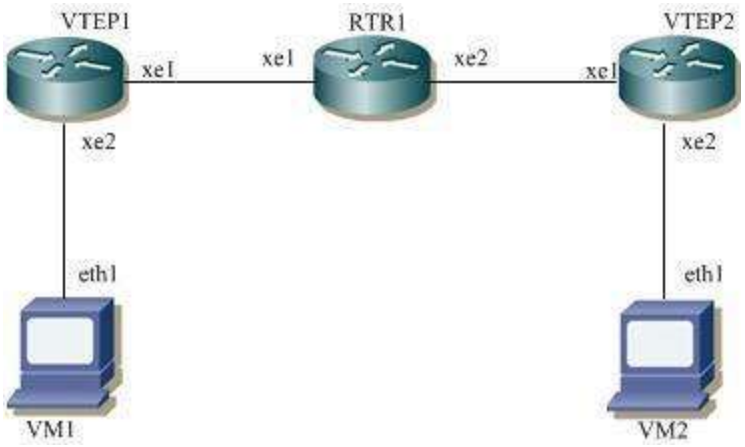


Figure 2-235: VXLAN unicast

VTEP1

`#configure terminal`	Enter the configure mode.
`(config)#interface xe2`	Enter the interface mode.
`(config-if)#switchport`	Configure the interface as switchport.
`(config-if)#no shutdown`	Bring the interface into operation with the no shutdown
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe1`	Enter the configure mode.
`(config-if)#ip address 2.2.2.4/24`	Configure IP address on the interface xe1.
`(config-if)#no shutdown`	Bring the interface into operation with the no shutdown
`(config-if)#exit`	Exit interface mode.
`(config)#ip route 3.3.3.0/24 2.2.2.1`	Configuring static route

(config)#nvo vxlan enable	Enable VXLAN globally on this vtep.
(config)#interface tunnel 4	Specify the interface (Tunnel4)to be configured and enter the interface mode.
(config-if)#tunnel mode vxlan	Assign this tunnel mode as VXLAN.
(config-if)#tunnel source 2.2.2.4	Configure the source IP of this tunnel as an IP address which is configured on the interface xe1 of VTEP1.
(config-if)#tunnel destination 3.3.3.4	Configure the destination IP of this tunnel as an IP address which is configured on the interface xe1 of VTEP2.
(config-if)#exit	Exit the interface mode.
(config)#nvo vxlan id 3	Configure a VNID on this VTEP and enter the nvo mode.
(config-nvo)#vxlan map-network tunnel Tunnel4	Map the tunnel 4 with this VNID
(config-nvo)#vxlan static-entry host-mac 0000.0000.aaaa remote-vtep-ip 3.3.3.4	Configure a static entry for remote VM with MAC address and IP address.
(config)#nvo vxlan access-if port xe2	Map the access port xe2 of this VTEP
(config-nvo-acc-if)#map vnid 3	Map the VNID 2 to access-port xe2
(config-nvo-acc-if)#exit	Exit NVO access-interface mode

RTR1

(config)#interface xe1	Enter the configure mode.
(config-if)#ip address 2.2.2.1/24	Configure IP address on the interface xe1.
(config-if)#no shutdown	Bring the interface into operation with the no shutdown
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter the configure mode.
(config-if)#ip address 3.3.3.1/24	Configure IP address on the interface xe2.
(config-if)#no shutdown	Bring the interface into operation with the no shutdown
(config-if)#exit	Exit interface mode.

VTEP2

#configure terminal	Enter the configure mode.
(config)#interface xe2	Enter the interface mode.
(config-if)#switchport	Configure the interface as switchport.
(config-if)#no shutdown	Bring the interface into operation with the no shutdown
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter the configure mode.
(config-if)#ip address 3.3.3.4/24	Configure IP address on the interface xe1.
(config-if)#no shutdown	Bring the interface into operation with the no shutdown
(config-if)#exit	Exit interface mode.

(config)#ip route 2.2.2.0/24 3.3.3.1	Configuring static route
(config)#nvo vxlan enable	Enable VXLAN globally on this vtep.
(config)#interface tunnel 4	Specify the interface (Tunnel4)to be configured and enter the interface mode.
(config-if)#tunnel mode vxlan	Assign this tunnel mode as VXLAN.
(config-if)#tunnel source 3.3.3.4	Configure the source IP of this tunnel as an IP address which is configured on the interface xe1 of VTEP1.
(config-if)#tunnel destination 2.2.2.4	Configure the destination IP of this tunnel as an IP address which is configured on the interface xe1 of VTEP2.
(config-if)#exit	Exit the interface mode.
(config)#nvo vxlan id 3	Configure a VNID on this VTEP and enter the nvo mode.
(config-nvo)#vxlan map-network tunnel Tunnel4	Map the tunnel 4 with this VNID
(config-nvo)#vxlan static-entry host-mac 0000.0000.bbbb remote-vtep-ip 2.2.2.4	Configure a static entry for remote VM with MAC address and IP address.
(config)#nvo vxlan access-if port xe2	Map the access port xe2 of this VTEP
(config-nvo-acc-if)#map vnid 3	Map the VNID 3 to access-port xe2
(config-nvo-acc-if)#exit	Exit the NVO access interface mode

Validation

VTEP1

```
VTEP1#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source            Destination     Status
==================================================
2.2.2.4           3.3.3.4         Installed Total  number
of entries are 1

VTEP1#show nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
VNID     Type Interface   Vlan  Src-addr        Dst-addr

_____________________________________________________________
3        NW     ----      ---- 2.2.2.4         3.3.3.4
3        AC   xe2         ALL    ----            ----
Total number of entries are 1

VTEP1#sh nvo vxlan mac-table
================================================================
                  VXLAN MAC Entries
================================================================

VNID      Interface    Mac-Addr           VTEP-Ip        Type
```

```
_____________________________________________________________________
3           ---         0000.0000.aaaa      3.3.3.4      Remote
3           xe2         0000.0000.bbbb      2.2.2.4      Dynamic Local
Total number of entries are 2

VTEP1#sh nvo vxlan mac-table vnid 3
=====================================================================
                  VXLAN MAC Entries
=====================================================================

VNID       Interface   Mac-Addr           VTEP-Ip          Type
_____________________________________________________________________
3           ---         0000.0000.aaaa     3.3.3.4        Remote
3           xe2         0000.0000.bbbb     2.2.2.4       Dynamic Local Total
number of entries are 2
```

VTEP2

```
VTEP2#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status
=================================================
3.3.3.4          2.2.2.4          Installed
Total  number of entries are 1

VTEP2#show nvo vxlan vnid 3
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
VNID    Type Interface   Vlan  Src-addr        Dst-addr
_____________________________________________________________________
3        NW     ----      ----  3.3.3.4        2.2.2.4
3        AC   xe2          ALL    ----            ----
Total number  of entries are 1

VTEP2#show nvo vxlan mac-table
=====================================================================
                  VXLAN MAC Entries
=====================================================================

VNID      Interface    Mac-Addr           VTEP-Ip        Type
_____________________________________________________________________
3          xe2         0000.0000.aaaa     3.3.3.4      Dynamic Local
3          ---         0000.0000.bbbb     2.2.2.4      Remote Total number
of entries are 2


VTEP2#show nvo vxlan mac-table vnid 3
=====================================================================
```

```
                    VXLAN MAC Entries
=================================================================

VNID      Interface    Mac-Addr           VTEP-Ip         Type
_________________________________________________________________
3          xe2         0000.0000.aaaa      3.3.3.4      Dynamic Local
3          ---         0000.0000.bbbb      2.2.2.4      Remote
Total number of entries are 2
```

CHAPTER 3 VXLAN Multicast Configuration

This chapter contains a Virtual eXtensible Local Area Network Multicast (VXLAN Multicast) configuration example.

Multicast transmission architecture is used for broadcast, multicast, and unknown unicast traffic.

Port Mapping

In this example, packet from VM1 reached VM2 using multicast tunnel.Once learning is done, when we send packet from VM2 back to VM1, it uses unicast tunnel.

Topology

The procedures in this section use the topology in Figure 3-236

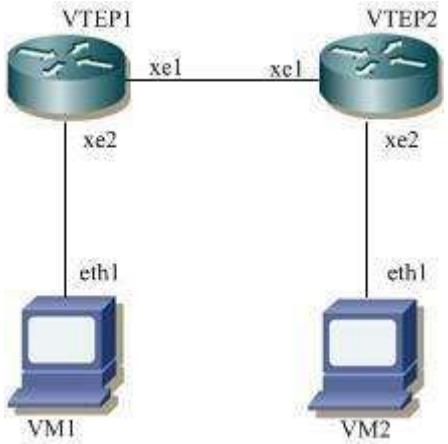


Figure 3-236: VXLAN multicast

VTEP1

`#configure terminal`	Enter the configure mode.
`(config)#interface lo`	Enter the configure mode.
`(config-if)#ip address 1.1.1.1/32`	Configure IP address on the interface xe1.
`(config-if)#no shutdown`	Bring the interface into operation with the no shutdown.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe2`	Enter the interface mode.
`(config-if)#switchport`	Configure the interface as switchport.
`(config-if)#no shutdown`	Bring the interface into operation with the no shutdown
`(config-if)#exit`	Exit interface mode.
`(config)#ip multicast-routing`	Configure multicast routing on VTEP1.
`(config)#interface xe1`	Enter the configure mode.
`(config-if)#ip address 5.5.5.2/24`	Configure IP address on the interface xe1.

(config-if)#ip igmp join-group 239.10.10.9	Configure interface with IGMP
(config-if)#ip pim sparse-mode	Configure PIM as sparse mode
(config-if)#no shutdown	Bring the interface into operation with the no shutdown
(config-if)#exit	Exit interface mode.
(config)#nvo vxlan enable	Enable VXLAN globally on this vtep.
(config)#interface tunnel 4	Specify the interface (Tunnel4)to be configured and enter the interface mode.
(config-if)#tunnel mode vxlan	Assign this tunnel mode as VXLAN.
(config-if)#tunnel add interface xe1	Add outging interface for multicast tunnels.
(config-if)#tunnel source 5.5.5.2	Configure the source IP of this tunnel as an IP address which is configured on the interface xe1 of VTEP1.
(config-if)#tunnel destination 239.10.10.9	Configure the destination IP of this tunnel as the multicast group address.
(config-if)#exit	Exit the interface mode.
(config)#ip route 2.2.2.2/32 5.5.5.4	Configure static route.
(config)#interface tunnel 5	Specify the interface (Tunnel5) to be configured and enter the interface mode.
(config-if)#tunnel mode vxlan	Assign this tunnel mode as VXLAN.
(config-if)#tunnel source 1.1.1.1	Configure the source IP of this tunnel as an IP address which is configured on the interface lo1 of VTEP1.
(config-if)#tunnel destination 2.2.2.2	Configure the destination IP of this tunnel IP address which is configured on the interface lo1 of VTEP2.
(config-if)#exit	Exit the interface mode.
(config)#nvo vxlan id 2 multicast 239.10.10.9	Configure a VNID on this VTEP and enter the nvo mode.
(config-nvo)#vxlan map-network tunnel Tunnel4	Map the tunnel 4 with VNID 2
(config-nvo)#vxlan map-network tunnel Tunnel5	Map the tunnel 5 with VNID 2
(config-nvo)#exit	Exit NVO mode
(config)#nvo vxlan access-if port xe2	Map the access port xe2 of this VTEP
(config-nvo-acc-if)#map vnid 2	Map the VNID 2 to access-port xe2
(config-nvo-acc-if)#exit	Exit NVO access interface mode

VTEP2

#configure terminal	Enter the configure mode.
(config)#interface lo	Enter the configure mode.
(config-if)#ip address 2.2.2.2/32	Configure IP address on the interface xe1.
(config-if)#no shutdown	Bring the interface into operation with the no shutdown.
(config-if)#exit	Exit interface mode.

(config)#interface xe2	Enter the interface mode.
(config-if)#switchport	Configure the interface as switchport.
(config-if)#no shutdown	Bring the interface into operation with the no shutdown
(config-if)#exit	Exit interface mode.
(config)#ip multicast-routing	Configure multicast routing on VTEP1.
(config)#interface xe1	Enter the configure mode.
(config-if)#ip address 5.5.5.4/24	Configure IP address on the interface xe1.
(config-if)#ip igmp join-group 239.10.10.9	Configure interface with IGMP
(config-if)#ip pim sparse-mode	Configure PIM as sparse mode
(config-if)#no shutdown	Bring the interface into operation with the no shutdown
(config-if)#exit	Exit interface mode.
(config)#nvo vxlan enable	Enable VXLAN globally on this vtep.
(config)#interface tunnel 4	Specify the interface (Tunnel4)to be configured and enter the interface mode.
(config-if)#tunnel mode vxlan	Assign this tunnel mode as VXLAN.
(config-if)#tunnel add interface xe1	Add outging interface for multicast tunnels.
(config-if)#tunnel source 5.5.5.4	Configure the source IP of this tunnel as an IP address which is configured on the interface xe1 of VTEP1.
(config-if)#tunnel destination 239.10.10.9	Configure the destination IP of this tunnel as the multicast group address.
(config-if)#exit	Exit the interface mode.
(config)#interface tunnel 5	Specify the interface (Tunnel5) to be configured and enter the interface mode.
(config-if)#tunnel mode vxlan	Assign this tunnel mode as VXLAN.
(config-if)#tunnel source 2.2.2.2	Configure the source IP of this tunnel as an IP address which is configured on the interface lo1 of VTEP1.
(config-if)#tunnel destination 1.1.1.1	Configure the destination IP of this tunnel IP address which is configured on the interface lo1 of VTEP2.
(config-if)#exit	Exit the interface mode.
(config)#ip route 1.1.1.1/32 5.5.5.2	Configure static route.
(config)#nvo vxlan id 2 multicast 239.10.10.9	Configure a VNID on this VTEP and enter the nvo mode.
(config-nvo)#vxlan map-network tunnel Tunnel4	Map the tunnel 4 with VNID 2
(config-nvo)#vxlan map-network tunnel Tunnel5	Map the tunnel 5 with VNID 2
(config)#nvo vxlan access-if port xe2	Map the access port xe2 of this VTEP
(config-nvo-acc-if)#map vnid 2	Map the VNID 2 to access-port xe2
(config-nvo-acc-if)#exit	Exit the nvo access-if mode

Validation

VTEP1

```
VTEP1#show nvo vxlan tunnel
VXLAN Network tunnel Entries
Source           Destination          Status
=================================================
5.5.5.2          239.10.10.9      Installed
1.1.1.1           2.2.2.2         Installed
VTEP1#show nvo vxlan vnid 2
VXLAN Information
=================
    Codes: NW - Network Port
           AC - Access Port
VNID     Type Interface   Vlan   Src-addr       Dst-addr
_________________________________________________________________
 2       NW      ----     ----    5.5.5.2       239.10.10.9
 2       NW      ----     ----    1.1.1.1         2.2.2.2
 2       AC       xe1      ALL      ----           ---Total
number of entries are 3
```

VTEP2

```
VTEP2#show nvo vxlan tunnel
VXLAN Network tunnel Entries
Source           Destination          Status
=================================================
5.5.5.4          239.10.10.9      Installed
2.2.2.2            1.1.1.1        Installed


VTEP2#show nvo vxlan vnid 2
VXLAN Information
=================
    Codes: NW - Network Port
           AC - Access Port
VNID     Type Interface   Vlan   Src-addr       Dst-addr
_________________________________________________________________
 2       NW      ----     ----    5.5.5.4       239.10.10.9
 2       NW      ----     ----    2.2.2.2         1.1.1.1
 2       AC       xe1      ALL      ----           ---Total
number of entries are 3
```

Intermediate Non-VXLAN Router

In this example, we have an intermediate router which doesn't understand VXLAN, so it does forwarding based on multicast mechanism.

Topology

The procedures in this section use the topology in Figure 3-237

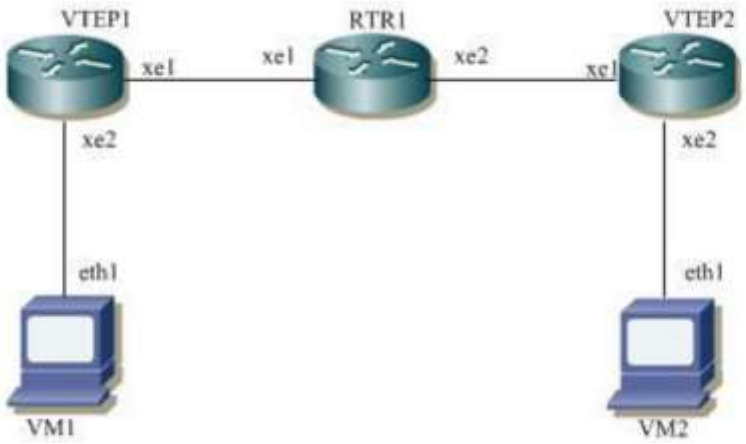


Figure 3-237: VXLAN multicast

VTEP1

`#configure terminal`	Enter the configure mode.
`(config)#interface xe2`	Enter the interface mode.
`(config-if)#switchport`	Configure the interface as switchport.
`(config-if)#no shutdown`	Bring the interface into operation with the no shutdown
`(config-if)#exit`	Exit interface mode.
`(config)#ip multicast-routing`	Configure multicast routing on VTEP1.
`(config)#interface xe1`	Enter the configure mode.
`(config-if)#ip address 2.2.2.4/24`	Configure IP address on the interface xe1.
`(config-if)#no shutdown`	Bring the interface into operation with the no shutdown
`(config-if)#ip igmp static-group 239.10.10.9`	Configure interface with IGMP.
`(config-if)#ip igmp version 3`	Configure interface with IGMP version 3
`(config-if)#ip pim sparse-mode`	Configure PIM mode as sparse mode.
`(config-if)#exit`	Exit interface mode.
`(config)# router ospf 1`	Configuring OSPF process id
`(config-router)# redistribute connected`	Configuring redistribution
`(config-router)# network 2.2.2.0/24 area 0`	Advertising 2.2.2.0 network
`(config-router)#exit`	Exit router mode
`(config)#nvo vxlan enable`	Enable VXLAN globally on this VTEP.
`(config)#interface tunnel 4`	Specify the interface (Tunnel4)to be configured and enter the interface mode.
`(config-if)#tunnel mode vxlan`	Assign this tunnel mode as VXLAN.
`(config-if)#tunnel add interface xe1`	Add outging interface for multicast tunnels.
`(config-if)#tunnel source 2.2.2.4`	Configure the source IP of this tunnel as an IP address which is configured on the interface xe1 of VTEP1.

(config-if)#tunnel destination 3.3.3.4	Configure the destination IP of this tunnel as an IP address which is configured on the interface xe1 of VTEP2.
(config-if)#exit	Exit the interface mode.
(config)#interface tunnel 5	Specify the interface (Tunnel5)to be configured and enter the interface mode.
(config-if)#tunnel mode vxlan	Assign this tunnel mode as VXLAN.
(config-if)#tunnel source 2.2.2.4	Configure the source IP of this tunnel as an IP address which is configured on the interface xe1 of VTEP1.
(config-if)#tunnel destination 239.10.10.9	Configure the destination IP of this tunnel as the multicast group address.
(config-if)#tunnel add interface xe1	Configure the exit interface for this tunnel.
(config-if)#exit	Exit the interface mode.
(config)#nvo vxlan id 3 multicast 239.10.10.9	Configure a VNID on this VTEP and enter the nvo mode.
(config-nvo)#vxlan map-network tunnel Tunnel4	Map the tunnel 4 with VNID 3
(config-nvo)#vxlan map-network tunnel Tunnel5	Map the tunnel 5 with VNID 3
(config-nvo)#exit	Exit NVO mode
(config)#nvo vxlan access-if port xe2	Map the access port xe2 of this VTEP
(config-nvo-acc-if)#map vnid 3	Map the VNID 3 to access-port xe2
(config-nvo-acc-if)#exit	Exit NVO access interface mode

RTR1

(config)#ip multicast-routing	Configure multicast routing on an intermediate router.
(config)# ip pim bsr-candidate lo	Configure bsr-candidate on middle router
(config)# ip pim rp-candidate lo	Configure rp-candidate on middle router
(config)# interface lo	Enter the configure mode.
(config-if)# ip address 6.6.6.6/32 secondary	Configure IP address on the interface lo
(config-if)# ip pim sparse-mode	Configure PIM mode as sparse mode
(config-if)#exit	Exit interface mode
(config)#interface xe1	Enter the configure mode.
(config-if)#ip address 2.2.2.1/24	Configure IP address on the interface xe1.
(config-if)#no shutdown	Bring the interface into operation with the no shutdown
(config-if)#ip igmp version 3	Configure interface with IGMP version 3
(config-if)#ip pim sparse-mode	Configure PIM mode as sparse mode.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter the configure mode.
(config-if)#ip address 3.3.3.1/24	Configure IP address on the interface xe2.

(config-if)#no shutdown	Bring the interface into operation with the no shutdown
(config-if)#ip igmp version 3	Configure interface with IGMP version 3
(config-if)#ip pim sparse-mode	Configure PIM mode as sparse mode.
(config-if)#exit	Exit interface mode.
(config)# router ospf 1	Configuring OSPF process id
(config-router)# network 6.6.6.6/32 area 0	Configuring redistribution
(config-router)# network 2.2.2.0/24 area 0	Advertising 2.2.2.0 network
(config-router)# network 3.3.3.0/24 area 0	Advertising 3.3.3.0 network
(config-router)#exit	Exit router mode

VTEP2

#configure terminal	Enter the configure mode.
(config)#interface xe2	Enter the interface mode.
(config-if)#switchport	Configure the interface as switchport.
(config-if)#no shutdown	Bring the interface into operation with the no shutdown
(config-if)#exit	Exit interface mode.
(config)#ip multicast-routing	Configure multicast routing on VTEP2.
(config)#interface xe1	Enter the configure mode.
(config-if)#ip address 3.3.3.4/24	Configure IP address on the interface xe1.
(config-if)#no shutdown	Bring the interface into operation with the no shutdown
(config-if)#ip igmp static-group 239.10.10.9	Configure interface with IGMP.
(config-if)#ip igmp version 3	Configure interface with IGMP version 3
(config-if)#ip pim sparse-mode	Configure PIM mode as sparse mode.
(config-if)#exit	Exit interface mode.
(config)# router ospf 1	Configuring OSPF process id
(config-router)# redistribute connected	Configuring redistribution
(config-router)# network 3.3.3.0/24 area 0	Advertising 2.2.2.0 network
(config-router)#exit	Exit router mode
(config)#nvo vxlan enable	Enable VXLAN globally on this vtep.
(config)#interface tunnel 4	Specify the interface (Tunnel4)to be configured and enter the interface mode.
(config-if)#tunnel mode vxlan	Assign this tunnel mode as VXLAN.
(config-if)#tunnel add interface xe1	Add outging interface for multicast tunnels.
(config-if)#tunnel source 3.3.3.4	Configure the source IP of this tunnel as an IP address which is configured on the interface xe1 of VTEP1.
(config-if)#tunnel destination 2.2.2.4	Configure the destination IP of this tunnel as an IP address which is configured on the interface xe1 of VTEP2.
(config-if)#exit	Exit the interface mode.

(config)#interface tunnel 5	Specify the interface (Tunnel5)to be configured and enter the interface mode.
(config-if)#tunnel mode vxlan	Assign this tunnel mode as VXLAN.
(config-if)#tunnel source 3.3.3.4	Configure the source IP of this tunnel as an IP address which is configured on the interface xe1 of VTEP1.
(config-if)#tunnel destination 239.10.10.9	Configure the destination IP of this tunnel as the multicast group address.
(config-if)#tunnel add interface xe1	Configure the exit interface for this tunnel.
(config-if)#exit	Exit the interface mode.
(config)#nvo vxlan id 3 multicast 239.10.10.9	Configure a VNID on this VTEP and enter the nvo mode.
(config-nvo)#vxlan map-network tunnel Tunnel4	Map the tunnel 4 with VNID 3
(config-nvo)#vxlan map-network tunnel Tunnel5	Map the tunnel 5 with VNID 3
(config-nvo)#exit	Exit NVO mode
(config)#nvo vxlan access-if port xe2	Map the access port xe2 of this VTEP
(config-nvo-acc-if)#map vnid 3	Map the VNID 3 to access-port xe2
(config-nvo-acc-if)#exit	Exit NVO access interface mode

Validation

VTEP1

```
VTEP1#show nvo vxlan vnid 3
VXLAN Information
=================
    Codes: NW - Network Port
           AC - Access Port
VNID     Type Interface   Vlan   Src-addr        Dst-addr
_____________________________________________________________
3        NW      ----     ----    2.2.2.4       239.10.10.9
3        NW      ----     ----    2.2.2.4         3.3.3.4
3        AC       xe2      ALL      ----           ---Total
number of entries are 2
```

RTR1

```
RTR1#show ip igmp groups
IGMP Connected Group Membership
Group Address     Interface           Uptime      Expires   State     Last
Reporter
239.10.10.9       xe1                 00:17:18 00:04:13    Active    2.2.2.4
239.10.10.9       xe2                 00:17:05 00:02:29    Active    3.3.3.4
```

VTEP2

```
VTEP1#show nvo vxlan vnid 3
```

```
VXLAN Information
=================
    Codes: NW - Network Port
           AC - Access Port
VNID    Type Interface   Vlan   Src-addr        Dst-addr
_____________________________________________________________________
 3       NW      ----     ----    3.3.3.4          2.2.2.4
 3       NW      ----     ----    2.2.2.4        239.10.10.9
 3       AC       xe2      ALL      ----           ----
Total number of entries are 2
```

CHAPTER 4 VXLAN-EVPN Configuration

This section contains basic VXLAN-EVPN configuration examples.

VXLAN (Virtual eXtended LAN) creates LAN segments using a MAC-in-IP encapsulation. The encapsulation carries the original L2 frame received from a host to the destination in another host using IP tunnels. The endpoints of the virtualized tunnel formed using VXLAN are called VTEPs (VXLAN Tunnel End Points). The VTEPs carry tenant data in L3 tunnels over the network which permits the network to support multiple tenants.The tenant data is not used in routing or switching. This aids in tenant machine movement and allows the tenants to have same IP/MAC addresses.

Information about the given VM to get to the VTEP is crucial in VXLAN protocol; therefore BGP-MP is used to carry this information across VTEPS.

Note: For port-channel/Static-channel interface, storm control will be applied on each member port. For Example: if Interface eth1 and interface eth2 is part of port-channel i.e. po1 and storm control 2mbps is applied for broadcast traffic, then the storm control settings will be applied on each member port and broadcast traffic on each member port will be rate limited to 2mbps each.

Topology

The procedures in this section use the topology in Figure 4-238.

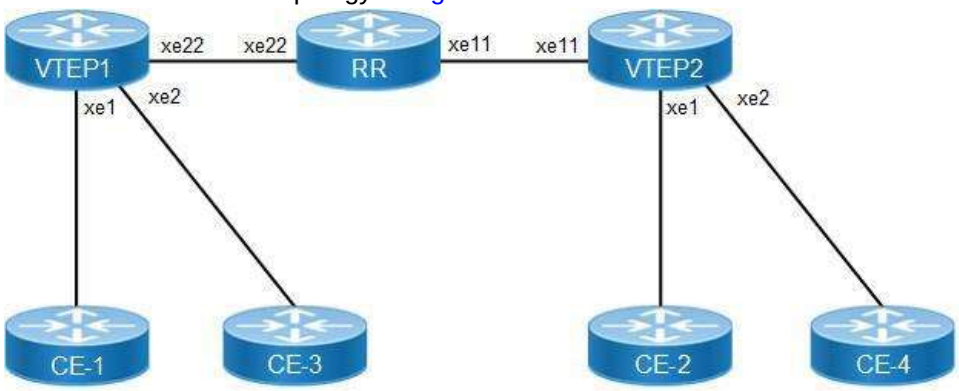


Figure 4-238: VXLAN EVPN

VTEP1

`#configure terminal`	Enter configure mode
`(config)#interface xe1`	Enter interface mode
`(config-if)#awitchport`	Configure the interface as a switch port.
`(config-if)#no shutdown`	Bring the interface into operation
`(config-if)#exit`	Exit interface mode
`(config)#interface xe2`	Enter configure mode
`(config-if)#switchport`	Configure the interface as switch port.
`(config-if)#no shutdown`	Bring the interface into operation.
`(config-if)#exit`	Exit interface mode.
`(config)#interface xe22`	Enter configure mode.

(config-if)#ip address 10.1.1.1/24	Set an IP address on the interface.

(config-if)#no shutdown	Bring the interface into operation.
(config-if)#exit	Exit interface mode.
(config)#interface lo	Enter configure mode.
(config-if)#ip address 1.1.1.1/32	Set an IP address on the interface.
(config-if)#no shutdown	Bring the interface into operation.
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance (ABC).
(config-router)#is-type level-1	Configure instance as level-1-only routing.
(config-router)#net 49.0001.1111.1111.1111.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#exit	Exit router mode.
(config)#interface xe22	Specify the interface (xe22) to configure
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface lo	Specify the interface (lo) to configure.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#mac vrf vrf_evpn_100	Configure a new VRF named vrf_evpn_100.
(config-vrf)#rd 1.1.1.1:1	Assign the Route Distinguisher value.
(config-vrf)#route-target both 100:1	Configure route target to import and export the routes.
(config-vrf)#exit	Exit VRF mode.
(config)#router bgp 1	Define the routing process. The number 1 specifies the AS number of VTEP1.
(config-router)#bgp router-id 1.1.1.1	Configure router-id for this BGP process.
(config-router)#neighbor 2.2.2.2 remote-as 1	Define BGP neighbor: 2.2.2.2 is the IP address of the neighbor (VTEP2), and 1 is the neighbor's AS number.
(config-router)# neighbor 2.2.2.2 updatesource 1.1.1.1	Define BGP neighbor: 1.1.1.1 is the peer interface.
(config-router)#address-family l2vpn evpn	Configure address-family L2VPN EVPN.
(config-router-af)#neighbor 2.2.2.2 activate	Activate the neighbor in the EVPN address family.
(config-router-af)#exit	Exit the address-family mode.
(config-router)#exit	Exit router mode.
(config)#nvo vxlan enable	Enable VXLAN globally on this VTEP.

(config)#nvo vxlan vtep-ip-global 1.1.1.1	Assign a global IP to the VTEP.
(config)#nvo vxlan id 100 ingressreplication	Configure a VNID on this VTEP and enter NVO mode.
(config-nvo)#vxlan host-reachabilityprotocol evpn-bgp vrf evpn 100	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with vrf evpn 100.
(config-nvo)#exit	Exit NVO mode.
(config)#nvo vxlan access-if port-vlan xe1 2	Configure access-port xe1 and map vlan 2
(config-nvo-acc-if)#map vnid 100	Map VNID 100 to access-port xe1.
(config-nvo-acc-if)#exit	Exit NVO access-if mode.
(config)#nvo vxlan id 200 ingressreplication	Configure second VNID on this VTEP and enter NVO mode.
(config-nvo)#vxlan host-reachabilityprotocol evpn-bgp vrf evpn 100	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with vrf evpn 100
(config-nvo)#exit	Exit NVO mode.
(config)#nvo vxlan access-if port-vlan xe2 3	Configure access-port xe2 and map vlan 3
(config-nvo-acc-if)#map vnid 200	Map VNID 200 to access-port xe2.
(config-nvo-acc-if)#exit	Exit NVO access-if mode.

RR

#configure terminal	Enter configure mode.
(config)#interface xe22	Enter interface mode.
(config-if)#ip address 10.1.1.2/24	Set an IP address on the interface.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe11	Enter configure mode.
(config-if)#ip address 20.1.1.2/24	Set an IP address on the interface.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance (ABC).
(config-router)#is-type level-1	Configure instance as level-1-only routing.
(config-router)#net 49.0001.3333.3333.3333.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#exit	Exit router mode.
(config)#interface xe22	Specify the interface (xe22) to configure.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface xe11	Specify the interface (xe11) to configure.

(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.

VTEP2

#configure terminal	Enter configure mode.
(config)#interface xe1	Enter interface mode.
(config-if)#switchport	Configure the interface as switchport.
(config-if)#no shutdown	Bring the interface into operation

(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter configure mode.
(config-if)#switchport	Configure the interface as switchport.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe11	Enter configure mode.
(config-if)#ip address 20.1.1.1/24	Set an IP address on the interface.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface lo	Enter configure mode.
(config-if)#ip address 2.2.2.2/32	Set an IP address on the interface.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance (ABC).
(config-router)#is-type level-1	Configure instance as level-1-only routing.
(config-router)#net 49.0001.2222.2222.2222.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#exit	Exit router mode.
(config)#interface xe11	Specify the interface (xe22) to configure.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface lo	Specify the interface (lo) to configure.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#mac vrf vrf_evpn_100	Configure a new VRF named vrf_evpn_100.

(config-vrf)#rd 2.2.2.1:1	Assign the Route Distinguisher value.
(config-vrf)#route-target both 100:1	Configure route target to import and export the routes.
(config-vrf)#exit	Exit VRF mode.
(config)#router bgp 1	Define the routing process. The number 1 specifies the AS number of VTEP1.
(config-router)#neighbor 1.1.1.1 remote-as 1	Define BGP neighbor: 1.1.1.1 is the IP address of the neighbor (VTEP1), and 1 is the neighbor's AS number.
(config-router)# neighbor 1.1.1.1 updatesource 2.2.2.2	Define BGP neighbor: 2.2.2.2 is the peer interface.
(config-router)#address-family l2vpn evpn	Configure address-family L2VPN EVPN.
(config-router-af)#neighbor 1.1.1.1 activate	Activate the neighbor in the EVPN address family.
(config-router-af)#exit	Exit address-family mode.
(config-router)#exit	Exit router mode.
(config)#nvo vxlan enable	Enable VXLAN globally on this VTEP.
(config)#nvo vxlan vtep-ip-global 2.2.2.2	Assign a global IP to the VTEP.
(config)#nvo vxlan id 100 ingressreplication	Configure a VNID on this VTEP and enter NVO mode.
(config-nvo)#vxlan host-reachabilityprotocol evpn-bgp vrf_evpn_100	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with `vrf evpn 100`.
(config-nvo)#exit	Exit NVO mode.
(config)#nvo vxlan access-if port-vlan xe1 2	Configure access-port xe1 and map vlan 2
(config-nvo-acc-if)#map vnid 100	Map VNID 100 to access-port xe1.
(config-nvo-acc-if)#exit	Exit NVO access-if mode.
(config)#nvo vxlan id 200 ingressreplication	Configure second VNID on this VTEP and enter NVO mode.
(config-nvo)#vxlan host-reachabilityprotocol evpn-bgp vrf evpn 100	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with `vrf evpn 100`
(config-nvo)#exit	Exit NVO mode.
(config)#nvo vxlan access-if port-vlan xe2 3	Configure access-port xe2 and map vlan 3
(config-nvo-acc-if)#map vnid 200	Map VNID 200 to access-port xe2.
(config-nvo-acc-if)#exit	Exit NVO access-if mode.

Validation

CE1 and CE2 have hosts configured with MAC addresses, IP addresses, and VLAN identifiers as shown below.

		VLAN	IP Address	Mac Address
VTEP1	CE-1	2	12.12.12.10	0000.0000.abab

VTEP2	CE-2	2	12.12.12.20	0000.0000.cdcd
VTEP1	CE-1	3	13.13.13.10	0000:0b60:25f2
VTEP2	CE-2	3	13.13.13.20	0000:0b60:25f3

Perform a tagged ping of VLAN 2 from CE1 to CE2 and vice-versa. Also perform a tagged ping of VLAN 3 from CE1 to CE2 and vice-versa.

VTEP Tunnel Status

```
VTEP-1#show nvo vxlan tunnel
VXLAN Network tunnel Entries
   Source           Destination             Status
================================================
   1.1.1.1          2.2.2.2                 Installed

VTEP-2#show nvo vxlan tunnel
VXLAN Network tunnel Entries
   Source           Destination             Status
================================================
    2.2.2.2         1.1.1.1                 Installed
```

VTEP ARP Cache

```
VTEP-1#show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
VNID Ip-Addr            Mac-Addr            Type

_____________________________________________
200     13.13.13.10     0000.0b60.25f2      Dynamic
200     13.13.13.20     0000.0b60.25f3      Evpn
100     12.12.12.20     0000.0000.cdcd      Evpn
100     12.12.12.10     0000.0000.abab      Dynamic

VTEP-2#show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
VNID Ip-Addr            Mac-Addr            Type

_____________________________________________
200     13.13.13.10     0000.0b60.25f2      Evpn
200     13.13.13.20     0000.0b60.25f3      Dynamic
100     12.12.12.10     0000.0000.abab      Evpn
100     12.12.12.20     0000.0000.cdcd      Dynamic
```

VTEP MAC Tables

```
VTEP-1#show nvo vxlan mac-table
================================================================= VXLAN MAC Entries

=================================================================

VNID Interface      Mac-Addr         VTEP-Ip   Type

_________________________________________________________________
```

```
 100   xe1           0000.0000.abab 1.1.1.1    Dynamic Local
 100   ---           0000.0000.cdcd 2.2.2.2    Remote
 200   xe1           0000.0b60.25f2  1.1.1.1    Dynamic Local
 200   ---           0000.0b60.25f3  2.2.2.2    Remote
VTEP-2#show nvo vxlan mac-table
============================================================== VXLAN MAC Entries

================================================================

VNID Interface      Mac-Addr         VTEP-Ip   Type
________________________________________________________________
100    ---           0000.0000.abab 1.1.1.1     Remote
100    xe1           0000.0000.cdcd 2.2.2.2     Dynamic Local
200    ---           0000.0b60.25f2 1.1.1.1     Remote
200    xe1           0000.0b60.25f3 2.2.2.2     Dynamic Local
```

VTEP MAC-IP BGP EVPN Entries

```
VTEP-1#show bgp l2vpn evpn mac-ip
RD[1.1.1.1:1] VRF[vrf_evpn_100]:
ESI    Eth-Tag   Mac-Address      IP-Address      VNID Nexthop
0         0      0000:0000:abab 12.12.12.10 100       1.1.1.1
0         0      0000:0000:cdcd 12.12.12.20 100       2.2.2.2
0         0      0000:0b60:25f2 13.13.13.10 200       1.1.1.1
0         0      0000:0b60:25f3 13.13.13.20 200       2.2.2.2
RD[1.1.1.1:1]
ESI    Eth-Tag   Mac-Address      IP-Address      VNID Nexthop
0         0      0000:0000:cdcd 12.12.12.20 100       2.2.2.2
0 0 0000:0b60:25f313.13.13.202002.2.2.2

VTEP-2#show   bgp   l2vpn   evpn   mac-ip   RD[1.1.1.1:1]
VRF[vrf_evpn_100]:
ESI     Eth-Tag  Mac-Address      IP-Address      VNID Nexthop
0          0      0000:0000:abab 12.12.12.10 100      1.1.1.1
0          0      0000:0000:cdcd 12.12.12.20 100      2.2.2.2
0          0      0000:0b60:25f2 13.13.13.10 200      1.1.1.1
0          0      0000:0b60:25f3 13.13.13.20 200      2.2.2.2
RD[1.1.1.1:1]
ESI     Eth-Tag  Mac-Address      IP-Address      VNID Nexthop
0          0      0000:0000:abab 12.12.12.10 100      1.1.1.1
0          0     0000:0b60:25f2  13.13.13.10 200      1.1.1.1
```

LAG as Access Port with ECMP on the Network Side

This section contains basic VXLAN EVPN configuration with LAG as an access port and ECMP on the network side.

Topology

The procedures in this section use the topology in Figure 4-239.

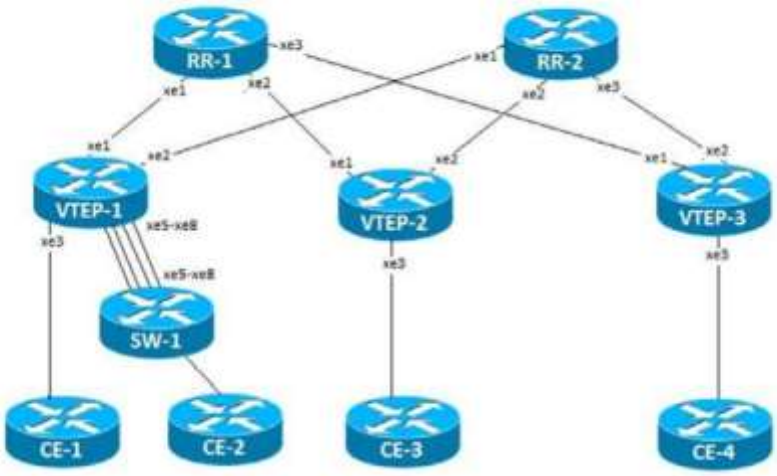


Figure 4-239: VXLAN EVPN with LAG and ECMP

VTEP1

#configure terminal	Enter configure mode.
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure the interface as switchport.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe5	Enter configure mode.
(config-if)#switchport	Configure the interface as switchport.
(config-if)#channel-group 1 mode active	Configure the interface to be part of port channel 1
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe6	Enter configure mode.
(config-if)#switchport	Configure the interface as switchport.
(config-if)#channel-group 1 mode active	Configure the interface to be part of port channel 1
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe7	Enter configure mode.
(config-if)#switchport	Configure the interface as switchport.
(config-if)#channel-group 1 mode active	Configure the interface to be part of port channel 1
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe8	Enter configure mode.
(config-if)#switchport	Configure the interface as switchport.
(config-if)#channel-group 1 mode active	Configure the interface to be part of port channel 1
(config-if)#no shutdown	Bring the interface into operation

(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter configure mode.
(config-if)#ip address 10.1.1.0/32	Configure IP address on the interface xe1.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter configure mode.
(config-if)#ip address 10.1.1.2/24	Configure IP address on the interface xe2.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface lo	Enter configure mode.
(config-if)#ip address 1.1.1.1/32	Configure IP address on the interface xe3.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance (ABC).
(config-router)#is-type level-1	Configure instance as level-1-only routing.

(config-router)#net	Set a Network Entity Title for this instance, specifying the
49.0001.1111.1111.1111.00	area address and the system ID.
(config-router)#exit	Exit router mode.
(config)#interface xe1	Specify the interface (xe1) to configure.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Specify the interface (xe2) to configure.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface lo	Specify the interface (lo) to configure.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#mac vrf vrf_evpn_100	Configure a new VRF named vrf_evpn_100.
(config-vrf)#rd 1.1.1.1:1	Assign the Route Distinguisher value.
(config-vrf)#route-target both 100:1	Configure route target to import and export the routes.
(config-vrf)#exit	Exit VRF mode.
(config)#load-balance rtag7	Enable load balancing for RTAG7 globally.

(config)#load-balance rtag7 ipv4 src-ipv4	Enable load balancing for RTAG7 for IPv4 for source IP.
(config)#router bgp 65535	Define the routing process. The number 65535 specifies the AS number of VTEP1.
(config-router)#bgp router-id 1.1.1.1	Configure router-id for this BGP process.
(config-router)#neighbor 2.2.2.2 remote-as 65535	Define BGP neighbor: 2.2.2.2 is the IP address of the neighbor (VTEP2), and 65535 is the neighbor's AS number.
(config-router)# neighbor 2.2.2.2 updatesource 1.1.1.1	Define BGP neighbor: 1.1.1.1 is the peer interface.
(config-router)#neighbor 3.3.3.3 remote-as 65535	Define BGP neighbor: 3.3.3.3 is the IP address of the neighbor (VTEP3), and 65535 is the neighbor's AS number.
(config-router)# neighbor 3.3.3.3 updatesource 1.1.1.1	Define BGP neighbor: 1.1.1.1 is the peer interface.
(config-router)#address-family l2vpn evpn	Configure address-family L2VPN EVPN.
(config-router-af)#neighbor 2.2.2.2 activate	Activate the neighbor at VTEP2 in the EVPN address family.
(config-router-af)#neighbor 3.3.3.3 activate	Activate the neighbor at VTEP3 in the EVPN address family.
(config-router-af)#exit	Exit address-family mode.
(config-router)#exit	Exit router mode.
(config)#nvo vxlan enable	Enable VXLAN globally on this VTEP.
(config)#nvo vxlan vtep-ip-global 1.1.1.1	Assign a global IP to the VTEP.
(config)#nvo vxlan id 100001 ingressreplication	Configure a VNID on this VTEP and enter NVO mode.
(config-nvo)#vxlan host-reachabilityprotocol evpn-bgp vrf_evpn_100	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with VRF vrf_evpn_100.
(config-nvo)#exit	Exit NVO mode.
(config)#nvo vxlan access-if port-vlan xe3 2	Configure access-port xe3 and map vlan 2
(config-nvo-acc-if)#map vnid 100001	Map VNID 100001 to access-port xe3.
(config-nvo-acc-if)#exit	Exit NVO access-if mode.
(config)#nvo vxlan access-if port-vlan po1 2	Configure access-port po1 and map vlan 2
(config-nvo-acc-if)#map vnid 100001	Map VNID 100001 to access-port po1.
(config-nvo-acc-if)#exit	Exit NVO access-if mode.
(config)#nvo vxlan id 200001 ingressreplication	Configure second VNID on this VTEP and enter NVO mode.
(config-nvo)#vxlan host-reachabilityprotocol evpn-bgp vrf_evpn_100	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with VRF vrf_evpn_100.
(config-nvo)#exit	Exit NVO mode.
(config)#nvo vxlan access-if port-vlan xe3 3	Configure access-port xe3 and map vlan 3
(config-nvo-acc-if)#map vnid 200001	Map VNID 200001 to access-port xe3.

(config-nvo-acc-if)#exit	Exit NVO access-if mode.
(config)#nvo vxlan access-if port-vlan po1 3	Configure access-port po1 and map vlan 3
(config-nvo-acc-if)#map vnid 200001	Map VNID 200001 to access-port xe3.
(config-nvo-acc-if)#exit	Exit NVO access-if mode.

RR-1

#configure terminal	Enter configure mode.
(config)#interface lo	Enter configure mode.
(config-if)#ip address 12.12.12.12/32	Set an IP address on the interface.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter configure mode.
(config-if)#ip address 10.1.1.1/31	Configure IP address on the interface xe1.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter configure mode.
(config-if)#ip address 20.1.1.1/31	Configure IP address on the interface xe2.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe3	Enter configure mode.
(config-if)#ip address 30.1.1.1/31	Configure IP address on the interface xe3.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance (ABC).
(config-router)#is-type level-1	Configure instance as level-1-only routing.
(config-router)#net 49.0001.4444.4444.4444.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#exit	Exit router mode.
(config)#interface lo	Specify the interface (lo) to configure.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Specify the interface (xe1) to configure.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Specify the interface (xe2) to configure.

(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface xe3	Specify the interface (xe3) to configure.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.

RR-2

#configure terminal	Enter configure mode.
(config)#interface lo	Enter configure mode.
(config-if)#ip address 13.13.13.13/32	Set an IP address on the interface.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter configure mode.
(config-if)#ip address 10.1.1.3/31	Configure IP address on the interface xe1.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter configure mode.
(config-if)#ip address 20.1.1.3/31	Configure IP address on the interface xe2.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe3	Enter configure mode.
(config-if)#ip address 30.1.1.3/31	Configure IP address on the interface xe3.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance (ABC).
(config-router)#is-type level-1	Configure instance as level-1-only routing.
(config-router)#net 49.0001.5555.5555.5555.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#exit	Exit router mode.
(config)#interface lo	Specify the interface (lo) to configure.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Specify the interface (xe1) to configure.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).

(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Specify the interface (xe2) to configure.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface xe3	Specify the interface (xe3) to configure.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.

VTEP-2

#configure terminal	Enter configure mode.
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure the interface as switchport.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter configure mode.
(config-if)#ip address 20.1.1.0/32	Configure IP address on the interface xe1.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter configure mode.
(config-if)#ip address 20.1.1.2/24	Configure IP address on the interface xe2.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface lo	Enter configure mode.
(config-if)#ip address 2.2.2.2/32	Configure IP address on the interface xe3.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance (ABC).
(config-router)#is-type level-1	Configure instance as level-1-only routing.

(config-router)#net 49.0001.2222.2222.2222.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#exit	Exit router mode.
(config)#interface xe1	Specify the interface (xe1) to configure.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).

(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Specify the interface (xe2) to configure.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface lo	Specify the interface (lo) to configure.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#mac vrf vrf_evpn_100	Configure a new VRF named vrf_evpn_100.
(config-vrf)#rd 1.1.1.1:1	Assign the Route Distinguisher value.
(config-vrf)#route-target both 100:1	Configure route target to import and export the routes.
(config-vrf)#exit	Exit VRF mode.
(config)#load-balance rtag7	Enable load balancing for RTAG7 globally.
(config)#load-balance rtag7 ipv4 src-ipv4	Enable load balancing for RTAG7 for IPv4 for source IP.
(config)#router bgp 65535	Define the routing process. The number 65535 specifies the AS number of VTEP1.
(config-router)#neighbor 1.1.1.1 remote-as 65535	Define BGP neighbor: 1.1.1.1 is the IP address of the neighbor (VTEP1), and 65535 is the neighbor's AS number.
(config-router)#neighbor 1.1.1.1 updatesource 2.2.2.2	Define BGP neighbor: 2.2.2.2 is the peer interface.
(config-router)#neighbor 3.3.3.3 remote-as 65535	Define BGP neighbor: 3.3.3.3 is the IP address of the neighbor (VTEP3), and 65535 is the neighbor's AS number.
(config-router)#neighbor 3.3.3.3 updatesource 2.2.2.2	Define BGP neighbor: 2.2.2.2 is the peer interface.
(config-router)#address-family l2vpn evpn	Configure address-family L2VPN EVPN.
(config-router-af)#neighbor 1.1.1.1 activate	Activate the neighbor at VTEP1 in the EVPN address family.
(config-router-af)#neighbor 3.3.3.3 activate	Activate the neighbor at VTEP3 in the EVPN address family.
(config-router-af)#exit	Exit address-family mode.
(config-router)#exit	Exit router mode.
(config)#nvo vxlan enable	Enable VXLAN globally on this VTEP.
(config)#nvo vxlan vtep-ip-global 2.2.2.2	Assign a global IP to the VTEP.
(config)#nvo vxlan id 100001 ingressreplication	Configure a VNID on this VTEP and enter NVO mode.
(config-nvo)#vxlan host-reachabilityprotocol evpn-bgp vrf_evpn_100	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with VRF vrf evpn 100.
(config-nvo)#exit	Exit NVO mode.

(config)#nvo vxlan access-if port-vlan xe3 2	Configure access-port xe3 and map vlan 2
(config-nvo-acc-if)#map vnid 100001	Map VNID 100001 to access-port xe3.
(config-nvo-acc-if)#exit	Exit NVO access-if mode.
(config)#nvo vxlan id 200001 ingressreplication	Configure second VNID on this VTEP and enter NVO mode.
(config-nvo)#vxlan host-reachabilityprotocol evpn-bgp vrf_evpn_100	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with VRF `vrf evpn 100`.
(config-nvo)#exit	Exit NVO mode.
(config)#nvo vxlan access-if port-vlan xe3 3	Configure access-port xe3 and map vlan 3
(config-nvo-acc-if)#map vnid 200001	Map VNID 200001 to access-port xe3.
(config-nvo-acc-if)#exit	Exit NVO access-if mode.

VTEP3

#configure terminal	Enter configure mode.
(config)#interface xe3	Enter interface mode.
(config-if)#switchport	Configure the interface as switchport.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe1	Enter configure mode.
(config-if)#ip address 30.1.1.0/32	Configure IP address on the interface xe1.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface xe2	Enter configure mode.
(config-if)#ip address 30.1.1.2/24	Configure IP address on the interface xe2.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#interface lo	Enter configure mode.
(config-if)#ip address 3.3.3.3/32	Configure IP address on the interface xe3.
(config-if)#no shutdown	Bring the interface into operation
(config-if)#exit	Exit interface mode.
(config)#router isis ABC	Create an IS-IS routing instance (ABC).
(config-router)#is-type level-1	Configure instance as level-1-only routing.
(config-router)#net 49.0001.3333.3333.3333.00	Set a Network Entity Title for this instance, specifying the area address and the system ID.
(config-router)#exit	Exit router mode.
(config)#interface xe1	Specify the interface (xe1) to configure.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).

(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.

(config)#interface xe2	Specify the interface (xe2) to configure.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#interface lo	Specify the interface (lo) to configure.
(config-if)#ip router isis ABC	Enable IS-IS routing on an interface for area 49 (ABC).
(config-if)#isis circuit-type level-1	Configure instance as level-1-only routing.
(config-if)#exit	Exit interface mode.
(config)#mac vrf vrf_evpn_100	Configure a new VRF named vrf_evpn_100.
(config-vrf)#rd 1.1.1.1:1	Assign the Route Distinguisher value.
(config-vrf)#route-target both 100:1	Configure route target to import and export the routes.
(config-vrf)#exit	Exit VRF mode.
(config)#load-balance rtag7	Enable load balancing for RTAG7 globally.
(config)#load-balance rtag7 ipv4 src-ipv4	Enable load balancing for RTAG7 for IPv4 for source IP.
(config)#router bgp 65535	Define the routing process. The number 65535 specifies the AS number of VTEP1.
(config-router)#neighbor 1.1.1.1 remote-as 65535	Define BGP neighbor: 1.1.1.1 is the IP address of the neighbor (RR1), and 65535 is the neighbor's AS number.
(config-router)#neighbor 1.1.1.1 updatesource 3.3.3.3	Define BGP neighbor: 3.3.3.3 is the peer interface.
(config-router)#neighbor 2.2.2.2 remote-as 65535	Define BGP neighbor: 2.2.2.2 is the IP address of the neighbor (VTEP3), and 65535 is the neighbor's AS number.
(config-router)#neighbor 2.2.2.2 updatesource 3.3.3.3	Define BGP neighbor: 3.3.3.3 is the peer interface.
(config-router)#address-family l2vpn evpn	Configure address-family L2VPN EVPN.
(config-router-af)#neighbor 1.1.1.1 activate	Activate the neighbor at VTEP1 in the EVPN address family.
(config-router-af)#neighbor 2.2.2.2 activate	Activate the neighbor at VTEP2 in the EVPN address family.
(config-router-af)#exit	Exit address-family mode.
(config-router)#exit	Exit router mode.
(config)#nvo vxlan enable	Enable VXLAN globally on this VTEP.
(config)#nvo vxlan vtep-ip-global 3.3.3.3	Assign a global IP to the VTEP.
(config)#nvo vxlan id 100001 ingressreplication	Configure a VNID on this VTEP and enter NVO mode.
(config-nvo)#vxlan host-reachabilityprotocol evpn-bgp vrf_evpn_100	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with VRF vrf evpn 100.

(config-nvo)#exit	Exit NVO mode.
(config)#nvo vxlan access-if port-vlan xe3 2	Configure access-port xe3 and map vlan 2
(config-nvo-acc-if)#map vnid 100001	Map VNID 100001 to access-port xe3.
(config-nvo-acc-if)#exit	Exit NVO access-if mode.
(config)#nvo vxlan id 200001 ingressreplication	Configure second VNID on this VTEP and enter NVO mode.
(config-nvo)#vxlan host-reachabilityprotocol evpn-bgp vrf_evpn_100	Configure host-reachability-protocol as BGP-EVPN and associate the VNID with VRF `vrf evpn 100`
(config-nvo)#exit	Exit NVO mode.
(config)#nvo vxlan access-if port-vlan xe3 3	Configure access-port xe3 and map vlan 3
(config-nvo-acc-if)#map vnid 200001	Map VNID 200001 to access-port xe3.
(config-nvo-acc-if)#exit	Exit NVO access-if mode.

Validation

CE1, CE2, CE3, and CE4 have hosts configured with MAC addresses, IP addresses, and VLAN identifiers as shown below.

		VLAN	IP Address	MAC Address
VTEP1	CE-1	2	12.12.12.10	0000.0000.aaaa
VTEP1	CE-2	2	12.12.12.20	0000.0000.bbbb
VTEP2	CE-3	2	12.12.12.30	0000.0000.cccc
VTEP3	CE-4	2	12.12.12.40	0000.0000.dddd
VTEP1	CE-1	3	14.14.14.10	0000.058e.2181
VTEP1	CE-2	3	14.14.14.20	0000.058e.2182
VTEP2	CE-3	3	14.14.14.30	0000.058e.2183
VTEP3	CE-4	3	14.14.14.40	0000.058e.2184

Perform a tagged ping of VLAN 2 from CE1 to CE2,CE3 and CE4 and vice-versa. Also perform a tagged ping of VLAN 3 from CE1 to CE2, CE3 and CE4 and vice-versa.

VTEP Tunnel Status

```
VTEP-1#show nvo vxlan tunnel
VXLAN Network tunnel Entries
```

```
Source     Destination Status
==================================================
1.1.1.1   3.3.3.3      Installed
1.1.1.1   2.2.2.2      Installed

VTEP-2#show nvo vxlan tunnel
VXLAN Network tunnel Entries
Source     Destination Status
==================================================
2.2.2.2   1.1.1.1      Installed
2.2.2.2   3.3.3.3      Installed

VTEP-3#show nvo vxlan tunnel
VXLAN Network tunnel Entries
Source     Destination Status
==================================================
   3.3.3.3   2.2.2.2      Installed
   3.3.3.3   1.1.1.1      Installed
```

VTEP ARP Tables

```
VTEP-1#show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
============================
    VNID Ip-Addr           Mac-Addr         Type

_____________________________________________________
   100001      12.12.12.30 0000.0000.cccc Evpn
   100001      12.12.12.10 0000.0000.aaaa Dynamic
   100001      12.12.12.20 0000.0000.bbbb Dynamic
   100001      12.12.12.40 0000.0000.dddd Evpn
   200001      14.14.14.20 0000.058e.2182 Dynamic
   200001      14.14.14.10 0000.058e.2181 Dynamic
   200001      14.14.14.30 0000.058e.2183 Evpn
   200001      14.14.14.40 0000.058e.2184 Evpn

VTEP-2#show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
============================
   VNID         Ip-Addr       Mac-Addr            Type

_____________________________________________________
   100001        12.12.12.30 0000.0000.cccc       Dynamic
100001 12.12.12.10 0000.0000.aaaa   Evpn 100001 12.12.12.20 0000.0000.bbbb    Evpn
100001      12.12.12.40 0000.0000.dddd    Evpn 200001 14.14.14.20 0000.058e.2182
Evpn 200001 14.14.14.10 0000.058e.2181    Evpn
   200001        14.14.14.30 0000.058e.2183       Dynamic
   200001        14.14.14.40 0000.058e.2184       Evpn

VTEP-3#show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
============================
   VNID         Ip-Addr          Mac-Addr            Type
```

```
_____________________________________________________
100001 12.12.12.20 0000.0000.bbbb    Evpn 100001 12.12.12.10 0000.0000.aaaa    Evpn
100001      12.12.12.30 0000.0000.cccc    Evpn
    100001        12.12.12.40     0000.0000.dddd      Dynamic
200001 14.14.14.30 0000.058e.2183    Evpn 200001 14.14.14.20 0000.058e.2182    Evpn
200001      14.14.14.10 0000.058e.2181    Evpn
    200001        14.14.14.40     0000.058e.2184      Dynamic
```

VTEP MAC Tables

```
VTEP-1#show nvo vxlan mac-table
================================================================= VXLAN MAC Entries
=================================================================

VNID      Interface    Mac-Addr         VTEP-Ip   Type

_____________________________________________________________________
 100001   xe3           0000.0000.aaaa 1.1.1.1    Dynamic Local
 100001   po1           0000.0000.bbbb 1.1.1.1    Dynamic Local
 100001     ---   0000.0000.cccc 2.2.2.2  Remote 100001     ---
      0000.0000.dddd 3.3.3.3  Remote
 200001   xe3           0000.058e.2181 1.1.1.1    Dynamic Local
 200001   po1           0000.058e.2182 1.1.1.1    Dynamic Local
 200001   ---           0000.058e.2183 2.2.2.2    Remote
 200001   ---           0000.058e.2184 3.3.3.3    Remote

VTEP-2#show nvo vxlan mac-table
=================================================================
VXLAN MAC Entries
=================================================================

VNID      Interface    Mac-Addr            VTEP-Ip          Type

_____________________________________________________________________
100001      ---   0000.0000.aaaa    1.1.1.1     Remote 100001     ---   0000.0000.bbbb
      1.1.1.1     Remote
100001    xe3           0000.0000.cccc      2.2.2.2          Dynamic Local
100001---   0000.0000.dddd    3.3.3.3     Remote 200001     ---   0000.058e.2181
1.1.1.1     Remote 200001     ---   0000.058e.2182     1.1.1.1    Remote
200001    xe3           0000.058e.2183      2.2.2.2          Dynamic Local
200001    ---           0000.058e.2184      3.3.3.3          Remote

VTEP-3#show nvo vxlan mac-table
================================================================= VXLAN MAC Entries

=================================================================

VNID      Interface    Mac-Addr            VTEP-Ip          Type

_____________________________________________________________________
100001    ---           0000.0000.aaaa      1.1.1.1          Remote
100001       ---  0000.0000.bbbb    1.1.1.1     Remote 100001     ---   0000.0000.cccc
      2.2.2.2     Remote
100001    xe3           0000.0000.dddd      3.3.3.3          Dynamic Local
```

```
200001---   0000.058e.2181    1.1.1.1     Remote 200001      ---  0000.058e.2182
1.1.1.1     Remote 200001     ---   0000.058e.2183     2.2.2.2    Remote
200001    xe3           0000.058e.2184       3.3.3.3         Dynamic Local
```

VTEP MAC-IP BGP EVPN Entries

```
VTEP-1#show bgp l2vpn evpn mac-ip

RD[1.1.1.1:1] VRF[vrf_evpn_100]:
ESI       Eth-Tag      Mac-Address            IP-Address     VNID Nexthop
0         0            0000:0000:aaaa          12.12.12.10 10000 11.1.1.1
0         0            0000:0000:bbbb          12.12.12.20 10000 11.1.1.1
0         0            0000:0000:cccc          12.12.12.30 10000 12.2.2.2
0         0            0000:0000:dddd          12.12.12.40 10000 13.3.3.3
0         0            0000:058e:2181         14.14.14.10 20000  11.1.1.1
0         0            0000:058e:2182         14.14.14.20 20000  11.1.1.1
0         0            0000:058e:2183         14.14.14.30 20000  12.2.2.2
0         0            0000:058e:2184         14.14.14.40 20000  13.3.3.3
RD[1.1.1.1:1]
ESI       Eth-Tag      Mac-Address            IP-Address     VNID Nexthop
0         0            0000:0000:cccc          12.12.12.30 10000 12.2.2.2
0         0            0000:0000:cccc          12.12.12.30 10000 12.2.2.2
0         0            0000:0000:dddd          12.12.12.40 10000 13.3.3.3
0         0            0000:0000:dddd          12.12.12.40 10000 13.3.3.3
0         0            0000:058e:2183         14.14.14.30 20000  12.2.2.2
0         0            0000:058e:2183         14.14.14.30 20000  12.2.2.2
0         0            0000:058e:2184              14.14.14.40  20000 13.3.3.3
0         0            0000:058e:2184              14.14.14.40  20000 13.3.3.3

VTEP-2#show bgp l2vpn evpn mac-ip
RD[1.1.1.1:1]
ESI       Eth-Tag      Mac-Address            IP-Address     VNID Nexthop
0         0            0000:0000:aaaa          12.12.12.10 10000 11.1.1.1
0         0            0000:0000:aaaa          12.12.12.10 10000 11.1.1.1
0         0            0000:0000:bbbb          12.12.12.20 10000 11.1.1.1
0         0            0000:0000:bbbb          12.12.12.20 10000 11.1.1.1
0         0            0000:0000:dddd          12.12.12.40 10000 13.3.3.3
0         0            0000:0000:dddd          12.12.12.40 10000 13.3.3.3
0         0            0000:058e:2181         14.14.14.10 20000  11.1.1.1
0         0            0000:058e:2181         14.14.14.10 20000  11.1.1.1
0         0            0000:058e:2182         14.14.14.20 20000  11.1.1.1
0         0            0000:058e:2182         14.14.14.20 20000  11.1.1.1
0         0            0000:058e:2184         14.14.14.40 20000  13.3.3.3
0         0            0000:058e:2184         14.14.14.40 20000  13.3.3.3
RD[1.1.1.1:1] VRF[vrf_evpn_100]:
ESI       Eth-Tag      Mac-Address            IP-Address     VNID Nexthop
0         0            0000:0000:aaaa          12.12.12.10 10000 11.1.1.1
0         0            0000:0000:bbbb          12.12.12.20 10000 11.1.1.1
0         0            0000:0000:cccc          12.12.12.30 10000 12.2.2.2
0         0            0000:0000:dddd          12.12.12.40 10000 13.3.3.3
0         0            0000:058e:2181         14.14.14.10 20000  11.1.1.1
```

```
0          0             0000:058e:2182          14.14.14.20  20000  11.1.1.1
0          0             0000:058e:2183          14.14.14.30  20000  12.2.2.2
0          0             0000:058e:2184          14.14.14.40  20000  13.3.3.3

VTEP-3#show bgp l2vpn evpn mac-ip
RD[1.1.1.1:1]
ESI        Eth-Tag       Mac-Address             IP-Address      VNID Nexthop
0          0             0000:0000:aaaa           12.12.12.10 10000  11.1.1.1
0          0             0000:0000:aaaa           12.12.12.10 10000  1.1.1.1
0      0    0000:0000:bbbb    12.12.12.20 10000 11.1.1.1 0  0
0000:0000:bbbb    12.12.12.20 10000  11.1.1.1  0 0     0000:0000:cccc
12.12.12.30 10000 12.2.2.2 0  0     0000:0000:cccc    12.12.12.30 10000
12.2.2.2  0 0     0000:058e:2181    14.14.14.10 20000  11.1.1.1  0  0
0000:058e:2181    14.14.14.10  20000 11.1.1.1  0 0     0000:058e:2182
14.14.14.20 20000  11.1.1.1  0  0    0000:058e:2182     14.14.14.20  20000
11.1.1.1  0 0      0000:058e:2183   14.14.14.30  20000  12.2.2.2
0          0             0000:058e:2183           14.14.14.30 20000 12.2.2.2
RD[1.1.1.1:1] VRF[vrf_evpn_100]:
ESI Eth-Tag Mac-Address IP-Address VNID Nexthop 0 0 0000:0000:aaaa 12.12.12.10
10000 11.1.1.1 0 0 0000:0000:bbbb 12.12.12.20 10000 11.1.1.1 0 0 0000:0000:cccc
12.12.12.30  10000  12.2.2.2
0          0             0000:0000:dddd           12.12.12.40 10000 13.3.3.3
0      0     0000:058e:2181   14.14.14.10  20000  11.1.1.1 0   0
0000:058e:2182    14.14.14.20 20000  11.1.1.1  0  0     0000:058e:2183
14.14.14.30  20000  12.2.2.2
0       0            0000:058e:2184           14.14.14.40 20000  13.3.3.3
```

VxLAN-EVPN with IRB Configuration

Overview

EVPN provides an extensible and flexible VPN solution for intra-subnet connectivity among Tenant Systems (TS's) over an MPLS/IP network, where an IP subnet is represented by an EVI for a VLAN-based service or by an <EVI, VLAN> for a VLAN-aware bundle service. However, there are scenarios where, in addition to intra-subnet forwarding, inter-subnet forwarding is required among TS's across different IP subnets at EVPN PE nodes, while maintaining the multi-homing capabilities of EVPN. In such scenarios, a solution that provides optimal forwarding of Layer 2 as well as Layer 3 traffic in a data center environment that handles requirements like Layer 3 VPN interoperability and VM mobility is necessary.

An EVPN-based Integrated Routing and Bridging solution meets these requirements of optimum Unicast and Multicast forwarding for intra-subnets and inter-subnets inside and across data centers. The solution is required to efficiently handle inter-subnet forwarding as well as virtual machine (VM) mobility.

There are 2 modes of IRB.

- Symmetric IRB
- Asymmetric IRB

Note: SWMRE supports Symmetric IRB only.

Anycast/Distributed Gateway

Topology

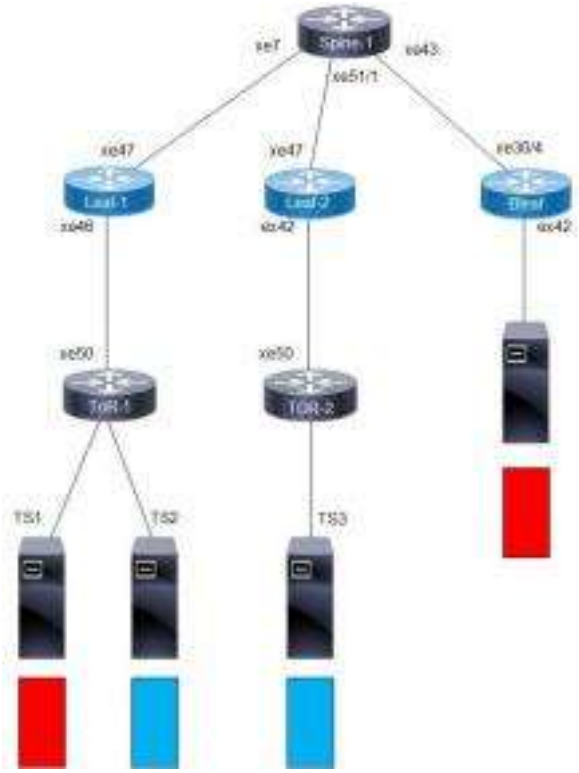


Figure 4-240: VxLAN_EVPN_IRB

Configuration

Leaf1

`#configure terminal`	Enter Configure mode.
`(config)#interface lo`	Enter Interface mode for loopback.
`(config-if)#ip address 172.16.100.186/32 secondary`	Assign secondary IP address.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#nvo vxlan enable`	Enable VXLAN
`(config)#nvo vxlan irb`	Enable IRB
`(config)#evpn irb-forwarding anycastgateway-mac 0000.0000.ffff`	Configure anycast gateway mac address
`(config)#mac vrf mac_vrf10000`	Create mac routing/forwarding instance with vrf10000 name and enter into vrf mode
`(config-vrf)# rd 10000:1`	Assign RD value
`(config-vrf)# route-target both 10000:10000`	Assign route-target value for export & Import of mac-ip routes

(config-vrf)#exit	Exit from vrf configuration mode
(config)#mac vrf mac vrf11000	Create mac routing/forwarding instance with vrf1 11000 name and enter into vrf mode
(config-vrf)# rd 11000:1	Assign RD value
(config-vrf)# route-target both 11000:11000	Assign route-target value for export & import of mac ip routes
(config-vrf)#exit	Exit from vrf configuration mode
(config)#ip vrf ip_vrf5000	Create Ip Vrf to bind different vnid ‘s together inorder to communicate between different L2VNID’s
(config-vrf)#rd 5000:1	Assign RD value
(config-vrf)#route-target both 5000:5000	Assign route-target for export and import of routes
(config-vrf)#l3vni 5000	Configure l3vni to communicate between different L2VNID’s
(config-vrf)#exit	Exit from vrf configuration mode
(config)#interface irb 1000	Configure IRB interface
(config-irb-if)#ip vrf forwarding ip_vrf5000	Assign above created ip vrf
(config-irb-if)#ip address 100.0.0.186/24	Configure IPV4 address
(config-irb-if)#ipv6 address 1000::186/64	Configure IPV6 address
(config-irb-if)#evpn irb-if-forwarding anycast-gateway-mac	Map above created anycast gateway mac
(config-irb-if)#exit	Exit from irb interface mode
(config)#interface irb 1100	Configure IRB interface
(config-irb-if)#ip vrf forwarding ip_vrf5000	Assign above created ip vrf
(config-irb-if)#ip address 110.0.0.186/24	Configure IPV4 address
(config-irb-if)#ipv6 address 1100::186/64	Configure IPV6 address
(config-irb-if)#evpn irb-if-forwarding anycast-gateway-mac	Map above created anycast gateway mac
(config-irb-if)#exit	Exit from irb interface mode
(config)#interface xe46	Enter interface mode for xe46
(config-if)#switchport	Make it L2 interface
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe47	Enter Interface mode for xe47
(config-if)#ip address 192.168.110.186/24	Configure ipv4 address
(config-if)#ip ospf network point-to-point	Make it an ospf interface and configure network type as P2P
(config-if)#ip ospf cost 100	Configure interface cost as 100
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router ospf	Enter into Router OSPF mode

(config-router)#ospf router-id 172.16.100.186	Configure OSPF Router-id
(config-router)#auto-cost referencebandwidth 100000	Configure auto cost reference bandwidth
(config-router)#bfd all-interfaces	Enable BFD for OSPF

(config-router)#network 172.16.100.186/32 area 0.0.0.0	Advertised loopback in OSPF
(config-router)#network 192.168.110.0/24 area 0.0.0.0	Advertised connected interface into OSPF
(config-router)#exit	Exit from router mode
(config)#router bgp 100	Enter into Router BGP mode
(config-router)#max-paths ibgp 4	Configure max paths for ecmp
(config-router)# neighbor 172.16.100.172 remote-as 100	Specify a neighbor router with peer ip address and remote-as defined
(config-router)# neighbor 172.16.100.172 update-source 172.16.100.186	Update neighbor with loopback interface
(config-router)#address-family l2vpn evpn	Enter into l2vpn evpn address family mode
(config-router-af)#neighbor 172.16.100.172 activate	Activate the peer into address family mode
(config-router-af)#exit-address-family	Exit from l2vpn address family mode
(config-router)#exit	Exit from Router BGP mode and enter into config mode
(config)#nvo vxlan vtep-ip-global 172.16.100.186	Configure Source vtep-ip-global configuration
(config)# nvo vxlan id 10000 ingressreplication inner-vid-disabled	Configure VXLAN Network identifier with/without inner-viddisabled configure and enter into VXLAN tenant mode
(config-nvo)#vxlan host-reachabilityprotocol evpn-bgp mac_vrf10000	Assign vrf for evpn-bgp to carry EVPN route
(config-nvo)# evpn irb1000	Map above created irb interface
(config-nvo)#exit	Exit from VXLAN tenant mode and enter into configuration mode.
(config)#nvo vxlan id 11000 ingressreplication inner-vid-disabled	Configure VXLAN Network identifier with/without inner-viddisabled configure and enter into VXLAN tenant mode
(config-nvo)#vxlan host-reachabilityprotocol evpn-bgp mac_vrf11000	Assign vrf for evpn-bgp to carry EVPN route
(config-nvo)#evpn irb1100	Map above created irb interface
(config-nvo)#exit	Exit from VXLAN tenant mode and enter into configuration mode
(config)# nvo vxlan access-if port-vlan xe46 1000	Enable port-vlan mapping i.e. access port to outer-vlan (SVLAN)
(config-nvo-acc-if)# map vnid 10000	Map VXLAN Identified to access-port for VXLAN
(config-nvo-acc-if)#exit	Exit from VXLAN access-interface mode and enter into configuration mode

(config)# nvo vxlan access-if port-vlan xe46 1100	Enable port-vlan mapping i.e. access port to outer-vlan (SVLAN)
(config-nvo-acc-if)# map vnid 11000	Map VXLAN Identified to access-port for VXLAN
(config-nvo-acc-if)#exit	Exit from VXLAN access-interface mode and enter into configuration mode
(config)#exit	Exit from configuration mode

Leaf2

#configure terminal	Enter Configure mode.
(config)#interface lo	Enter Interface mode for loopback.
(config-if)#ip address 172.16.100.184/32 secondary	Assign secondary IP address.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#nvo vxlan enable	Enable VXLAN
(config)#nvo vxlan irb	Enable IRB
(config)#evpn irb-forwarding anycastgateway-mac 0000.0000.ffff	Configure anycast gateway mac address
(config)#mac vrf mac_vrf10000	Create mac routing/forwarding instance with vrf10000 name and enter into vrf mode
(config-vrf)# rd 10000:2	Assign RD value
(config-vrf)# route-target both 10000:10000	Assign route-target value for export & Import of mac-ip routes
(config-vrf)#exit	Exit from vrf configuration mode
(config)#mac vrf mac_vrf11000	Create mac routing/forwarding instance with vrf1 11000 name and enter into vrf mode
(config-vrf)# rd 11000:2	Assign RD value
(config-vrf)# route-target both 11000:11000	Assign route-target value for export & import of mac ip routes
(config-vrf)#exit	Exit from vrf configuration mode
(config)#ip vrf ip_vrf5000	Create Ip Vrf to bind different vnid ‘s together inorder to communicate between different L2VNID’s
(config-vrf)#rd 5000:2	Assign RD value
(config-vrf)#route-target both 5000:5000	Assign route-target for export and import of routes
(config-vrf)#l3vni 5000	Configure l3vni to communicate between different L2VNID’s
(config-vrf)#exit	Exit from vrf configuration mode
(config)#interface irb 1000	Configure IRB interface
(config-irb-if)#ip vrf forwarding ip_vrf5000	Assign above created ip vrf
(config-irb-if)#ip address 100.0.0.186/24	Configure IPV4 address
(config-irb-if)#ipv6 address 1000::186/64	Configure IPV6 address

(config-irb-if)#evpn irb-if-forwarding anycast-gateway-mac	Map above created anycast gateway mac
(config-irb-if)#exit	Exit from irb interface mode
(config)#interface irb 1100	Configure IRB interface
(config-irb-if)#ip vrf forwarding ip_vrf5000	Assign above created ip vrf
(config-irb-if)#ip address 110.0.0.186/24	Configure IPV4 address
(config-irb-if)#ipv6 address 1100::186/64	Configure IPV6 address
(config-irb-if)#evpn irb-if-forwarding anycast-gateway-mac	Map above created anycast gateway mac
(config-irb-if)#exit	Exit from irb interface mode

(config)#interface xe42	Enter interface mode for xe46
(config-if)#switchport	Make it L2 interface
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe47	Enter Interface mode for xe47
(config-if)#ip address 192.168.110.184/24	Configure ipv4 address
(config-if)#ip ospf network point-to-point	Make it an ospf interface and configure network type as P2P
(config-if)#ip ospf cost 100	Configure interface cost as 100
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router ospf	Enter into Router OSPF mode
(config-router)#ospf router-id 172.16.100.184	Configure OSPF Router-id
(config-router)#auto-cost referencebandwidth 100000	Configure auto cost reference bandwidth
(config-router)#bfd all-interfaces	Enable BFD for OSPF
(config-router)#network 172.16.100.184/32 area 0.0.0.0	Advertised loopback in OSPF
(config-router)#network 192.168.111.0/24 area 0.0.0.0	Advertised connected interface into OSPF
(config-router)#exit	Exit from router mode
(config)#router bgp 100	Enter into Router BGP mode
(config-router)#max-paths ibgp 4	Configure max paths for ecmp
(config-router)# neighbor 172.16.100.172 remote-as 100	Specify a neighbor router with peer ip address and remote-as defined
(config-router)# neighbor 172.16.100.172 update-source 172.16.100.184	Update neighbor with loopback interface
(config-router)#address-family l2vpn evpn	Enter into l2vpn evpn address family mode
(config-router-af)#neighbor 172.16.100.172 activate	Activate the peer into address family mode

(config-router-af)#exit-address-family	Exit from l2vpn address family mode
(config-router)#exit	Exit from Router BGP mode and enter into config mode
(config)#nvo vxlan vtep-ip-global 172.16.100.184	Configure Source vtep-ip-global configuration
(config)# nvo vxlan id 10000 ingressreplication inner-vid-disabled	Configure VXLAN Network identifier with/without inner-viddisabled configure and enter into VXLAN tenant mode
(config-nvo)#vxlan host-reachabilityprotocol evpn-bgp mac_vrf10000	Assign vrf for evpn-bgp to carry EVPN route
(config-nvo)# evpn irb1000	Map above created irb interface
(config-nvo)#exit	Exit from VXLAN tenant mode and enter into configuration mode.
(config)#nvo vxlan id 11000 ingressreplication inner-vid-disabled	Configure VXLAN Network identifier with/without inner-viddisabled configure and enter into VXLAN tenant mode
(config-nvo)#vxlan host-reachabilityprotocol evpn-bgp mac_vrf11000	Assign vrf for evpn-bgp to carry EVPN route
(config-nvo)#evpn irb1100	Map above created irb interface
(config-nvo)#exit	Exit from VXLAN tenant mode and enter into configuration mode
(config)# nvo vxlan access-if port-vlan xe42 1000	Enable port-vlan mapping i.e. access port to outer-vlan (SVLAN)
(config-nvo-acc-if)# map vnid 10000	Map VXLAN Identified to access-port for VXLAN
(config-nvo-acc-if)#exit	Exit from VXLAN access-interface mode and enter into configuration mode
(config)#exit	Exit from configuration mode

BLeaf

#configure terminal	Enter Configure mode.
(config)#interface lo	Enter Interface mode for loopback.
(config-if)#ip address 172.16.100.174/32 secondary	Assign secondary IP address.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#nvo vxlan enable	Enable VXLAN
(config)#nvo vxlan irb	Enable IRB
(config)#evpn irb-forwarding anycastgateway-mac 0000.0000.ffff	Configure anycast gateway mac address
(config)#mac vrf mac_vrf10000	Create mac routing/forwarding instance with vrf10000 name and enter into vrf mode
(config-vrf)# rd 10000:10	Assign RD value
(config-vrf)# route-target both 10000:10000	Assign route-target value for export & Import of mac-ip routes
(config-vrf)#exit	Exit from vrf configuration mode
(config)#mac vrf mac_vrf11000	Create mac routing/forwarding instance with vrf1 11000 name and enter into vrf mode

(config-vrf)# rd 11000:10	Assign RD value
(config-vrf)# route-target both 11000:11000	Assign route-target value for export & import of mac ip routes
(config-vrf)#exit	Exit from vrf configuration mode
(config)#ip vrf ip_vrf5000	Create Ip Vrf to bind different vnid ‘s together inorder to communicate between different L2VNID’s
(config-vrf)#rd 5000:10	Assign RD value
(config-vrf)#route-target both 5000:5000	Assign route-target for export and import of routes
(config-vrf)#l3vni 5000	Configure l3vni to communicate between different L2VNID’s
(config-vrf)#exit	Exit from vrf configuration mode
(config)#interface irb 1000	Configure IRB interface
(config-irb-if)#ip vrf forwarding ip_vrf5000	Assign above created ip vrf
(config-irb-if)#ip address 100.0.0.186/24	Configure IPV4 address
(config-irb-if)#ipv6 address 1000::186/64	Configure IPV6 address
(config-irb-if)#evpn irb-if-forwarding anycast-gateway-mac	Map above created anycast gateway mac
(config-irb-if)#exit	Exit from irb interface mode
(config)#interface irb 1100	Configure IRB interface

(config-irb-if)#ip vrf forwarding ip_vrf5000	Assign above created ip vrf
(config-irb-if)#ip address 110.0.0.186/24	Configure IPV4 address
(config-irb-if)#ipv6 address 1100::186/64	Configure IPV6 address
(config-irb-if)#evpn irb-if-forwarding anycast-gateway-mac	Map above created anycast gateway mac
(config-irb-if)#exit	Exit from irb interface mode
(config)#interface xe42	Enter interface mode for xe46
(config-if)#switchport	Make it L2 interface
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe30/4	Enter Interface mode for xe47
(config-if)#ip address 192.168.125.174/24	Configure ipv4 address
(config-if)#ip ospf network point-to-point	Make it an ospf interface and configure network type as P2P
(config-if)#ip ospf cost 100	Configure interface cost as 100
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router ospf	Enter into Router OSPF mode
(config-router)#ospf router-id 172.16.100.174	Configure OSPF Router-id

(config-router)#auto-cost referencebandwidth 100000	Configure auto cost reference bandwidth
(config-router)#bfd all-interfaces	Enable BFD for OSPF
(config-router)#network 172.16.100.174/32 area 0.0.0.0	Advertised loopback in OSPF
(config-router)#network 192.168.115.0/24 area 0.0.0.0	Advertised connected interface into OSPF
(config-router)#exit	Exit from router mode
(config)#router bgp 100	Enter into Router BGP mode
(config-router)# neighbor 172.16.100.172 remote-as 100	Specify a neighbor router with peer ip address and remote-as defined
(config-router)# neighbor 172.16.100.172 update-source 172.16.100.174	Update neighbor with loopback interface
(config-router)#address-family l2vpn evpn	Enter into l2vpn evpn address family mode
(config-router-af)#neighbor 172.16.100.172 activate	Activate the peer into address family mode
(config-router-af)#exit-address-family	Exit from l2vpn address family mode
(config-router)#exit	Exit from Router BGP mode and enter into config mode
(config)#nvo vxlan vtep-ip-global 172.16.100.184	Configure Source vtep-ip-global configuration
(config)# nvo vxlan id 10000 ingressreplication inner-vid-disabled	Configure VXLAN Network identifier with/without inner-viddisabled configure and enter into VXLAN tenant mode
(config-nvo)#vxlan host-reachabilityprotocol evpn-bgp mac_vrf10000	Assign vrf for evpn-bgp to carry EVPN route
(config-nvo)# evpn irb1000	Map above created irb interface
(config-nvo)#exit	Exit from VXLAN tenant mode and enter into configuration mode.
(config)#nvo vxlan id 11000 ingressreplication inner-vid-disabled	Configure VXLAN Network identifier with/without inner-viddisabled configure and enter into VXLAN tenant mode
(config-nvo)#vxlan host-reachabilityprotocol evpn-bgp mac_vrf11000	Assign vrf for evpn-bgp to carry EVPN route
(config-nvo)#evpn irb1100	Map above created irb interface
(config-nvo)#exit	Exit from VXLAN tenant mode and enter into configuration mode
(config)# nvo vxlan access-if port-vlan xe42 1000	Enable port-vlan mapping i.e. access port to outer-vlan (SVLAN)
(config-nvo-acc-if)# map vnid 10000	Map VXLAN Identified to access-port for VXLAN
(config-nvo-acc-if)#exit	Exit from VXLAN access-interface mode and enter into configuration mode
(config)#exit	Exit from configuration mode

Spine Node

#configure terminal	Enter Configure mode.
(config)#interface lo	Enter Interface mode for loopback.

(config-if)#ip address 172.16.100.172/32 secondary	Assign secondary IP address.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe7	Enter Interface mode for xe7
(config-if)#ip address 192.168.110.172/24	Assign IP address
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe51/1	Enter Interface mode for xe51/1
(config-if)#ip address 192.168.111.172/24	Assign IP address
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe43	Enter Interface mode for xe43
(config-if)#ip address 192.168.115.172/24	Assign IP address
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router ospf	Enter into Router OSPF mode
(config-router)#ospf router-id 172.16.100.174	Configure OSPF Router-id
(config-router)#auto-cost referencebandwidth 100000	Configure auto cost reference bandwidth
(config-router)#bfd all-interfaces	Enable BFD for OSPF
(config-router)#network 172.16.100.172/32 area 0.0.0.0	Advertised loopback in OSPF
(config-router)#network 192.168.115.0/24 area 0.0.0.0	Advertised connected interface into OSPF
(config-router)#network 192.168.110.0/24 area 0.0.0.0	Advertised connected interface into OSPF
(config-router)#network 192.168.111.0/24 area 0.0.0.0	Advertised connected interface into OSPF
(config-router)#exit	Exit from router mode
(config)#router bgp 100	Enter into Router BGP mode
(config-router)#neighbor 172.168.100.174 remote-as 100	Specify a neighbor router with peer ip address and remote-as defined
(config-router)#neighbor 172.168.100.174 update-source 172.16.100.172	Update neighbor with loopback interface
(config-router)#neighbor 172.168.100.174 route-reflector-client	Configure neighbor as Route Reflector Client
(config-router)#neighbor 172.168.100.184 remote-as 100	Specify a neighbor router with peer ip address and remote-as defined
(config-router)#neighbor 172.168.100.184 update-source 172.16.100.172	Update neighbor with loopback interface

(config-router)#neighbor 172.168.100.184 route-reflector-client	Configure neighbor as Route Reflector Client
(config-router)#neighbor 172.168.100.186 remote-as 100	Specify a neighbor router with peer ip address and remote-as defined
(config-router)#neighbor 172.168.100.186 update-source 172.16.100.172	Update neighbor with loopback interface
(config-router)#neighbor 172.168.100.186 route-reflector-client	Configure neighbor as Route Reflector Client
(config-router)#address-family l2vpn evpn	Enter into l2vpn address family mode
(config-router-af)#neighbor 172.16.100.174 activate	Activate the peer into address family mode
(config-router-af)#neighbor 172.16.100.174 route-reflector-client	Activate RR in l2vpn family
(config-router-af)#neighbor 172.16.100.184 activate	Activate the peer into address family mode
(config-router-af)#neighbor 172.16.100.184 route-reflector-client	Activate RR in l2vpn family
(config-router-af)#neighbor 172.16.100.186 activate	Activate the peer into address family mode
(config-router-af)#neighbor 172.16.100.186 route-reflector-client	Activate RR in l2vpn family
(config-router-af)#exit-address-family	Exit from l2vpn address family mode
(config-router)#exit	Exit from Router BGP mode and enter into config mode
(config)#exit	Exit from configuration mode

TOR1

#configure terminal	Enter Configure mode.
(config)#bridge 1 protocol ieee vlanbridge	Configure ieee vlan bridge
(config)#vlan 1000-1100 bridge 1 state enable	Configure vlans from 2-4042 and associate with bridge 1
(config)#interface xe50	Enter Interface mode for xe50
(config-if)#switchport	Make xe50 as L2 port by configuring switchport
(config-if)#bridge-group 1	Associate xe50 to bridge 1
(config-if)#switchport mode trunk	Configure xe50 as trunk port
(config-if)#switchport trunk allowed vlan all	Allow all configured vlans on xe50
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface vlan1.1000	Enter Interface mode for vlan 1.1000
(config-if)# ip address 100.0.0.1/24	Configure ip address
(config-if)# ipv6 address 1000::1/64	Configure ipv6 address
(config)#exit	Exit from configuration mode

TOR2

#configure terminal	Enter Configure mode.
(config)#bridge 1 protocol ieee vlanbridge	Configure ieee vlan bridge
(config)#vlan 1000-1100 bridge 1 state enable	Configure vlans from 2-4042 and associate with bridge 1
(config)#interface xe50	Enter Interface mode for xe50
(config-if)#switchport	Make xe50 as L2 port by configuring switchport
(config-if)#bridge-group 1	Associate xe50 to bridge 1
(config-if)#switchport mode trunk	Configure xe50 as trunk port
(config-if)#switchport trunk allowed vlan all	Allow all configured vlans on xe50
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface vlan1.1000	Enter Interface mode for vlan 1.1000
(config-if)# ip address 100.0.0.2/24	Configure ip address
(config-if)# ipv6 address 1000::2/64	Configure ipv6 address
(config)#exit	Exit from configuration mode

Validations

TOR2

```
#ping 100.0.0.1
    Press CTRL+C to exit
    PING 100.0.0.1 (100.0.0.1) 56(84) bytes of data.
    64 bytes from 100.0.0.1: icmp_seq=1 ttl=63 time=0.259 ms
    64 bytes from 100.0.0.1: icmp_seq=2 ttl=63 time=0.231 ms
    64 bytes from 100.0.0.1: icmp_seq=3 ttl=63 time=0.251 ms
    64 bytes from 100.0.0.1: icmp_seq=4 ttl=63 time=0.231 ms

    --- 100.0.0.1 ping statistics ---
    4 packets transmitted, 4 received, 0% packet loss, time 2999ms
    rtt min/avg/max/mdev = 0.231/0.243/0.259/0.012 ms

#ping ipv6 1000::1
    Press CTRL+C to exit
    PING 1000::1(1000::1) 56 data bytes
    64 bytes from 1000::1: icmp_seq=1 ttl=63 time=0.237 ms
    64 bytes from 1000::1: icmp_seq=2 ttl=63 time=0.261 ms
    64 bytes from 1000::1: icmp_seq=3 ttl=63 time=0.268 ms
    64 bytes from 1000::1: icmp_seq=4 ttl=63 time=0.279 ms
    --- 1000::1 ping statistics ---
    4 packets transmitted, 4 received, 0% packet loss, time 3000ms
    rtt min/avg/max/mdev = 0.237/0.261/0.279/0.019 ms
```

Leaf1

```
#show bgp l2vpn evpn mac-ip
```

```
RD[5000:1] VRF[ip_vrf5000]:
ESI                               Eth-Tag     Mac-Address    IP-Address
VNID     L3VNID   Nexthop
0                                 10000       6400:6a8e:48a1 100.0.0.1
10000      5000     172.16.100.186
0                                 10000       6400:6a8e:48a1 1000::1
10000      5000     172.16.100.186
0                                 11000       6400:6a8e:48a1 110.0.0.176
11000      5000     172.16.100.186
0                                 11000       6400:6a8e:48a1 1100::176
11000     5000      172.16.100.186

RD[5000:2]
ESI                               Eth-Tag     Mac-Address    IP-Address
VNID     L3VNID   Nexthop
0                                 11000       6400:6a2d:eaa1 110.0.0.2
11000      5000     172.16.100.184
0                                 11000       6400:6a2d:eaa1 1100::2
11000     5000      172.16.100.184

RD[10000:1] VRF[mac_vrf10000]:
ESI                               Eth-Tag     Mac-Address    IP-Address
VNID     L3VNID   Nexthop
0                                 10000       6400:6a8e:48a1 --
10000      0        172.16.100.186
0                                 10000       6400:6a8e:48a1 100.0.0.1
10000      5000     172.16.100.186
0                                 10000       6400:6a8e:48a1 1000::1
10000     5000      172.16.100.186

RD[10000:3]
ESI                               Eth-Tag     Mac-Address    IP-Address
VNID     L3VNID   Nexthop
0                                 10000       0000:1000:1201 --
10000     0         172.16.100.182

RD[11000:1] VRF[mac_vrf11000]:
ESI                               Eth-Tag     Mac-Address    IP-Address
VNID     L3VNID   Nexthop
0                                 11000       6400:6a8e:48a1 --
11000      0        172.16.100.186
0                                 11000       6400:6a8e:48a1 110.0.0.176
11000      5000     172.16.100.186
0                                 11000       6400:6a8e:48a1 1100::176
11000     5000      172.16.100.186

RD[11000:2]
ESI                               Eth-Tag     Mac-Address    IP-Address
VNID     L3VNID   Nexthop
0                                 11000       6400:6a2d:eaa1 --
11000      0        172.16.100.184
```

```
    0                                11000       6400:6a2d:eaa1 110.0.0.2
    11000      5000      172.16.100.184
    0                                11000       6400:6a2d:eaa1 1100::2
    11000      5000      172.16.100.184

    RD[11000:3]
    ESI                              Eth-Tag     Mac-Address    IP-Address
    VNID     L3VNID   Nexthop
    0 11000        0000:1100:1201 --                                        11000     0
      172.16.100.182

#show bgp l2vpn evpn
    BGP table version is 45, local router ID is 172.16.100.186
    Status codes: s suppressed, d damped, h history, * valid, > best, i -
                  internal, l - labeled, S Stale
    Origin codes: i - IGP, e - EGP, ? - incomplete

    [EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
    1 - Ethernet Auto-discovery Route
    2 - MAC/IP Route
    3 - Inclusive Multicast Route
    4 - Ethernet Segment Route
    5 - Prefix Route

        Network          Next Hop            Metric    LocPrf       Weight
    Path  Peer          Encap

    RD[5000:1] VRF[ip_vrf5000]:
    *>   [2]:[0]:[10000]:[48,6400.6a8e.48a1]:[32,100.0.0.1]:[10000]:[5000]
                         172.16.100.186                          0 100   32768 i     --
    --------      VXLAN
    *>   [2]:[0]:[10000]:[48,6400.6a8e.48a1]:[128,1000::1]:[10000]:[5000]
                         172.16.100.186                          0 100   32768 i     --
    --------      VXLAN
* i  [2]:[0]:[11000]:[48,6400.6a2d.eaa1]:[32,110.0.0.2]:[11000]:[5000]
                          172.16.100.184       0         100           0        i
    172.16.100.172  VXLAN
* i  [2]:[0]:[11000]:[48,6400.6a2d.eaa1]:[128,1100::2]:[11000]:[5000]
                          172.16.100.184       0         100           0        i
    172.16.100.172  VXLAN
    *>   [2]:[0]:[11000]:[48,6400.6a8e.48a1]:[32,110.0.0.176]:[11000]:[5000]
                         172.16.100.186                          0 100   32768 i     --
    --------      VXLAN
    *>   [2]:[0]:[11000]:[48,6400.6a8e.48a1]:[128,1100::176]:[11000]:[5000]
                         172.16.100.186                          0 100   32768 i     --
    --------      VXLAN
* i  [3]:[5000]:[32,172.16.100.174]
                          172.16.100.174       0         100           0        i
    172.16.100.172  VXLAN
* i  [3]:[5000]:[32,172.16.100.184]
```

```
                          172.16.100.184       0         100           0       i
    172.16.100.172  VXLAN
    *>   [3]:[5000]:[32,172.16.100.186]
                          172.16.100.186      0         100          32768    i  --
    --------       VXLAN
RD[5000:2]
*>i  [2]:[0]:[11000]:[48,6400.6a2d.eaa1]:[32,110.0.0.2]:[11000]:[5000]
                        172.16.100.184       0         100           0       i
172.16.100.172  VXLAN
* i                      172.16.100.184       0         100           0       i
  172.16.100.173   VXLAN
*>i   [2]:[0]:[11000]:[48,6400.6a2d.eaa1]:[128,1100::2]:[11000]:[5000]
                        172.16.100.184       0         100           0       i
172.16.100.172  VXLAN
* i                      172.16.100.184       0         100           0       i
  172.16.100.173   VXLAN
*>i  [3]:[5000]:[32,172.16.100.184]
                        172.16.100.184       0         100           0       i
172.16.100.172  VXLAN
* i                      172.16.100.184       0         100           0       i
172.16.100.173  VXLAN

RD[5000:10]
*>i  [3]:[5000]:[32,172.16.100.174]
                        172.16.100.174       0         100           0       i
172.16.100.172  VXLAN
* i                      172.16.100.174       0         100           0       i
  172.16.100.173   VXLAN

RD[10000:1] VRF[mac_vrf10000]:
* i  [2]:[0]:[10000]:[48,0000.1000.1201]:[0]:[10000]
                        172.16.100.182       0         100           0       i
172.16.100.172  VXLAN
*>   [2]:[0]:[10000]:[48,6400.6a8e.48a1]:[0]:[10000]
                        172.16.100.186      0         100          32768    i  ------
----       VXLAN
*>   [2]:[0]:[10000]:[48,6400.6a8e.48a1]:[32,100.0.0.1]:[10000]:[5000]
                       172.16.100.186      0         100          32768    i  ------
----       VXLAN
*>   [2]:[0]:[10000]:[48,6400.6a8e.48a1]:[128,1000::1]:[10000]:[5000]
                       172.16.100.186      0         100          32768    i  ------
----       VXLAN
* i  [3]:[10000]:[32,172.16.100.174]
                        172.16.100.174       0         100           0       i
172.16.100.172   VXLAN
* i   [3]:[10000]:[32,172.16.100.182]
                        172.16.100.182       0         100           0       i
172.16.100.172   VXLAN
* i   [3]:[10000]:[32,172.16.100.184]
```

```
                        172.16.100.184       0         100            0       i
172.16.100.172  VXLAN
*>   [3]:[10000]:[32,172.16.100.186]
                        172.16.100.186      0         100           32768   i
----------      VXLAN

RD[10000:2]
*>i  [3]:[10000]:[32,172.16.100.184]
                        172.16.100.184       0         100            0       i
172.16.100.172  VXLAN
* i                     172.16.100.184       0         100            0       i
172.16.100.173  VXLAN

RD[10000:3]
*>i  [2]:[0]:[10000]:[48,0000.1000.1201]:[0]:[10000]
                        172.16.100.182       0         100            0       i
172.16.100.172  VXLAN
* i                     172.16.100.182       0         100            0       i
  172.16.100.173   VXLAN
*>i  [3]:[10000]:[32,172.16.100.182]
                        172.16.100.182       0         100            0       i
172.16.100.172  VXLAN
* i                     172.16.100.182       0         100            0       i
172.16.100.173  VXLAN

RD[10000:10]
*>i  [3]:[10000]:[32,172.16.100.174]
                        172.16.100.174       0         100            0       i
172.16.100.172  VXLAN
* i                     172.16.100.174       0         100            0       i
  172.16.100.173   VXLAN

RD[11000:1] VRF[mac_vrf11000]:
* i  [2]:[0]:[11000]:[48,0000.1100.1201]:[0]:[11000]
                        172.16.100.182       0         100            0       i
172.16.100.172  VXLAN
* i  [2]:[0]:[11000]:[48,6400.6a2d.eaa1]:[0]:[11000]
                        172.16.100.184       0         100            0       i
172.16.100.172  VXLAN
* i  [2]:[0]:[11000]:[48,6400.6a2d.eaa1]:[32,110.0.0.2]:[11000]:[5000]
                        172.16.100.184       0         100            0       i
172.16.100.172  VXLAN
* i   [2]:[0]:[11000]:[48,6400.6a2d.eaa1]:[128,1100::2]:[11000]:[5000]
                        172.16.100.184       0         100            0       i
172.16.100.172  VXLAN
*>   [2]:[0]:[11000]:[48,6400.6a8e.48a1]:[0]:[11000]
                        172.16.100.186      0         100           32768   i  ------
----      VXLAN
*>   [2]:[0]:[11000]:[48,6400.6a8e.48a1]:[32,110.0.0.176]:[11000]:[5000]
                       172.16.100.186      0         100           32768    i  ------
----      VXLAN
```

```
*>   [2]:[0]:[11000]:[48,6400.6a8e.48a1]:[128,1100::176]:[11000]:[5000]
                       172.16.100.186      0          100            32768     i  ------
----       VXLAN
    * i  [3]:[11000]:[32,172.16.100.174]
                       172.16.100.174       0          100            0        i
172.16.100.172  VXLAN
    * i  [3]:[11000]:[32,172.16.100.182]
                       172.16.100.182       0          100            0        i
172.16.100.172  VXLAN
    * i  [3]:[11000]:[32,172.16.100.184]
                       172.16.100.184       0          100            0        i
172.16.100.172  VXLAN
*>   [3]:[11000]:[32,172.16.100.186]
                       172.16.100.186      0          100            32768    i
----------      VXLAN

RD[11000:2]
*>i  [2]:[0]:[11000]:[48,6400.6a2d.eaa1]:[0]:[11000]
                       172.16.100.184       0          100            0        i
172.16.100.172  VXLAN
    * i                    172.16.100.184       0          100            0        i
      172.16.100.173  VXLAN
*>i  [2]:[0]:[11000]:[48,6400.6a2d.eaa1]:[32,110.0.0.2]:[11000]:[5000]
172.16.100.184       0          100            0        i
    172.16.100.172  VXLAN
    * i                    172.16.100.184       0          100            0        i
      172.16.100.173  VXLAN
    *>i   [2]:[0]:[11000]:[48,6400.6a2d.eaa1]:[128,1100::2]:[11000]:[5000]
                           172.16.100.184       0          100            0        i
    172.16.100.172  VXLAN
    * i                    172.16.100.184       0          100            0        i
      172.16.100.173  VXLAN
    *>i  [3]:[11000]:[32,172.16.100.184]
                           172.16.100.184       0          100            0        i
    172.16.100.172  VXLAN
    * i                    172.16.100.184       0          100            0        i
    172.16.100.173  VXLAN

    RD[11000:3]
    *>i  [2]:[0]:[11000]:[48,0000.1100.1201]:[0]:[11000]
                           172.16.100.182       0          100            0        i
    172.16.100.172  VXLAN
    * i                    172.16.100.182       0          100            0        i
      172.16.100.173  VXLAN
    *>i  [3]:[11000]:[32,172.16.100.182]
                           172.16.100.182       0          100            0        i
    172.16.100.172  VXLAN
    * i                    172.16.100.182       0          100            0        i
    172.16.100.173  VXLAN
```

```
    RD[11000:10]
    *>i   [3]:[11000]:[32,172.16.100.174]
                          172.16.100.174       0         100           0       i
    172.16.100.172   VXLAN
    * i                   172.16.100.174       0         100           0       i
    172.16.100.173   VXLAN

    RD[12000:3]
    *>i   [3]:[12000]:[32,172.16.100.182]
                          172.16.100.182       0         100           0       i
    172.16.100.172   VXLAN
    * i                   172.16.100.182       0         100           0       i
    172.16.100.173   VXLAN

    RD[20000:3]
    *>i   [3]:[20000]:[32,172.16.100.182]
                          172.16.100.182       0         100           0       i
    172.16.100.172   VXLAN
    * i                   172.16.100.182       0         100           0       i
      172.16.100.173   VXLAN

    Total number of prefixes 45

#show nvo vxlan nd-cache
    VXLAN ND-CACHE Information
    ============================
    VNID     Ip-Addr                                 Mac-Addr       Type          Age-
    Out    Retries-Left

    ____________________________________________________________________________________
    ________________________
    10000    1000::186                               0000.0000.ffff
    ----
    10000    1000::1                                 6400.6a8e.48a1 Dynamic Local
    ----
    11000    1100::176                               6400.6a8e.48a1 Dynamic Local
    ----
    11000    1100::2                                 6400.6a2d.eaa1 Remote Dynamic
    ----
    11000    1100::186                               0000.0000.ffff                --
    --
    Total number of entries are 5

#show nvo vxlan tunnel
    VXLAN Network tunnel Entries
     Source           Destination      Status          Up/Down        Update
    ================================================================================
    ======
     172.16.100.186   172.16.100.184  Installed      00:56:16    00:56:16
     172.16.100.186   172.16.100.174  Installed      01:44:23    01:44:23
     172.16.100.186   172.16.100.182  Installed      02:33:54    02:33:54
    Total number of entries are 3
```

```
#show nvo vxlan mac-table
================================================================================
================================================================================
                          VXLAN MAC Entries
================================================================================
================================================================================
VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status              AccessPortDesc
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
10000      ----       ----    ----        0000.1000.1201 172.16.100.182
Remote Dynamic        -------             -------
10000      xe46       1000    ----        6400.6a8e.48a1 172.16.100.186
Dynamic Local         -------             -------
11000      ----       ----    ----        0000.1100.1201 172.16.100.182
Remote Dynamic        -------             -------
11000      xe46       1100    ----        6400.6a8e.48a1 172.16.100.186
Dynamic Local         -------             -------
11000      ----       ----    ----        6400.6a2d.eaa1 172.16.100.184
Remote Dynamic        -------             -------

Total number of entries are : 5
```

Centralized Gateway

Topology

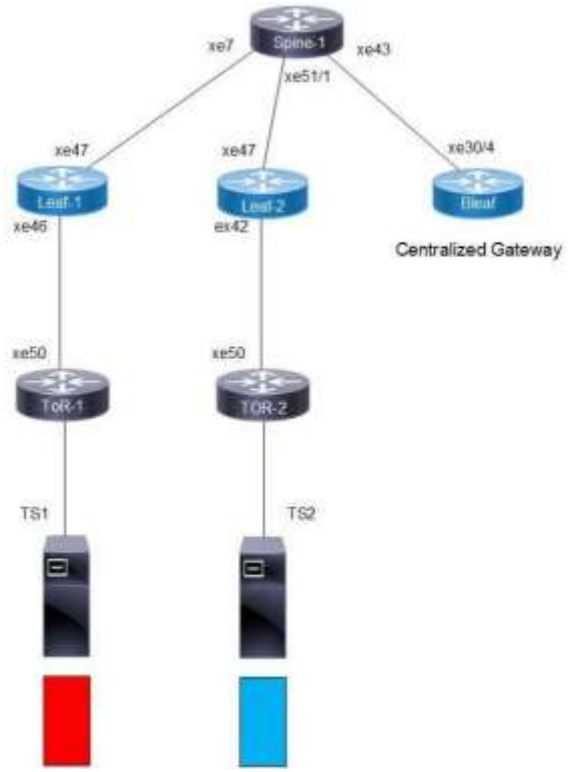


Figure 4-241: VxLAN_EVPN_IRB_centralized

Configuration

Leaf1

`#configure terminal`	Enter Configure mode.
`(config)#interface lo`	Enter Interface mode for loopback.
`(config-if)#ip address 172.16.100.186/32 secondary`	Assign secondary IP address.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#nvo vxlan enable`	Enable VXLAN
`(config)#mac vrf mac_vrf10000`	Create mac routing/forwarding instance with vrf10000 name and enter into vrf mode
`(config-vrf)#description MAC VRF RED`	Add a description to the VRF
`(config-vrf)#rd 10000:1`	Assign RD value
`(config-vrf)#route-target both 10000:10000`	Assign route-target value for export & Import of mac-ip routes
`(config-vrf)#exit`	Exit from vrf configuration mode
`(config)#mac vrf mac_vrf11000`	Create mac routing/forwarding instance with vrf1 11000 name and enter into vrf mode

(config-vrf)#rd 11000:1	Assign RD value
(config-vrf)#route-target both 11000:11000	Assign route-target value for export & import of mac ip routes
(config-vrf)#exit	Exit from vrf configuration mode
(config)#interface xe46	Enter interface mode for xe46
(config-if)#switchport	Make it L2 interface
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe47	Enter Interface mode for xe47
(config-if)#ip address 192.168.110.186/24	Configure ipv4 address
(config-if)#ip ospf network point-to-point	Make it an ospf interface and configure network type as P2P
(config-if)#ip ospf cost 100	Configure interface cost as 100
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router ospf	Enter into Router OSPF mode
(config-router)#ospf router-id 172.16.100.186	Configure OSPF Router-id
(config-router)#auto-cost referencebandwidth 100000	Configure auto cost reference bandwidth
(config-router)#bfd all-interfaces	Enable BFD for OSPF
(config-router)#network 172.16.100.186/32 area 0.0.0.0	Advertised loopback in OSPF
(config-router)#network 192.168.110.0/24 area 0.0.0.0	Advertised connected interface into OSPF
(config-router)#exit	Exit from router mode
(config)#router bgp 100	Enter into Router BGP mode
(config-router)#max-paths ibgp 4	Configure max paths for ecmp
(config-router)# neighbor 172.16.100.172 remote-as 100	Specify a neighbor router with peer ip address and remote-as defined
(config-router)# neighbor 172.16.100.172 update-source 172.16.100.186	Update neighbor with loopback interface
(config-router)#address-family l2vpn evpn	Enter into l2vpn evpn address family mode
(config-router-af)#neighbor 172.16.100.172 activate	Activate the peer into address family mode
(config-router-af)#exit-address-family	Exit from l2vpn address family mode
(config-router)#exit	Exit from Router BGP mode and enter into config mode
(config)#nvo vxlan vtep-ip-global 172.16.100.186	Configure Source vtep-ip-global configuration
(config)# nvo vxlan id 10000 ingressreplication inner-vid-disabled	Configure VXLAN Network identifier with/without inner-viddisabled configure and enter into VXLAN tenant mode
(config-nvo)#vxlan host-reachabilityprotocol evpn-bgp mac_vrf10000	Assign vrf for evpn-bgp to carry EVPN route

(config-nvo)# evpn irb1000	Map above created irb interface
(config-nvo)#exit	Exit from VXLAN tenant mode and enter into configuration mode.
(config)#nvo vxlan id 11000 ingressreplication inner-vid-disabled	Configure VXLAN Network identifier with/without inner-viddisabled configure and enter into VXLAN tenant mode
(config-nvo)#vxlan host-reachabilityprotocol evpn-bgp mac_vrf11000	Assign vrf for evpn-bgp to carry EVPN route
(config-nvo)#evpn irb1100	Map above created irb interface
(config-nvo)#exit	Exit from VXLAN tenant mode and enter into configuration mode
(config)# nvo vxlan access-if port-vlan xe46 1000	Enable port-vlan mapping i.e. access port to outer-vlan (SVLAN)
(config-nvo-acc-if)# map vnid 10000	Map VXLAN Identified to access-port for VXLAN
(config-nvo-acc-if)#exit	Exit from VXLAN access-interface mode and enter into configuration mode
(config)#exit	Exit from configuration mode

Leaf2

#configure terminal	Enter Configure mode.
(config)#interface lo	Enter Interface mode for loopback.
(config-if)#ip address 172.16.100.184/32 secondary	Assign secondary IP address.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#nvo vxlan enable	Enable VXLAN
(config)#mac vrf mac_vrf10000	Create mac routing/forwarding instance with vrf10000 name and enter into vrf mode
(config-vrf)#description MAC VRF BLUE	Add a description to the VRF
(config-vrf)#rd 10000:2	Assign RD value
(config-vrf)#route-target both 11000:11000	Assign route-target value for export & Import of mac-ip routes
(config-vrf)#exit	Exit from vrf configuration mode
(config)#interface xe42	Enter interface mode for xe46
(config-if)#switchport	Make it L2 interface
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe47	Enter Interface mode for xe47
(config-if)#ip address 192.168.110.184/24	Configure ipv4 address
(config-if)#ip ospf network point-to-point	Make it an ospf interface and configure network type as P2P
(config-if)#ip ospf cost 100	Configure interface cost as 100
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router ospf	Enter into Router OSPF mode

(config-router)#ospf router-id 172.16.100.184	Configure OSPF Router-id
(config-router)#auto-cost referencebandwidth 100000	Configure auto cost reference bandwidth
(config-router)#bfd all-interfaces	Enable BFD for OSPF
(config-router)#network 172.16.100.184/32 area 0.0.0.0	Advertised loopback in OSPF
(config-router)#network 192.168.111.0/24 area 0.0.0.0	Advertised connected interface into OSPF
(config-router)#exit	Exit from router mode
(config)#router bgp 100	Enter into Router BGP mode
(config-router)#max-paths ibgp 4	Configure max paths for ecmp
(config-router)# neighbor 172.16.100.172 remote-as 100	Specify a neighbor router with peer ip address and remote-as defined
(config-router)# neighbor 172.16.100.172 update-source 172.16.100.184	Update neighbor with loopback interface
(config-router)#address-family l2vpn evpn	Enter into l2vpn evpn address family mode
(config-router-af)#neighbor 172.16.100.172 activate	Activate the peer into address family mode
(config-router-af)#exit-address-family	Exit from l2vpn address family mode
(config-router)#exit	Exit from Router BGP mode and enter into config mode
(config)#nvo vxlan vtep-ip-global 172.16.100.184	Configure Source vtep-ip-global configuration
(config)# nvo vxlan id 11000 ingressreplication inner-vid-disabled	Configure VXLAN Network identifier with/without inner-viddisabled configure and enter into VXLAN tenant mode
(config-nvo)#vxlan host-reachabilityprotocol evpn-bgp mac_vrf11000	Assign vrf for evpn-bgp to carry EVPN route
(config-nvo)#exit	Exit from VXLAN tenant mode and enter into configuration mode.
(config)# nvo vxlan access-if port-vlan xe42 1100	Enable port-vlan mapping i.e. access port to outer-vlan (SVLAN)
(config-nvo-acc-if)# map vnid 11000	Map VXLAN Identified to access-port for VXLAN
(config-nvo-acc-if)#exit	Exit from VXLAN access-interface mode and enter into configuration mode
(config)#exit	Exit from configuration mode

Bleaf

#configure terminal	Enter Configure mode.
(config)#interface lo	Enter Interface mode for loopback.
(config-if)#ip address 172.16.100.174/32 secondary	Assign secondary IP address.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#nvo vxlan enable	Enable VXLAN

(config)#mac vrf mac_vrf10000	Create mac routing/forwarding instance with vrf10000 name and enter into vrf mode
(config-vrf)#rd 10000:10	Assign RD value
(config-vrf)#route-target both 10000:10000	Assign route-target value for export & Import of mac-ip routes
(config-vrf)#exit	Exit from vrf configuration mode

(config)#mac vrf mac_vrf11000	Create mac routing/forwarding instance with vrf1 11000 name and enter into vrf mode
(config-vrf)#rd 11000:10	Assign RD value
(config-vrf)#route-target both 11000:11000	Assign route-target value for export & import of mac ip routes
(config-vrf)#exit	Exit from vrf configuration mode
(config)#ip vrf ip_vrf5000	Create Ip Vrf to bind different vnid 's together inorder to communicate between different L2VNID's
(config-vrf)#rd 5000:10	Assign RD value
(config-vrf)#route-target both 5000:5000	Assign route-target for export and import of routes
(config-vrf)#l3vni 5000	Configure l3vni to communicate between different L2VNID's
(config-vrf)#exit	Exit from vrf configuration mode
(config)#interface irb 1000	Configure IRB interface
(config-irb-if)#ip vrf forwarding ip_vrf5000	Assign above created ip vrf
(config-irb-if)#ip address 100.0.0.186/24	Configure IPV4 address
(config-irb-if)#ipv6 address 1000::186/64	Configure IPV6 address
(config-irb-if)#exit	Exit from irb interface mode
(config)#interface irb 1100	Configure IRB interface
(config-irb-if)#ip vrf forwarding ip_vrf5000	Assign above created ip vrf
(config-irb-if)#ip address 110.0.0.186/24	Configure IPV4 address
(config-irb-if)#ipv6 address 1100::186/64	Configure IPV6 address
(config-irb-if)#exit	Exit from irb interface mode
(config)#interface xe42	Enter interface mode for xe46
(config-if)#switchport	Make it L2 interface
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe30/4	Enter Interface mode for xe47
(config-if)#ip address 192.168.125.174/24	Configure ipv4 address
(config-if)#ip ospf network point-to-point	Make it an ospf interface and configure network type as P2P
(config-if)#ip ospf cost 100	Configure interface cost as 100
(config-if)#exit	Exit Interface mode and return to Configure mode.

(config)#router ospf	Enter into Router OSPF mode
(config-router)#ospf router-id 172.16.100.174	Configure OSPF Router-id
(config-router)#auto-cost referencebandwidth 100000	Configure auto cost reference bandwidth
(config-router)#bfd all-interfaces	Enable BFD for OSPF
(config-router)#network 172.16.100.174/32 area 0.0.0.0	Advertised loopback in OSPF
(config-router)#network 192.168.115.0/24 area 0.0.0.0	Advertised connected interface into OSPF
(config-router)#exit	Exit from router mode
(config)#router bgp 100	Enter into Router BGP mode
(config-router)# neighbor 172.16.100.172 remote-as 100	Specify a neighbor router with peer ip address and remote-as defined
(config-router)# neighbor 172.16.100.172 update-source 172.16.100.174	Update neighbor with loopback interface
(config-router)#address-family l2vpn evpn	Enter into l2vpn evpn address family mode
(config-router-af)#neighbor 172.16.100.172 activate	Activate the peer into address family mode
(config-router-af)#exit-address-family	Exit from l2vpn address family mode
(config-router)#exit	Exit from Router BGP mode and enter into config mode
(config)#nvo vxlan vtep-ip-global 172.16.100.184	Configure Source vtep-ip-global configuration
(config)# nvo vxlan id 10000 ingressreplication inner-vid-disabled	Configure VXLAN Network identifier with/without inner-viddisabled configure and enter into VXLAN tenant mode
(config-nvo)#vxlan host-reachabilityprotocol evpn-bgp mac_vrf10000	Assign vrf for evpn-bgp to carry EVPN route
(config-nvo)# evpn irb1000	Map above created irb interface
(config-nvo)#exit	Exit from VXLAN tenant mode and enter into configuration mode.
(config)#nvo vxlan id 11000 ingressreplication inner-vid-disabled	Configure VXLAN Network identifier with/without inner-viddisabled configure and enter into VXLAN tenant mode
(config-nvo)#vxlan host-reachabilityprotocol evpn-bgp mac_vrf11000	Assign vrf for evpn-bgp to carry EVPN route
(config-nvo)#evpn irb1100	Map above created irb interface
(config-nvo)#exit	Exit from VXLAN tenant mode and enter into configuration mode
(config)# nvo vxlan access-if port-vlan xe42 1100	Enable port-vlan mapping i.e. access port to outer-vlan (SVLAN)
(config-nvo-acc-if)# map vnid 11000	Map VXLAN Identified to access-port for VXLAN
(config-nvo-acc-if)#exit	Exit from VXLAN access-interface mode and enter into configuration mode
(config)#exit	Exit from configuration mode

Spine Node

#configure terminal	Enter Configure mode.
(config)#interface lo	Enter Interface mode for loopback.
(config-if)#ip address 172.16.100.172/32 secondary	Assign secondary IP address.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe7	Enter Interface mode for xe7
(config-if)#ip address 192.168.110.172/24	Assign IP address
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe51/1	Enter Interface mode for xe51/1
(config-if)#ip address 192.168.111.172/24	Assign IP address
(config-if)#exit	Exit Interface mode and return to Configure mode.

(config)#interface xe43	Enter Interface mode for xe43
(config-if)#ip address 192.168.115.172/24	Assign IP address
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router ospf	Enter into Router OSPF mode
(config-router)#ospf router-id 172.16.100.174	Configure OSPF Router-id
(config-router)#auto-cost referencebandwidth 100000	Configure auto cost reference bandwidth
(config-router)#bfd all-interfaces	Enable BFD for OSPF
(config-router)#network 172.16.100.172/32 area 0.0.0.0	Advertised loopback in OSPF
(config-router)#network 192.168.115.0/24 area 0.0.0.0	Advertised connected interface into OSPF
(config-router)#network 192.168.110.0/24 area 0.0.0.0	Advertised connected interface into OSPF
(config-router)#network 192.168.111.0/24 area 0.0.0.0	Advertised connected interface into OSPF
(config-router)#exit	Exit from router mode
(config)#router bgp 100	Enter into Router BGP mode
(config-router)#neighbor 172.168.100.174 remote-as 100	Specify a neighbor router with peer ip address and remote-as defined
(config-router)#neighbor 172.168.100.174 update-source 172.16.100.172	Update neighbor with loopback interface
(config-router)#neighbor 172.168.100.174 route-reflector-client	Configure neighbor as Route Reflector Client

(config-router)#neighbor 172.168.100.184 remote-as 100	Specify a neighbor router with peer ip address and remote-as defined
(config-router)#neighbor 172.168.100.184 update-source 172.16.100.172	Update neighbor with loopback interface
(config-router)#neighbor 172.168.100.184 route-reflector-client	Configure neighbor as Route Reflector Client
(config-router)#neighbor 172.168.100.186 remote-as 100	Specify a neighbor router with peer ip address and remote-as defined
(config-router)#neighbor 172.168.100.186 update-source 172.16.100.172	Update neighbor with loopback interface
(config-router)#neighbor 172.168.100.186 route-reflector-client	Configure neighbor as Route Reflector Client
(config-router)#address-family l2vpn evpn	Enter into l2vpn address family mode
(config-router-af)#neighbor 172.16.100.174 activate	Activate the peer into address family mode
(config-router-af)#neighbor 172.16.100.174 route-reflector-client	Activate RR in l2vpn family
(config-router-af)#neighbor 172.16.100.184 activate	Activate the peer into address family mode
(config-router-af)#neighbor 172.16.100.184 route-reflector-client	Activate RR in l2vpn family
(config-router-af)#neighbor 172.16.100.186 activate	Activate the peer into address family mode
(config-router-af)#neighbor 172.16.100.186 route-reflector-client	Activate RR in l2vpn family
(config-router-af)#exit-address-family	Exit from l2vpn address family mode
(config-router)#exit	Exit from Router BGP mode and enter into config mode
(config)#exit	Exit from configuration mode

TOR1

#configure terminal	Enter Configure mode.
(config)#bridge 1 protocol ieee vlanbridge	Configure ieee vlan bridge
(config)#vlan 1000-1100 bridge 1 state enable	Configure vlans from 2-4042 and associate with bridge 1
(config)#interface xe50	Enter Interface mode for xe50
(config-if)#switchport	Make xe50 as L2 port by configuring switchport
(config-if)#bridge-group 1	Associate xe50 to bridge 1
(config-if)#switchport mode trunk	Configure xe50 as trunk port
(config-if)#switchport trunk allowed vlan all	Allow all configured vlans on xe50
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface vlan1.1000	Enter Interface mode for vlan 1.1000

(config-if)# ip address 100.0.0.1/24	Configure ip address
(config-if)# ipv6 address 1000::1/64	Configure ipv6 address
(config)#exit	Exit from configuration mode

TOR2

#configure terminal	Enter Configure mode.
(config)#bridge 1 protocol ieee vlanbridge	Configure ieee vlan bridge
(config)#vlan 1000-1100 bridge 1 state enable	Configure vlans from 2-4042 and associate with bridge 1
(config)#interface xe50	Enter Interface mode for xe50
(config-if)#switchport	Make xe50 as L2 port by configuring switchport
(config-if)#bridge-group 1	Associate xe50 to bridge 1
(config-if)#switchport mode trunk	Configure xe50 as trunk port
(config-if)#switchport trunk allowed vlan all	Allow all configured vlans on xe50
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface vlan1.1000	Enter Interface mode for vlan 1.1000
(config-if)# ip address 100.0.0.2/24	Configure ip address
(config-if)# ipv6 address 1000::2/64	Configure ipv6 address
(config)#exit	Exit from configuration mode

Validation

TOR2

```
#ping 100.0.0.1
    Press CTRL+C to exit
    PING 100.0.0.1 (100.0.0.1) 56(84) bytes of data.
    64 bytes from 100.0.0.1: icmp_seq=1 ttl=63 time=0.259 ms
    64 bytes from 100.0.0.1: icmp_seq=2 ttl=63 time=0.231 ms
    64 bytes from 100.0.0.1: icmp_seq=3 ttl=63 time=0.251 ms
    64 bytes from 100.0.0.1: icmp_seq=4 ttl=63 time=0.231 ms

    --- 100.0.0.1 ping statistics ---
    4 packets transmitted, 4 received, 0% packet loss, time 2999ms
    rtt min/avg/max/mdev = 0.231/0.243/0.259/0.012 ms

#ping ipv6 1000::1
    Press CTRL+C to exit
    PING 1000::1(1000::1) 56 data bytes
    64 bytes from 1000::1: icmp_seq=1 ttl=63 time=0.237 ms
    64 bytes from 1000::1: icmp_seq=2 ttl=63 time=0.261 ms
    64 bytes from 1000::1: icmp_seq=3 ttl=63 time=0.268 ms
    64 bytes from 1000::1: icmp_seq=4 ttl=63 time=0.279 ms
    --- 1000::1 ping statistics ---
```

```
    4 packets transmitted, 4 received, 0% packet loss, time 3000ms
    rtt min/avg/max/mdev = 0.237/0.261/0.279/0.019 ms
```

Bleaf

```
#show nvo vxlan tunnel
    VXLAN Network tunnel Entries
     Source           Destination      Status          Up/Down        Update
    ================================================================================
    ======
    172.16.100.174   172.16.100.184   Installed     00:22:04     00:22:04
    172.16.100.174   172.16.100.186   Installed     00:22:17     00:22:17
    172.16.100.174 172.16.100.182 Installed 00:22:25 00:22:25 Total
    number of entries are 3

    #show nvo vxlan mac-table
    ================================================================================
    ================================================================
                                                              VXLAN MAC Entries
    ================================================================================
    ================================================================
    VNID      Interface  VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
    Type                 Status              AccessPortDesc
    ________________________________________________________________________________
    ________________________________________________________________

    11000     ----       ----   ----         6400.6a2d.eaa1 172.16.100.184
    Remote Dynamic       -------             -------
    10000     ----       ----   ----         6400.6a8e.48a1 172.16.100.186
    Remote Dynamic       -------             -------

    Total number of entries are : 2

#show nvo vxlan arp-cache
    VXLAN ARP-CACHE Information
    ===========================
    VNID     Ip-Addr          Mac-Addr       Type        Age-Out    Retries-Left
    ________________________________________________________________________
    11000    110.0.0.174      1418.7790.9901                ----
    11000    110.0.0.2        6400.6a2d.eaa1 Remote Dynamic ----
    10000    100.0.0.174      1418.7790.9901                ----
    10000    100.0.0.1        6400.6a8e.48a1 Remote Dynamic ---Total
    number of entries are 4

#show nvo vxlan nd-cache
    VXLAN ND-CACHE Information
    ===========================
    VNID     Ip-Addr                                  Mac-Addr       Type         Age-
    Out    Retries-Left

    ________________________________________________________________________________
    ________________________
```

```
11000    1100::174                                  1418.7790.9901
----
11000    1100::2                                   6400.6a2d.eaa1 Remote Dynamic
----
10000    1000::174                                  1418.7790.9901
----
10000    1000::1                                   6400.6a8e.48a1 Remote Dynamic --
--
Total number of entries are 4

#show bgp l2vpn evpn mac-ip
RD[5000:10] VRF[ip_vrf5000]:
ESI                              Eth-Tag     Mac-Address     IP-Address
VNID    L3VNID    Nexthop
0                                10000       1418:7790:9901 100.0.0.174
10000     5000      172.16.100.174
0                                10000       1418:7790:9901 1000::174
10000     5000      172.16.100.174
0                                11000       1418:7790:9901 110.0.0.174
11000     5000      172.16.100.174
0                                11000       1418:7790:9901 1100::174
11000     5000      172.16.100.174

RD[10000:1]
ESI                              Eth-Tag     Mac-Address     IP-Address
VNID    L3VNID    Nexthop
0                                10000       6400:6a8e:48a1 --
10000     0         172.16.100.186
0                                10000       6400:6a8e:48a1 100.0.0.1
10000     0         172.16.100.186
0                                10000       6400:6a8e:48a1 1000::1
10000     0         172.16.100.186

RD[10000:10] VRF[mac_vrf10000]:
ESI                              Eth-Tag     Mac-Address     IP-Address
VNID    L3VNID    Nexthop
0                                10000       1418:7790:9901 100.0.0.174
10000     5000      172.16.100.174
0                                10000       1418:7790:9901  1000::174
10000     5000      172.16.100.174

RD[11000:2]
ESI                              Eth-Tag     Mac-Address     IP-Address
VNID     L3VNID   Nexthop
0                                11000       6400:6a2d:eaa1 --
11000     0         172.16.100.184
0                                11000       6400:6a2d:eaa1 110.0.0.2
11000     0         172.16.100.184
0                                11000       6400:6a2d:eaa1 1100::2
11000     0         172.16.100.184
```

```
RD[11000:10] VRF[mac_vrf11000]:
ESI                               Eth-Tag     Mac-Address    IP-Address
VNID     L3VNID   Nexthop
0                                 11000       1418:7790:9901 110.0.0.174
11000      5000      172.16.100.174
0                                 11000       1418:7790:9901 1100::174
11000      5000      172.16.100.174
```

TYPE-5 EVPN

Configuration

Configuring TYPE-5 EVPN prefix route using ip vrf with IRB interface with any type of gateway

Leaf1

#configure terminal	Enter Configure mode.
(config)# ip route vrf ip_vrf5000 19.1.1.0/ 24 100.0.0.50 irb1000	Configure prefix route using ip vrf mapped for irb interface with irb interface and connected host gateway ip(10.1.1.50 is host ip).
(config)#exit	Exit from configuration mode

Validations

Leaf1

```
#show running-config ip route
    ! ip route vrf management 0.0.0.0/0 10.12.37.1 eth0

    ip route vrf ip_vrf5000 19.1.1.0/24 100.0.0.50 irb1000 !
#show ip route vrf all
    Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
           O - OSPF, IA - OSPF inter area
                     N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
           E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-
          IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
          area, E - EVPN, v - vrf leaked
           * - candidate default

    IP Route Table for VRF "default"
    C     127.0.0.0/8 is directly connected, lo, 00:28:55
    O     172.16.100.172/32 [110/10100] via 192.168.110.172, xe47, 00:28:45
    O172.16.100.174/32 [110/10200] via 192.168.110.172, xe47, 00:28:45
    O172.16.100.184/32 [110/10200] via 192.168.110.172, xe47, 00:28:45
    C172.16.100.186/32 is directly connected, lo, 00:28:54
    C192.168.110.0/24 is directly connected, xe47, 00:28:54
    O192.168.111.0/24 [110/200] via 192.168.110.172, xe47, 00:28:45
    O192.168.115.0/24 [110/200] via 192.168.110.172, xe47, 00:28:45
    O 192.168.125.0/24 [110/300] via 192.168.110.172, xe47, 00:28:45 IP
    Route Table for VRF "management"
    Gateway of last resort is 10.12.37.1 to network 0.0.0.0

    S* 0.0.0.0/0 [1/0] via 10.12.37.1, eth0, 00:28:55
    C     10.12.37.0/24 is directly connected, eth0, 00:28:55
    C     127.0.0.0/8 is directly connected, lo.management, 00:28:54
    IP Route Table for VRF "ip_vrf5000"
    S  19.1.1.0/24 [1/0] via 100.0.0.50, irb1000, 00:10:46 >>>>>>>> Static route
```

```
   C     100.0.0.0/24 is directly connected, irb1000, 00:28:54
   E100.0.0.1/32 [0/0] is directly connected, irb1000
   E100.0.0.50/32 [0/0] is directly connected, irb1000
   C110.0.0.0/24 is directly connected, irb1100, 00:28:54
   E110.0.0.2/32 [0/0] is directly connected, irb1100
   C127.0.0.0/8 is directly connected, lo.ip_vrf5000, 00:28:54

Gateway of last resort is not set
```

Leaf2

```
#sh ip route vrf all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS,
      L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area,
      E - EVPN, v - vrf leaked
       * - candidate default

IP Route Table for VRF "default"
   C     127.0.0.0/8 is directly connected, lo, 00:31:15
   O     172.16.100.172/32 [110/10100] via 192.168.111.172, xe47, 00:30:56
   O172.16.100.174/32 [110/10200] via 192.168.111.172, xe47, 00:30:14
   C172.16.100.184/32 is directly connected, lo, 00:31:15
   O172.16.100.186/32 [110/10200] via 192.168.111.172, xe47, 00:28:22
   O192.168.110.0/24 [110/200] via 192.168.111.172, xe47, 00:28:32
   C192.168.111.0/24 is directly connected, xe47, 00:31:13
   O192.168.115.0/24 [110/200] via 192.168.111.172, xe47, 00:30:25
   O192.168.125.0/24 [110/300] via 192.168.111.172, xe47, 00:30:14
IP Route Table for VRF "management"
Gateway of last resort is 10.12.37.1 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 10.12.37.1, eth0, 00:31:15
   C     10.12.37.0/24 is directly connected, eth0, 00:31:15
   C     127.0.0.0/8 is directly connected, lo.management, 00:31:14
IP Route Table for VRF "ip_vrf5000"
E 19.1.1.0/24 [0/0] via 100.0.0.50, irb1000 (recursive is directly
connected, irb1000))>>>EVPN Route learnt with irb inteface C
100.0.0.0/24 is directly connected, irb1000, 00:31:14
   E100.0.0.1/32 [0/0] is directly connected, irb1000
   E100.0.0.50/32 [0/0] is directly connected, irb1000
   C110.0.0.0/24 is directly connected, irb1100, 00:31:14
   E110.0.0.2/32 [0/0] is directly connected, irb1100
   C127.0.0.0/8 is directly connected, lo.ip_vrf5000, 00:31:14

Gateway of last resort is not set

# sh interface brief

Codes: ETH - Ethernet, LB - Loopback, AGG - Aggregate, MLAG - MLAG Aggregate FR
            - Frame Relay, TUN -Tunnel, PBB - PBB Logical Port, VP - Virtual
```

```
    Port
           CVP - Channelised Virtual Port, METH - Management Ethernet, UNK-
           Unknown ED - ErrDisabled, PD - Protocol Down, AD - Admin Down, IA -
           InActive PD(Min-links) - Protocol Down Min-links DV - DDM Violation, NA
           - Not Applicable
           NOM - No operational members, PVID - Port Vlan-id
           Ctl - Control Port (Br-Breakout/Bu-Bundle) HD -
           ESI Hold Timer Down
    ------------------------------------------------------------------------------
    --
      Ethernet Type PVID Mode                   Status Reason Speed Port Ctl Br/
    Bu
    Interface                                                        Ch #
    ------------------------------------------------------------------------------

       1388.ac1064ae ETH -- routed               up       none 0       --
    No No >>>>> This interface is created when tunnel is established with L3VNI
    (its VNID value.VTEPIP in hexadecimal value)

       1388.ac1064ba ETH -- routed               up       none 0       --
    No No


    ------------------------------------------------------------------------------
    Interface     Type              Status Reason Speed
    ------------------------------------------------------------------------------
    --
    eth0    METH  up    --    100m irb1000     IRB   up    --
       0 irb1100  IRB   up    --    0
    ------------------------------------------------------------------------------
      Interface Status       Description
    ------------------------------------------------------------------------------
    --
    lo           up           --

#show nvo vxlan tunnel
    VXLAN Network tunnel Entries
     Source            Destination      Status          Up/Down        Update
    ================================================
       172.16.100.184 172.16.100.186 Installed       00:28:27     00:28:27
    172.16.100.184 172.16.100.174 Installed    00:30:17   00:30:17 Total number
    of entries are 2
```

Configuring EVPN prefix route using mac vrf with IRB interface in distributed centralised gateway/ Centralized gateway

Leaf1

`#configure terminal`	Enter Configure mode.
`(config)# ip route vrf ip_vrf5000 18.1.1.0/ 24 100.0.0.50 irb1000`	Configure prefix route using ip vrf mapped for irb interface with irb interface and connected host gateway ip(10.1.1.50 is host ip).

(config)#exit	Exit from configuration mode

Validation

Leaf1

```
#show bgp l2vpn evpn prefix-route

    RD[10000:1] VRF[mac_vrf10000]:
         ESI Eth-Tag Prefix-Length IP-Address GW-IPAddress L3VNID Nexthop
       0        0       24            18.1.1.0 00.0.0.50      0    172.16.100.186
```

Bleaf

```
#show bgp l2vpn evpn prefix-route

     RD[10000:1]
       ESI       Eth-Tag    Prefix-Length IP-Address GW-IP Address L3VNID Nexthop
          0     0            24           18.1.1.0            100.0.0.50 0  72.16.100.186
```

Note: Do not configure same VLAN for both VxLAN and MPLS EVPN, use unique values

CHAPTER 5 VXLAN Quality of Service Configuration

This chapter contains the configurations for VXLAN Quality of Service (QoS) .

Overview

VXLAN enables multiple tenants to operate in a data center. Each tenant is assigned a priority group to prioritize their traffic. Cloud carriers want to use quality of service to differentiate different applications.

Data center networks are being increasingly used by telecommunications operators as well as by enterprises. Currently these networks are organized as one large Layer 2 network in a single building. In some cases such a network is extended geographically using Virtual Local Area Network (VLAN) technologies as an even larger Layer 2 network connecting the virtual machines (VM), each with its own MAC address.

Multiple tenants might want their own isolated network domain. In a data center hosting multiple tenants, each tenant may independently assign MAC addresses and VLAN IDs and this might lead to duplication.

Cloud carriers wish to categorize the traffic based on the application such as voice, video, etc. Based on the type of the application different traffic classes may be identified and different priority levels can be assigned to each. To do so, quality of service marking is needed in VXLAN.

This chapter shows how to mark packet headers with the VXLAN tunnel end point (VTEP) when the frames are introduced by the virtual machines. The (re)marking /setting of QoS field DSCP/TOS in the VXLAN IP header is done with the two modes which are set globally.

Topology

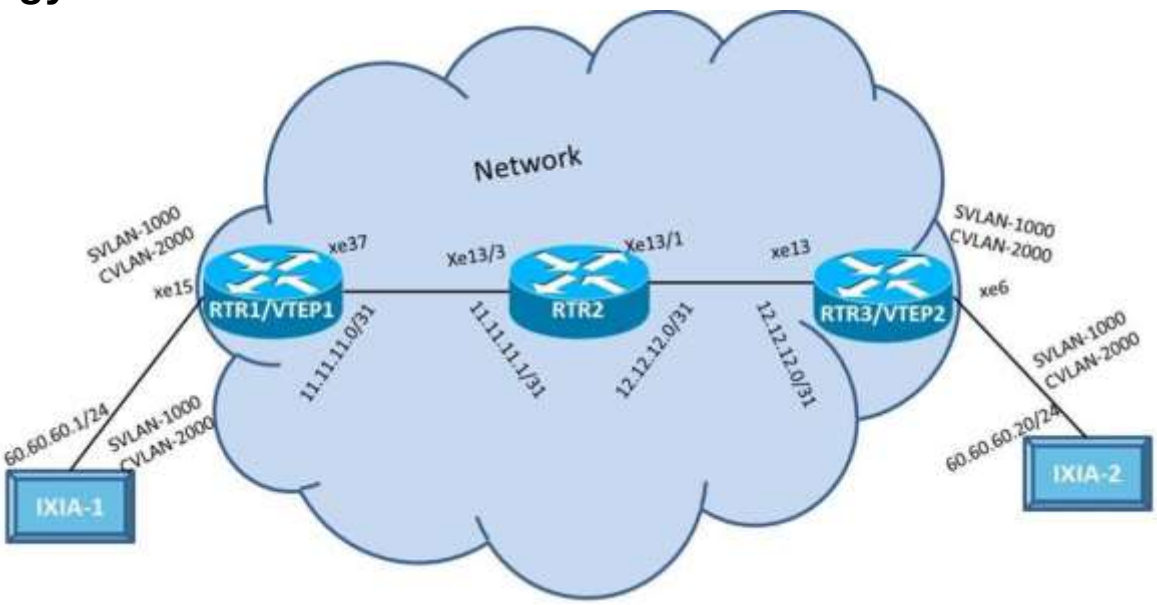


Figure 5-242: VXLAN QoS

COS-DSCP

RTR1/VTEP1

#configure terminal	Enter Configure mode.
(config)#interface lo	Enter Interface mode for loopback.
(config-if)#ip address 33.33.33.0/31 secondary	Assign secondary IP address.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#mac vrf vrf1	Create mac routing/forwarding instance with vrf1 name and enter into vrf mode
(config-vrf)#rd 100:11	Assign RD value
(config-vrf)#route-target export 200:11	Assign route-target value for export
(config-vrf)#route-target import 400:11	Assign route-target value for import
(config-vrf)#exit	Exit from vrf configuration mode
(config)#interface xe37	Enter Interface mode for xe37.
(config-if)#ip address 11.11.11.0/31	Assign IP address in /31 mask.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe15	Enter Interface mode for xe15.
(config-if)#switchport	Make it L2 interface
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router bgp 100	Enter into Router BGP mode
(config-router)#bgp router-id 1.1.1.1	Assign BGP router ID
(config-router)#network 33.33.33.0/31	Advertise loopback network into BGP for VTEP ID reachability
(config-router)#neighbor 11.11.11.1 remoteas 200	Specify a neighbor router with peer ip address and remote-as defined
(config-router)#neighbor 11.11.11.1 fallover bfd	Configure single-hop BFD session for its BGP peer
(config-router)#address-family l2vpn evpn	Enter into l2vpn address family mode
(config-router-af)#neighbor 11.11.11.1 activate	Activate the peer into address family mode
(config-router-af)#exit-address-family	Exit from l2vpn address family mode
(config-router)#exit	Exit from Router BGP mode and enter into config mode
(config)#qos enable	Enable QoS.
(config)#qos dscp-queue-profile egress 65	Configure DSCP-Q profile with the ID.
(config-dscp-queue)#dscp 48 queue 3	Configure particular DSCP value to the queue value for configured profile.
(config-dscp-queue)#exit	Exit from dscp queue profile mode.
(config)#qos cos-queue-profile ingress 1	Configure COS-Q profile with the ID.

(config-cos-queue)#cos 2 queue 3	Configure particular COS value to the queue value for configured profile.
(config-cos-queue)#exit	Exit from cos queue profile mode.
(config)#nvo vxlan enable	Enable VXLAN
(config)#nvo vxlan vtep-ip-global 33.33.33.0	Configure Source vtep-ip-global configuration
(config)#nvo vxlan tunnel qos-map-mode cosdscp egress 65	Configure mapping type cos-dscp in egress.
(config)#nvo vxlan id 1 ingress-replication inner-vid-disabled	Configure VXLAN Network identifier with inner-vid-disabled configure and enter into VXLAN tenant mode
(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf1	Assign vrf for evpn-bgp to carry EVPN route
(config-nvo)#exit	Exit from VXLAN tenant mode and enter into configuration mode.
(config)#nvo vxlan access-if port-vlan xe15 1000 inner-vlan 2000	Enable port-vlan mapping i.e. access port to outer-vlan (SVLAN) and inner-vlan (CVLAN) mapping
(config-nvo-acc-if)#map vnid 1	Map VXLAN Identified to access-port for VXLAN
(config-nvo-acc-if)#map qos-profile ingress 1	Map QoS profile created to given VXLAN access port.
(config-nvo-acc-if)#exit	Exit from VXLAN access-interface mode and enter into configuration mode
(config)#exit	Exit from configuration mode

RTR2

#configure terminal	Enter Configure mode.
(config)#interface xe13/3	Enter Interface mode for xe13/3.
(config-if)#ip address 11.11.11.1/31	Assign IP address in /31 mask.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe13/1	Enter Interface mode for xe13/1.
(config-if)#ip address 12.12.12.1/31	Assign IP address in /31 mask.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router bgp 200	Enter into Router BGP mode
(config-router)#bgp router-id 2.2.2.2	Assign BGP router ID
(config-router)#neighbor 11.11.11.0 remoteas 100	Specify a neighbor router with peer ip address and remote-as defined
(config-router)#neighbor 11.11.11.0 fallover bfd	Configure single-hop BFD session for its BGP peer
(config-router)#neighbor 12.12.12.0 remoteas 300	Specify a neighbor router with peer ip address and remote-as defined
(config-router)#neighbor 12.12.12.0 fallover bfd	Configure single-hop BFD session for its BGP peer
(config-router)#address-family l2vpn evpn	Enter into l2vpn address family mode
(config-router-af)#neighbor 11.11.11.0 activate	Activate the peer into address family mode

(config-router-af)#neighbor 12.12.12.0 activate	Activate the peer into address family mode
(config-router-af)#exit-address-family	Exit from l2vpn address family mode
(config-router)#exit	Exit from Router BGP mode and enter into config mode

RTR3/VTEP2

#configure terminal	Enter Configure mode.
(config)#interface lo	Enter Interface mode for loopback.
(config-if)#ip address 34.34.34.0/31 secondary	Assign secondary IP address.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#mac vrf vrf1	Create mac routing/forwarding instance with vrf1 name and enter into vrf mode
(config-vrf)#rd 300:11	Assign RD value
(config-vrf)#route-target export 400:11	Assign route-target value for export
(config-vrf)#route-target import 200:11	Assign route-target value for import
(config-vrf)#exit	Exit from vrf configuration mode
(config)#interface xe13	Enter Interface mode for xe13.
(config-if)#ip address 12.12.12.0/31	Assign IP address in /31 mask.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe6	Enter Interface mode for xe6.
(config-if)#switchport	Make it L2 interface
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router bgp 300	Enter into Router BGP mode
(config-router)#bgp router-id 3.3.3.3	Assign BGP router ID
(config-router)#network 34.34.34.0/31	Advertise loopback network into BGP for VTEP ID reachability
(config-router)#neighbor 12.12.12.1 remoteas 200	Specify a neighbor router with peer ip address and remote-as defined
(config-router)#neighbor 12.12.12.1 fallover bfd	Configure single-hop BFD session for its BGP peer
(config-router)#address-family l2vpn evpn	Enter into l2vpn address family mode
(config-router-af)#neighbor 12.12.12.1 activate	Activate the peer into address family mode
(config-router-af)#exit-address-family	Exit from l2vpn address family mode
(config-router)#exit	Exit from Router BGP mode and enter into config mode
(config)#qos enable	Enable QoS.
(config)#qos dscp-queue-profile ingress 65	Configure DSCP-Q profile with the ID.
(config-dscp-queue)#dscp 48 queue 3	Configure particular DSCP value to the queue value for configured profile.
(config-dscp-queue)#exit	Exit from dscp queue profile mode.

(config)#qos cos-queue-profile egress 1	Configure COS-Q profile with the ID.
(config-cos-queue)#cos 2 queue 3	Configure particular COS value to the queue value for configured profile.
(config-cos-queue)#exit	Exit from cos queue profile mode.
(config)#nvo vxlan enable	Enable VXLAN
(config)#nvo vxlan vtep-ip-global 34.34.34.0	Configure Source vtep-ip-global configuration
(config)#nvo vxlan tunnel qos-map-mode cosdscp ingress 65	Configure mapping type cos-dscp in ingress.
(config)#nvo vxlan id 1 ingress-replication inner-vid-disabled	Configure VXLAN Network identifier with inner-vid-disabled configure and enter into VXLAN tenant mode
(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf1	Assign vrf for evpn-bgp to carry EVPN route
(config-nvo)#exit	Exit from VXLAN tenant mode and enter into configuration mode.
(config)#nvo vxlan access-if port-vlan xe6 1000 inner-vlan 2000	Enable port-vlan mapping i.e. access port to outer-vlan (SVLAN) and inner-vlan (CVLAN) mapping
(config-nvo-acc-if)#map vnid 1	Map VXLAN Identified to access-port for VXLAN
(config-nvo-acc-if)#mac 0000.0000.2222	Configure static mac.
(config-nvo-acc-if)#map qos-profile egress 1	Map QoS profile created to given VXLAN access port.
(config-nvo-acc-if)#exit	Exit from VXLAN access-interface mode and enter into configuration mode
(config)#exit	Exit from configuration mode

Validation

RTR1/VTEP1

```
#show running-config qos qos enable !
! ! qos cos-queue-profile ingress 1 cos 2 queue 3 ! qos dscp-
queue-profile egress 65 dscp 48 queue 3 ! #

#show running-config nvo vxlan !
nvo vxlan enable !
nvo vxlan vtep-ip-global 33.33.33.0 !
nvo vxlan tunnel qos-map-mode cos-dscp egress 65 ! nvo vxlan id 1 ingress-
replication inner-vid-disabled vxlan host-reachability-protocol evpn-bgp vrf1 !
nvo vxlan access-if port-vlan xe15 1000 inner-vlan 2000  no shutdown  map vnid 1  map
qos-profile ingress 1 !
#show bgp l2vpn evpn summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 2
2 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv    MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd     AD  MACIP  MCAST    ESI
```

```
11.11.11.1                  4     200    63           64         2       0       0  00:27:50
1       0       0       1       0

Total number of neighbors 1

Total number of Established sessions 1

#show bgp l2vpn evpn
BGP table version is 2, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route

    Network           Next Hop            Metric    LocPrf Weight Path  Peer

RD[100:11] VRF[vrf1]:
*>    [3]:[1]:[32,33.33.33.0]
                        33.33.33.0          0         100           32768    i
*     [3]:[1]:[32,34.34.34.0]
                        34.34.34.0           0         100           0       200 300 i
11.11.11.1

RD[300:11]
*>    [3]:[1]:[32,34.34.34.0]
                        34.34.34.0           0         100           0       200 300 i
11.11.11.1

Total number of prefixes 3

#show nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged
VNID     Type Interface     Vlan   Inner-Vlan Src-addr         Dst-addr
_____________________________________________________________________
1        NW     -----        ----      ----   33.33.33.0      34.34.34.0
1        AC    xe15         1000   2000     ----        ----
Total number of entries are 2
#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source            Destination     Status           Up/Down        Update
================================================================================
```

```
33.33.33.0        34.34.34.0      Installed     00:12:13
00:12:13 Total number of entries are 1 #

#show nvo vxlan mac-table
=====================================================================================
=
==
                  VXLAN MAC Entries
=====================================================================================
=
==

VNID     Interface    VlanId  Inner-VlanId  Mac-Addr      VTEP-Ip      Type        Status
Time-out     AccessPortDesc
_____________________________________________________________________________________
_
_____________________
1          ---          ---     ---    0000.0000.2222 34.34.34.0    Remote         -----
---
1          xe15      1000     2000 0000.0100.0100 33.33.33.0 Dynamic Local     -----
300
Total number of entries are 2 #

#show interface counters queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
+----------+-------------------+-------+----------------+-------------------+-----
----------+-------------------+
| Interface |     Queue/Class-map  | Q-Size |        Tx pkts      |        Tx  bytes      |
Dropped pkts     |   Dropped bytes   |
+----------+-------------------+-------+----------------+-------------------+-----
-
----------+-------------------+
cpu          hw-bfd            (E) 0        17                 1258                  0
0
cpu          bgp               (E) 0        1                  81                    0
0
xe37         q3               (E) 0        4416               503424             0
0
xe37         q7                 (E) 0         22                  1541                  0
0

#

RTR3/VTEP2

#show running-config
qos qos enable !
! ! qos cos-queue-profile
egress 1 cos 2 queue 3 ! qos
dscp-queue-profile ingress 65
dscp 48 queue 3 ! #
```

```
#show running-config nvo vxlan !
nvo  vxlan  enable
!
nvo  vxlan  vtep-ip-global  34.34.34.0
!
nvo vxlan tunnel qos-map-mode cos-dscp ingress 65 !
nvo vxlan id 1 ingress-replication inner-vid-disabled
vxlan host-reachability-protocol evpn-bgp vrf1 ! nvo
vxlan access-if port-vlan xe6 1000 inner-vlan 2000
no shutdown  map vnid 1  mac 0000.0000.2222  map qos-
profile egress 1 ! #

#
#show bgp l2vpn evpn summary
BGP router identifier 3.3.3.3, local AS number 300
BGP table version is 5
2 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V  AS    MsgRcv    MsgSen TblVer  InQ   OutQ    Up/Down   State/
PfxRcd      AD  MACIP   MCAST    ESI
12.12.12.1                   4    200   101         101        5       0       0  00:46:50
2       0      1      1      0

Total number of neighbors 1

Total number of Established sessions 1
#

#show bgp l2vpn evpn
BGP table version is 5, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route

    Network          Next Hop            Metric    LocPrf Weight Path  Peer

RD[100:11]
*>   [2]:[0]:[1]:[48,0000:0100:0100]:[0]:[1]
                        33.33.33.0           0         100           0       200 100 i
12.12.12.1
*>   [3]:[1]:[32,33.33.33.0]
                        33.33.33.0           0         100           0       200 100 i
12.12.12.1
```

```
RD[300:11] VRF[vrf1]:
*>    [2]:[0]:[1]:[48,0000:0000:2222]:[0]:[1]
                        34.34.34.0          0         100           32768    i
*     [2]:[0]:[1]:[48,0000:0100:0100]:[0]:[1]
                        33.33.33.0           0         100           0       200  100 i
12.12.12.1
*    [3]:[1]:[32,33.33.33.0]
                        33.33.33.0           0         100           0       200 100 i
12.12.12.1
*>   [3]:[1]:[32,34.34.34.0]
                        34.34.34.0          0         100           32768    i

Total number  of  prefixes 6
#

#show nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged
VNID     Type Interface    Vlan   Inner-Vlan Src-addr         Dst-addr
_____________________________________________________________________________
1        NW    -----        ----       ----  34.34.34.0      33.33.33.0
1        AC   xe6         1000    2000    ----        ----
Total number of entries are 2
#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
=============================================================================
34.34.34.0       33.33.33.0       Installed     00:36:38     00:36:38 Total
number of entries are 1
#
#show nvo vxlan mac-table
=============================================================================
=
==
                  VXLAN MAC Entries
=============================================================================
=
==

VNID     Interface    VlanId  Inner-VlanId  Mac-Addr     VTEP-Ip      Type        Status
Time-out     AccessPortDesc
_____________________________________________________________________________
_
_____________________
1          xe6      1000    2000 0000.0000.2222 34.34.34.0 Static Local      -----      -
--
1          ---         ---    ---    0000.0100.0100 33.33.33.0   Remote         -----
```

```
---
Total number of entries are 2 #

#show interface counters queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
+-----------+------------------+--------+-----------------+------------------+-----
-----------+------------------+
| Interface |    Queue/Class-map   |  Q-Size |      Tx pkts       |       Tx bytes       |
Dropped pkts    |  Dropped bytes    |
+-----------+------------------+--------+-----------------+------------------+-----
-
-----------+------------------+
cpu          hw-bfd            (E) 0        16                1184                0
0
xe13       q7               (E) 0         18                1260               0
0
xe6        q3                 (E)  0         4702               319736              0
0

#
```

COS-DSCP with a Default Tunnel

Using the previous configuration on VTEP1 and VTEP-2, un-configure cos profile mapped to access interface and also tunnel configure in egress on VTEP-1, do below configuration for VTEP1.

VTEP1

(config)#no nvo vxlan tunnel qos-map-mode cos-dscp egress	Un-configure cos-dscp tunnel mapped in egress direction.
(config)#nvo vxlan tunnel qos-map-mode cosdscp egress	Configure mapping type cos-dscp in egress without any profile id.
(config)#nvo vxlan access-if port-vlan xe15 1000 inner-vlan 2000	Enable port-vlan mapping i.e. access port to outer-vlan (SVLAN) and inner-vlan (CVLAN) mapping
(config-nvo-acc-if)#cos 5 ingress	Configure explicit cos value on access port.
(config-nvo-acc-if)#exit	Exit from VXLAN access-interface mode and enter into configuration mode
(config)#exit	Exit from configuration mode

RTR1/VTEP1

```
#show running-config
qos qos enable !
! ! qos cos-queue-profile
ingress 1  cos 2 queue 3 ! qos
dscp-queue-profile egress 65
dscp 48 queue 3 ! #
#show running-config nvo vxlan !
nvo  vxlan  enable
!
```

```
nvo  vxlan  vtep-ip-global  33.33.33.0
!
nvo vxlan tunnel qos-map-mode cos-dscp egress ! nvo
vxlan id 1 ingress-replication inner-vid-disabled
vxlan host-reachability-protocol evpn-bgp vrf1 !
nvo vxlan access-if port-vlan xe15 1000 inner-vlan
2000 no shutdown map vnid 1 cos 5 ingress ! #

#show interface counters queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
+-----------+-----------------+--------+----------------+------------------+-----
----------+-----------------+
| Interface  |    Queue/Class-map  | Q-Size |       Tx pkts     |       Tx bytes      |
Dropped pkts    |   Dropped bytes    |
+-----------+-----------------+--------+----------------+------------------+-----
-
-----------+-----------------+
cpu          hw-bfd           (E) 0        35                2590                0
0
cpu           bpdu            (E) 0        16                1088                0
0
cpu           ospf            (E) 0        1                 86                  0
0
xe37           q5               (E) 0          3120              355566              0
0
xe37           q7               (E) 0          35                2450                0
0

#
#show nvo vxlan mac-table
=====================================================================================
=
==
                  VXLAN MAC Entries
=====================================================================================
=
==

VNID     Interface    VlanId  Inner-VlanId  Mac-Addr     VTEP-Ip      Type       Status
Time-out     AccessPortDesc
_____________________________________________________________________________________
_
____________________
1           xe15         1000      2000 0000.0000.0022 33.33.33.0 Dynamic Local     -----
300
1          ---         ---    ---     0000.0000.2222 34.34.34.0   Remote         -----
---
Total number of entries are 2 #

#show nvo vxlan
VXLAN Information
=================
```

```
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged
VNID     Type Interface     Vlan   Inner-Vlan Src-addr          Dst-addr
_____________________________________________________________________________
1        NW     -----        ----       ---- 33.33.33.0       34.34.34.0
1        AC    xe15          1000    2000   ----        ----          Total
number of entries are 2
#
#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source            Destination      Status          Up/Down        Update
================================================================================
33.33.33.0        34.34.34.0      Installed     00:07:30
00:07:30 Total number of entries are 1 #
```

DSCP-DSCP

Using the previous configuration on VTEP1 and VTEP-2, un-configure VXLAN and QoS on both the VTEPs and perform the configuration below for VTEP1 and VTEP2.

VTEP1

(config)#qos disable	Disable QoS.
(config)#nvo vxlan disable	Disable VXLAN.
(config)#qos enable	Enable QoS.
(config)#qos dscp-queue-profile ingress 128	Configure DSCP-Q profile with the ID.
(config-dscp-queue)#dscp 16 queue 4	Configure particular DSCP value to the queue value for configured profile.
(config-dscp-queue)#exit	Exit from dscp queue profile mode.
(config)#qos dscp-queue-profile egress 65	Configure DSCP-Q profile with the ID.
(config-dscp-queue)#dscp 32 queue 6	Configure particular DSCP value to the queue value for configured profile.
(config-dscp-queue)#exit	Exit from dscp queue profile mode.
(config)#nvo vxlan enable	Enable VXLAN
(config)#nvo vxlan vtep-ip-global 33.33.33.0	Configure Source vtep-ip-global configuration
(config)#nvo vxlan tunnel qos-map-mode dscpdscp egress 65	Configure mapping type dscp-dscp in egress.
(config)#nvo vxlan id 1 ingress-replication inner-vid-disabled	Configure VXLAN Network identifier with inner-vid-disabled configure and enter into VXLAN tenant mode
(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf1	Assign vrf for evpn-bgp to carry EVPN route
(config-nvo)#exit	Exit from VXLAN tenant mode and enter into configuration mode.

(config)#nvo vxlan access-if port-vlan xe15 1000 inner-vlan 2000	Enable port-vlan mapping i.e. access port to outer-vlan (SVLAN) and inner-vlan (CVLAN) mapping
(config-nvo-acc-if)#map vnid 1	Map VXLAN Identified to access-port for VXLAN
(config-nvo-acc-if)#map qos-profile ingress 128	Map QoS profile created to given VXLAN access port.
(config-nvo-acc-if)#exit	Exit from VXLAN access-interface mode and enter into configuration mode
(config)#exit	Exit from configuration mode

VTEP2

(config)#qos enable	Enable QoS.
(config)#qos dscp-queue-profile egress 128	Configure DSCP-Q profile with the ID.
(config-dscp-queue)#dscp 16 queue 4	Configure particular DSCP value to the queue value for configured profile.
(config-dscp-queue)#exit	Exit from dscp queue profile mode.
(config)#qos dscp-queue-profile ingress 65	Configure DSCP-Q profile with the ID.
(config-dscp-queue)#dscp 32 queue 6	Configure particular DSCP value to the queue value for configured profile.
(config-dscp-queue)#exit	Exit from dscp queue profile mode.
(config)#nvo vxlan enable	Enable VXLAN.
(config)#nvo vxlan vtep-ip-global 34.34.34.0	Configure Source vtep-ip-global configuration
(config)#nvo vxlan tunnel qos-map-mode dscpdscp ingress 65	Configure mapping type dscp-dscp in egress.
(config)#nvo vxlan id 1 ingress-replication inner-vid-disabled	Configure VXLAN Network identifier with inner-vid-disabled configure and enter into VXLAN tenant mode
(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf1	Assign vrf for evpn-bgp to carry EVPN route
(config-nvo)#exit	Exit from VXLAN tenant mode and enter into configuration mode.
(config)#nvo vxlan access-if port-vlan xe15 1000 inner-vlan 2000	Enable port-vlan mapping i.e. access port to outer-vlan (SVLAN) and inner-vlan (CVLAN) mapping
(config-nvo-acc-if)#map vnid 1	Map VXLAN Identified to access-port for VXLAN
(config-nvo-acc-if)#map qos-profile egress 128	Map QoS profile created to given VXLAN access port.
(config-nvo-acc-if)#exit	Exit from VXLAN access-interface mode and enter into configuration mode
(config)#exit	Exit from configuration mode

RTR1/VTEP1

```
#show running-config nvo vxlan !
nvo vxlan enable !
nvo vxlan vtep-ip-global 33.33.33.0 !
nvo vxlan tunnel qos-map-mode dscp-dscp egress 65 ! nvo vxlan id 1 ingress-replication
inner-vid-disabled vxlan host-reachability-protocol evpn-bgp vrf1 ! nvo vxlan access-
```

```
if port-vlan xe15 1000 inner-vlan 2000 no shutdown map vnid 1 map qos-profile
ingress 128 !
#
#show running-config qos qos enable !
! ! qos dscp-queue-profile egress 65  dscp 32 queue 6 !
qos dscp-queue-profile ingress 128  dscp 16 queue 4 ! #
#show nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged
VNID     Type Interface    Vlan   Inner-Vlan Src-addr         Dst-addr
_____________________________________________________________________
1        NW    -----        ----       ----  33.33.33.0      34.34.34.0
1        AC   xe15           1000    2000    ----        ----          Total
number of entries are 2
#
#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
33.33.33.0 34.34.34.0 Installed 00:04:08 00:04:08 Total number of entries
are 1

#
#show nvo vxlan mac-table
================================================================================
=
==
                  VXLAN MAC Entries
================================================================================
=
==

VNID     Interface    VlanId  Inner-VlanId  Mac-Addr     VTEP-Ip      Type        Status
Time-out     AccessPortDesc
_____________________________________________________________________________
_
_____________________
1          xe15          1000      2000  0000.0000.0022 33.33.33.0 Dynamic  Local     -----
300
1          ---          ---    ---     0000.0000.2222 34.34.34.0   Remote          -----
---
Total number of entries are 2 #

#show interface counters queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
+ ----------+------------------     +--------+----------------+------------------          +-----
           +------------------   +
| Interface  |    Queue/Class-map  | Q-Size |       Tx  pkts      |      Tx bytes       |
Dropped pkts    |   Dropped bytes    |
```

```
+----------+------------------   +--------+----------------+------------------ +-----
-
-----------+------------------- +
cpu          hw-bfd            (E) 0        264               19536                0
0
cpu          bpdu              (E) 0        124               8944                 0
0
cpu          ospf              (E) 0        6                 516                  0
0
cpu          bgp               (E) 0        4                 298                  0
0
xe37         q4                (E) 0        23132             2637048              0
0
xe37          q7                 (E) 0         269                18832                0
0
#
```

RTR3/VTEP2

```
#show running-config qos qos
enable !
! ! qos dscp-queue-profile ingress 65
dscp 32 queue 6 ! qos dscp-queue-
profile egress 128 dscp 16 queue 4 ! #
#show running-config nvo vxlan
! nvo vxlan enable !
nvo vxlan vtep-ip-global 34.34.34.0 !
nvo vxlan tunnel qos-map-mode dscp-dscp ingress 65 ! nvo
vxlan id 1 ingress-replication inner-vid-disabled vxlan host-
reachability-protocol evpn-bgp vrf1 ! nvo vxlan access-if
port-vlan xe6 1000 inner-vlan 2000 no shutdown map vnid 1 mac
0000.0000.2222 map qos-profile egress 128 ! #

#
#show nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged
VNID     Type Interface    Vlan   Inner-Vlan Src-addr         Dst-addr
_____________________________________________________________________
1        NW    -----        ----       ----  34.34.34.0      33.33.33.0
1        AC    xe6            1000    2000    ----        ----          Total number
of entries are 2
#
#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
```

```
34.34.34.0        33.33.33.0      Installed      00:13:44    00:13:44 Total
number of entries are 1
#
#show nvo vxlan mac-table
=====================================================================================
=
==
                  VXLAN MAC Entries
=====================================================================================
=
==

VNID     Interface    VlanId  Inner-VlanId  Mac-Addr      VTEP-Ip      Type        Status
Time-out     AccessPortDesc
_____________________________________________________________________________________
_
_____________________
1          ---          ---    ---     0000.0000.0022 33.33.33.0    Remote         -----
---
1         xe6          1000    2000 0000.0000.2222 34.34.34.0 Static Local     -----
---
Total number of entries are 2
#
#show interface counters queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
+----------+-------------------+--------+----------------+-----------------+-----
----------+-------------------+
| Interface |    Queue/Class-map   | Q-Size |      Tx pkts      |       Tx bytes      |
Dropped pkts    |   Dropped bytes    |
+----------+-------------------+--------+----------------+-----------------+-----
-
----------+-------------------+
cpu          hw-bfd            (E) 0        883               65342               0
0
cpu          bpdu              (E) 0        97                6208                0
0
cpu          ospf              (E) 0        19                1634                0
0
cpu          bgp               (E) 0        14                1043                0
0
xe6          q6                (E) 0        77955             5300940             0
0
xe13          q7                 (E) 0         903                63217                 0
0

#
```

DSCP-DSCP with a Default Tunnel

Using the previous configuration on VTEP1 and VTEP-2, un-configure the DSCP profile mapped to access interface and also tunnel configure in egress on VTEP-1, do below configuration for VTEP1.

VTEP1

(config)#no nvo vxlan tunnel qos-map-mode dscp-dscp egress	Un-Configure dscp-dscp tunnel mapping from egress.
(config)#nvo vxlan tunnel qos-map-mode dscpdscp egress	Configure mapping type dscp-dscp in egress without any profile id.
(config)#nvo vxlan access-if port-vlan xe15 1000 inner-vlan 2000	Enable port-vlan mapping i.e. access port to outer-vlan (SVLAN) and inner-vlan (CVLAN) mapping
(config-nvo-acc-if)#dscp 48 ingress	Configure explicit dscp value on access port.
(config-nvo-acc-if)#exit	Exit from VXLAN access-interface mode and enter into configuration mode
(config)#exit	Exit from configuration mode

RTR1/VTEP1

```
#show running-config qos qos
enable !
! ! qos dscp-queue-profile egress 65 dscp
32 queue 6 ! qos dscp-queue-profile
ingress 128 dscp 16 queue 4 !
#show running-config nvo vxlan
! nvo vxlan enable !
nvo vxlan vtep-ip-global 33.33.33.0 !
nvo vxlan tunnel qos-map-mode dscp-dscp egress !
nvo vxlan id 1 ingress-replication inner-vid-disabled vxlan
host-reachability-protocol evpn-bgp vrf1 !
nvo vxlan access-if port-vlan xe15 1000 inner-vlan 2000 no
shutdown map vnid 1 dscp 48 ingress ! #

#show nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged
VNID         Type  Interface       Vlan     Inner-Vlan  Src-addr                Dst-addr
_____________________________________________________________________________
1        NW    -----        ----       ----  33.33.33.0      34.34.34.0
1        AC   xe15          1000    2000    ----        ----          Total
number of entries are 2
#
#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
33.33.33.0       34.34.34.0      Installed      00:00:36    00:00:36 Total
number of entries are 1
#
#show nvo vxlan mac-table
================================================================================
=
```

```
==
                  VXLAN MAC Entries
=====================================================================================
=
==

VNID     Interface    VlanId  Inner-VlanId  Mac-Addr      VTEP-Ip      Type        Status
Time-out     AccessPortDesc
_____________________________________________________________________________________
_
_____________________
1          xe15          1000      2000 0000.0000.0022  33.33.33.0 Dynamic  Local     -----
300
1          ---          ---    ---     0000.0000.2222 34.34.34.0   Remote         -----
---
Total number of entries are 2 #

#show interface counters queue-stats
E - Egress, I - Ingress, Q-Size is in bytes
+----------+-------------------+--------+----------------+-----------------+-----
----------+-------------------+
| Interface  |    Queue/Class-map  | Q-Size |       Tx pkts        |       Tx bytes       |
Dropped pkts    |    Dropped bytes   |
+----------+-------------------+--------+----------------+-----------------+-----
-
----------+-------------------+
cpu          hw-bfd            (E) 0        385                28490                0
0
cpu          bpdu              (E) 0        180                13008                0
0
cpu          ospf              (E) 0        9                  774                  0
0
cpu          bgp               (E) 0        6                  447                  0
0
xe37         q6                (E) 0        33914              3866196              0
0
xe37          q7                 (E) 0         396                  27723                0
0
```

CHAPTER 6 VXLAN EVPN EVC Configuration

This chapter shows how to configure VXLAN EVPN Ethernet Virtual Circuit (EVC) which embeds the functionality of EVPN-VXLAN access ports to allow EVC frames across VTEPs. With this configuration, customers in the same VLAN can communicate even they are placed across distributed data centers.

Overview

An EVC represents a logical relationship between Ethernet User Network Interface (UNI) in a provider-based Ethernet service. An EVC represents the service offered and is carried through the provider network. Each EVC is configured by a unique name across the provider network.

An EVC is an end–to–end representation of a single instance of a Layer 2 service that a service provider offers. An EVC embodies the different parameters based on which the service is offered. EVC prevents data transfer between sites that are not part of the same EVC.

EVC is an A–Z circuit that enables you to pass customer VLANs from one port on a node to another port on another node in the network. EVC represents a Carrier Ethernet service and is an entity that provides end–to–end connection between two or more customer end points.

Topology

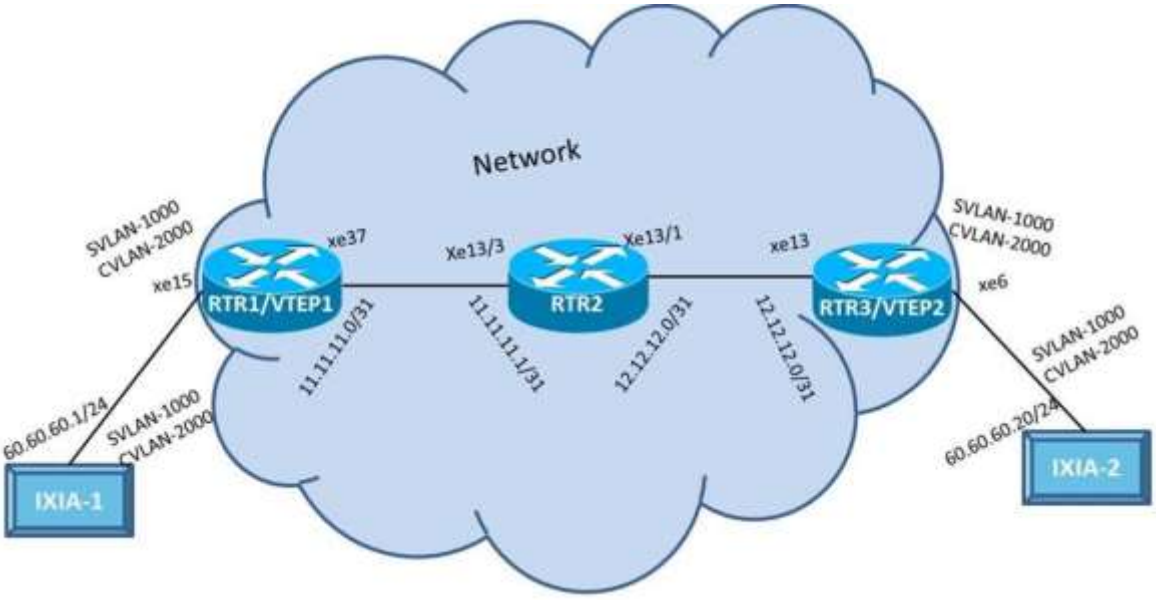


Figure 6-243: VXLAN EVPN EVC

RTR1/VTEP1

`#configure terminal`	Enter Configure mode.
`(config)#interface lo`	Enter Interface mode for loopback.
`(config-if)#ip address 33.33.33.0/31 secondary`	Assign secondary IP address.

(config-if)#exit	Exit Interface mode.
(config)#mac vrf vrf1	Create mac routing/forwarding instance with vrf1 name and enter into VRF mode
(config-vrf)# rd 100:11	Assign RD value
(config-vrf)# route-target export 200:11	Assign route-target value for export
(config-vrf)# route-target import 400:11	Assign route-target value for import
(config-vrf)#exit	Exit VRF configuration mode
(config)#interface xe37	Enter Interface mode for xe37
(config-if)#ip address 11.11.11.0/31	Assign IP address in /31 mask.
(config-if)#exit	Exit Interface mode.
(config)#interface xe15	Enter Interface mode for xe15
(config-if)#switchport	Make it L2 interface
(config-if)#exit	Exit Interface mode.
(config)#router bgp 100	Enter BGP router mode
(config-router)# bgp router-id 1.1.1.1	Assign BGP router ID
(config-router)#network 33.33.33.0/31	Advertise loopback network into BGP for VTEP ID reachability
(config-router)#neighbor 11.11.11.1 remoteas 200	Specify a neighbor router with peer IP address and remote-as defined
(config-router)#neighbor 11.11.11.1 fallover bfd	Configure single-hop BFD session for its BGP peer
(config-router)#address-family l2vpn evpn	Enter into l2vpn address family mode
(config-router-af)#neighbor 11.11.11.1 activate	Activate the peer into address family mode
(config-router-af)#exit-address-family	Exit l2vpn address family mode
(config-router)#exit	Exit BGP router mode
(config)#nvo vxlan enable	Enable VXLAN
(config)#nvo vxlan vtep-ip-global 33.33.33.0	Configure Source vtep-ip-global configuration
(config)#nvo vxlan id 1 ingress-replication inner-vid-disabled	Configure VXLAN Network identifier with/without inner-viddisabled configure and enter into VXLAN tenant mode
(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf1	Assign VRF for evpn-bgp to carry EVPN route
(config-nvo)#exit	Exit VXLAN tenant mode.
(config)#nvo vxlan access-if port-vlan xe15 1000 inner-vlan 2000	Enable port-vlan mapping i.e. access port to outer-vlan (SVLAN) and inner-vlan (CVLAN) mapping
(config-nvo-acc-if)#map vnid 1	Map VXLAN Identified to access-port for VXLAN
(config-nvo-acc-if)#exit	Exit VXLAN access-interface mode
(config)#exit	Exit configuration mode

RTR2

#configure terminal	Enter Configure mode.
(config)#interface xe13/3	Enter Interface mode for xe13/3
(config-if)#ip address 11.11.11.1/31	Assign IP address in /31 mask.
(config-if)#exit	Exit Interface mode.
(config)#interface xe13/1	Enter Interface mode for xe13/1
(config-if)#ip address 12.12.12.1/31	Assign IP address in /31 mask.
(config-if)#exit	Exit Interface mode
(config)#router bgp 200	Enter BGP router mode
(config-router)# bgp router-id 2.2.2.2	Assign BGP router ID
(config-router)#neighbor 11.11.11.0 remoteas 100	Specify a neighbor router with peer ip address and remote-as defined
(config-router)#neighbor 11.11.11.0 fallover bfd	Configure single-hop BFD session for its BGP peer
(config-router)#neighbor 12.12.12.0 remoteas 300	Specify a neighbor router with peer ip address and remote-as defined
(config-router)#neighbor 12.12.12.0 fallover bfd	Configure single-hop BFD session for its BGP peer
(config-router)#address-family l2vpn evpn	Enter into l2vpn address family mode
(config-router-af)#neighbor 11.11.11.0 activate	Activate the peer into address family mode
(config-router-af)#neighbor 12.12.12.0 activate	Activate the peer into address family mode
(config-router-af)#exit-address-family	Exit l2vpn address family mode
(config-router)#exit	Exit BGP router mode

RTR3/VTEP2

#configure terminal	Enter Configure mode.
(config)#interface lo	Enter Interface mode for loopback.
(config-if)#ip address 34.34.34.0/31 secondary	Assign secondary IP address.
(config-if)#exit	Exit Interface mode.
(config)#mac vrf vrf1	Create mac routing/forwarding instance with vrf1 name and enter into vrf mode
(config-vrf)#rd 300:11	Assign RD value
(config-vrf)#route-target export 400:11	Assign route-target value for export
(config-vrf)#route-target import 200:11	Assign route-target value for import
(config-vrf)#exit	Exit vrf configuration mode
(config)#interface xe13	Enter Interface mode for xe13
(config-if)#ip address 12.12.12.0/31	Assign IP address in /31 mask.
(config-if)#exit	Exit Interface mode.
(config)#interface xe6	Enter Interface mode for xe6

(config-if)#switchport	Make it L2 interface
(config-if)#exit	Exit Interface mode.
(config)#router bgp 300	Enter BGP router mode
(config-router)# bgp router-id 3.3.3.3	Assign BGP router ID
(config-router)#network 34.34.34.0/31	Advertise loopback network into BGP for VTEP ID reachability
(config-router)#neighbor 12.12.12.1 remoteas 200	Specify a neighbor router with peer ip address and remote-as defined
(config-router)#neighbor 12.12.12.1 fallover bfd	Configure single-hop BFD session for its BGP peer
(config-router)#address-family l2vpn evpn	Enter into l2vpn address family mode
(config-router-af)#neighbor 12.12.12.1 activate	Activate the peer into address family mode
(config-router-af)#exit-address-family	Exit l2vpn address family mode
(config-router)#exit	Exit BGP router mode
(config)#nvo vxlan enable	Enable VXLAN
(config)#nvo vxlan vtep-ip-global 34.34.34.0	Configure Source vtep-ip-global configuration
(config)#nvo vxlan id 1 ingress-replication inner-vid-disabled	Configure VXLAN Network identifier with/without inner-viddisabled configure and enter into VXLAN tenant mode
(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf1	Assign VRF for evpn-bgp to carry EVPN route
(config-nvo)#exit	Exit VXLAN tenant mode.
(config)#nvo vxlan access-if port-vlan xe6 1000 inner-vlan 2000	Enable port-vlan mapping i.e. access port to outer-vlan (SVLAN) and inner-vlan (CVLAN) mapping
(config-nvo-acc-if)#map vnid 1	Map VXLAN Identified to access-port for VXLAN
(config-nvo-acc-if)#exit	Exit VXLAN access-interface mode
(config)#exit	Exit configuration mode

Validation

Retaining SVLAN and CVLAN tags across Data Centers

RTR1/VTEP1

```
#show running-config nvo vxlan !
nvo vxlan enable !
nvo vxlan vtep-ip-global 33.33.33.0 ! nvo vxlan id 1 ingress-replication vxlan
host-reachability-protocol evpn-bgp vrf1 ! nvo vxlan access-if port-vlan xe15
1000 inner-vlan 2000 no shutdown map vnid 1 !

#show bgp l2vpn evpn summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 3
2 BGP AS-PATH entries
```

```
0 BGP community entries
Neighbor                 V  AS    MsgRcv    MsgSen TblVer  InQ   OutQ    Up/Down   State/
PfxRcd     AD  MACIP   MCAST    ESI
11.11.11.1                   4   200    24          26        3       0       0  00:08:31
1       0      0      1      0

Total number of neighbors 1

Total number of Established sessions 1
#show bgp l2vpn evpn
BGP table version is 3, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route

    Network          Next Hop            Metric    LocPrf      Weight Path   Peer

RD[100:11] VRF[vrf1]:
*>    [2]:[0]:[1]:[48,1212:1212:1212]:[0]:[1]
                         33.33.33.0          0         100          32768     i
*>    [3]:[1]:[32,33.33.33.0]
                         33.33.33.0          0         100          32768     i
*    [3]:[1]:[32,34.34.34.0]
                         34.34.34.0           0         100           0       200 300 i
11.11.11.1

RD[300:11]
*>    [3]:[1]:[32,34.34.34.0]
                         34.34.34.0          0         100           0       200 300 i
11.11.11.1

Total number of prefixes 4
#
#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default

IP Route Table for VRF "default"
C       11.11.11.0/31 is directly connected, xe37
C33.33.33.0/31 is directly connected, lo
```

```
B       34.34.34.0/31 [20/0] via 11.11.11.1, xe37, 00:02:47
C       127.0.0.0/8 is directly connected, lo

Gateway of last resort is not set
#
#show nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged
VNID     Type Interface    Vlan   Inner-Vlan Src-addr         Dst-addr
_____________________________________________________________________
1        NW    -----        ----       ----  33.33.33.0      34.34.34.0
1        AC   xe15           1000    2000    ----        ----
Total number of entries are 2
#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
=============================================================================
33.33.33.0 34.34.34.0 Installed 00:03:01 00:03:01 Total number of entries
are 1

#
#show nvo vxlan mac-table
=============================================================================
=
==
                  VXLAN MAC Entries
=============================================================================
=
==

VNID     Interface    VlanId  Inner-VlanId  Mac-Addr     VTEP-Ip      Type        Status
Time-out     AccessPortDesc
_____________________________________________________________________________
_
_____________________
1         xe15         1000    2000 1212.1212.1212 33.33.33.0 Dynamic Local    -----
300
Total number of entries are 1
```

RTR3/VTEP2

```
#show running-config  nvo vxlan
!
nvo  vxlan  enable
!
nvo vxlan vtep-ip-global
34.34.34.0 ! nvo vxlan id 1
ingress-replication
```

```
 vxlan host-reachability-protocol evpn-bgp vrf1 ! nvo
vxlan access-if port-vlan xe6 1000 inner-vlan 2000
no shutdown   map vnid 1 !
#show bgp l2vpn evpn summary
BGP router identifier 3.3.3.3, local AS number 300
BGP table version is 3
2 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V  AS    MsgRcv    MsgSen TblVer  InQ   OutQ    Up/Down   State/
PfxRcd      AD  MACIP  MCAST    ESI
12.12.12.1                4    200    19          19        3       0       0  00:05:31
2       0      1      1      0

Total number of neighbors 1

Total number of Established sessions 1

#show bgp l2vpn evpn
BGP table version is 3, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route

    Network          Next Hop            Metric    LocPrf       Weight Path   Peer

RD[100:11]
*>   [2]:[0]:[1]:[48,1212:1212:1212]:[0]:[1]
                       33.33.33.0           0         100            0       200 100 i
12.12.12.1
*>   [3]:[1]:[32,33.33.33.0]
                       33.33.33.0           0         100            0       200 100 i
12.12.12.1

RD[300:11] VRF[vrf1]:
*    [2]:[0]:[1]:[48,1212:1212:1212]:[0]:[1]
                      33.33.33.0           0         100            0       200 100 i
12.12.12.1
*    [3]:[1]:[32,33.33.33.0]
                       33.33.33.0           0         100            0       200  100 i
12.12.12.1
*>    [3]:[1]:[32,34.34.34.0]
                       34.34.34.0           0         100            32768   i
```

```
Total number of prefixes 5
#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default

IP Route Table for VRF "default"
C       12.12.12.0/31 is directly connected, xe13
B       33.33.33.0/31 [20/0] via 12.12.12.1, xe13, 00:05:33
C       34.34.34.0/31 is directly connected, lo
C       127.0.0.0/8 is directly connected, lo

Gateway of last resort is not set
#show nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged
VNID     Type Interface    Vlan   Inner-Vlan Src-addr         Dst-addr
_____________________________________________________________________
1        NW    -----        ----       ----  34.34.34.0      33.33.33.0
1        AC   xe6            1000    2000    ----        ----
Total number of entries are 2
#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
=============================================================================
34.34.34.0       33.33.33.0      Installed      00:05:31    00:05:31
Total number of entries are 1
#show nvo vxlan mac-table
=============================================================================
=
==
                  VXLAN MAC Entries
=============================================================================
=
==

VNID     Interface    VlanId  Inner-VlanId  Mac-Addr     VTEP-Ip      Type        Status
Time-out     AccessPortDesc
_____________________________________________________________________________
_
_____________________
1          ---         ---    ---    1212.1212.1212 33.33.33.0   Remote        -----
---
Total number of entries are 1
```

```
#
```

Popping SVLAN Tag

Use the previous configuration on VTEP1 and perform the configuration below on VTEP2.

VTEP2

(config)#nvo vxlan access-if port xe6	Enable port-only mapping for access port
(config-nvo-acc-if)#map vnid 1	Map VXLAN Identified to access-port for VXLAN
(config-nvo-acc-if)#exit	Exit VXLAN access-interface mode
(config)#exit	Exit configuration mode

RTR3/VTEP2

```
#show running-config  nvo vxlan
!
nvo  vxlan  enable
!
nvo vxlan vtep-ip-global
34.34.34.0 ! nvo vxlan id 1
ingress-replication
 vxlan host-reachability-protocol evpn-bgp
vrf1 ! nvo vxlan access-if port xe6  no
shutdown  map vnid 1 !
#show nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged
VNID     Type Interface    Vlan   Inner-Vlan Src-addr         Dst-addr
_____________________________________________________________________
1        NW    -----        ----       ----  34.34.34.0      33.33.33.0
1        AC   xe6           ALL    ----             ---Total
number of entries are 2

#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
=============================================================================
34.34.34.0       33.33.33.0      Installed      00:03:46    00:03:46
Total number of entries are 1
#show nvo vxlan mac-table
=============================================================================
=
==
                  VXLAN MAC Entries
=============================================================================
=
==
```

```
VNID     Interface    VlanId  Inner-VlanId  Mac-Addr      VTEP-Ip      Type        Status
Time-out     AccessPortDesc
_____________________________________________________________________________________
_
_____________________
1          ---          ---     ---     1212.1212.1212 33.33.33.0    Remote        -----
---
Total number of entries are 1
#
```

Popping and Later Pushing SVLAN Tag

Use the previous configuration on VTEP1 and perform the configuration below on VTEP2.

(config)#nvo vxlan access-if port-vlan xe6 3000 inner-vlan 2000	Enable port-vlan mapping i.e. access port to outer-vlan (SVLAN) and inner-vlan (CVLAN) mapping
(config-nvo-acc-if)#map vnid 1	Map VXLAN Identified to access-port for VXLAN
(config-nvo-acc-if)#exit	Exit VXLAN access-interface mode
(config)#exit	Exit configuration mode

RTR3/VTEP2

```
#show  running-config  nvo  vxlan
!
nvo  vxlan  enable
!
nvo vxlan vtep-ip-global 34.34.34.0
! nvo vxlan id 1
ingress-replication
 vxlan host-reachability-protocol evpn-bgp vrf1 ! nvo
vxlan access-if port-vlan xe6 3000 inner-vlan 2000 no
shutdown map vnid 1 !
#show nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
           AC - Access Port
          (u) - Untagged
VNID     Type Interface    Vlan   Inner-Vlan Src-addr         Dst-addr
_____________________________________________________________________
1        NW    -----        ----       ----  34.34.34.0      33.33.33.0
1        AC   xe6            3000    2000    ----        ----
Total number of entries are 2

#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
=============================================================================
34.34.34.0       33.33.33.0      Installed     00:06:48    00:06:48 Total
number of entries are 1
```

```
#show nvo vxlan mac-table
================================================================================
=
==
                  VXLAN MAC Entries
================================================================================
= ==
VNID      Interface    VlanId  Inner-VlanId  Mac-Addr      VTEP-Ip      Type        Status
Time-out     AccessPortDesc
________________________________________________________________________________
_
_____________________
1          ---          ---     ---     1212.1212.1212 33.33.33.0    Remote        -----
---
Total number of entries are 1
#
```

CHAPTER 7 VXLAN Hybrid Access Port Configuration

This chapter shows how to configure a hybrid access port which is a Layer 2 Port (configured switchport) that is part of both a VXLAN domain and a Layer 2 bridge with different VLANs.

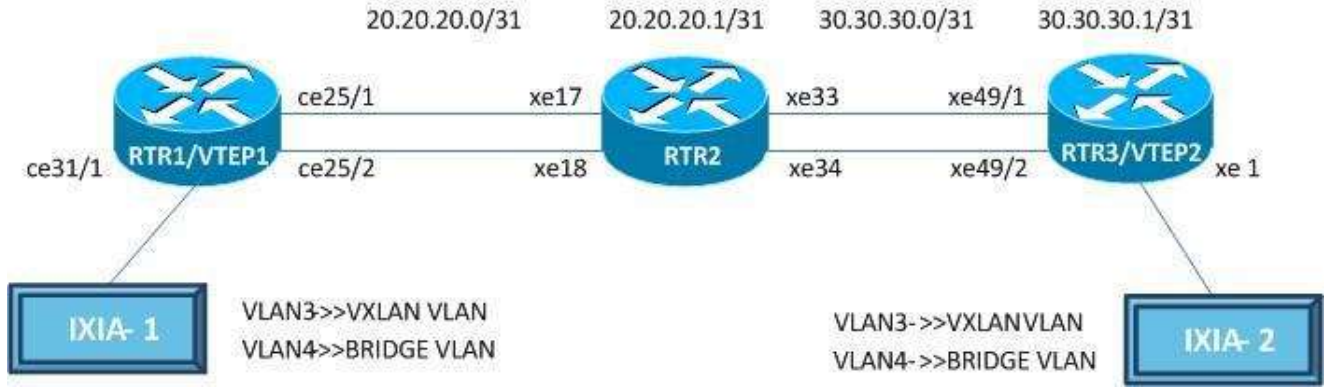
Overview

A hybrid VXLAN access port is Layer 2 port that is part of regular Layer 2 bridge (RSTP/MSTP/STP) and a VXLAN bridge at the same time. A switchport cannot be a part of VXLAN domain and Layer 2 Bridge if the VXLAN port is created with “port only” mapping. The same VLAN cannot be a part of both a VXLAN domain and a Layer 2 bridge.

If a port is created with “all” VLANS, then the port should not allow VXLAN access-port configurations. If a VXLAN with a specific VLAN is mapped, then configuring VLAN “all” on the same port does not allow that specified VLAN in a Layer 2 bridge. If the VXLAN access-port configurations are removed, then the specified VLAN is added immediately in a Layer 2 bridge.

Ingress traffic with a VXLAN VLAN does not receive Layer 2 traffic or vice-versa. STP states on the Port P1 do not affect VXLAN traffic.

Topology



RTR1/VTEP1

`#configure terminal`	Enter Configure mode.
`(config)#interface lo`	Enter Interface mode for loopback.
`(config-if)#ip address 10.10.10.10/32 secondary`	Assign secondary IP address.
`(config-if)#exit`	Exit Interface mode.
`(config)#mac vrf vrf12345`	Create mac routing/forwarding instance with vrf12345 name and enter VRF mode.
`(config-vrf)#rd 1.1.1.1:1`	Assign Rd value.
`(config-vrf)#route-target both 10.10.10.10:10`	Assign route-target both value.
`(config-vrf)#exit`	Exit VRF configuration mode.

(config)#bridge 32 protocol ieee vlan-bridge	Configure the ieee vlan-bridge with Id 32.
(config)#vlan 2-5 bridge 32	Configure the vlans 2-5 for the configured bridge Id 32.
(config)#interface ce25/1	Enter Interface mode for ce25/1.
(config-if)#ip address 20.20.20.0/31	Assign IP address 20.20.20.0 in /31 mask.
(config-if)#exit	Exit Interface mode.
(config)#interface ce25/2	Enter Interface mode for ce25/2.
(config-if)#switchport	Make it L2 interface.
(config-if)#bridge-group 32	Associate the bridge-group 32 to the interface.
(config-if)#switchport mode hybrid	Configure the Hybrid mode.
(config-if)# switchport hybrid allowed vlan add 4 egress-tagged enable	Configure hybrid allowed vlan add 4 to support the created vlan in the L2 Bridge.
(config-if)#exit	Exit Interface mode.
(config)#interface ce31/1	Enter Interface mode for ce31/1.
(config-if)#switchport	Make it L2 interface.
(config-if)#bridge-group 32	Associate the bridge-group 32 to the interface.
(config-if)#switchport mode hybrid	Configure the Hybrid mode.
(config-if)# switchport hybrid allowed vlan all add 4 egress-tagged enable	Configure hybrid allowed vlan add 4 to support the created vlan in the L2 Bridge.
(config-if)#exit	Exit Interface mode.
(config)#router bgp 64512	Enter BGP router mode.
(config-router)# network 10.10.10.10/32	Advertise the loopback network to learn the Vtep-ip in Bgp table.
(config-router)#neighbor 20.20.20.1 remoteas 64513	Specify a neighbor router with peer ip address and remote-as defined.
(config-router)#address-family l2vpn evpn	Enter l2vpn address family mode.
(config-router-af)#neighbor 20.20.20.1 activate	Activate the peer into address family mode.
(config-router-af)#exit-address-family	Exit l2vpn address family mode.
(config-router)#exit	Exit BGP router mode.
(config)#nvo vxlan enable	Enable Vxlan.
(config)#nvo vxlan vtep-ip-global 10.10.10.10	Configure the source Vtep-ip.
(config)#nvo vxlan id 16777215 ingressreplication inner-vid-disabled	Configure Vxlan Network identifier with/without inner-viddisabled configure and enter Vxlan tenant mode.
(config-nvo)#vxlan host-reachabilityprotocol evpn-bgp vrf12345	Assign VRF for evpn-bgp to carry evpn route.
(config-nvo)#exit	Exit Vxlan tenant mode.
(config)#nvo vxlan access-if port-vlan ce31/ 1 3	Enable port-vlan mapping i.e. access port to outer-vlan (SVLAN) mapping.

(config-nvo-acc-if)#map vnid 16777215	Map Vxlan Identifier to access-port.
(config-nvo-acc-if)#exit	Exit Vxlan access-interface mode.

RTR2

#configure terminal	Enter Configure mode.
(config)#bridge 32 protocol ieee vlan-bridge	Configure the ieee vlan-bridge with Id 32.
(config)#vlan 2-5 bridge 32	Configure the vlans 2-5 for the configured bridge Id 32.
(config)#interface xe17	Enter Interface mode for xe17.
(config-if)#ip address 20.20.20.1/31	Assign IP address 20.20.20.1 in /31 mask.
(config-if)#exit	Exit Interface mode.
(config)#interface xe18	Enter Interface mode for xe18.
(config-if)#switchport	Make it L2 interface .
(config-if)#bridge-group 32	Associate the bridge-group 32 to the interface.
(config-if)#switchport mode hybrid	Configure the Hybrid mode.
(config-if)#switchport hybrid allowed vlan all add 4 egress-tagged enable	Configure hybrid allowed vlan add 4 to support the created vlan in the L2 Bridge.
(config-if)#exit	Exit Interface mode.
(config)#interface xe33	Enter Interface mode for xe33.
(config-if)#ip address 30.30.30.0/31	Assign IP address 30.30.30.0 in /31 mask.
(config-if)#exit	Exit Interface mode.
(config)#interface xe34	Enter Interface mode for xe34.
(config-if)#switchport	Make it L2 interface.
(config-if)#bridge-group 32	Associate the bridge-group 32 to the interface.
(config-if)#switchport mode hybrid	Configure the Hybrid mode.
(config-if)#switchport hybrid allowed vlan add 4 egress-tagged enable	Configure hybrid allowed vlan add 4 to support the created vlan in the L2 Bridge.
(config-if)#exit	Exit Interface mode.
(config)#router bgp 64513	Enter BGP router mode.
(config-router)#neighbor 20.20.20.0 remoteas 64512	Specify a neighbor router with peer ip address and remote-as defined.
(config-router)#neighbor 30.30.30.1 remoteas 64514	Specify a neighbor router with peer ip address and remote-as defined.
(config-router)#address-family l2vpn evpn	Enter l2vpn address family mode.
(config-router-af)#neighbor 20.20.20.0 activate	Activate the peer into address family mode.
(config-router-af)#neighbor 30.30.30.1 activate	Activate the peer into address family mode.
(config-router-af)#exit-address-family	Exit l2vpn address family mode.
(config-router)#exit	Exit BGP router mode.

RTR3/VTEP2

#configure terminal	Enter Configure mode.
(config)#interface lo	Enter Interface mode for loopback.
(config-if)#ip address 40.40.40.40/32 secondary	Assign secondary IP address.
(config-if)#exit	Exit Interface mode.
(config)#mac vrf vrf12345	Create mac routing/forwarding instance with vrf12345 name and enter VRF mode.
(config-vrf)#rd 2.2.2.2:2	Assign Rd value.

(config-vrf)#route-target both 10.10.10.10:10	Assign route-target both value.
(config-vrf)#exit	Exit VRF configuration mode.
(config)#bridge 32 protocol ieee vlan-bridge	Configure the ieee vlan-bridge with Id 32.
(config)#vlan 2-5 bridge 32	Configure the vlans 2-5 for the configured bridge Id 32.
(config)#interface xe 49/1	Enter Interface mode for xe49/1.
(config-if)#ip address 30.30.30.1/31	Assign Ip address 30.30.30.1 in /31 mask.
(config-if)#exit	Exit Interface mode.
(config)#interface xe49/2	Enter Interface mode for xe49/2.
(config-if)#switchport	Make it L2 interface .
(config-if)#bridge-group 32	Associate the bridge-group 32 to the interface.
(config-if)#switchport mode hybrid	Configure the Hybrid mode.
(config-if)#switchport hybrid allowed vlan add 4 egress-tagged enable	Configure hybrid allowed vlan add 4 to support the created vlan in the L2 Bridge.
(config-if)#exit	Exit Interface mode.
(config)#interface xe1	Enter Interface mode for xe1.
(config-if)#switchport	Make it L2 interface .
(config-if)#bridge-group 32	Associate the bridge-group 32 to the interface.
(config-if)#switchport mode hybrid	Configure the Hybrid mode.
(config-if)#switchport hybrid allowed vlan add 4 egress-tagged enable	Configure hybrid allowed vlan add 4 to support the created vlan in the L2 Bridge.
(config-if)#exit	Exit Interface mode.
(config)#router bgp 64514	Enter BGP router mode.
(config-router)# network 40.40.40.40/32	Advertise the loopback network to learn the Vtep-ip in Bgp table.
(config-router)#neighbor 30.30.30.0 remoteas 64513	Specify a neighbor router with peer IP address and remote-as defined.
(config-router)#address-family l2vpn evpn	Enter l2vpn address family mode.
(config-router-af)#neighbor 30.30.30.0 activate	Activate the peer into address family mode.
(config-router-af)#exit-address-family	Exit l2vpn address family mode.

(config-router)#exit	Exit BGP router mode.
(config)#nvo vxlan enable	Enable Vxlan.
(config)#nvo vxlan vtep-ip-global 40.40.40.40	Configure the source Vtep-ip.
(config)#nvo vxlan id 16777215 ingressreplication inner-vid-disabled	Configure Vxlan Network identifier with/without inner-viddisabled configure and enter Vxlan tenant mode.
(config-nvo)#vxlan host-reachabilityprotocol evpn-bgp vrf12345	Assign VRF for evpn-bgp to carry evpn route.
(config-nvo)#exit	Exit Vxlan tenant mode.
(config)#nvo vxlan access-if port-vlan xe1 3	Enable port-vlan mapping i.e. access port to outer-vlan (SVLAN) mapping.
(config-nvo-acc-if)#map vnid 16777215	Map Vxlan Identifier to access-port.
(config-nvo-acc-if)#exit	Exit Vxlan access-interface mode.

Validation

VTEP1

```
#show running-config nvo vxlan !
nvo vxlan enable !
nvo vxlan vtep-ip-global 10.10.10.10 ! nvo vxlan id 16777215 ingress-
replication inner-vid-disabled  vxlan host-reachability-protocol
evpn-bgp vrf12345 ! nvo vxlan access-if port-vlan ce31/1 3  no
shutdown  map vnid 16777215 !
#show nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged
VNID     Type Interface    Vlan   Inner-Vlan Src-addr          Dst-addr
_____________________________________________________________________
16777215 NW     -----       ----        ---- 10.10.10.10      40.40.40.40
16777215 AC    ce31/1         3      ----    ----         ----
Total number of entries are 2

#show nvo vxlan vnid 16777215
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged
VNID     Type Interface    Vlan   Inner-Vlan Src-addr          Dst-addr
_____________________________________________________________________
16777215 NW     -----       ----        ---- 10.10.10.10      40.40.40.40
16777215 AC    ce31/1         3       ----     ----         ----          Total number
of entries are 2
```

```
#show nvo vxlan access-if-config nvo vxlan
access-if port-vlan ce31/1 3 no shutdown map
vnid 16777215 !
#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default

IP Route Table for VRF "default"
C       10.10.10.10/32 is directly connected, lo
C       20.20.20.0/31 is directly connected, ce25/1
B       40.40.40.40/32 [20/0] via 20.20.20.1, ce25/1, 00:06:08
C       127.0.0.0/8 is directly connected, lo

Gateway of last resort is not set

#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================
10.10.10.10       40.40.40.40     Installed      00:08:06    00:08:06
Total number of entries are 1

#show bgp l2vpn evpn summary
BGP router identifier 10.10.10.10, local AS number 64512
BGP table version is 5
3 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer  InQ   OutQ    Up/Down   State/
PfxRcd      AD  MACIP  MCAST    ESI
20.20.20.1                4  64513    29          34        5       0       0  00:11:52
1       0      0      1      0

Total number of neighbors 1

Total number of Established sessions 1

#show bgp l2vpn evpn
BGP table version is 5, local router ID is 10.10.10.10
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
1 - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
```

```
3 - Inclusive Multicast Route
4 - Ethernet Segment Route

    Network          Next Hop            Metric    LocPrf Weight Path  Peer

RD[1.1.1.1:1] VRF[vrf12345]:
*>   [2]:[0]:[16777215]:[48,0000:0034:5678]:[0]:[16777215]
                        10.10.10.10         0         100            32768   i
*>   [2]:[0]:[16777215]:[48,0000:0034:5678]:[32,7.7.7.1]:[16777215]
                        10.10.10.10         0         100            32768   i
*>   [3]:[16777215]:[32,10.10.10.10]
                        10.10.10.10         0         100            32768   i
*    [3]:[16777215]:[32,40.40.40.40]
                        40.40.40.40          0         100            0      64513 64514
i  20.20.20.1

RD[2.2.2.2:2]
*>   [3]:[16777215]:[32,40.40.40.40]
                        40.40.40.40          0         100            0      64513 64514
i  20.20.20.1

Total number of prefixes 5

#show nvo vxlan mac-table
=============================================================================================
=
==
                  VXLAN MAC Entries
=============================================================================================
=
==

VNID     Interface    VlanId  Inner-VlanId  Mac-Addr      VTEP-Ip      Type        Status
Time-out     AccessPortDesc
_____________________________________________________________________________________________
_
_____________________
16777215  ce31/1      3       ---    0000.0034.5678 10.10.10.10 Dynamic Local    -----
300
Total number of entries are 1

#show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
VNID     Ip-Addr          Mac-Addr       Type
_____________________________________________________
16777215 7.7.7.1          0000.0034.5678 Dynamic
Total number of entries are 1
#show vlan brief
Bridge   VLAN ID    Name         State   H/W Status      Member ports
                                                      (u)-Untagged, (t)-Tagged
```

```
======= =======   ================ ======= ========== ========================
32      1         default          ACTIVE  Up         ce25/2(u) ce31/1(u)
32      2        VLAN0002          ACTIVE  Up         ce25/2(t) ce31/1(t)
32      3        VLAN0003          ACTIVE  Up         ce25/2(t)
32      4        VLAN0004          ACTIVE   Up         ce25/2(t) ce31/1(t)
32      5        VLAN0005          ACTIVE  Up         ce25/2(t) ce31/1(t)
#show bridge
```

Ageout time is global and if something is configured for vxlan then it will be affected here also

```
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 --------  +------ +------+------+-----------+---------------     +-----+--------- +
 32        1                    ce31/2       3417.ebd6.2dd1     1      300       32
4                    ce31/2       0000.0500.0000    1      300
```

RTR2

```
#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default

IP Route Table for VRF "default"
B       10.10.10.10/32 [20/0] via 20.20.20.0, xe17, 00:09:58
C       20.20.20.0/31 is directly connected, xe17
C       30.30.30.0/31 is directly connected, xe33
B       40.40.40.40/32 [20/0] via 30.30.30.1, xe33, 00:07:03
C       127.0.0.0/8 is directly connected, lo

#show bgp l2vpn evpn summary
BGP router identifier 20.20.20.1, local AS number 64513
BGP table version is 7
3 BGP AS-PATH entries
0      BGP community entries

Neighbor                V   AS    MsgRcv   MsgSen TblVer   InQ   OutQ    Up/Down   State/
PfxRcd     AD  MACIP  MCAST    ESI
30.30.30.1                4 64514   18          24        7      0      0   00:07:23
1      0       0     1      0
20.20.20.0                 4  64512    29          26        7       0       0  00:10:22
3      2       0     0      2       0

Total number of neighbors 2

Total number of Established sessions 2

#show vlan brief
Bridge  VLAN ID     Name         State   H/W Status      Member ports
                                                        (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ========================
```

```
32       1      default          ACTIVE  Up         xe18(u) xe34(u)
32        2       VLAN0002          ACTIVE   Up
32       3      VLAN0003         ACTIVE  Up
32       4      VLAN0004         ACTIVE  Up         xe18(t) xe34(t)
32       5      VLAN0005         ACTIVE  Up

#show bridge
```

Ageout time is global and if something is configured for vxlan then it will be affected here also

```
 Bridge    CVLAN  SVLAN  BVLAN   Port        MAC Address         FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 32         1                    xe18        cc37.ab27.5aea     1      300  32        4
xe18         0000.0500.0000    1      300
```

VTEP2

```
#show running-config nvo vxlan !
nvo vxlan enable !
nvo vxlan vtep-ip-global 40.40.40.40 ! nvo vxlan id 16777215 ingress-
replication inner-vid-disabled vxlan host-reachability-protocol evpn-bgp
vrf12345 ! nvo vxlan access-if port-vlan xe1 3  no shutdown  map vnid
16777215 !

#show nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged
VNID     Type Interface     Vlan  Inner-Vlan Src-addr         Dst-addr
_____________________________________________________________________
16777215 NW     -----        ----      ----  40.40.40.40     10.10.10.10
16777215 AC    xe1            3     ----     ----         ----
Total number of entries are 2

#show nvo vxlan vnid 16777215
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged
VNID     Type Interface     Vlan  Inner-Vlan Src-addr         Dst-addr
_____________________________________________________________________
16777215 NW     -----        ----      ----  40.40.40.40     10.10.10.10
16777215 AC    xe1             3      ----      ----        ---Total number of
entries are 2

#show nvo vxlan access-if-config nvo vxlan
access-if port-vlan xe1 3 no shutdown map vnid
16777215 !
```

```
#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default

IP Route Table for VRF "default"
B       10.10.10.10/32 [20/0] via 30.30.30.0, xe49/1, 00:06:16
C       30.30.30.0/31 is directly connected, xe49/1
C       40.40.40.40/32 is directly connected, lo
C127.0.0.0/8 is directly connected, lo

Gateway of last resort is not set

#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source            Destination     Status           Up/Down        Update
================================================================================
====
40.40.40.40       10.10.10.10     Installed      00:10:23     00:10:23
Total number of entries are 1
#show bgp l2vpn evpn summary
BGP router identifier 40.40.40.40, local AS number 64514
BGP table version is 5
3 BGP AS-PATH entries
0 BGP community entries

Neighbor                 V   AS   MsgRcv    MsgSen TblVer  InQ   OutQ    Up/Down   State/
 PfxRcd      AD  MACIP  MCAST    ESI
30.30.30.0                4  64513    21          16        5       0       0  00:06:11
2       0      0      2      0

Total number of neighbors 1

Total number of Established sessions 1

#show bgp l2vpn evpn
BGP table version is 6, local router ID is 40.40.40.40
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route

    Network          Next Hop            Metric    LocPrf       Weight Path  Peer
```

```
RD[1.1.1.1:1]
*>   [2]:[0]:[16777215]:[48,0000:0034:5678]:[0]:[16777215]
                        10.10.10.10          0         100            0       64513 64512
i   30.30.30.0
*>   [2]:[0]:[16777215]:[48,0000:0034:5678]:[32,7.7.7.1]:[16777215]
                        10.10.10.10          0         100            0       64513 64512
i   30.30.30.0
*>   [3]:[16777215]:[32,10.10.10.10]
                        10.10.10.10          0         100            0       64513 64512
i   30.30.30.0

RD[2.2.2.2:2] VRF[vrf12345]:
*    [2]:[0]:[16777215]:[48,0000:0034:5678]:[0]:[16777215]
                       10.10.10.10          0         100            0       64513 64512
i  30.30.30.0
*    [2]:[0]:[16777215]:[48,0000:0034:5678]:[32,7.7.7.1]:[16777215]
                        10.10.10.10          0         100            0       64513 64512
i   30.30.30.0
*     [3]:[16777215]:[32,10.10.10.10]
                        10.10.10.10          0         100            0       64513 64512
i   30.30.30.0
*>    [3]:[16777215]:[32,40.40.40.40]
                        40.40.40.40          0         100            32768   i

Total number of prefixes 7

#show nvo vxlan mac-table
================================================================================
=
==
                  VXLAN MAC Entries
================================================================================
=
==

VNID     Interface    VlanId  Inner-VlanId  Mac-Addr      VTEP-Ip      Type        Status
Time-out     AccessPortDesc

--------------------------------------------------------------------------------
-
-------------------------
16777215   ---         ---     ---    0000.0034.5678 10.10.10.10   Remote        -----
---
Total number of entries are 1

#show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
VNID      Ip-Addr         Mac-Addr        Type

-------------------------------------------------------
16777215 7.7.7.1          0000.0034.5678 Evpn Dynamic

#show vlan brief
```

```
Bridge  VLAN ID      Name         State   H/W Status      Member ports
                                                          (u)-Untagged, (t)-Tagged
======= ======= ================ ======= ========== ==========================
32      1        default         ACTIVE  Up         xe1(u) xe49/2(u)
32      2        VLAN0002        ACTIVE  Up         xe1(t) xe49/2(t)
32      3        VLAN0003        ACTIVE  Up         xe49/2(t)
32      4        VLAN0004        ACTIVE  Up         xe1(t) xe49/2(t)
32      5        VLAN0005        ACTIVE  Up         xe1(t) xe49/2(t)

#show bridge
```

Ageout time is global and if something is configured for vxlan then it will be affected here also

```
 Bridge    CVLAN  SVLAN  BVLAN  Port         MAC Address        FWD   Time-out
 ---------+------+------+------+-----------+-----------------+-----+---------+
 32        1                    xe49/2      3417.eba8.54e7    1     300  32        4
xe49/2      0000.0500.0000    1     300
```

CHAPTER 8 VXLAN Multi-homing Configuration

This chapter contains the configurations for VXLAN Multi-homing feature.

Overview

VXLAN EVPN Multi-homing features enables to connect a CE/Host node to two VTEPs with all-active redundancy mode.EVPN Multi-homing helps in VTEP to host failure and VTEP failure. If one VTEP goes down, other will forward the entire traffic.

Below are Multi-homing concepts:

- Ethernet Segment: Set of links which connect host/CE to two active-active multi-homed VTEP (only two VTEPs are supported) which appears as LACP link for host.
- Ethernet Segment Identifier: Ethernet Segment Identifier (ESI) which is an 10 octet-value, which can be configured in two ways, system mac is configured as esi in case of Dynamic Lag and 10-octet ESI format config is used on physical interface ES.
- Ethernet Segment Route (ES route): When a multi-homed CE is configured as an VXLAN access-port, Ethernet segment route is sent. The main purpose of this route is to discover other VTEPs which share the ES and to perform DF election.
- Ethernet A-D route per ESI: This route is used for Fast Convergence and Split Horizon.
- Ethernet A-D route per EVI: This route is used for load sharing between DF and NON-DF by the remote VTEPs

Topology

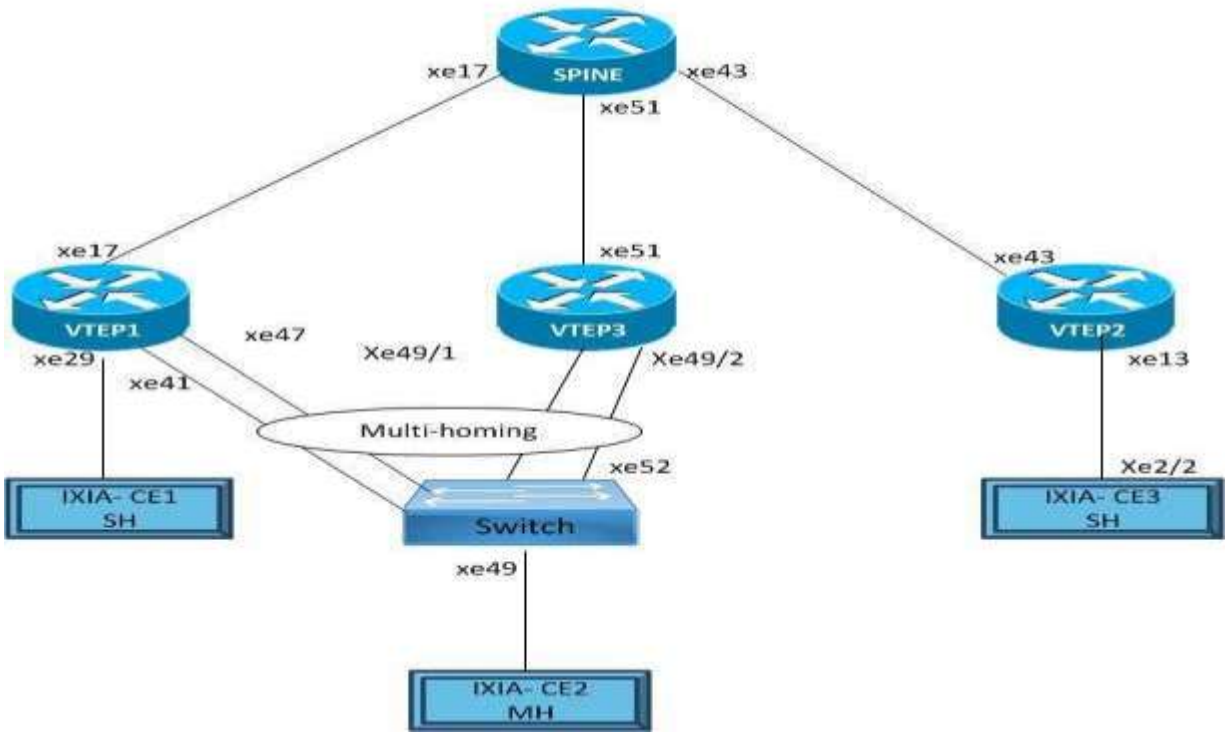


Figure 8-244: VxLAN-Multihoming

Configurations

VXLAN-EVPN MH Configuration

ESI can be configured in below two ways

Ethernet Segment through Dynamic Lag interface

`#configure terminal`	Enter Configure mode.
`(config)#interface po1`	Enter Interface mode for po1
`(config-if)#switchport`	Make it L2 interface
`(config-if)#evpn multi-homed system-mac 8899.4400.6745`	Configure system mac as ESI value for Lag (po1) interface
`(config-if)#exit`	Exit Interface mode.

OR

Ethernet Segment through Physical interface

`#configure terminal`	Enter Configure mode.
`(config)#interface xe41`	Enter Interface mode for xe41
`(config-if)#switchport`	Make it L2 interface
`(config-if)# evpn multi-homed esi 00:01:02:03:04:05:06:07:08`	Configure 9-octet ESI value for xe41 interface (in static config, out of 10-octet ESI value, first octet is reserved)
`(config-if)#exit`	Exit Interface mode.

VTEP1 (Multi-homed group1) – Part of both Multi-homed with po1 and single homed with xe29 as access-ports respectively

`#configure terminal`	Enter Configure mode.
`(config)#evpn multihoming enable`	Enable Multihoming, save configs and reboot the board for multihoming to be effective
`(config)#interface lo`	Enter Interface mode for loopback.
`(config-if)#ip address 27.27.27.27/32 secondary`	Assign secondary IP address.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#mac vrf vrf1`	Create mac routing/forwarding instance with vrf1 name and enter into vrf mode
`(config-vrf)# rd 1:100`	Assign RD value
`(config-vrf)# route-target export 1:1000`	Assign route-target value for export
`(config-vrf)# route-target import 1:1000`	Assign route-target value for import
`(config-vrf)#exit`	Exit from vrf configuration mode
`(config)#mac vrf evpn-gvrf-1`	Create global vrf for every 200 mac-vrf for exchange of Ethernet AD per ES and ES routes

(config-vrf)# rd 2:1	Assign route-distinguisher with unique value (No need to configure route-target, auto ES-import RT is used to get ES routes)
(config-vrf)#exit	Exit from vrf configuration mode
(config)#interface xe7	Enter Interface mode for xe7.
(config-if)#ip address 10.10.1.0/31	Assign IP address in /31 mask.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface po1	Enter Interface mode for po1
(config-if)#switchport	Make it L2 interface
(config-if)#evpn multi-homed system-mac 8899.4400.6745	Configure system mac as ESI value for Lag (po1) interface
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe41	Enter Interface mode for xe41
(config-if)#channel-group 1 mode active	Make it member port of po1
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe47	Enter Interface mode for xe47
(config-if)#channel-group 1 mode active	Make it member port of po1
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe29	Enter Interface mode for xe29
(config-if)#switchport	Make it L2 interface
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router bgp 100	Enter into Router BGP mode
(config-router)#network 27.27.27.27/32	Advertise loopback network into BGP for VTEP ID reachability
(config-router)#neighbor 10.10.1.1 remote-as 400	Specify a neighbor router with peer ip address and remote-as defined
(config-router)#neighbor 10.10.1.1 fall-over bfd	Configure single-hop BFD session for its BGP peer
(config-router)#address-family l2vpn evpn	Enter into l2vpn EVPN address family mode
(config-router-af)#neighbor 10.10.1.1 activate	Activate the peer into address family mode
(config-router-af)#exit-address-family	Exit from l2vpn address family mode
(config-router)#exit	Exit from Router BGP mode and enter into config mode
(config)#nvo vxlan enable	Enable VXLAN
(config)#evpn esi hold-time 50	Configure ESI holdtime to allow tunnel to come up at the time of vxlan initialization before making the ESI up
(config)#nvo vxlan vtep-ip-global 27.27.27.27	Configure Source vtep-ip-global configuration
(config)# nvo vxlan id 2 ingress-replication inner-vid-disabled	Configure VXLAN Network identifier with/without inner-viddisabled configure and enter into VXLAN tenant mode

(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf1	Assign vrf for evpn-bgp to carry EVPN route
(config-nvo)#exit	Exit from VXLAN tenant mode and enter into configuration mode.
(config)#nvo vxlan access-if port-vlan po1 2	Enable port-vlan mapping i.e. access port to outer-vlan (SVLAN) – Multihomed access port
(config-nvo-acc-if)#map vnid 2	Map VXLAN Identified to access-port for VXLAN
(config-nvo-acc-if)#exit	Exit from VXLAN access-interface mode and enter into configuration mode
(config)#nvo vxlan access-if port-vlan xe29 2	Enable port-vlan mapping i.e. access port to outer-vlan (SVLAN) – Multihomed access port
(config-nvo-acc-if)#map vnid 2	Map VXLAN Identified to access-port for VXLAN
(config-nvo-acc-if)#exit	Exit from VXLAN access-interface mode and enter into configuration mode
(config)#exit	Exit from configuration mode

VTEP2 (Multi-homed group1) – Part of both Multi-homed with po1

#configure terminal	Enter Configure mode.
(config)#evpn multihoming enable	Enable Multihoming, save configs and reboot the board for multihoming to be effective
(config)#interface lo	Enter Interface mode for loopback.
(config-if)#ip address 31.31.31.31/32 secondary	Assign secondary IP address.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#mac vrf vrf1	Create mac routing/forwarding instance with vrf1 name and enter into vrf mode
(config-vrf)# rd 1:200	Assign RD value
(config-vrf)# route-target export 1:1000	Assign route-target value for export
(config-vrf)# route-target import 1:1000	Assign route-target value for import
(config-vrf)#exit	Exit from vrf configuration mode
(config)#mac vrf evpn-gvrf-1	Create global vrf for every 200 mac-vrf for exchange of Ethernet AD per ES and ES routes

(config-vrf)# rd 2:2	Assign route-distinguisher with unique value (No need to configure route-target, auto ES-import RT is used to get ES routes)
(config-vrf)#exit	Exit from vrf configuration mode
(config)#interface xe51/1	Enter Interface mode for xe51/1
(config-if)#ip address 10.10.2.0/31	Assign IP address in /31 mask.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface po1	Enter Interface mode for po1
(config-if)#switchport	Make it L2 interface

(config-if)#evpn multi-homed system-mac 8899.4400.6745	Configure system mac as ESI value for Lag (po1) interface
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe49/1	Enter Interface mode for xe49/1
(config-if)#channel-group 1 mode active	Make it member port of po1
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe49/2	Enter Interface mode for xe49/2
(config-if)#channel-group 1 mode active	Make it member port of po1
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router bgp 100	Enter into Router BGP mode
(config-router)#network 31.31.31.31/32	Advertise loopback network into BGP for VTEP ID reachability
(config-router)#neighbor 10.10.2.1 remote-as 400	Specify a neighbor router with peer ip address and remote-as defined
(config-router)#neighbor 10.10.2.1 fall-over bfd	Configure single-hop BFD session for its BGP peer
(config-router)#address-family l2vpn evpn	Enter into l2vpn address family mode
(config-router-af)#neighbor 10.10.2.1 activate	Activate the peer into address family mode
(config-router-af)#exit-address-family	Exit from l2vpn address family mode
(config-router)#exit	Exit from Router BGP mode and enter into config mode
(config)#nvo vxlan enable	Enable VXLAN
(config)#evpn esi hold-time 50	Configure esi holdtime to allow tunnel to come up at the time of vxlan initialization before making the ESI up
(config)#nvo vxlan vtep-ip-global 31.31.31.31	Configure Source vtep-ip-global configuration
(config)# nvo vxlan id 2 ingress-replication inner-vid-disabled	Configure VXLAN Network identifier with/without inner-viddisabled configure and enter into VXLAN tenant mode
(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf1	Assign vrf for evpn-bgp to carry EVPN route
(config-nvo)#exit	Exit from VXLAN tenant mode and enter into configuration mode.
(config)#nvo vxlan access-if port-vlan po1 2	Enable port-vlan mapping i.e. access port to outer-vlan (SVLAN) and inner-vlan (CVLAN) mapping
(config-nvo-acc-if)#map vnid 2	Map VXLAN Identified to access-port for VXLAN
(config-nvo-acc-if)#exit	Exit from VXLAN access-interface mode and enter into configuration mode
(config)#exit	Exit from configuration mode
VTEP3 Single homed VTEP	
#configure terminal	Enter Configure mode.
(config)#evpn multihoming enable	Enable Multihoming, save configs and reboot the board for multihoming to be effective

(config)#interface lo	Enter Interface mode for loopback.
(config-if)#ip address 32.32.32.32/32 secondary	Assign secondary IP address.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#mac vrf vrf1	Create mac routing/forwarding instance with vrf1 name and enter into vrf mode
(config-vrf)#rd 1:300	Assign RD value
(config-vrf)#route-target export 1:1000	Assign route-target value for export
(config-vrf)#route-target import 1:1000	Assign route-target value for import
(config-vrf)#exit	Exit from vrf configuration mode
(config)#interface xe43	Enter Interface mode for xe43
(config-if)#ip address 10.10.3.0/31	Assign IP address in /31 mask.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe13	Enter Interface mode for xe13
(config-if)#switchport	Make it L2 interface
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router bgp 300	Enter into Router BGP mode
(config-router)#network 32.32.32.32/32	Advertise loopback network into BGP for VTEP ID reachability
(config-router)#neighbor 10.10.3.1 remote-as 400	Specify a neighbor router with peer ip address and remote-as defined
(config-router)#neighbor 10.10.3.1 fall-over bfd	Configure single-hop BFD session for its BGP peer
(config-router)#address-family l2vpn evpn	Enter into l2vpn address family mode
(config-router-af)#neighbor 10.10.3.1 activate	Activate the peer into address family mode
(config-router-af)#exit-address-family	Exit from l2vpn address family mode
(config-router)#exit	Exit from Router BGP mode and enter into config mode
(config)#nvo vxlan enable	Enable VXLAN
(config)#nvo vxlan vtep-ip-global 32.32.32.32	Configure Source vtep-ip-global configuration
(config)#nvo vxlan id 2 ingress-replication inner-vid-disabled	Configure VXLAN Network identifier with/without inner-viddisabled configure and enter into VXLAN tenant mode
(config-nvo)#vxlan host-reachability-protocol evpn-bgp vrf1	Assign vrf for evpn-bgp to carry EVPN route
(config-nvo)#exit	Exit from VXLAN tenant mode and enter into configuration mode.
(config)#nvo vxlan access-if port-vlan xe13 2	Enable port-vlan mapping i.e. access port to outer-vlan (SVLAN) and inner-vlan (CVLAN) mapping
(config-nvo-acc-if)#map vnid 2	Map VXLAN Identified to access-port for VXLAN
(config-nvo-acc-if)#exit	Exit from VXLAN access-interface mode and enter into configuration mode

(config)#exit	Exit from configuration mode

Spine-Spine node where all VTEPs are connected

#configure terminal	Enter Configure mode.
(config)#interface lo	Enter Interface mode for loopback.
(config-if)#ip address 25.25.25.25/32 secondary	Assign secondary IP address.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe7	Enter Interface mode for xe7
(config-if)#ip address 10.10.1.1/31	Assign IP address in /31 mask.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe51/1	Enter Interface mode for xe51/1
(config-if)#ip address 10.10.2.1/31	Assign IP address in /31 mask.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe43	Enter Interface mode for xe43
(config-if)#ip address 10.10.3.1/31	Assign IP address in /31 mask.
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#router bgp 400	Enter into Router BGP mode
(config-router)#network 25.25.25.25/32	Advertise loopback network into BGP for VTEP ID reachability
(config-router)#neighbor 10.10.1.0 remote-as 100	Specify a neighbor router with peer ip address and remote-as defined
(config-router)#neighbor 10.10.1.0 fall-over peer bfd	Configure single-hop BFD session for its BGP
(config-router)#neighbor 10.10.2.0 remote-as 200	Specify a neighbor router with peer ip address and remote-as defined
(config-router)#neighbor 10.10.2.0 fall-over peer bfd	Configure single-hop BFD session for its BGP
(config-router)#neighbor 10.10.3.0 remote-as 300	Specify a neighbor router with peer ip address and remote-as defined
(config-router)#neighbor 10.10.3.0 fall-over peer bfd	Configure single-hop BFD session for its BGP
(config-router)#address-family l2vpn evpn	Enter into l2vpn address family mode
(config-router-af)#neighbor 10.10.1.0 activate	Activate the peer into address family mode
(config-router-af)#neighbor 10.10.2.0 activate	Activate the peer into address family mode
(config-router-af)#neighbor 10.10.3.0 activate	Activate the peer into address family mode
(config-router-af)#exit-address-family	Exit from l2vpn address family mode
(config-router)#exit	Exit from Router BGP mode and enter into config mode
(config)#exit	Exit from configuration mode

Switch(CE2) Multihomed to 2-VTEPs (VTEP1 and VTEP2)

#configure terminal	Enter Configure mode.
(config)#bridge 1 protocol ieee vlan-bridge	Configure ieee vlan bridge
(config)#vlan 2-100 bridge 1 state enable	Configure vlans from 2-100 and associate with bridge 1
(config)#interface ge15	Enter Interface mode for ge15
(config-if)#switchport	Make ge15 as L2 port by configuring switchport
(config-if)#bridge-group 1	Associate ge15 to bridge 1
(config-if)#switchport mode trunk	Configure ge15 as trunk port
(config-if)#switchport trunk allowed vlan add 2-100	Allow 2-100 configured vlans on ge15
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface po1	Enter Interface mode for po1
(config-if)#switchport	Make po1 as L2 port by configuring switchport
(config-if)#bridge-group 1	Associate po1 to bridge 1
(config-if)#switchport mode trunk	Configure po1 as trunk port
(config-if)#switchport trunk allowed vlan add 2-100	Allow 2-100 configured vlans on po1
(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface xe49	Enter Interface mode for xe49
(config-if)#channel-group 1 mode active	Make it member port of po1
(config)#interface xe51	Enter Interface mode for xe51
(config-if)#channel-group 1 mode active	Make it member port of po1
(config)#exit	Exit from configuration mode

Validation

With the given configuration VTEP1 will be elected as DF and VTEP 2 will be Non-DF for Vlan-2 and Ethernet AD per ES and per EVI are exchanged. Both MH Vtep's are in sync through ESI config on Lag interface

VTEP1

```
#sh nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
          AC - Access Port
         (u) - Untagged

VNID   Vni-name  Type Interface ESI  Vlan DF-Status Src-addr     Dst-addr
_____________________________________________________________________
 2       ----      NW   ----      ----  --- ----    27.27.27.27    32.32.32.32
 2       ----      NW    ----    ----  ---- ----    27.27.27.27       31.31.31.31
 2      ----      AC     xe29     --- Single Hommed port ---   2   ----      ---
 2        ----         AC   po1        00:88:99:44:00:67:45:00:00:00 2    DF
```

```
----              ----

Total number of entries are 4

#show bgp l2vpn evpn summary
BGP router identifier 27.27.27.27, local AS number
100 BGP table version is 6
4 BGP AS-PATH entries
0 BGP community entries

Neighbor                  V   AS    MsgRcv    MsgSen TblVer    InQ    OutQ    Up/ Down
State/PfxRcd     AD  MACIP  MCAST     ESI
10.10.1.1                 4   400    83          79       6       0       0  00:36:29
5       2       0       2      1

Total number of neighbors 1

Total number of Established sessions 1

#sh nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination       Status          Up/Down         Update
================================================================================
27.27.27.27       32.32.32.32      Installed      00:36:27      00:36:27
27.27.27.27       31.31.31.31      Installed      00:36:27      00:36:27 Total
number of entries are 2

#show bgp l2vpn evpn multihoming es-route

RD[2:1] VRF[evpn-gvrf-1]:
ESI                              PE IP-Address   Nexthop IP
00:88:99:44:00:67:45:00:00:00  27.27.27.27     27.27.27.27

RD[2:2]
ESI                              PE IP-Address   Nexthop IP
00:88:99:44:00:67:45:00:00:00  31.31.31.31     31.31.31.31

#show bgp l2vpn evpn multihoming ethernet-ad-per-es

RD[2:1] VRF[evpn-gvrf-1]:
ESI                              Eth-Tag     VNID      Nexthop IP
00:88:99:44:00:67:45:00:00:00  4294967295  0         27.27.27.27

RD[2:2]
ESI                              Eth-Tag     VNID      Nexthop IP
00:88:99:44:00:67:45:00:00:00  4294967295  0         31.31.31.31

#show bgp l2vpn evpn multihoming ethernet-ad-per-evi

RD[1:100] VRF[vrf1]:
ESI                              Eth-Tag     VNID      Nexthop IP
00:88:99:44:00:67:45:00:00:00  2           2         27.27.27.27
RD[1:200]
```

```
ESI                             Eth-Tag     VNID      Nexthop IP
00:88:99:44:00:67:45:00:00:00  2           2         31.31.31.31

#show bgp l2vpn evpn
BGP table version is 6, local router ID is 27.27.27.27
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route

    Network          Next Hop            Metric    LocPrfWeight     Path  Peer
Encap

RD[1:100] VRF[vrf1]:
*    [1]:[00:88:99:44:00:67:45:00:00:00]:[2]:[2]
                        31.31.31.31           0         100            0       400 200 i
10.10.1.1        VXLAN
*>                      27.27.27.27          0         100            32768    i  ------
----       VXLAN
*    [1]:[00:88:99:44:00:67:45:00:00:00]:[4294967295]:[0]
                        31.31.31.31           0         100            0
400 200 i  10.10.1.1        VXLAN
*>   [3]:[2]:[32,27.27.27.27]
                        27.27.27.27          0         100            32768    i  ------
----       VXLAN
*    [3]:[2]:[32,31.31.31.31]
                        31.31.31.31           0         100            0
400 200 i   10.10.1.1       VXLAN
*    [3]:[2]:[32,32.32.32.32]
                        32.32.32.32           0         100            0
400 300 i   10.10.1.1       VXLAN

RD[1:200]
*>   [1]:[00:88:99:44:00:67:45:00:00:00]:[2]:[2]
                        31.31.31.31           0         100            0
400 200 i   10.10.1.1       VXLAN
*>   [3]:[2]:[32,31.31.31.31]
                        31.31.31.31           0         100            0
400 200 i   10.10.1.1       VXLAN

RD[1:300]
*>   [3]:[2]:[32,32.32.32.32]
                        32.32.32.32           0         100            0
400 300 i   10.10.1.1       VXLAN

RD[2:1] VRF[evpn-gvrf-1]:
```

```
*>    [1]:[00:88:99:44:00:67:45:00:00:00]:[4294967295]:[0]
                      27.27.27.27          0          100             32768    i  ------
----       VXLAN
*>    [4]:[00:88:99:44:00:67:45:00:00:00]:[32,27.27.27.27]
                      27.27.27.27          0          100             32768    i  ------
----      VXLAN
    *     [4]:[00:88:99:44:00:67:45:00:00:00]:[32,31.31.31.31]
                            31.31.31.31           0          100             0
    400 200 i   10.10.1.1       VXLAN

    RD[2:2]
    *>    [1]:[00:88:99:44:00:67:45:00:00:00]:[4294967295]:[0]
                            31.31.31.31           0          100             0       400
    200 i   10.10.1.1       VXLAN
    *>    [4]:[00:88:99:44:00:67:45:00:00:00]:[32,31.31.31.31]
                            31.31.31.31           0          100             0
    400 200 i   10.10.1.1       VXLAN

    Total number of prefixes 13
```

VTEP2

```
    #show nvo vxlan
    VXLAN Information
    =================
       Codes: NW - Network Port
              AC - Access Port
             (u) - Untagged

    VNID     Vni-name    Type Interface ESI Vlan DF-Status  Src-addr       Dst-addr
    ____________________________________________________________________________________
     2        ----      NW    ----      ----  ---- ----    31.31.31.31    27.27.27.27
     2        ----      NW    ----    ----  ---- ----    31.31.31.31      32.32.32.32
     2        ----     AC    po1       00:88:99:44:00:67:45:00:00:00  2 NON-DF    ---
     -              ----

    Total number of entries are 3

    #show bgp l2vpn evpn summary
    BGP router identifier 31.31.31.31, local AS number 200
    BGP table version is 7
    4 BGP AS-PATH entries
    0 BGP community entries

    Neighbor                 V   AS    MsgRcv    MsgSen TblVer    InQ   OutQ    Up/
    Down   State/PfxRcd     AD  MACIP  MCAST    ESI
    10.10.2.1                4   400   91          91       7      0      0 00:41:27
    5      2       0      2     1

    Total number of neighbors 1

    Total number of Established sessions 1
```

```
    #show nvo vxlan tunnel
    VXLAN Network tunnel Entries
     Source           Destination      Status          Up/Down        Update
    ================================================================================
    ===
    31.31.31.31       27.27.27.27     Installed     00:41:06     00:41:06
    31.31.31.31       32.32.32.32     Installed     00:41:06     00:41:06 Total
    number of entries are 2

    #show bgp l2vpn evpn multihoming es-route
RD[2:1]
ESI                             PE IP-Address   Nexthop IP
00:88:99:44:00:67:45:00:00:00  27.27.27.27     27.27.27.27

RD[2:2] VRF[evpn-gvrf-1]:
ESI                             PE IP-Address   Nexthop IP
00:88:99:44:00:67:45:00:00:00  31.31.31.31     31.31.31.31

#show bgp l2vpn evpn multihoming ethernet-ad-per-es

RD[2:1]
ESI                             Eth-Tag     VNID      Nexthop IP
00:88:99:44:00:67:45:00:00:00  4294967295  0         27.27.27.27

RD[2:2] VRF[evpn-gvrf-1]:
ESI                             Eth-Tag     VNID      Nexthop IP
00:88:99:44:00:67:45:00:00:00  4294967295  0         31.31.31.31

#show bgp l2vpn evpn multihoming ethernet-ad-per-evi

RD[1:100]
ESI                             Eth-Tag     VNID      Nexthop IP
00:88:99:44:00:67:45:00:00:00  2           2         27.27.27.27

RD[1:200] VRF[vrf1]:
ESI                             Eth-Tag     VNID      Nexthop IP
00:88:99:44:00:67:45:00:00:00  2           2         31.31.31.31

#show bgp l2vpn evpn
BGP table version is 7, local router ID is 31.31.31.31
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route

    Network          Next Hop            Metric    LocPrfWeight     Path  Peer
Encap
```

```
RD[1:100]
*>   [1]:[00:88:99:44:00:67:45:00:00:00]:[2]:[2]
                        27.27.27.27          0         100           0
400 100 i   10.10.2.1       VXLAN
*>   [3]:[2]:[32,27.27.27.27]
                        27.27.27.27          0         100           0
400 100 i   10.10.2.1       VXLAN

RD[1:200] VRF[vrf1]:
    *    [1]:[00:88:99:44:00:67:45:00:00:00]:[2]:[2]
                        27.27.27.27          0         100           0       400 100 i
10.10.2.1        VXLAN
*>                      31.31.31.31         0         100           32768   i  ------
----      VXLAN
    *    [1]:[00:88:99:44:00:67:45:00:00:00]:[4294967295]:[0]
                           27.27.27.27          0         100           0
    400 100 i   10.10.2.1       VXLAN
    *     [3]:[2]:[32,27.27.27.27]
                           27.27.27.27          0         100           0
    400 100 i   10.10.2.1       VXLAN
    *>    [3]:[2]:[32,31.31.31.31]
                           31.31.31.31         0         100           32768   i  --
    --------       VXLAN
    *    [3]:[2]:[32,32.32.32.32]
                          32.32.32.32          0         100           0
    400 300 i   10.10.2.1      VXLAN

    RD[1:300]
    *>    [3]:[2]:[32,32.32.32.32]
                          32.32.32.32          0         100           0
    400 300 i   10.10.2.1      VXLAN

    RD[2:1]
    *>    [1]:[00:88:99:44:00:67:45:00:00:00]:[4294967295]:[0]
                          27.27.27.27          0         100           0       400
    100 i   10.10.2.1      VXLAN
    *>    [4]:[00:88:99:44:00:67:45:00:00:00]:[32,27.27.27.27]
                          27.27.27.27          0         100           0
    400 100 i   10.10.2.1      VXLAN

    RD[2:2] VRF[evpn-gvrf-1]:
    *>    [1]:[00:88:99:44:00:67:45:00:00:00]:[4294967295]:[0]
                          31.31.31.31          0         100           32768   i  --
    --------       VXLAN
    *    [4]:[00:88:99:44:00:67:45:00:00:00]:[32,27.27.27.27]
                           27.27.27.27          0         100           0       400
    100 i  10.10.2.1       VXLAN
     *>   [4]:[00:88:99:44:00:67:45:00:00:00]:[32,31.31.31.31]
                           31.31.31.31          0         100           32768   i  --
    --------      VXLAN
```

```
    Total number of prefixes 13
```

VTEP3

```
    #show nvo vxlan
    VXLAN Information
    =================
       Codes: NW - Network Port
              AC - Access Port
             (u) - Untagged

    VNID     Vni-name     Type Interface ESI                              Vlan DFStatus
     Src-addr         Dst-addr
    ____________________________________________________________________________________
    ____________________________________
    2          ----         NW    ----      ----                           ---- ----
    32.32.32.32      31.31.31.31
    2          ----         NW    ----      ----                           ---- ----
     32.32.32.32      27.27.27.27
    2          ----         AC    xe13      --- Single Hommed port ---     2    ----
    ----             ----

    Total number of entries are 3
#show bgp l2vpn evpn summary
BGP router identifier 32.32.32.32, local AS number
300 BGP table version is 5
4 BGP AS-PATH entries
0 BGP community entries

Neighbor                  V   AS   MsgRcv     MsgSen TblVer   InQ   OutQ   Up/ Down
State/PfxRcd      AD MACIP  MCAST    ESI
10.10.3.1                 4   400  102          94       5      0      0  00:44:38
8       4      0     2      2

Total number of neighbors 1

Total number of Established sessions 1

#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source           Destination      Status          Up/Down        Update
================================================================================ ===
32.32.32.32       31.31.31.31     Installed      00:44:36     00:44:36
32.32.32.32       27.27.27.27     Installed      00:45:04     00:45:04 Total
number of entries are 2

#show bgp l2vpn evpn multihoming es-route

RD[2:1]
ESI                           PE IP-Address    Nexthop IP
00:88:99:44:00:67:45:00:00:00  27.27.27.27      27.27.27.27

RD[2:2]
```

```
ESI                             PE IP-Address   Nexthop IP
00:88:99:44:00:67:45:00:00:00   31.31.31.31     31.31.31.31

#show bgp l2vpn evpn multihoming ethernet-ad-per-es

RD[2:1]
ESI                             Eth-Tag     VNID      Nexthop IP
00:88:99:44:00:67:45:00:00:00   4294967295  0         27.27.27.27

RD[2:2]
ESI                             Eth-Tag     VNID      Nexthop IP
00:88:99:44:00:67:45:00:00:00   4294967295  0         31.31.31.31

#show bgp l2vpn evpn multihoming ethernet-ad-per-evi

RD[1:100]
ESI                             Eth-Tag     VNID      Nexthop IP
00:88:99:44:00:67:45:00:00:00   2           2         27.27.27.27

RD[1:200]
ESI                             Eth-Tag     VNID      Nexthop IP
00:88:99:44:00:67:45:00:00:00   2           2         31.31.31.31

#show bgp l2vpn evpn
BGP table version is 5, local router ID is 32.32.32.32
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

[EVPN route type]:[ESI]:[VNID]:[relevent route informantion]
1 - Ethernet Auto-discovery Route
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route

    Network           Next Hop            Metric    LocPrfWeight    Path  Peer
Encap

RD[1:100]
*>   [1]:[00:88:99:44:00:67:45:00:00:00]:[2]:[2]
                       27.27.27.27          0         100          0
400 100 i   10.10.3.1        VXLAN
*>   [3]:[2]:[32,27.27.27.27]
                       27.27.27.27          0         100          0
400 100 i   10.10.3.1        VXLAN

RD[1:200]
*>   [1]:[00:88:99:44:00:67:45:00:00:00]:[2]:[2]
                       31.31.31.31          0         100          0
400 200 i   10.10.3.1        VXLAN
*>   [3]:[2]:[32,31.31.31.31]
                       31.31.31.31          0         100          0
```

```
400 200 i  10.10.3.1       VXLAN

RD[1:300] VRF[vrf1]:
*    [1]:[00:88:99:44:00:67:45:00:00:00]:[2]:[2]
                        31.31.31.31          0         100           0
400 200 i   10.10.3.1       VXLAN
*                       27.27.27.27          0         100           0
400 100 i   10.10.3.1       VXLAN
*    [1]:[00:88:99:44:00:67:45:00:00:00]:[4294967295]:[0]
                        31.31.31.31          0         100           0
400 200 i   10.10.3.1       VXLAN
*                       27.27.27.27          0         100           0
400 100 i   10.10.3.1       VXLAN
*    [3]:[2]:[32,27.27.27.27]
                        27.27.27.27          0         100           0
400 100 i  10.10.3.1        VXLAN
*    [3]:[2]:[32,31.31.31.31]
                        31.31.31.31          0         100            0
400 200 i   10.10.3.1      VXLAN
*>    [3]:[2]:[32,32.32.32.32]
                        32.32.32.32         0         100            32768    i
----------      VXLAN

RD[2:1]
*>    [1]:[00:88:99:44:00:67:45:00:00:00]:[4294967295]:[0]
                        27.27.27.27          0         100            0       400 100 i
 10.10.3.1      VXLAN
*>    [4]:[00:88:99:44:00:67:45:00:00:00]:[32,27.27.27.27]
                        27.27.27.27          0         100            0       400 100 i
 10.10.3.1      VXLAN
    RD[2:2]
    *>     [1]:[00:88:99:44:00:67:45:00:00:00]:[4294967295]:[0]
                            31.31.31.31           0         100           0       400
     200 i  10.10.3.1      VXLAN
    *>     [4]:[00:88:99:44:00:67:45:00:00:00]:[32,31.31.31.31]
                            31.31.31.31           0         100           0
    400 200 i  10.10.3.1        VXLAN

    Total number of prefixes 13
```

Switch (CE2)

```
    #sh etherchannel summary
      Aggregator po1 100001
      Aggregator Type: Layer2
      Admin Key: 0001 - Oper Key 0001
     Link: xe50 (5049) sync: 1
     Link: xe49 (5050) sync: 1
     Link: xe52 (5051) sync: 1
     Link: xe51 (5052) sync: 1
```

Static MAC-IP advertise through Single Home and Multihomed VTEPs

Advertise static mac ipv4 from MH VTEPs (VTEP1 & VTEP2- same mac should be configured on both VTEPs under po access-port, configs should be symmetric between MH VTEPs) and Single homed VTEP (VTEP3)

VTEP1(MH-1): Configuring with Mac-IP

`#configure terminal`	Enter Configure mode.
`(config)# nvo vxlan access-if port-vlan po1 2`	Enter into VxLAN MH po1 access-port
`(config-nvo-acc-if)#mac 0000.0000.1212 ip 24.1.1.1`	Configure static mac IP
`(config-nvo-acc-if)#exit`	Exit from VxLAN access-port config mode
`(config)#exit`	Exit from configuration mode

VTEP2(MH-1): Configuring with Mac-IP

`#configure terminal`	Enter Configure mode.
`(config)# nvo vxlan access-if port-vlan po1 2`	Enter into VxLAN MH po1 access-port
`(config-nvo-acc-if)#mac 0000.0000.1212 ip 24.1.1.1`	Configure static mac IP
`(config-nvo-acc-if)#exit`	Exit from VxLAN access-port config mode
`(config)#exit`	Exit from configuration mode

VTEP3(SH): Configuring with Mac-IP

`#configure terminal`	Enter Configure mode.
`(config)# nvo vxlan access-if port-vlan po1 2`	Enter into VxLAN MH po1 access-port
`(config-nvo-acc-if)#mac 0000.0000.1212 ip 24.1.1.1`	Configure static mac IP
`(config-nvo-acc-if)#exit`	Exit from VxLAN access-port config mode
`(config)#exit`	Exit from configuration mode

Validation

Verify MAC-table in MH VTEPs and Single Home VTEP, Mac will be advertised through ESI value which is advertised from VTEP1&VTEP2 and VTEP IP from SH VTEP VTEP3

Verify ARP-cache table in all VTEPs, VTEP1&VTEP2 will learn VTEP3 ip and any arp request comes for 24.1.1.2, VTEP1/VTEP2 will do proxy-arp

VTEP1

```
#sh nvo vxlan mac-table
================================================================================
================================================================================
                          VXLAN MAC Entries
================================================================================
 ================================================================================
VNID       Interface VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status            AccessPortDesc
```

```
_____________________________________________________________________________
_____________________________________________________________________

2          po1       2      ---           0000.0000.1212
00:88:99:44:00:67:45:00:00:00  Static Local          -----             ---
2          ---       ---    ---           0000.0000.1223 32.32.32.32
Remote                -----               ---

Total number of entries are 2

#sh nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
VNID     Ip-Addr          Mac-Addr       Type
_____________________________________________________
2        24.1.1.2         0000.0000.1223 Remote Static
2        24.1.1.1         0000.0000.1212 Static Local  Total
number of entries are 2
```

VTEP2

```
#sh nvo vxlan mac-table
=============================================================================
=============================================================================
                      VXLAN MAC Entries
=============================================================================
=============================================================================
VNID       Interface VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status           AccessPortDesc
_____________________________________________________________________________
_____________________________________________________________________

2          po1       2      ---           0000.0000.1212
00:88:99:44:00:67:45:00:00:00  Static Local          -----             ---
2          ---       ---    ---           0000.0000.1223 32.32.32.32
Remote                -----               ---
Total number of entries are 2

#sh nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
VNID     Ip-Addr          Mac-Addr       Type
_____________________________________________________
2        24.1.1.2         0000.0000.1223 Remote Static
2        24.1.1.1         0000.0000.1212 Static Local  Total
number of entries are 2
```

VTEP3

```
#show nvo vxlan mac-table
=============================================================================
=============================================================================
```

```
                          VXLAN MAC Entries
================================================================================
 ==============================================================
VNID       Interface VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                  Status            AccessPortDesc
_____________________________________________________________________________
_____________________________________________________________

2          ---       2       ---          0000.0000.1212
00:88:99:44:00:67:45:00:00:00  Remote                -----             ---
2          xe13      2       ---          0000.0000.1223 32.32.32.32
Static Local          -----               ---

Total number of entries are 2

#show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
VNID     Ip-Addr          Mac-Addr       Type
_____________________________________________
2        24.1.1.2         0000.0000.1223 Static Local
2        24.1.1.1 0000.0000.1212 Remote Static Total number
of entries are 2
```

Advertise static mac ipv6 from MH VTEPs (VTEP1 & VTEP2- same mac should be configured on both VTEPs under po access-port, configs should be symmetric between MH VTEPs) and Single homed VTEP (VTEP3)

VTEP1(MH-1): Configuring with Mac-IPv6

`#configure terminal`	Enter Configure mode.
`(config)# nvo vxlan access-if port-vlan po1 2`	Enter into VxLAN MH po1 access-port
`(config-nvo-acc-if)#mac 0000.0000.1444 ipv6 2ffe::1`	Configure static mac IPv6
`(config-nvo-acc-if)#exit`	Exit from VxLAN access-port config mode
`(config)#exit`	Exit from configuration mode

VTEP2(MH-1): Configuring with Mac-IP

`#configure terminal`	Enter Configure mode.
`(config)# nvo vxlan access-if port-vlan po1 2`	Enter into VxLAN MH po1 access-port
`(config-nvo-acc-if)#mac 0000.0000.1444 ipv6 2ffe::1`	Configure static mac IPv6
`(config-nvo-acc-if)#exit`	Exit from VxLAN access-port config mode
`(config)#exit`	Exit from configuration mode

VTEP3(SH): Configuring with Mac-IP

`#configure terminal`	Enter Configure mode.

(config)# nvo vxlan access-if port-vlan po1 2	Enter into VxLAN MH po1 access-port
(config-nvo-acc-if)#mac 0000.0000.1444 ipv6 2ffe::1	Configure static mac IPv6
(config-nvo-acc-if)#exit	Exit from VxLAN access-port config mode
(config)#exit	Exit from configuration mode

Validation

Verify nd-cache table in all VTEPs, VTEP1&VTEP2 will learn VTEP3 ipv6 mac and any arp request comes for 2fee::2, VTEP1/VTEP2 will do proxy-arp

VTEP1

```
#sh nvo vxlan mac-table
================================================================================
================================================================
                          VXLAN MAC Entries
================================================================================
================================================================
VNID       Interface VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status            AccessPortDesc
________________________________________________________________________________
________________________________________________________________

2           ---      ---     ---          0000.0000.1441 32.32.32.32
Remote               -----               ---
2           po1      2       ---          0000.0000.1444
00:88:99:44:00:67:45:00:00:00  Static Local         -----             ---

Total number of entries are 2

#sh nvo vxlan nd-cache
VXLAN ND-CACHE Information
==========================
VNID     Ip-Addr                                  Mac-Addr       Type
________________________________________________________________________________
2        2ffe::1                                  0000.0000.1444 Static Local
2        2ffe::2                                  0000.0000.1441 Remote Static
Total number of entries are 2
```

VTEP2

```
#show nvo vxlan mac-table
================================================================================
================================================================
                          VXLAN MAC Entries
================================================================================
================================================================
VNID       Interface VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status            AccessPortDesc
```

```
_____________________________________________________________________________________
_____________________________________________________________________________

2           ---      ---     ---          0000.0000.1441 32.32.32.32
Remote               -----               ---
2           po1      2       ---          0000.0000.1444
00:88:99:44:00:67:45:00:00:00  Static Local          -----            ---

Total number of entries are 2

#show nvo vxlan nd-cache
VXLAN ND-CACHE Information
============================
VNID     Ip-Addr                                    Mac-Addr       Type
_____________________________________________________________________________
2        2ffe::1                                   0000.0000.1444 Static Local
2        2ffe::2                                   0000.0000.1441 Remote Static
Total number of entries are 2
```

VTEP3

```
#show nvo vxlan mac-table
=============================================================================
=============================================================================
                         VXLAN MAC Entries
=============================================================================
=============================================================================
VNID       Interface VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status           AccessPortDesc
_____________________________________________________________________________
_____________________________________________________________________________

2           ---      ---    ---           0000.0000.1441 32.32.32.32
Remote               -----              ---
2         po1        2      ---      0000.0000.1444
00:88:99:44:00:67:45:00:00:00   Static Local         -----            ---

Total number of entries are  2

#show nvo vxlan nd-cache
VXLAN ND-CACHE Information
============================
VNID     Ip-Addr                                    Mac-Addr       Type
_____________________________________________________________________________
 2       2ffe::1                                   0000.0000.1444 Static Local
 2       2ffe::2                                   0000.0000.1441 Remote Static

Total number of entries are 2
```

Dynamic MAC advertise through Single Home and Multihomed VTEPs

Advertise 2 Mac's through CE1 connected IXIA , dynamic mac entries and verify mac-table in all VTEPs. One MAC will be dynamic local in VTEP1 and same will be remote in VTEP2 and other be dynamic local in VTEP2 and same will be remote in VTEP1 and in remaining VTEPs it will be remote.

VTEP1

```
 #show nvo vxlan mac-table
================================================================================
================================================================================
                            VXLAN MAC Entries
================================================================================
================================================================================
VNID       Interface VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status            AccessPortDesc
________________________________________________________________________________
________________________________________________________________________________

2          ---       ---    ---          0000.0000.0011 32.32.32.32
Remote               -----              ---
2          po1       2      ---          0000.0011.1122
00:88:99:44:00:67:45:00:00:00  Dynamic Local         -----            300
2          ---       2      ---          0000.0011.1133
00:88:99:44:00:67:45:00:00:00  Remote                -----            ---
2          ---       ---    ---          0000.0022.2211 32.32.32.32
Remote               -----              ---

Total number of entries are 4

#show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
============================
VNID      Ip-Addr          Mac-Addr       Type
_____________________________________________________
 2        41.1.1.2         0000.0022.2211 Remote Dynamic
 2        41.1.1.1         0000.0011.1122 Dynamic Local
 2        51.1.1.2         0000.0000.0011 Remote Dynamic
2        51.1.1.1 0000.0011.1133 Remote Dynamic Total number
of entries are 4
```

VTEP2

```
 #show nvo vxlan mac-table
================================================================================
================================================================================
                          VXLAN MAC Entries
================================================================================
================================================================================
VNID       Interface VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status            AccessPortDesc
```

```
_____________________________________________________________________________
_____________________________________________________________________

2           ---       ---    ---          0000.0000.0011 32.32.32.32
Remote                -----              ---
2           ---       2      ---          0000.0011.1122
00:88:99:44:00:67:45:00:00:00  Remote               -----            ---
2           po1       2      ---          0000.0011.1133
00:88:99:44:00:67:45:00:00:00  Dynamic Local        -----
2           ---       ---    ---          0000.0022.2211 32.32.32.32
Remote                -----              ---

Total number of entries are 4

#show nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
VNID      Ip-Addr          Mac-Addr       Type
_____________________________________________________
 2         41.1.1.2         0000.0022.2211 Remote Dynamic
 2         41.1.1.1         0000.0011.1122 Remote Dynamic
 2         51.1.1.1         0000.0011.1133 Dynamic Local
2         51.1.1.2 0000.0000.0011 Remote Dynamic Total number
of entries are 4
```

VTEP3

```
#show nvo vxlan mac-table
=============================================================================
=============================================================
                          VXLAN MAC Entries
=============================================================================
=============================================================
VNID       Interface VlanId Inner-VlanId Mac-Addr       VTEP-Ip/ESI
Type                 Status            Time-out AccessPortDesc
_____________________________________________________________________________
_____________________________________________________________________

2          xe13      2      ---          0000.0000.0011  32.32.32.32
Dynamic Local        -----
2          ---       2      ---          0000.0011.1122
00:88:99:44:00:67:45:00:00:00  Remote               -----            ---
2          ---       2      ---          0000.0011.1133
00:88:99:44:00:67:45:00:00:00  Remote               -----            ---
2          xe13      2      ---          0000.0022.2211  32.32.32.32
Dynamic Local        -----

Total number of entries are 4

#show nvo vxlan arp-cache
```

```
VXLAN ARP-CACHE Information
===========================
VNID     Ip-Addr          Mac-Addr       Type
_____________________________________________________
 2        41.1.1.2        0000.0022.2211 Dynamic Local
 2        41.1.1.1        0000.0011.1122 Remote Dynamic
 2        51.1.1.2        0000.0000.0011 Dynamic Local
 2        51.1.1.1        0000.0011.1133 Remote Dynamic
Total number of entries are 4
```

Virtual eXtensible Local Area Network Command Reference

Contents

This document contains these chapters and appendices:

- Chapter 1, *VXLAN Commands*

© Symanitron

Virtual eXtensible Local Area Network Command Reference

CHAPTER 1 VXLAN Commands

This chapter describes the VXLAN commands:

- arp-cache disable
- arp-nd flood-suppress
- arp-nd refresh timer
- clear mac address table dynamic vxlan
- clear nvo vxlan counters
- clear nvo vxlan mac-stale-entries
- cos
- cos queue
- description
- disable l3-protocols-cpu vxlan
- dscp
- dscp queue
- dynamic-learning disable
- encapsulation
- evpn esi holdtime
- evpn multi-homing enable
- evpn multi-homed
- evpn irb-forwarding anycast-gateway-mac
- evpn irb-if-forwarding anycast-gateway-mac
- evpn irb1
- Interface irb
- ip evpn prefix route
- Ipv6 evpn prefix route
- ip vrf forwarding
- Ip route vrf <vrfname>
- Ipv6 route vrf <vrfname>
- load-balance rtag7 vxlan inner-l2
- load-balance rtag7 vxlan inner-l3
- l3vni
- mac
- mac vrf
- mac-holdtime
- map qos-profile

- map vnid
- nd-cache disable
- no nvo vxlan
- nvo vxlan
- nvo vxlan access-if
- nvo vxlan id
- nvo vxlan mac-ageing-time
- nvo vxlan max-cache-disable
- nvo vxlan irb
- nvo vxlan tunnel qos-map-mode
- nvo vxlan vtep-ip-global
- qos cos-queue-profile
- qos dscp-queue-profile
- show bgp l2vpn evpn
- show bgp l2vpn evpn summary
- show nvo vxlan
- show nvo vxlan access-if-config
- show nvo vxlan arp-cache
- show nvo vxlan counters access-port
- show nvo vxlan counters network-port
- show nvo vxlan interface counters
- show nvo vxlan mac-table
- show nvo vxlan nd-cache
- show nvo vxlan static host state
- show nvo vxlan tunnel
- show running-config nvo vxlan • show evpn multi-homing all
- show evpn multihoming-status
- show nvo vxlan route-count
- show nvo vxlan vni-name
- show nvo vxlan irb-status
- show running-config interface irb
- show interface irb
- show bgp l2vpn evpn prefix-route
- shutdown
- vxlan host-reachability-protocol evpn-bgp
- vxlan static-entry host-mac

© Symanitron Proprietary

arp-cache disable

Use this command to disable the ARP cache for MAC/IP.

When the ARP cache is disabled on a VxLAN access port, SWMRE does not reply to any ARP arriving on this port from the cache. SWMRE withdraws all MAC/IPs configured/learned on this access port and removes the MAC/IP entry for this access port from the local ARP cache.

SWMRE also makes sure that on withdrawing the MAC/IP route, the MAC does not become unknown. If all routes for this MAC are being withdrawn because of this command, then SWMRE advertises a MAC-only route. This is done so that the MAC does not become unknown and only the cache functionality becomes disabled.

See also nvo vxlan max-cache-disable.

Use the `no` form of this command to enable ARP cache for MAC/IP.

Note: On enabling the cache, an IP will be in conflict, then the cache enable will fail. The conflict has to be manually removed and then the cache enabled.

Command Syntax `arp-cache disable no arp-cache disable`

Parameters

None

Default

By default, the arp-cache option is enabled.

Command Mode

NVO access interface mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#arp-cache disable
(config-nvo-acc-if)#exit
```

arp-nd flood-suppress

Use this command to restrict the flood of ARP/ND packets towards remote VTEPs or other access ports.

This command applies only when the ARP cache and ND cache are enabled. When the ARP cache is disabled, ARP flooding is not suppressed even if this command is given. When the ND cache is disabled, ND flooding is not disabled, even if this command is given.

Use the `no` form of this command to not restrict the flood of ARP/ND packets.

Command Syntax `arp-nd flood-suppress no arp-nd flood-suppress`

Parameters

None

Default

By default, the arp-nd flood-suppress option is enabled.

Command Mode

NVO access interface mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#arp-nd flood-suppress
(config-nvo-acc-if)#exit
```

arp-nd refresh timer

Use this command to configure aging out the arp-cache and nd-cache entries for given time multiplied by 3 in secs

Use the no form of this command to remove the configuration

Note:This command is not enabled if VXLAN IRB is enabled.

Command Syntax `nvo vxlan arp-nd refresh-timer <3-300000> no nvo vxlan arp-nd refresh-timer`

Parameters

`<3-300000>` refresh time in seconds

Command Mode

Config mode

Applicability

This command was introduced in SWMRE version 1.3.5

Example

```
#config mode
(config)#nvo vxlan arp-nd refresh-timer 100
(config)#no nvo vxlan arp-nd refresh-timer
```

clear mac address table dynamic vxlan

Use this command to clear dynamically learned MACs.

Command Syntax `clear mac address table dynamic vxlan`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#clear mac address table dynamic vxlan
```

clear nvo vxlan counters

Use this command to clear the counters of access ports or network ports.

Command Syntax

```
clear nvo vxlan counters((access-port (port IFNAME | port-vlan IFNAME VLAN_ID |
all)) | (network-port (dst A.B.C.D | all)))
```

Parameters

port	Port
IFNAME	Interface name
port-vlan	VLAN port
IFNAME	Interface name
VLAN_ID	VLAN identifier
A.B.C.D	Tunnel destination IPv4 address
all	All access or network ports

Command Mode

Exec mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

Example for clearing a VLAN port counter:

```
#clear nvo vxlan counters access-port port-vlan xe1 2
```

Example for clearing all access port counters:

```
#clear nvo vxlan counters access-port all
```

Example for clearing network port counters:

```
#clear nvo vxlan counters network-port dst 1.1.1.1
```

clear nvo vxlan mac-stale-entries

Use this command to clear MAC entries that are in discard state in the forwarding database.

Command Syntax `clear nvo vxlan mac-stale-entries (vnid <1-16777215> |)`

Parameters

<1-16777215>	VXLAN network identifier

Command Mode

Exec mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#clear nvo vxlan mac-stale-entries vnid 100
```

cos

Use this command to set a COS value and its direction.

Use the `no` form of this command to reset the COS value.

COS-DSCP mapping mode is configured globally.

The COS value is not supported in configuring the access-port only.

Command Syntax `cos <0-7> (ingress|egress) no cos <0-7> (ingress|egress)`

Parameters

`<0-7>`	COS value
`ingress`	Ingress direction
`egress`	Egress direction

Default

By default, the COS priority is 0.

Command Mode

NVO access interface mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#cos 2 ingress (config-
nvo-acc-if)#cos 3 egress (config)#exit
```

cos queue

Use this command to map a CoS to a queue.

Use the `no` form of this command to unmap a CoS from a queue.

Command Syntax `cos <0-7> queue <0-7> no cos <0-7>`

Parameters

`<0-7>`	CoS value
`<0-7>`	Queue value

Default

By default, the COS priority is 0.

Command Mode

CoS queue profile mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#configure terminal
                                        (config)#qos cos-queue-profile ingress 64
(config-cos-queue)#cos 2 queue 4
(config-cos-queue)#exit
```

description

Use this command to set a description for a port.

Use the `no` form of this command to remove the description for a port.

Command Syntax `description LINE no description`

Parameters

`LINE`	Maximum 32 characters describing this port.

Default

No default value is specified for description LINE commands.

Command Mode

NVO access interface mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2 (config-nvo-acc-if)#description
                      member-port xe1 with vlan 2
(config-nvo-acc-if)#exit
```

disable l3-protocols-cpu vxlan

Use this command to keep control plane packets on VxLAN access interfaces and Core facing interfaces from getting uplifted to the CPU.

Use the `no` form of the command to remove this configuration.

Command Syntax `disable l3-protocols-cpu vxlan no disable l3-protocols-cpu vxlan`

Parameters

None

Default

None

Command Mode

NVO access interface mode

Applicability

This command was introduced in SWMRE version 1.3.4.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe3/1 11 (config-nvo-acc-
if)#disable l3-protocols-cpu vxlan
(config-nvo-acc-if)#exit
```

dscp

Use this command to map an explicit DSCP value to an access-port.

Use the `no` form of this command to reset the DSCP value.

DSCP-DSCP mapping mode is configured globally.

Command Syntax `dscp <0-63> (ingress|egress)` `no dscp <0-63> (ingress|egress)`

Parameters

`<0-63>`	DSCP value
`ingress`	Ingress direction
`egress`	Egress direction

Default

By default, the dscp priority is 0.

Command Mode

NVO access interface mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#dscp 24 ingress (config-
nvo-acc-if)#dscp 32 egress
```

```
(config-nvo-acc-if)#exit

#configure terminal
(config)#nvo vxlan access-if port xe1
(config-nvo-acc-if)#dscp 24 ingress
(config-nvo-acc-if)#dscp 32 egress
(config-nvo-acc-if)#exit
```

dscp queue

Use this command to map a DSCP value to a queue.

Use the `no` form of this command to unmap a DSCP value from a queue.

Command Syntax `dscp <0-63> queue <0-7> no dscp <0-63>`

Parameters

`<0-63>`	DSCP value
`<0-7>`	Queue

Default

By default, the dscp priority is 0.

Command Mode

DSCP queue configure mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#configure terminal
                (config)#qos dscp-queue-profile ingress 128
(config-dscp-queue)#dscp 24 queue 4 (config-dscp-
queue)#exit
```

dynamic-learning disable

Use this command to disable dynamic learning of MACs at the access port. This command also disables dynamic learning of MAC/IP from ARP/ND messages received on this access port.

Use the `no` form of this command to enable dynamic learning of MACs at the access port.

Command Syntax `dynamic-learning disable` `no dynamic-learning disable`

Parameters

None

Default

By default, the dynamic-learning option is enabled.

Command Mode

NVO access interface mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#dynamic-learning disable
(config-nvo-acc-if)#exit
```

encapsulation

Use this command to assign a Tag Protocol Identifier (TPID) to an access port.

Use the `no` form of this command to set the default TPID (0x8100: IEEE 802.1Q VLAN-tagged frame) to an access port.

Command Syntax

```
encapsulation  TPID
no encapsulation
```

Parameters

`TPID`	Tag Protocol Identifier: Ox88A8: IEEE 802.1ad Provider Bridging Ox9100: IEEE 802.1Q VLAN-tagged frame with double tagging

Default

The encapsulation TPID default is 0X8100.

Command Mode

NVO access interface mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#encapsulation 0x9100
(config-nvo-acc-if)#exit
```

evpn esi holdtime

Use this command to allow some time for the tunnels to come at the time of vxlan initialization before making the esi up. This avoids traffic to be black-holed when a new PE is added and connected to an already running CE for multihoming.

Use the no form of this command to make the esi up immediately when configuring the access-if cli.

Command Syntax `evpn esi holdtime <10-300> no evpn esi holdtime <10-300>`

Parameters

`<10-300>`	Hold time in seconds

Default

Default value is 0.

Command Mode

Configuration Mode

Applicability

This command was introduced in SWMRE version 1.3.4.

Example

```
#configure terminal
(config)# evpn esi holdtime 100
(config)# exit
```

evpn multi-homing enable

Use this command to enable evpn multi-homing

Use the no form of this command to disable evpn multi-homing.

Note: Node will have to be restarted for this to be applicable. If there are some nodes in topology which have multihomed CEs, then nodes which do not have multi-homed CEs should also enable multihoming so, that they can load share traffic to the multi-homed CEs.

Command Syntax `evpn multihoming enable no evpn multihoming enable`

Parameters

None

Default

By Default Multi-homing will be disabled

Command Mode

Configuration Mode

Applicability

This command was introduced in SWMRE version 1.3.4.

Example

```
#configure terminal
#(config)# evpn multihoming enable
#(config)# exit
```

evpn multi-homed

Use this command to configure interfaces as multi-homed and configure esi-value in case of physical and static lag and system-mac in case of Dynamic lag.

Use the no parameter of this command to unconfigure multi-homed on the interface.

Command Syntax

```
evpn multi-homed (esi XX:XX:XX:XX:XX:XX:XX:XX:XX | system-mac (XX-XX-XX-XX-XX-
  XX|XX:XX:XX:XX:XX:XX|XXXX.XXXX.XXXX)
no evpn multi-homed (esi | system-mac)
```

Parameters

XX:XX:XX:XX:XX:XX:XX:XX:XX:XX	ESI value in HH:HH:HH:HH:HH:HH:HH:HH:HH:HH - 9 octet format
XX-XX-XX-XX-XX-XX	Host MAC address (Option 1)
XX:XX:XX:XX:XX:XX	Host MAC address (Option 2)
XXXX.XXXX.XXXX	Host MAC address (Option 3)

Default

Default value is 0.

Command Mode

Interface Mode

Applicability

This command was introduced in SWMRE version 1.3.4.

Example

```
#configure terminal
(config)# interface xe1
(config)# evpn multi-homed esi 00:11:22:33:44:55:66:77:88
(config)# exit
```

```
configure terminal
(config)# interface po1
(config)# evpn multi-homed system-mac
0000.0000.1111 (config)# exit
```

evpn irb-forwarding anycast-gateway-mac

Use this command to configure common anycast mac-address for all IRB interfaces Use the no form of this command to remove MAC address on all the IRB interfaces.

Command Syntax `evpn irb-forwarding anycast-gateway-mac XXXX.XXXX.XXXX`

`no evpn irb-forwarding anycast-gateway-mac`

Parameters

`XX-XX-XX-XX-XX-XX`	Source MAC address (Option 1)
`XX:XX:XX:XX:XX:XX`	Source MAC address (Option 2)
`XXXX.XXXX.XXXX`	Source MAC address (Option 3)

Command Mode

Config Mode

Applicability

This command was introduced in SWMRE version 1.3.5

Example

```
#configure terminal
(config)#evpn irb-forwarding anycast-gateway-mac 0000.0000.1313 Or
(config)#evpn irb-forwarding anycast-gateway-mac 00:00:00:00:13:13
Or
(config)#evpn irb-forwarding anycast-gateway-mac 00-00-00-00-13-13
(config)# no evpn irb-forwarding anycast-gateway-mac
```

evpn irb-if-forwarding anycast-gateway-mac

Use this command to enable an IRB interface to use the global anycast IRB mac-address.

Use the no form of this command to un-configure anycast MAC at IRB interface

Command Syntax `evpn irb-if-forwarding anycast-gateway-mac no evpn irb-if-forwarding anycast-gateway-mac`

Parameters

None

Command Mode

IRB_IF_Mode

Applicability

This command was introduced in SWMRE version 1.3.5.

Example

```
#configure teminal
(config)# interface irb 1
(config-irb-if)# ip vrf forwarding vrfip
(config-irb-if)#evpn irb-if-forwarding anycast-gateway-mac
(config-irb-if)#no evpn irb-if-forwarding anycast-gateway-mac
```

evpn irb1

Use this command to configure default gateway behavior on a VTEP for particular VNID.

Use the no form this command to un-configure default gateway behavior on a VTEP for the particular VNID

Command Syntax `evpn`

```
<NAME> no evpn  <NAME>
```

Parameters

`NAME` irb interface name

Command Mode

NVO mode

Applicability

This command was introduced in SWMRE version 1.3.5.

Example

```
#config mode
    (config)# nvo vxlan id 2000 ingress-replication inner-vid-disabled
(config-nvo)# evpn irb1
(config-nvo)# no evpn irb1
```

Interface irb

Use this command to configure IRB interface

Use the no form of this command to un-configure IRB interface

Command Syntax `interface irb <1-4094> no interface irb <1-4094>`

Parameters

`<1-4094>` irb interface number

Command Mode

Config Mode

Applicability

This command was introduced in SWMRE version 1.3.5.

Example

```
#configure teminal
(config)#interface irb 1
(config)#no interface irb 1
```

ip evpn prefix route

Use this command to configure the IPv4 prefix route attached to a VNID behind Tenant System on the non-default gateway VTEP.

Use the no form of this command to un-configure the IPv4 prefix route attached to a VNID behind Tenant System on the non-default gateway VTEP.

Command Syntax `ip evpn prefix route vrf < NAME><A.B.C.D/M>`

`<A.B.C.D> no ip evpn prefix route vrf < NAME> <A.B.C.D/M>`

`<A.B.C.D>`

Parameters

`NAME`	VPN Routing/Forwarding instance name. Maximum limit 32 characters.
`A.B.C.D/M`	IP destination prefix (e.g. 10.0.0.0/8)
`A.B.C.D`	IP gateway address

Command Mode

Config mode

Applicability

This command was introduced in SWMRE version 1.3.5.

Example

```
#config mode
(config)# ip evpn prefix route vrf vrf1 100.100.100.0/24 144.144.144.1
(config)#no ip evpn prefix route vrf vrf1 100.100.100.0/24 144.144.144.1
```

Ipv6 evpn prefix route

Use this command to configure the IPv6 prefix route attached to a VNID behind Tenant System on the non-default gateway VTEP.

Use the no form of this command to un-configure the IPv6 prefix route attached to a VNID behind Tenant System on the non-default gateway VTEP.

Command Syntax `ipv6 evpn prefix route vrf < NAME> <X:X::X:X/M> <`

`X:X::X:X > no Ipv6 evpn prefix route vrf < NAME> <X:X::X:X/M> <`

`X:X::X:X >`

Parameters

`NAME` VPN Routing/Forwarding instance name. Maximum limit 32 characters.

`X:X::X:X/M` IPv6 destination prefix (e.g. ffe:506::/32) `X:X::X:X`

IPv6 gateway address

Command Mode

Config mode

Applicability

This command was introduced in SWMRE version 1.3.5.

Example

```
#config mode
(config)# ipv6 evpn prefix route vrf vrf1 2201::/48 1201::10
(config)#no ipv6 evpn prefix route vrf vrf1 2201::/48 1201::10
```

ip vrf forwarding

Use this command to configure vrf forwarding on IRB interface

Use the no form this command to un-configure vrf forwarding on IRB interface

Command Syntax `ip vrf forwarding <NAME> no`

```
ip vrf forwarding <NAME>
```

Parameters

NAME	VPN Routing/Forwarding instance name. Maximum limit 32 characters

Command Mode

IRB_IF_Mode

Applicability

This command in introduced in SWMRE version 1.3.5.

Example

```
#configure teminal
(config)#interface irb 1
(config-irb-if)#ip vrf forwarding vrfip
(config-irb-if)#no ip vrf forwarding vrfip
```

Ip route vrf <vrfname>

Use this command to configure the IPv4 prefix route attached to a VNID behind Tenant System on the default gateway VTEP.

Use the no form of this command to un-configure the IPv4 prefix route attached to a VNID behind Tenant System on the default gateway VTEP.

Command Syntax `ip route vrf <NAME>  < A.B.C.D/M>  <A.B.C.D>`

```
<IFNAME> no ip route vrf <NAME>  < A.B.C.D/M>  <A.B.C.D>
<IFNAME>
```

Parameters

NAME	VPN Routing/Forwarding instance name. Maximum limit 32 characters.
A.B.C.D/M	IP destination prefix (e.g. 10.0.0.0/8)
A.B.C.D	IP gateway address

IFNAME	IP gateway Interface Name

Command Mode

Config mode

Applicability

This is an existing command which is now being used for EVPN routes as well from SWMRE version 1.3.5 onwards.

Example

```
#config mode
(config)#ip route vrf vrfip 100.100.100.0/24 144.144.144.10 irb1
(config)#no ip route vrf vrfip 100.100.100.0/24 144.144.144.10 irb1
```

Ipv6 route vrf <vrfname>

Use this command to configure the IPv6 prefix route attached to a VNID behind Tenant System on the default gateway VTEP.

Use the no form of this command to un-configure the IPv6 prefix route attached to a VNID behind Tenant System on the default gateway VTEP.

Command Syntax `ip route vrf <NAME> < X:X::X:X/M> <X:X::X:X> <IFNAME> no ip route vrf <NAME> < X:X::X:X/M> <X:X::X:X> <IFNAME>`

Parameters

NAME	VPN Routing/Forwarding instance name. Maximum limit 32 characters.
X:X::X:X/M	IPv6 destination prefix (e.g. ffe:506::/32)
X:X::X:X	IPv6 gateway address
IFNAME	IP gateway Interface Name

Command Mode

Config mode

Applicability

This is an existing command which is now being used for EVPN routes as well from SWMRE version 1.3.5 onwards.

Example

```
#config mode
(config)#ipv6 route vrf vrfip 2201::/48 1201::10 irb1
(config)#no ipv6 route vrf vrfip 2201::/48 1201::10 irb1
```

load-balance rtag7 vxlan inner-l2

Use this command to enable RTAG7 load balancing for VxLAN for inner-L2 packets on the access side for load sharing of traffic on tunnel paths. This command also enables random UDP source port generation for the VxLAN UDP tunnels based on the L2 frame being received on the VxLAN access port.

Use the `no` parameter of this command to disable load balance for RTAG7 for VxLAN for inner-L2 frames.

Command load-balance rtag7 vxlan inner-l2 (dest-mac |

Syntax src- load-balance rtag7 vxlan inner-l2 (dest-mac |

mac) no

src-mac)

Parameter dest-mac Destination MAC Address.

src-mac Source MAC Address.

Default

By default, the load-balance rtag7 vxlan inner-l2 default is src-mac.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#load-balance rtag7 vxlan inner-l2 dest-mac

(config)#no load-balance rtag7 vxlan inner-l2 dest-mac
```

load-balance rtag7 vxlan inner-l3

Use this command to enable RTAG7 load balancing for VxLAN for inner-L3 IPv4 and IPv6 packets on the access side for load sharing of traffic on tunnel paths. This command also enables random UDP source port generation for the VxLAN UDP tunnels based on the L3 frame being received on the VxLAN access port.

Use the no parameter of this command to disable load balance for RTAG7 for VxLAN for inner-L3 IPv4 and IPv6 frames.

Command Syntax

```
load-balance rtag7 vxlan inner-l3 (dest-ip | destl4-port | protocol-id | src-ip |
  srcl4-port)

no load-balance rtag7 vxlan inner-l3 (dest-ip | destl4-port | protocol-id | src-ip
  | srcl4-port)
```

Parameter

dest-ip	Destination IP.
destl4-port	Destination l4 port.
protocol-id	Protocol (IPv4).
src-ip	Source IP.
srcl4-port	Source l4 port.

Default

By default, the load-balance rtag7 vxlan inner-l3 default is src-ip.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#load-balance rtag7 vxlan inner-l3 dest-ip

(config)#no load-balance rtag7 vxlan inner-l3 dest-ip
```

l3vni

Use this command to configure L3 Virtual Network Identifier on the ip vrf

Use the no form of this command to remove L3 Virtual Network Identifier

Command Syntax

```
l3vni <L3 VNID>
```

Parameters

<1-16777215>	L3 VNID. Cannot be same as L2 VNID which is configured by the nvo vxlan id command.

Command Mode

Config_VRF Mode

Applicability

This command was introduced in SWMRE version 1.3.5.

Example

```
#Config mode
(config)#ip vrf vrfip
(config-vrf)#l3vni 10002
(config-vrf)#no l3vni 10002
```

mac

Use this command to associate a static MAC address and a static IPv4 or IPv6 address on an access interface.

Use the `no` form of this command to disassociate a static MAC address and an IPv4 or IPv6 address for an access interface.

Note: When a static host is configured on an access port which is in the down state, its state is Inactive.

Note: The same static mac configuration is not allowed on a different access port as then there will be a chance of conflict. However, if a dynamic packet is sent at another access port which is up and running with the same MAC, it learns as usual. As soon as the port on which the static MAC is configured comes up, static learning is given precedence and the dynamically learned MAC is moved to the port where it is configured statically.

Command Syntax `mac XXXX.XXXX.XXXX mac XXXX.XXXX.XXXX`

`(ip A.B.C.D | ipv6 X:X::X:X) no mac XXXX.XXXX.XXXX`

`(ip A.B.C.D | ipv6 X:X::X:X)`

Parameters

`XXXX.XXXX.XXXX` Static MAC address. The following formats are supported:

XX-XX-XX-XX-XX-XX Source MAC address (Option 1)

XX:XX:XX:XX:XX:XX Source MAC address (Option 2)

XXXX.XXXX.XXXX Source MAC address (Option

3) `A.B.C.D` Static IPv4 address. `X:X::X:X` Static IPv6 address.

Default

No default value is specified for mac command.

Command Mode

NVO access interface mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#mac 0000.0000.aaaa ip 10.10.10.1
(config-nvo-acc-if)#mac 0000.0000.aaaa ipv6 1201::1
(config-nvo-acc-if)#exit
```

mac vrf

Use this command to create a MAC VRF to use in EVPN routes.

Limitation: If the VRF is linked with a VxLAN identifier, then it cannot be deleted and any route distinguisher or route target configured on it cannot be changed.

See also vxlan host-reachability-protocol evpn-bgp.

Use the `no` parameter of this command to delete the MAC VRF.

Command Syntax `mac`

```
vrf WORD no mac
vrf WORD
```

Parameter

`WORD`	MAC routing or forwarding instance name.

Default

No default value is specified for mac vrf WORD command.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#mac vrf vrf1

(config)#no mac vrf vrf1
```

mac-holdtime

Use this command to set the MAC hold time for a MAC/IP or MAC.

The feature holds the MAC in hardware until BGP has withdrawn from the neighbors. This helps to reduce flooding to other access ports.

This setting applies when the access port is shut down, the physical port on which the access port is down, or the access port is removed from the VNID using the `no` form of the map vnid command.

When the MAC hold time is configured as -1, then the MAC is not removed from the hardware and is also not withdrawn from EVPN BGP.

Use the `no` form of this command to remove the MAC hold time for the MAC/IP or MAC.

Note: When a MAC is moved to discard state, traffic to and from this MAC is discarded. This is applicable only on statically configured MAC/MAC-IPs.

Command Syntax `mac-holdtime <-1-300> no mac-holdtime`

Parameters

`<-1-300>`	MAC hold time in seconds. Specify -1 to “never expire”.

Default

The default holdtime for mac is 3 seconds.

Command Mode

NVO mode and NVO_ACC_IF_MODE mode

Note: When configured in both modes, then the NVO_ACC_IF_MODE value takes preference for that access port.

Applicability

This command was introduced in SWMRE version 1.3.3.

This command in NVO_ACC_IF_MODE mode is introduced in SWMRE version 1.3.4.

Example

```
#configure terminal
(config)#nvo vxlan id 3 ingress-replication inner-vid-disabled
(config-nvo)#mac-holdtime -1
(config-nvo)#exit
```

map qos-profile

Use this command to map a QoS profile created with qos cos-queue-profile or qos dscp-queue-profile to an access port.

Use the `no` form of this command to unmap a QoS profile from an access port

Command Syntax `map qos-profile (ingress|egress) <1-128>` `no map qos-profile (ingress|egress)`

Parameters

`ingress`	Ingress direction (access network)
`egress`	Egress direction (network access)
`<1-128>`	QoS profile identifier

Default

No default value is specified for map qos-profile command.

Command Mode

NVO access interface mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#map qos-profile ingress 64
(config-nvo-acc-if)#map qos-profile egress 100
(config-nvo-acc-if)#exit
```

map vnid

Use this command to map a tenant to an access-port.

Use the no form of this command to remove the tenant from an access-port

Command Syntax map vnid <1-16777215> no map vnid <1-16777215>

Parameters

<1-16777215> VxLAN network identifier.

Default

No default value is specified for map vnid command.

Command Mode

NVO access interface mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#configure terminal
                (config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#map vnid 100 (config-nvo-acc-if)#exit
```

nd-cache disable

Use this command to disable ND cache for MAC/IPv6.

When the ARP cache is disabled on a VxLAN access port, SWMRE does not reply to any ARP arriving on this port from the cache. SWMRE withdraws all MAC/IPs configured/learned on this access port and removes the MAC/IP entry for this access port from the local ARP cache.

SWMRE also makes sure that on withdrawing the MAC/IP route, the MAC does not become unknown. If all routes for this MAC are being withdrawn because of this command, then SWMRE advertises a MAC-only route. This is done so that the MAC does not become unknown and only the cache functionality becomes disabled.

See also arp-cache disable.

Use the no form of this command to enable ND cache for MAC/IPv6.

Note: On enabling the cache, an IP will be in conflict, then the cache enable will fail. The conflict has to be manually removed and then the cache enabled.

Command Syntax nd-cache disable no nd-cache disable

Parameters

None

Default

By default, the nd-cache option is enabled.

Command Mode

NVO access interface mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#nd-cache disable
(config-nvo-acc-if)#exit
```

no nvo vxlan

Use this command to delete a given tenant or all tenants/VPNs.

Command Syntax `no nvo vxlan (id <1-16777215>|all-vnids)`

Parameters

`<1-16777215>` VXLAN Network Identifier. `all-vnids` Delete all VxLAN network identifiers.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#no nvo vxlan id 100
```

nvo vxlan

Use this command to enable or disable VxLAN.

Command Syntax `nvo vxlan (enable | disable)`

Parameters

None

Default

By default, the nvo vxlan option is enabled.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan enable

(config)#nvo vxlan disable
```

nvo vxlan access-if

Use this command to map a complete interface or a VLAN on an interface to identify the tenant traffic and to enter NVO access interface mode.

Use the `no` form of this command to unmap an interface or a VLAN.

Note: When a VxLAN access interface configured as a port VLAN is unconfigured, the traffic sent on the VLAN for that port hits some QoS policies which are set to not accept VLAN traffic on a port for which the VLAN is not configured. Such traffic is counted as VxLAN/ACL discards.

Command Syntax

```
nvo vxlan access-if (port IFNAME | port-vlan IFNAME VLAN_ID (inner-vlan
  INNER_VLAN_ID |)) no nvo vxlan access-if (port IFNAME | port-vlan
IFNAME VLAN_ID (inner-vlan INNER_VLAN_ID |))
```

Parameters

`port`	A physical port.
`IFNAME`	Interface name.
`port-vlan`	The physical port on which VLANs are configured.
`IFNAME`	Interface name.
`VLAN_ID`	VLAN identifier.
`inner-vlan`	Inner VLAN.
`INNER_VLAN_ID`	

Inner VLAN identifier.

Default

By default, the nvo vxlan access-if option is port VLAN ID.

Command Mode

Configure mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#exit

#configure terminal
(config)#nvo vxlan access-if port xe1
(config-nvo-acc-if)#exit

#configure terminal
(config)#nvo vxlan access-if port-vlan xe1 2 inner-vlan 4 (config-nvo-acc-
if)#exit
```

nvo vxlan id

Use this command to add a tenant and the type of VPN. This command changes the mode to NVO mode.

Command Syntax

```
nvo vxlan id <1-16777215> (|unicast | multicast A.B.C.D) | (ingress-replication (|
  inner-vid-disabled)))
```

Parameters

`<1-16777215>` VxLAN Network Identifier (VNID).

`unicast` Unicast mode (point to point). `multicast`

Multicast mode (point to multipoint). `A.B.C.D`

Indicates the multicast IP address `ingress-`

`replication`

Use head end replication for forwarding BUM (Broadcast, Unknown Unicast, Multicast) traffic.

`inner-vid-disabled`

Do not carry VID out of network port.

Default

No default value is specified for nvo vxlan id command.

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan id 300
(config-nvo)#exit

(config)#nvo vxlan id 200 unicast
(config-nvo)#exit
```

The following is a sample output for multicast mode.

```
(config)#nvo vxlan id 100 multicast 239.10.10.10 (config-
nvo)#exit
```

nvo vxlan mac-ageing-time

Use this command to set the dynamically learned MAC aging time.

Use the `no` form of this command to set the age out the MACs in hardware to its default (300 seconds).

Command Syntax `nvo vxlan mac-ageing-time <10-1000000>`

```
no nvo vxlan mac-ageing-time
```

Parameters

`<10-1000000>` Ageing time in seconds.

Default

The default age out time is 300 seconds.

Command Mode

Configure mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#configure terminal
(config)#nvo vxlan mac-ageing-time 10
```

nvo vxlan max-cache-disable

Use this command to configure the maximum number of ARP and ND cache disables on access ports configured with the port+VLAN options. This command does not limit the ARP and ND cache disables on access ports created with only the port option.

Use the no form of this command to set the maximum number of ARP and ND cache disables to its default (0).

Note: If any mac is in conflict when the max cache disable is being unconfigured, then the corresponding caches will not be enabled. This can be enabled after manually, removing the conflict. Caches where there is no conflict, will be enabled.

Command Syntax `nvo vxlan max-cache-disable <1-200> no nvo vxlan max-cache-disable`

Parameters

<-1-200>	Number of ARP/ND cache disable allowed

Default

The default maximum number of ARP and ND cache disables is 0.

Command Mode

Configuration mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#configure terminal
(config)#nvo vxlan max-cache-disable 10
(config-nvo)#exit
```

nvo vxlan irb

Use this command to enable IRB functionality

Use the no form of this command to disable IRB functionality

Note: To make irb disable and enable effective, system reboot is required.

Command Syntax `nvo vxlan irb no nvo vxlan irb`

Parameters

None

Command Mode

Config Mode

Applicability

This command was introduced in SWMRE version 1.3.5.

Example

```
#configure terminal
```

```
(config)#nvo vxlan irb
(config)#no nvo vxlan irb
```

nvo vxlan tunnel qos-map-mode

Use this command to configure QoS COS-DSCP or DSCP-DSCP mapping for a tunnel in the ingress or egress direction.

Use the `no` form of this command to remove QoS mapping for a tunnel.

Command Syntax `nvo vxlan tunnel qos-map-mode (cos-dscp|dscp-dscp) (ingress|egress)`
`(<65-128>|) no nvo vxlan tunnel qos-map-mode (cos-dscp|dscp-dscp) (ingress|egress)`

Parameters

`cos-dscp`	COS-to-DSCP mapping: the COS in packets entering on an access port is copied to the DSCP field of VXLAN header in packets exiting the tunnel
`dscp-dscp`	DSCP-to-DSCP mapping: the DSCP in packets entering on an access port is copied to the DSCP field of VXLAN header in packets exiting the tunnel
`ingress`	Ingress direction (access network)
`egress`	Egress direction (network access)
`<65-128>`	QoS profile ID

Default

No default value is specified for nvo vxlan tunnel qos-map-mode command.

Command Mode

Configure mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#configure terminal
(config)#nvo vxlan tunnel qos-map-mode cos-dscp ingress
(config)#nvo vxlan tunnel qos-map-mode cos-dscp egress 128
(config)#exit

#configure terminal
(config)#nvo vxlan tunnel qos-map-mode dscp-dscp ingress
(config)#nvo vxlan tunnel qos-map-mode dscp-dscp egress 128 (config)#exit
```

nvo vxlan vtep-ip-global

Use this command to set the source IP address of the VxLAN tunnels.

Use the `no` form of this command to remove the source IP address of the VxLAN tunnels.

Command Syntax `nvo vxlan vtep-ip-global A.B.C.D no nvo vxlan vtep-ip-global A.B.C.D`

Parameters

A.B.C.D	Source VTEP IP address of the global configuration

Default

No default value is specified for nvo vxlan vtep-ip-global command.

Command Mode

NVO mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
(config-nvo)#nvo vxlan vtep-ip-global 10.10.11.1
```

qos cos-queue-profile

Use this command to create a QoS COS queue profile and enter COS queue profile mode.

Use the no form of this command to remove a COS queue profile.

Command Syntax `qos cos-queue-profile (ingress|egress) <1-64> no qos cos-queue-profile <1-64>`

Parameters

egress	Egress direction
ingress	Ingress direction
<1-64>	QoS profile identifier

Default

No default value is specified for qos cos-queue-profile command.

Command Mode

Configure mode

Applicability

This command was introduced in SWMRE version 1.3.

Example

```
#configure terminal
(config)#qos cos-queue-profile ingress 64
(config-cos-queue)#exit
```

qos dscp-queue-profile

Use this command to configure create a QoS DSCP queue profile and enter DSCP queue profile mode.

Use the no form of this command to remove a QoS DSCP queue profile.

Command Syntax `qos dscp-queue-profile (ingress|egress) <65-128> no qos dscp-queue-profile <65-128>`

Parameters

egress	Egress direction
ingress	Ingress direction
<65-128>	QoS profile identifier

Default

No default value is specified for qos dscp-queue-profile command.

Command Mode

Configure mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#configure terminal
(config)#qos dscp-queue-profile ingress 128
(config-dscp-queue)#exit
```

show bgp l2vpn evpn

Use this command to display details about Layer 2 Virtual Private Network (L2VPN) Ethernet Virtual Private Network (EVPN) routes.

Note: A BGP EVPN route update received for an unreachable IP address is also listed by this command and as a best route. This is because the next hop tracking feature is not supported for the EVPN address family. However, the tunnel to this IP address is shown in unresolved state by the show nvo vxlan tunnel output.

Note: An E-tag (Ethernet tag) can have the value of zero/VID/VNID based on the use case. An E-tag can go up to 32 bits and no restrictions are noted in the RFC. Since an E-tag can have different values, it should not be compared with the label/VNID.

Command Syntax `show bgp l2vpn evpn ((vrf WORD)|(rd WORD)| time|) show bgp l2vpn evpn mac-ip ((vrf WORD)|(rd WORD)|) show bgp l2vpn evpn mcast show bgp l2vpn evpn multihoming es-route <(rd WORD)|(vrf WORD)> show bgp l2vpn evpn multihoming ethernet-ad-per-evi <(rd WORD)|(vrf WORD)> show bgp l2vpn evpn multihoming ethernet-ad-per-es <(rd WORD)|(vrf WORD)>` **Parameters**

vrf	Virtual Routing and Forwarding instance
WORD	VRF name
rd	Route distinguisher
WORD	Route distinguisher: ASN:nn or IP:nn
time	Display learned time for EVPN routes
mac-ip	MAC/IP routes (EVPN type 2)
mcast	Multicast routes (EVPN type 3)

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show bgp l2vpn evpn

BGP table version is 25, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
l - labeled, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

[EVPN route type]:[ESI]:[VNID]:[relevent route
informantion] 1 - Ethernet Auto-discovery Route
```

```
2 - MAC/IP Route
3 - Inclusive Multicast Route
4 - Ethernet Segment Route

    Network          Next Hop            Metric    LocPrf      Weight Path  Peer

RD[1.1.1.1:1] VRF[vrfblue]:
*>   [2]:[0]:[100]:[48,0000:00aa:aaaa]:[32,10.1.1.2]:[100]
                      1.1.1.1             0         100           32768    i
*>i  [2]:[0]:[100]:[48,0000:00bb:bbbb]:[32,10.1.1.3]:[100]
                      4.4.4.4             0         100           0        i   10.1.1.1
*>   [3]:[100]:[32,1.1.1.1]
                      1.1.1.1             0         100           32768    i
*>i  [3]:[100]:[32,4.4.4.4]
                      4.4.4.4             0         100           0        i   10.1.1.1
*>   [3]:[101]:[32,1.1.1.1]
```

Status code	Description	Comments
s	suppressed	Whether the route is suppressed and is not advertised to neighbors.
d	damped	When the penalty of a flapping route exceeds the suppress limit, the route is damped and remains in a withdrawn state until its penalty decreases below the reuse limit.
h	history	When the penalty of a flapping route does not exceed the suppress limit, the route is not damped and BGP maintains a history of the flapping route.
*	valid	Whether the route is valid. When a route is not suppressed, damped, or present in the history, it is valid.
>	best	The selected route to be installed in the kernel routing table.
i	internal	The prefix was learned from an iBGP peer.

l	labeled	BGP Labeled Unicast advertises route information between inter region routers.

```
                         1.1.1.1              0          100           32768     i
*>i   [3]:[101]:[32,4.4.4.4]
                         4.4.4.4              0          100           0         i   10.1.1.1

RD[2.2.2.2:1]
*>i   [2]:[0]:[100]:[48,0000:00bb:bbbb]:[32,10.1.1.3]:[100]
                         4.4.4.4               0          100           0        i   10.1.1.1
*>i   [3]:[100]:[32,4.4.4.4]
                         4.4.4.4               0          100           0        i   10.1.1.1
*>i   [3]:[101]:[32,4.4.4.4]
                         4.4.4.4               0          100           0        i   10.1.1.1

Total number of prefixes 9
```

Table 1-243 shows the status codes displayed at the start of a route entry.

Table 1-243: status codes

Table 1-244 shows the codes at the end of each route entry that indicate where the route originated.

Table 1-244: origin codes

Origin Code	Description	Comments
i	IGP	The route is from an Interior Gateway Protocol.
e	EGP	The route is from an Exterior Gateway Protocol.
?	incomplete	Origin not known. Typically, these are routes redistributed from an IGP.

Table 1-245 explains the fields for each route.

Table 1-245: route entry fields

Field	Description
RD	Route distinguisher: AS number or IP address.
VRF	Name of the VRF.

Network	EVPN route information. The route type indicates the type of routing information advertised by the EVPN control plane: 2 MAC/IP Route: Endpoint reachability information, including MAC and IP addresses of the endpoints. 3 Inclusive Multicast Route: Information about how to forward Broadcast, Unknown Unicast and Multicast (BUM) traffic. The other fields included depend on the route type: Type 2: [ESI]:[E-Tag]:[Length, Host MAC address]:[Length, Host IP address]:[Label/VNID] Type 3: [E-Tag]:[Length, PE IP address] ESI (Ethernet Segment Identifier): a unique non-zero identifier that identifies an Ethernet segment, which is a set of links that connects a network or device to one or more PEs. ESI 0 denotes a single-homed site. E-Tag (Ethernet tag): identifies a particular broadcast domain such as a VLAN or VNID in the VxLAN case. An EVPN instance consists of one or more broadcast domains. VNID (VXLAN network identifier): identifies Layer 2 segments and maintains Layer 2 isolation between the segments, allowing the addressing of up to 16 million logical networks in the same administrative domain. The status codes are explained in Table 1-243.
Next Hop	IP address of the nexthop for this route.
Metric	Multiple-Exit Discriminator (MED). If there are multiple paths to the same destination from a single routing protocol, then the multiple paths have the same administrative distance and the best path is selected based on this metric. The path with the lowest metric is selected as the optimal path and installed in the routing table.
LocPrf	Local preference set with the `set local-preference` command. This value is used only with iBGP sessions within the local autonomous system to determine if a route towards a destination is the “best” one. The path with the highest local preference is preferred.
Weight	This field applies only to routes within an individual router. If a route was learned from a peer, it has a default weight of 0. All routes generated by the local router have a weight of 32,768.

Table 1-245: route entry fields (Continued)

Field	Description
Path	The autonomous systems through which the prefix advertisement passed. The origin codes are explained in Table 1-244.
Peer	Neighbor address.
Total number of prefixes	The total number of prefixes listed.

show bgp l2vpn evpn summary

Use this command to display a summary of BGP EVPN neighbor status.

Command Syntax `show bgp l2vpn evpn summary`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show bgp l2vpn evpn summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 17
1 BGP AS-PATH entries
0 BGP community entries

Neighbor                V   AS   MsgRcv     MsgSen TblVer   InQ   OutQ    Up/Down   State/PfxRcd      AD  MACIP  MCAST    ESI
8.8.8.8                 4   100  111         112      17      0      0  00:53:03              3       0      0      3      0
 9.9.9.9                4   100  110         110      17      0      0  00:52:10             15       0     13      2      0
13.13.13.13             4   100  132         109      17      0      0  00:51:57              4       0      2      2      0

Total number of neighbors 3

Total number of Established sessions 3
```

The start of the output shows:

- The BGP router identifier and the local router AS number.
- The BGP table version tracks the local BGP table version. Any time the BGP best path algorithm executes, the table version increments.
- BGP AS-PATH entry and community entries.

Table 1-246 explains the fields for each neighbor entry.

Table 1-246: neighbor fields

Field	Description
Neighbor	IP address of peer.
V	BGP version of peer.
AS	Autonomous system number of peer.

MsgRcvd	Messages received since the BGP connection was established.
MsgSent	Messages sent since the BGP connection was established.

Table 1-246: neighbor fields (Continued)

Field	Description
TblVer	Last version of the local router's BGP database advertised to the peer.
InQ	Received messages waiting in the input queue for further processing.
OutQ	Messages waiting in the output queue to be sent.
Up/Down	Connection up time in the interface.
State/PfxRcd	If the TCP session is up and the BGP peers have formed an adjacency, this field shows how many prefixes have been received from the remote neighbor. Other states: Idle: The local router has not allocated resources for the peer connection, so incoming connection requests are refused Idle (Admin): The peer has shut down Idle (PfxCt): Prefix overflow Idle (G-shut): Graceful shutdown Connect: BGP is waiting for the TCP connection to complete Active: the local router is trying to establish a TCP connection to the remote peer. You might see this if the local peer has been configured, but the remote peer is unreachable or has not been configured. OpenSent: BGP is waiting for an open message from its peer OpenConfirm: BGP received an open message from the peer and is now waiting for a keepalive or notification message. If BGP receives a keep alive message from the peer, the state changes to established. If the message is a notification, the state changes to idle. Established: BGP is ready to exchange update, notification, and keep alive messages with its peer Invalid: The session state is invalid.
AD	Number of EVPN type 1 Ethernet Auto-discovery routes: Only originated for multi-homed sites. Type 1 routes allow fast convergence where PE devices can change the next-hop adjacencies for all MAC addresses associated with a particular Ethernet Segment and aliasing where traffic can be balanced across multiple egress points

MACIP	Number of EVPN type 2 MAC/IP routes: Endpoint reachability information, including MAC and IP addresses of the endpoints.
MCAST	Number of EVPN type 3 Inclusive Multicast routes: Broadcast, Unknown Unicast and Multicast (BUM) traffic.
ESI	Number of EVPN type 4 Ethernet Segment Routes: Used in multi-homing for Designated Forwarder Election. The Designated Forwarder sends BUM traffic to the CE on a particular Ethernet Segment.

show nvo vxlan

Use this command to display VXLAN information.

Command Syntax `show nvo vxlan (vnid <1-16777215>|)`

Parameters

`<1-16777215>` VXLAN network identifier.

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#sh nvo vxlan
VXLAN Information
=================
   Codes: NW - Network Port
        AC - Access Port  (u)
        - Untagged

VNID     Vni-name     Type Interface ESI                            Vlan DF-
Status Src-addr         Dst-addr
_____________________________________________________________________________
_____________________________________
10        ----         NW ----        ----                          ---- ----
      1.1.1.1         3.3.3.3
10        ----         NW ----        ----                          ---- ----
      1.1.1.1         2.2.2.2
10        ----           AC ce21/1 00:00:11:22:33:44:55:66:77:88 2
DF         ----             ----
20        ----         NW ----        ----                          ---- ----
      1.1.1.1         3.3.3.3
20        ----         NW ----        ----                          ---- ----
      1.1.1.1         2.2.2.2
20        ----            AC ce21/1 00:00:11:22:33:44:55:66:77:88 3 NON-
```

```
  DF ----                ----

Total number of entries are 6
```

Table 1-247 explains the fields in the output.

Table 1-247: VxLAN fields

Field	Description
VNID	VXLAN network identifier.
Type	NW - Network Port: VxLAN tunnel AC - Access Port: Host connection

Table 1-247: VxLAN fields

Field	Description
Interface	Name of the Interface.
Vlan	VLAN identifier
Src-addr	Source address in the interface.
Dst-addr	Destination address in the interface.
Total number of entries	The total number of entries listed.

show nvo vxlan access-if-config

Use this command to display the current running configuration of the access interface.

Command Syntax `show nvo vxlan access-if-config (LINE|)`

Parameters

`LINE`	Access port description.

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.3.

Example

```
#show nvo vxlan access-if-config      nvo vxlan access-if
port-vlan xe1 2       map vnid 100
access-if-description member-port with xe1 as vlan 2 dynamic-learning
disable arp-nd flood-suppress arp-cache disable nd-cache disable shutdown
mac 0000.0000.1111 mac 0000.0000.aaaa ip 12.12.12.1 mac 0000.0000.bbbb
ipv6 1201::1 map qos-profile ingress 100 cos 2 egress
     !      nvo vxlan access-if port-vlan po1 6 inner-vlan 5
encapsulation 0x9100       no shutdown       map vnid 100
     !
```

show nvo vxlan arp-cache

Use this command to display the ARP cache information.

Command Syntax `show nvo vxlan arp-cache (vnid <1-16777215>|)`

Parameters

`<1-16777215>`	VXLAN network identifier.

Command Mode

Exec mode

Applicability

This command was introduced in a version before SWMRE version 1.3, modified to include new fields – Age-Out and Retries-Left in SWMRE version 1.3.5

Example

```
#sh nvo vxlan arp-cache
VXLAN ARP-CACHE Information
===========================
```

```
ARP Timeout :  300 sec   Random-Jitter-Max : 640

VNID     Ip-Addr          Mac-Addr       Type        Age-Out     Retries-Left
_____________________________________________________________________________
10       11.11.11.2       0000.0000.bbbb Dynamic Local  224       2
10       11.11.11.1 0000.0000.aaaa Remote Dynamic ---Total
number of entries are 2
```

Table 1-248 explains the fields in the output.

Table 1-248: arp cache fields

Field	Description
VNID	VXLAN network identifier.
Ip-Addr	IP address of the vxlan.
Mac-Addr	Device MAC address.
Type	How a host learns a MAC/IP pair: Dynamic: Learned by data plane source learning Evpn: Learned by EVPN Type 2 (MAC/IP) routes Static Remote: Statically configured for remote; used only for static VxLAN, not with EVPN Static Local: Configured on local VTEP
Total number of entries	The total number of entries listed.

show nvo vxlan counters access-port

Use this command to display the receive and transmit counters of an access port.

Note: This command does not display the ARP/ND transmit counters when ARP/ND is enabled on this port. To view the ARP/ND counters, use the `show nvo vxlan interface counters` command.

Note: Due to a limitation in the hardware, the transmit packet counters includes the BUM traffic received on that port.

Command Syntax `show nvo vxlan counters access-port (port IFNAME | port-vlan IFNAME VLAN_ID)`

Parameters

`IFNAME`	Access port name
`VLAN_ID`	VLAN identifier

Command Mode

Exec mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#show nvo vxlan counters access-port port-vlan xe1 2
RX:    packets: 74718            bytes   : 4982068
TX:    packets: 193322            bytes  : 14545436

#show nvo vxlan counters access-port port xe2
RX:    packets: 74718            bytes  :
4982068     TX:    packets: 193322
bytes  : 14545436
```

Table 1-249 explains the fields in the output.

Table 1-249: access port counters

Field	Description
RX: packets	Number of packets received.
RX: bytes	Number of bytes received.
TX: packets	Number of packets transmitted.
TX: bytes	Number of bytes transmitted.

show nvo vxlan counters network-port

Use this command to display the receive and transmit counters of a network port.

Note: This command does not display the ARP/ND transmit counters when ARP/ND is tunneled after cache lookup. To view the ARP/ND counters, use the show nvo vxlan interface counters command.

Command Syntax `show nvo vxlan counters network-port`

```
dst A.B.C.D
```

Parameters

`A.B.C.D`	Tunnel IPv4 address

Command Mode

Exec mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#show nvo vxlan counters network-port dst 1.1.1.1
RX:    packets: 74718            bytes  : 4982068
```

```
TX:    packets: 193322            bytes  :
14545436
```

Table 1-250 explains the each network entry fields.

Table 1-250: show nvo vxlan counters network-port output fields

Field	Description
RX: packets	Number of hello packets received from neighbor.
RX: bytes	Number of hello packets received from neighbor in bytes received.
TX: packets	Number of hello packets transmitted to neighbor.
TX: bytes	Number of hello packets transmitted to neighbor in bytes transmitted.

show nvo vxlan interface counters

Use this command to see the ARP/ND counters for VxLAN access ports.

Command Syntax `show nvo vxlan interface (IFNAME|) counters (active|)`

Parameters

`IFNAME`	Interface name.
`active`	Statistics for running interfaces.

Command Mode

Exec mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#show nvo vxlan interface counters

Interface xe1/1
 Rx Vxlan Arp discard count: 0
 Rx Vxlan Nd discard count: 0
 Rx Vxlan Arp Request count: 0
 Rx Vxlan Arp Reply count: 0
 Tx Vxlan Arp Reply count: 0
 Rx Vxlan ND Request count: 0
 Rx Vxlan ND Reply count: 0
 Tx Vxlan ND Reply count: 0

Interface xe1/2
 Rx Vxlan Arp discard count: 0
 Rx Vxlan Nd discard count: 0
```

```
Rx Vxlan Arp Request count: 0
Rx Vxlan Arp Reply count: 0
Tx Vxlan Arp Reply count: 0
Rx Vxlan ND Request count: 0
Rx Vxlan ND Reply count: 0
Tx Vxlan ND Reply count: 0
```

Table 1-250 explains the each interface counter entry fields.

Table 1-251: show nvo vxlan interface counters output details

Field	Description
Rx Vxlan Arp discard count	Number of discarded ARP that is received from neighbor.
Rx Vxlan Nd discard count	Number of discarded ND that is received from neighbor.
Rx Vxlan Arp Request count	Number of request ARP that is received from neighbor.

Table 1-251: show nvo vxlan interface counters output details

Field	Description
Rx Vxlan Arp Reply count	Number of replied ARP that is received from neighbor.
Tx Vxlan Arp Reply count	Number of replied ARP which is transmitted to peer.
Rx Vxlan ND Request count	Number of request ND that is received from neighbor.
Rx Vxlan ND Reply count	Number of replied ND that is received from neighbor.
Tx Vxlan ND Reply count	Number of replied ND which is transmitted to peer.

show nvo vxlan mac-table

Use this command to display the host MAC address table. Use the hardware option to see the ageout time for the dynamically learn macs.

Command Syntax `show nvo vxlan mac-table (vnid <1-16777215>|) (summary | hardware |)`

Parameters

`<1-16777215>` VXLAN network identifier.

`summary` Count the MAC addresses.

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show nvo vxlan mac-table
================================================================================
================================================================================
                     VXLAN MAC Entries
================================================================================
================================================================================
VNID       Interface VlanId Inner-VlanId Mac-Addr       VTEP-Ip/
                ESI  Type  Status          AccessPortDesc

_____________________________________________________________________________
_____________________________________________________________________________
10         ce21/1     2      ----          0000.0000.1111
1.1.1.1 partner-               Static Local          -------
port
10         ----       ---- ----            0000.0000.2222
3.3.3.3                        Remote Static         -------             -----
-                                                                         -
20         ce21/1     3      ----          0000.0000.cccc
1.1.1.1                        Static Local          Discard             -----
-                                                                         -
20         ----       ---- ----            0000.0000.dddd
3.3.3.3                        Remote Static         -------             -----
-                                                                         -
Total number of entries are : 4

#show nvo vxlan mac-table hardware
================================================================================
================================================================================
                        VXLAN MAC Entries
================================================================================
================================================================================
```

```
VNID       Interface VlanId Inner-VlanId Mac-Addr       VTEP-Ip/
ESI                    Type                  Status            Time-out
AccessPortDesc
_____________________________________________________________________________
_____________________________________________________________________
10          ce21/1 2       ---           0000.0000.1111
1.1.1.1     Static Local     ----partner-port                        ---
10         ---          --- ---           0000.0000.2222
3.3.3.3                       Remote                -----             ---
10         ---          --- ---           0000.0000.aa11
3.3.3.3                       Remote                -----             ---
10          ce21/1 2       ---           0000.0000.bb11
1.1.1.1     Dynamic Local    ----partner-port                        300
10          ce21/1 2       ---           0000.0000.bb12
1.1.1.1     Dynamic Local    ----partner-port                        277
20            ce21/1 --- ---              0000.0000.cccc
1.1.1.1                       Static Local          Discard           ---
20         ---          --- ---           0000.0000.dddd
3.3.3.3                       Remote                -----             ---
Total number of entries are 7
```

Table 1-252 explains the fields in the output.

Table 1-252: MAC table fields

Field	Description
VNID	VXLAN network identifier
Interface	Interface name
VlanId	VLAN identifier
Mac-Addr	MAC address
VTEP-Ip	VTEP identifier
Type	How a host learns a MAC/IP pair: Remote: Statically configured for remote; used only for static VxLAN, not with EVPN Static Local: Configured on local VTEP Dynamic Local: Learned by data plane source learning

Status	Max Move conflict: When a MAC has moved too many times (5 or more times in 180 seconds). This is according to the procedures defined in RFC 7432, Section 15.1. Discard: If a MAC hold time is configured, then if the VxLAN access port goes down (admin or operational), the MAC is moved to the discard state for the period of the hold time. The MAC is also moved to the discard state if the VNID is unmapped from the port. In dynamically learned cases, the MAC is also moved to discard when learning is disabled.
Time-out	Age timeout for dynamically learned MACs.
AccessPortDesc	Access port description.
Total number of entries	The total number of entries listed.

show nvo vxlan nd-cache

Use this command to display the Neighbor Discovery cache.

Command Syntax `show nvo vxlan nd-cache (vnid <1-16777215>|)`

Parameters

`<1-16777215>` VXLAN network identifier.

Command Mode

Exec mode

Applicability

This command was introduced in a version before SWMRE version 1.3, modified to include new fields – Age-Out and Retries-Left in SWMRE version 1.3.5.

Example

```
#show nvo vxlan nd-cache
VXLAN ND-CACHE Information
==========================
ND Timeout :  300 sec   Random-Jitter-Max : 640

VNID     Ip-Addr          Mac-Addr       Type          Age-Out    Retries-Left
_____________________________________________________________________________
 10       2001::1       0000.0000.1111  Dynamic Local    274          2
 10       2001::2       0000.0000.2222  Remote Dynamic    ---Total
number of entries are 2
```

Table 1-253 explains the output fields.

Table 1-253: ND cache fields

Field	Description
VNID	VXLAN network identifier
Ip-Addr	IP address
Mac-Addr	MAC address
Type	How a host learns a MAC/IP pair: Static Remote: Statically configured for remote; used only for static VxLAN, not with EVPN Static Local: Configured on local VTEP Dynamic: Learned by data plane source learning Evpn: Learned by EVPN Type 2 (MAC/IP) routes
Total number of entries	The total number of entries listed.

show nvo vxlan static host state

Use this command to display the state of the host which is configured statically.

Command Syntax `show nvo vxlan static host state`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#sh nvo vxlan static host state
VNID Ifname     Vlan     Ip-Addr        Mac-Addr         Status

_____________________________________________________________________
100      xe1           2     12.12.12.1       0000.0000.aaaa      Inactive
100      xe2           2     1201::1          0000.0000.bbbb      Conflict
100      xe3           2     120.120.120.1    0000.0000.bb11      Active
```

Table 1-254 explains the output fields.

Table 1-254: Static host fields

Field	Description

VNID	VXLAN network identifier
Ifname	Interface name
Vlan	VLAN name
Ip-Addr	IP address

Table 1-254: Static host fields

Field	Description
Mac-Addr	MAC address
Status	Status of the MAC/IP on the host: Conflict: When a MAC/IP was configured, the conflict was not known as the VNID was not mapped to the access port. After the VNID is mapped, if the same MAC/IP is present statically on some other port on the same VNID, then it is in conflict state. Learnt Conflict: When a MAC/IP was configured, the conflict was not known. However, it is now in conflict because the same MAC/IP is configured on an access port on VTEP1 and on an access port on VTEP2. Because the BGP session/tunnel was not up, the MAC/IP was not known to the other VTEP and the configuration was allowed. When the BGP session/tunnel comes up and it finds such a conflicted route, it marks the state as Learnt Conflict. Inactive: Configured but not operating, such as when the port is not mapped to any VNID. The port is down and the ARP/ND cache is disabled. Active: Operating host MAC/IP.

© Symanitron Proprietary

show nvo vxlan tunnel

Use this command to view the source, destination, and status of the VxLAN tunnel entries.

Command Syntax `show nvo vxlan tunnel`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

The following is a sample output of the `show nvo vxlan tunnel` command.

```
#show nvo vxlan tunnel
VXLAN Network tunnel Entries
 Source Destination      Status Up/Down Update
=================================================
1.1.1.1 2.2.2.2          Installed 00:00:20 00:00:20
Total number of entries are 1
#
```

Table 1-255 explains the output fields.

Table 1-255: VxLAN tunnel fields

Field	Description
Source	Tunnel source IP address.
Destination	Tunnel destination IP address.
Status	Installed: Tunnel Installed in the hardware and operating. Resolved: Tunnel destination IP is reachable, but VxLAN tunnel not installed in hardware. Therefore, not operating. Unresolved: Tunnel destination IP not reachable because L3 route is down.
Up/Down	When the tunnel came up or went down
Update	When the tunnel was last updated

Total number of entries	The total number of entries listed.

show running-config nvo vxlan

Use this command to display the current running configuration of VxLANs.

Command Syntax `show running-config`

```
nvo vxlan
```

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in a version before SWMRE version 1.3.3 and added few CLIs for IRB and ARP-ND refresh timer for SWMRE version 1.3.5.

Example

```
#show running-config nvo vxlan
!
     nvo multihoming enable
!      nvo vxlan enable
     !
     nvo vxlan irb
     !
     nvo vxlan vtep-ip-global 1.1.1.1
     !
     nvo vxlan max-cache-disable 10
     !
     nvo vxlan tunnel qos-map-mode cos-dscp ingress
     !
     nvo vxlan tunnel qos-map-mode dscp-dscp egress 128
     !
     nvo vxlan id 100 ingress-replication inner-vid-disabled
vxlan host-reachability-protocol evpn-bgp vrf1 evpn irb1 mac-
holdtime 20
     !      nvo vxlan access-if port-vlan
xe1 2       map vnid 100
access-if-description member-port with xe1 as vlan
2 dynamic-learning disable arp-nd flood-suppress
arp-cache disable nd-cache disable shutdown mac
0000.0000.1111
mac 0000.0000.aaaa  ip 12.12.12.1
mac 0000.0000.bbbb  ipv6 1201::1
```

```
  map qos-profile ingress 100 cos 2
  egress
    !     nvo vxlan access-if port-vlan po1 6 inner-vlan 5       encapsulation
0x9100      no shutdown       map vnid 100
    !
```

show evpn multi-homing all

Use this command to display the multi-homed VTEP details.

Command Syntax `show evpn multi-homing (all |)`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in SWMRE version 1.3.4.

Example

```
#show evpn multi-homing all
ESI                               Access-IF PE-IP-ADDRESS
                    ============================================================
00:00:11:22:33:44:55:66:77:88 ce21/1      1.1.1.1
00:00:11:22:33:44:55:66:77:88 ----  2.2.2.2 Total number of entries are 2
```

Table 1-256 explains the output fields.

Table 1-256: show evpn multi-homing all output details

Field	Description
ESI	An Ethernet segment has an unique nonzero identifier, called the Ethernet segment identifier (ESI). The ESI is encoded as a 10-octet integer that identifies this segment. When manually configuring an ESI value, the most significant octet, known as the type byte, must be 00. When a single-homed CE device is attached to an Ethernet segment, the entire ESI value is zero.
Access-IF	Map the access port ce21/1 for evpn.
PE-IP-ADDRESS	Address of the provider edge router in the interface.

show evpn multihoming-status

Use this command to display the status of multihoming on a VTEP.

Command Syntax `show evpn multihoming-status`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in SWMRE version 1.3.4.

Example

```
#show evpn multihoming-status
Multihoming is ACTIVE in Hardware
```

show nvo vxlan route-count

Use this command to display the vxlan active route (MAC-IP.MAC-IPv6 and MAC-only) count information.

Command Syntax `show nvo vxlan route-count (|vnid <1-16777215>)`

Parameters

`<1-16777215>` Range supported for VNID.

Command Mode

Exec mode

Applicability

This command was introduced in a version before SWMRE version 1.3.3 and modified to include new fields – GW-IPv4, GW_IPv6, Prefix IPv4 and Prefix IPv6 in SWMRE version 1.3.5.

Example

```
#show nvo vxlan route-count
VXLAN Active route count information
====================================
Max route count   : 32768
Active route count: 7

Note: Prefix count refers only local routes
      It does not include evpn prefix routes

-------------------------------------------------------------------------------
---------
 VNID     Total    MACONLY  MACIPv4  MACIPv6  GW          GW          Prefix
Prefix
                                              MACIPv4     MACIPv6     IPv4
IPv6
-------------------------------------------------------------------------------
---------
 2000     3        1        1        1        0           0           0
0
 1000     0        0        0        0        0           0           0
0
 10002    4        0        0        0        1           1           1
1

Total number of entries are 3
```

Table 1-257 explains the output fields.

Table 1-257: show nvo vxlan route-count output details

Field	Description

Max route count	Maximum number of route count in vxlan.
Active route count	Number of active route count in the interface.

Table 1-257: show nvo vxlan route-count output details

Field	Description
VNID	VNID is used to identify Layer 2 segments and to maintain Layer 2 isolation between the segments.
Total	Total number of entries for the interface.
MACONLY	The MAC-only route for the local interface appears in the VXLAN instance route table.
MACIPv4	IPv4 media access control (MAC) address for a default virtual gateway.
MACIPv6	IPv6 media access control (MAC) address for a default virtual gateway.

show nvo vxlan vni-name

Use this command to display the vxlan results bashed on vni-name.

Command Syntax `show nvo vxlan vni-name (WORD)`

Parameters

WORD	vxlan id name.

Command Mode

Exec mode

Applicability

This command was introduced in SWMRE version 1.3.4.

Example

```
#show nvo vxlan vni-name SITEA-PRO
VXLAN Information
=================
Codes: NW - Network Port
AC - Access Port
(u) - Untagged
VNID Vni-name Type Interface ESI Vlan DF-Status Src-addr Dst-addr
_____________________________________________________________________________
_____________________________
1 ---- NW ---- ---------- ---- ------ 10.0.1.1 10.0.6.8
1 ---- NW ---- ---------- ---- ------ 10.0.1.1 10.0.6.9
1 ---- NW ---- ---------- ---- ------ 10.0.1.1 10.0.3.1
1 ---- NW ---- ---------- ---- ------ 10.0.1.1 10.0.1.2
1 ---- NW ---- ---------- ---- ------ 10.0.1.1 10.0.5.1
1 ---- NW ---- ---------- ---- ------ 10.0.1.1 10.0.2.2
1 ---- NW ---- ---------- ---- ------ 10.0.1.1 10.0.2.1
1 SITEA-PRO AC xe7 — Single Hommed port — 2 ------ ---- ----
1 SITEA-PRO AC xe1 — Single Hommed port — 1010 ------ ---- ----
1 SITEA-PRO AC xe1 — Single Hommed port — 100 ------ ---- ----
1 SITEA-PRO AC xe1 — Single Hommed port — 2020 ------ ---- ----
1 SITEA-PRO AC po1 — Single Hommed port — 100 ------ ---- ----
1 SITEA-PRO AC po1 — Single Hommed port — 2 ------ ---- ----
1 SITEA-PRO AC po1 — Single Hommed port — 200 ------ ---- ----
1 SITEA-PRO AC xe8 — Single Hommed port — ---- ------ ---- ----
1 SITEA-PRO AC po2 — Single Hommed port — ---- ------ ---- ----
Total number of entries are 16
```

show nvo vxlan irb-status

Use this command to verify the following IRB status

Command Syntax `sh nvo vxlan irb-status`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in SWMRE version 1.3.5.

Example

```
#sh nvo vxlan irb-status IRB is
not enabled.

#sh nvo vxlan irb-status
IRB is ACTIVE in Hardware

#sh nvo vxlan irb-status
IRB is NOT-ACTIVE in Hardware. System reboot is required to activate it.
```

show running-config interface irb

Use this command to display the current running configuration of IRB interface.

Command Syntax `show running-config interface irb<1-4094>`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in a version SWMRE version 1.3.5.

Example

```
#show running-config interface irb1
!      interface irb1       ip vrf forwarding vrfip
ip address 144.144.144.1/24       ipv6 address 1201::1/48
```

```
 evpn irb-if-forwarding anycast-gateway-mac       shutdown
!
```

show interface irb

Use this command to display the current running configuration of IRB interface.

Command Syntax `show interface irb<1-4094>`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in a version SWMRE version 1.3.5.

Example

```
#show interface irb1
Interface irb1
  Scope: both
  Hardware is IRB  Current HW addr: 0000.0000.1313
  Physical:(Not Applicable)  Logical:0000.0000.1313
  Port Mode is Router
  Interface index: 1000001
  Metric 0 mtu 1500
  <UP,BROADCAST,RUNNING,MULTICAST>   VRF Binding:
Associated with vrfip
  DHCP client is disabled.
  Last Flapped: Never
  Statistics last cleared: Never
  inet 144.144.144.1/24 broadcast 144.144.144.255 inet6 1201::1/48
  inet6 fe80::200:ff:fe00:1313/64 RX
    unicast packets 0 multicast packets 0 broadcast packets 0     input
packets 0 bytes 0     jumbo packets 0
    undersize 0 oversize 0 CRC 0 fragments 0 jabbers 0        input error 0
   input with dribble 0 input discard 0
   Rx pause 0  TX
   unicast packets 0 multicast packets 0 broadcast packets 0    output
packets 0 bytes 0    jumbo packets 0
   output errors 0 collision 0 deferred 0 late collision 0    output
discard 0          Tx pause 0
```

show bgp l2vpn evpn prefix-route

Use this command to display prefix-routes attached behind Tenant System.

Command Syntax `show bgp l2vpn evpn prefix-route <vrf WORD | rd Word>`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced in a version SWMRE version 1.3.5.

Example

```
#show bgp l2vpn evpn prefix-route

RD[100:1]
ESI  Eth-Tag Prefix-Length  IP-Address    GW-IP Address    L3VNID    Nexthop
0       0       24          100.100.100.0 144.144.144.10   0002
97.97.97.1 0       0       48             2201::       1201::10      10002
97.97.97.1

RD[300:1] VRF[vrfip]:
ESI    Eth-Tag Prefix-Length  IP-Address  GW-IP Address    L3VNID    Nexthop
0         0       24         100.100.100.0  144.144.144.10  10002
99.99.99.1
0         0       48            2201::       01::10        10002
99.99.99.1
```

shutdown

Use this command to administratively shut down an NVO access interface.

Use the `no` form of this command to start an NVO access interface.

Command Syntax `shutdown no shutdown`

Parameters

None

Default

The NVO access interface is running by default.

Command Mode

NVO access interface mode

Applicability

This command was introduced in SWMRE version 1.3.3.

Example

```
#configure terminal
                (config)#nvo vxlan access-if port-vlan xe1 2
(config-nvo-acc-if)#shutdown
(config-nvo-acc-if)#exit
```

vxlan host-reachability-protocol evpn-bgp

Use this command to set the host reachable protocol to Ethernet-VPN over BGP. This defines BGP as the mechanism for host reachability advertisement.

Use use the no form of this command to remove Ethernet-VPN as the host reachable protocol.

Command Syntax `vxlan host-reachability-protocol evpn-bgp NAME no vxlan host-reachability-protocol evpn-bgp`

Parameters

`NAME`	Name of the VRF to carry VNID routes.

Default

No default value is specified for vxlan host-reachability-protocol command.

Command Mode

NVO mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
(config)#nvo vxlan id 3
(config-nvo)#vxlan host-reachability-protocol evpn-bgp Blue
```

vxlan static-entry host-mac

Use this command to create a static route to reach a destination MAC in the VXLAN forwarding table. This command helps to supports different tenants so that they can have the same MAC/IP, but different VNIDs.This command is required for unicast tunnels to map the remote VTEP.

Use no form of this command to delete a static entry in the VXLAN forwarding table.

Command Syntax `vxlan static-entry host-mac MAC (remote-vtep-ip A.B.C.D) no vxlan static-entry host-mac MAC (remote-vtep-ip A.B.C.D)`

Parameters

`MAC`	MAC address of the host.
`A.B.C.D`	Unicast IP address of the destination VTEP.

Default

No default value is specified for vxlan static-entry host-mac command.

Command Mode

NVO mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#nvo vxlan id 2
(config-nvo)#vxlan static-entry host-mac 5254.0059.424f remote-vtep-ip
10.11.0.1
(config-nvo)#exit

(config)#nvo vxlan id 2
(config-nvo)#no vxlan static-entry host-mac 5254.0059.424f remote-vtep-
ip 10.11.0.1
(config-nvo)#exit
```

 © Symanitron Proprietary

SECTION 15 Neighbor Discovery

Symanitron

Neighbor Discovery Configuration Guide

Contents

This document contains these chapters:

- Chapter 1, *Neighbor Discovery Configuration*

CHAPTER 1 Neighbor Discovery Configuration

This chapter provides an overview of Neighbor Discovery (ND) configuration.

The Address Resolution Protocol (ARP) translates network layer addresses into link-layer addresses. ARP converts a an IPv4 address to an Ethernet address (MAC address).

In Internet Protocol Version 6 (IPv6) networks, the functionality of ARP is provided by the Neighbor Discovery (ND) protocol. Neighbor Discovery operates at the link layer and is responsible for auto configuration of nodes, discovery of other nodes on the link, determining the link layer addresses of other nodes, duplicate address detection, finding available routers and Domain Name System (DNS) servers, address prefix discovery, and maintaining reachability information about the paths to other active neighbor nodes.

Configuring ARP for IPV4

The procedures in this section use the topology in Figure 1-245

Figure 1-245: ARP for IPV4

RTR1

`#configure terminal`	Enter the configure mode.
`(config)#interface xe1`	Enter the interface mode.
`(config-if)#ip address 2.2.2.2/24`	Configure IP address on the interface.
`(config-if)#exit`	Exit the interface mode.
`(config)#ip arp 2.2.2.3 0000.0000.0003`	Configure ARP entry for neighbor.
`(config)#exit`	Exit configure mode.

RTR2

`#configure terminal`	Enter the configure mode.
`(config)#interface xe1`	Enter the interface mode.
`(config-if)#ip address 2.2.2.3/24`	Configure IP address on the interface.
`(config-if)#exit`	Exit the interface mode.
`(config)#ip arp 2.2.2.2 0000.0000.0004`	Configure ARP entry for neighbor.
`(config)#exit`	Exit configure mode.

Validation

```
#show arp

Flags: D - Static Adjacencies attached to down interface
```

```
Total number of entries: 2
```

© Symanitron

Neighbor Discovery Configuration

```
Address           Age      MAC Address     Interface  State
10.12.17.1        00:00:29 44e4.d982.274a  eth0       REACHABLE
2.2.2.3               -    0000.0000.0003  ge2        PERMANENT
```

Configuring Neighbor Discovery for IPV6

The procedures in this section use the topology in Figure 1-246.

Figure 1-246: ND for IPv6

RTR1

`#configure terminal`	Enter the configure mode.
`(config)#interface xe1`	Enter the interface mode.
`(config-if)#ipv6 address 3ffe:506::1/48`	Configure IPv6 address on the interface.
`(config-if)#exit`	Exit the interface mode.
`(config)# ipv6 neighbor 3ffe:506::2 xe1 0000.0000.0004`	Configure neighbor IPv6 address and MAC.
`(config)#exit`	Exit configure mode.

RTR2

`#configure terminal`	Enter the configure mode.
`(config)#interface xe1`	Enter the interface mode.
`(config-if)#ipv6 address 3ffe:506::2/48`	Configure IPv6 address on the interface.
`(config-if)#exit`	Exit the interface mode.
`(config)# ipv6 neighbor 3ffe:506::1 xe1 0000.0000.0003`	Configure neighbor IPv6 address and MAC.
`(config)#exit`	Exit configure mode.

Validation

```
#sh ipv6 neighbors

R - Reachable, I - Incomplete, S - Stale, F - Failed, P - Probe, D
- Delay, PR - Permanent

Flags: (D) - Static neighbors attached to down interface
```

```
Total number of entries:1
Address         Age       MAC Address     Source  Interface       State
3ffe:506::2       -       0000.0000.0004  Static  xe3             PR
```


Neighbor Discovery Command Reference

Contents

This document contains these chapters:

- Chapter 1, *Neighbor Discovery Commands*

CHAPTER 1 Neighbor Discovery Commands

This chapter provides a description, syntax, and examples of the ND commands. It includes the following commands:

- arp-ageing-timeout
- arp-reachable-time
- clear arp
- clear ipv6 neighbors
- debug ip arp
- debug ipv6 nd
- ip arp
- ip arp vrf
- ip proxy-arp
- ipv6 neighbor
- nd-ageing-timeout
- nd-reachable-time
- no debug all
- show arp
- show debugging ip arp
- show debugging ipv6 nd
- show ipv6 neighbors

arp-ageing-timeout

Use this command to set the ARP ageing timeout.

Use `no` form of this command to set the ageing to its default value.

Command Syntax `arp-ageing-timeout <60-28800> no arp-ageing-timeout`

Parameter

`<60-28800>`	Specify the ARP ageing timeout.

Default value

By default, arp-ageing-timeout value is 1500

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface xe2
(config-if)#arp-ageing-timeout 5000
(config-if)#exit

(config)#interface xe2
(config-if)#no arp-ageing-timeout
```

arp-reachable-time

Use this command to set the ARP reachable time.

Use `no` form of this command to set the reachable time to its default value.

Command Syntax `arp-reachable-time <10-3600> no arp-reachable-time`

Parameters

`<10-3600>`	Specify the ARP reachable time.

Default value

By default, arp-reachable-time is 60

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface xe2
(config-if)#arp-reachable-time 120
(config-if)#exit

(config)#interface xe2
(config-if)#no arp-reachable-time
```

clear arp

Use this command to clear dynamic ARP entries.

Command Syntax `clear arp (| A.B.C.D) (| vrf (all | VRFNAME | default)) clear arp IFNAME (| vrf (all | VRFNAME | default))`

Parameters

`A.B.C.D`	Specify the IP address of the ARP entry.
`IFNAME`	Specify the name of the interface.
`all`	All VRFs.
`VRFNAME`	VPN routing/forwarding instance name.
`default`	Default VRF.

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear arp
#clear arp xe1
#clear arp 10.10.10.10
#clear arp vrf VRF1
```

clear ipv6 neighbors

Use this command to clear dynamic neighbor entries.

Command Syntax `clear ipv6 neighbors (|X:X::X:X) (|vrf (all | VRFNAME | default)) clear ipv6 neighbors IFNAME (|vrf (all | VRFNAME | default))`

Parameters

`X:X::X:X`	Specify the neighbor's IPv6 address.
`IFNAME`	Specify the name of the interface.
`all`	All VRFs.
`VRFNAME`	VPN routing/forwarding instance name.
`default`	Default VRF.

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#clear ipv6 neighbors
#clear ipv6 neighbors xe1
#clear ipv6 neighbors 2000::3
#clear ipv6 neighbors vrf VRF1
```

debug ip arp

Use this command to enable debugging for ARP events or packets.

Use the `no` parameter with this command to disable event or packet debugging.

Command Syntax `debug ip arp (event | packet)` `no debug ip arp (event | packet)`

Parameters

`event`	ARP event debugging.
`packet`	ARP packet debugging.

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#debug ip arp event
```

debug ipv6 nd

Use this command to enable debugging for neighbor events or packets.

Use the `no` parameter with this command to disable event or packet debugging.

Command Syntax `debug ipv6 nd (event | packet) no debug ipv6 nd (event | packet)`

Parameters

`event`	ARP event debugging.
`packet`	ARP packet debugging.

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#debug ipv6 nd packet
```

ip arp

Use this command to create a static ARP entry.

Use the `no` parameter to remove the static ARP entry.

Command Syntax `ip arp A.B.C.D XXXX.XXXX.XXXX (alias|) no ip arp A.B.C.D`

Parameters

`A.B.C.D` Specify the IP address of the ARP entry.

`XXXX.XXXX.XXXX` Specify the MAC (hardware) address of the ARP entry. `alias` Specify the response to ARP requests for the IP address.

Default value

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#ip arp 10.10.10.10 0000.0001.4566
(config)#no ip arp 10.10.10.10
```

ip arp vrf

Use this command to create a static ARP entry for the non-default VRF.

Note: This command is supported only for multiple VRF support.

Command Syntax `ip arp vrf NAME A.B.C.D XXXX.XXXX.XXXX (alias|)`

Parameter

`NAME` Specify VRF name to which entry need to be added. `A.B.C.D` Specify the IP address of the ARP entry.

`XXXX.XXXX.XXXX` Specify the MAC (hardware) address of the ARP entry. `alias` Specify the response to ARP requests for the IP address.

Default value

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
          (config)#ip arp vrf VRF1 10.10.10.10 0000.0001.4566
```

ip proxy-arp

Use this command to enable the proxy ARP feature.

Use the `no` parameter to disable the proxy ARP feature.

Command Syntax `ip proxy-arp no ip proxy-arp`

Parameter

None

Default value

No default value is specified

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#ip proxy-arp
(config-if)#no ip proxy-arp
```

ipv6 neighbor

Use this command to add a static neighbor entry.

Use the `no` form of this command to remove a static neighbor entry.

Command Syntax `ipv6 neighbor X:X::X:X IFNAME XXXX.XXXX.XXXX no ipv6 neighbor X:X::X:X IFNAME`

Parameter

`X:X::X:X`	Specify the neighbor's IPv6 address.
`IFNAME`	Specify the name of the interface.
`XXXX.XXXX.XXXX`	Specify the MAC hardware address.

Default value

No default value is specified

Command Mode

Configure mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
                                (config)#ipv6 neighbor 2000::3 xe1 0000.0002.3dc1
(config)#no ipv6 neighbor 2000::3 xe1
```

nd-ageing-timeout

Use this command to set the neighbor ageing timeout value.

Use `no` form of this command to set the ageing to its default value.

Command Syntax `nd-ageing-timeout <60-28800> no nd-ageing-timeout`

Parameters

`<60-2880>`	ND ageing timeout in seconds.
`IFNAME`	Specify the name of the interface.
`XXXX.XXXX.XXXX`	Specify the MAC hardware address.

Default value

By default, nd-ageing-timeout is 1500 seconds

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#configure terminal
(config)#interface xe1
(config-if)#nd-ageing-timeout 3600
(config-if)#no nd-ageing-timeout
```

nd-reachable-time

Use this command to set neighbor reachable time value.

Use `no` form of this command to set the reachable time to its default value.

Command Syntax `nd-reachable-time <10-3600> no nd-reachable-time`

Parameter

`<10-3600>`	ND reachable time in seconds.

Default value

By default, nd-reachable-time is 60 seconds

Command Mode

Interface mode

Applicability

This command was introduced before SWMRE version 1.3.

Examples

```
#configure terminal
(config)#interface xe1
(config-if)#nd-reachable-time 300
(config-if)#no nd-reachable-time
```

no debug all

Use this command to disable all ARP and the neighbor debugging.

Command Syntax `no debug all undebug all`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#no debug all
```

show arp

Use this command to display ARP entry information.

Command Syntax `show arp (| (A.B.C.D | detail | static) (| vrf (all | VRFNAME | default))) show arp IFNAME (| vrf (all | VRFNAME | default)) show arp summary (|IFNAME) (| vrf (all | VRFNAME | default))`

Parameters

`detail`	Display detailed information.
`static`	Display static ARP entries.
`A.B.C.D`	Specify the IP address of the ARP entry.
`IFNAME`	Specify the name of the interface.
`all`	All VRFs.
`VRFNAME`	VPN routing/forwarding instance name.
`default`	Default VRF.

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show arp

Flags: D - Static Adjacencies attached to down interface

IP ARP Table for context default
Total number of entries: 2
Address          Age      MAC Address     Interface  State
10.12.18.1       00:00:18 44e4.d982.274b  eth0       REACHABLE
10.10.10.20      00:02:33 a8b1.d433.4140  xe1        STALE

#show arp summary vrf default

IP ARP Table - Adjacency Summary

  Resolved   : 2
  Incomplete : 0
  Unknown    : 0
  Total      : 2
```

Table 1-258 explains the show command output fields.

Table 1-258: show arp output details

Entry	Description
Address	ARP entry's IP address in the device.
Age	The number of minutes before the ARP entry was refreshed. If this value reaches the ARP aging period, the entry is removed from the table. Static entries do not age out.
MAC Address	Physical address of the host.
Interface	Logical address to connect the device over network.
State	INCOMPLETE – first ARP request sent, send ARP request. REACHABLE – normal expiration reset use counter. STALE – still usable; needs verification reset use counter; change state to delay. DELAY – schedule ARP request; needs verification reset use counter. PROBE – sending ARP request reset use counter. FAILED – no response received send ARP request. NOARP – normal expiration; never verified reset use counter. PERMANENT – never expires; never verified reset use counter.

Network devices are considered adjacent if they can reach each other with a single hop. The summary command shows the count of the state of devices that are adjacencies.

Table 1-259 explains the show command output fields.

Table 1-259: show arp summary output details

Field	Description
Resolved	Count of working/known adjacencies.
Incomplete	Count of yet to be established adjacencies.
unknown	Count of adjacencies not currently in ARP table.
Total	Total count of all adjacencies.

show debugging ip arp

Use this command to display debugging information for ARP.

Command Syntax `show debugging ip arp`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show debugging ip arp ND IP Debugging status:
                       ND ip arp event debugging is off
                       ND ip arp packet debugging is off
```

show debugging ipv6 nd

Use this command to display debugging information for the neighbor.

Command Syntax `show debugging ipv6 nd`

Parameters

None

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show debugging ipv6 nd
ND IPV6 Debugging status:
  ND ipv6 event debugging is off
  ND ipv6 packet debugging is off
```

show ipv6 neighbors

Use this command to display the neighbor information.

Command Syntax

```
show ipv6 neighbors (| (X:X::X:X | detail | static) (| vrf (all | VRFNAME |
  default)))
show ipv6 neighbors IFNAME (| vrf (all | VRFNAME | default)) show ipv6
neighbors summary (| IFNAME) (| vrf (all | VRFNAME | default))
```

Parameters

detail	Show detail information of neighbor.
static	Static entry.
X:X::X:X	Specify the neighbor's IPv6 address.
IFNAME	Specify the name of the interface.
all	All VRFs.
VRFNAME	VPN routing/forwarding instance name.
default	Default VRF.

Command Mode

Exec mode

Applicability

This command was introduced before SWMRE version 1.3.

Example

```
#show ipv6 neighbors

R - Reachable, I - Incomplete, S - Stale, F - Failed, P - Probe,
D - Delay, PR - Permanent

Flags: (D) - Static neighbors attached to down interface

IPv6 Neighbor Table for context default
Total number of entries:2
Address        Age       MAC Address     Source  Interface      State
fe80::210:18ff:fe7f:f758
                00:43:04  0010.187f.f758  icmpv6  eth0            S 2000::5
00:55:25  0000.0001.0242  icmpv6  xe1             S

#show ipv6 neighbors summary

IPv6 Neighbors Table - Adjacency Summary

  Resolved   : 2
  Incomplete : 0
  Unknown    : 0
  Total      : 2
```

Table 1-260 shows the status codes displayed at the start of a route entry.

Table 1-260: status code output details

Status Code	Field	Description
R	Reachable	Normal expiration reset use counter.
I	Incomplete	First ARP request sent, send ARP request.
S	Stale	Still usable; needs verification reset use counter; change state to delay.
F	Failed	ARP requests response not received.
P	Probe	ARP request reset use counter.
D	Delay	Schedule ARP request; needs verification reset use counter.
PR	Permanent	Never expires; never verified reset use counter.

Table 1-261 explains the show command output fields.

Table 1-261: show ipv6 neighbors output details

Field	Description
Address	ARP entry's IP address in the device.
Age	The number of minutes before the ARP entry was refreshed. If this value reaches the ARP aging period, the entry is removed from the table. Static entries do not age out.
MAC Address	Physical address of the host.
Source	ARP request source in the interface.
Interface	Logical address to connect the device over network.
State	ARP request state that is being handled by the IPv6 neighbor session.

Table 1-262 explains the show command output fields.

Table 1-262: show arp summary output details

Field	Description
Resolved	Count of working/known adjacencies.
Incomplete	Count of yet to be established adjacencies.
unknown	Count of adjacencies not currently in ARP table.
Total	Total count of all adjacencies.

SECTION 16 Glossary

Glossary

Conventions

This document uses the conventions described below.

Sort Order

The terms are arranged in ASCII order with the case of the characters ignored. This is the same as if the terms were sorted by this Linux command:

sort -f

This means that spaces, symbols, and digits come before alphabetic characters. Digits are sorted as strings, not numeric values (“10” comes before “2”).

The exact ASCII collating sequence is as shown below, with a space character in the first position:

```
 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
```

There are some exceptions to this rule when it makes more sense than strict ASCII order:

- (S,G) is under S
- G.8032 and G.8032 are under Numbers

Acronyms

The full phrase is shown before the acronym. For example:

- network address translation (NAT)
- Local Area Network (LAN)

An exception is when the acronym is used exclusively to refer to the term, in which case the acronym is shown before the full form:

- I-SID (Service Instance Identifier)
- NETCONF (Network Configuration Protocol)

- BGP confederation
- FEC-to-NHLFE (FTN) map
- GARP VLAN Registration Protocol (GVRP)
- MAC address

Case

As shown in the examples above, all lowercase is used for terms except when the predominant usage is initial uppercase or all uppercase.

Terms

Numbers

1588v2. IEEE specification for Precision Time Protocol (PTP).

802. A family of IEEE Local Area Network (LAN) standards. The services and protocols specified by the 802 standards map to Layer 1 (L1) and Layer 2 (L2) of the Open Systems Interconnection (OSI) Reference Model:

- 802.1: Overview architecture of LANs and interneworking
- 802.2: The logical link control (LLC) sublayer of Layer 2 (L2)
- 802.3: Layer 1 (L1) and the Media Access Control (MAC) sublayer of Layer 2 (L2), Also called Ethernet.

802.1AB. IEEE specification for Link Layer Discovery Protocol (LLDP).

802.1ad. Amendment to IEEE 802.1Q for Provider Bridging (PB).

802.1ag. Amendment to IEEE 802.1Q for Connectivity Fault Management (CFM).

802.1ah. IEEE specification that adds Provider Backbone Bridging (PBB) to 802.1ad Provider Bridging (PB):

802.1ak. Amendment to IEEE 802.1Q for Multiple Registration Protocol (MRP).

802.1aq. Amendment to IEEE 802.1D for Shortest Path Bridging (SPB).

802.1AX. IEEE specification for link aggregation and Multi-Chassis Link Aggregation (MC-LAG).

802.1D. IEEE specification which allows multiple LANs to be connected together through what the standard calls a “MAC bridge” which filters data sent between LAN segments, allowing networks to be partitioned for administrative purposes and reducing network congestion. The more common term for a MAC bridge is switch. The 802.1D standard includes Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP).

802.1p. IEEE 802.1Q defines priority signaling for traffic that can be used by Quality of Service (QoS) mechanisms to differentiate traffic. Packets are tagged as belonging to a queue, which determines the priority of the packet. Although this technique is often called “802.1p”, there is no standard by that name. Instead, the technique is incorporated into 802.1Q standard.

802.1Q. IEEE Virtual Local Area Network (VLAN) and Multiple Spanning Tree Protocol (MSTP) specifications. This standard refers to VLANs as “virtual bridged networks”. The 802.1D standard covers “VLAN-unaware” switches, while 802.1Q extends 802.1D for “VLAN-aware” switches.

802.1Qau. Amendment to IEEE 802.1Q for Quantized Congestion Notification (QCN).

802.1Qay. Amendment to IEEE 802.1Q for Provider Backbone Bridge-Traffic Engineering (PBB-TE).

802.1Qaz. Amendment to IEEE 802.1Q for Data Center Bridging Capability Exchange (DCBX) and Enhanced Transmission Selection (ETS).

802.1Qbb. Amendment to IEEE 802.1Q for Priority-based Flow Control (PFC).

802.1Qbg. Amendment to IEEE 802.1Q for Edge Virtual Bridging (EVB).

802.1v. Amendment to IEEE 802.1Q to classify incoming packets based on data link layer protocol identification.

802.1X. IEEE specification for port authentication.

802.3ah. IEEE specification for Ethernet to the First Mile (EFM).

802.3x. IEEE specification for flow control.

G.8032. ITU-T specification for Ethernet Linear Protection Switching (ELPS).

G.8032. ITU-T specification for Ethernet Ring Protection Switching (ERPS).

A

Access Control List (ACL). A set of rules used to filter traffic. Each rule specifies a set of conditions (such as source address, destination address, type of packet, or combination of these items) that a packet must meet to match the rule. When a device determines that an ACL applies to a packet, it tests the packet against the conditions of all rules. The first match determines whether the packet is permitted or denied.

access layer. In the network design model, the layer that connects devices such as desktops, laptops, servers, and printers to the network and provides end users access to network resources. This layer accepts traffic into a network and can pass that traffic to the distribution layer. The access layer is usually built using Layer 2 (L2) switching such as Spanning Tree Protocol (STP). This layer connects logical broadcast domains and provides isolation to groups of users. Typically, Virtual Local Area Network (VLAN) instances are implemented as broadcast domains in the access layer. Also called the edge layer. See also customer edge (CE), provider edge (PE).

acknowledgment (ACK). Notification sent from one network device to another to acknowledge that some event (for example, receipt of a message) has occurred.

active route. Route chosen from all routes in a Routing Information Base (RIB) to reach a destination. Active routes are installed in the Forwarding Information Base (FIB).

address. A unique identifier for a device on a network, either as a sender or receiver. An address can be a physical address or a logical address.

See also address family, address resolution, Classless Interdomain Routing (CIDR), domain name, Domain Name Service (DNS), dynamic address, IP address, MAC address, name resolution, static address.

address family. A specific type of network addressing supported by a routing protocol. Examples are IPv4 unicast and IPv4 multicast.

address resolution. The process of translating the address of an entity on one system to the equivalent address of the same entity on another system. For instance, translating an IP address to its Domain Name Service (DNS) name. See also Address Resolution Protocol (ARP).

Address Resolution Protocol (ARP). A Transmission Control Protocol/Internet Protocol (TCP/IP) mechanism that maps a MAC address to an IP address in the ARP cache data structure. Defined in RFC 826. See also Neighbor Discovery Protocol (NDP).

adjacency. The relationship between neighboring devices for exchanging routing information. Adjacent devices share a common network segment.

A given device can have multiple adjacencies, but each adjacency consists of only two devices connected by one link. A protocol data unit (PDU) that goes between them does not have to pass through any other network devices. See also neighbor.

administrative distance. How reliable the source of the route is considered to be. A lower value is preferred over a higher value. An administrative distance of 255 indicates no confidence in the source; routes with this distance are not installed in the Routing Information Base (RIB). Also called route preference.

Advanced Encryption Standard (AES). A cryptographic algorithm for use by U.S. Government organizations to protect sensitive (unclassified) information. Defined in Federal Information Processing Standards (FIPS) PUB 197.

advertising. Process in which routing or service updates are sent at specified intervals so that other devices on the network can maintain lists of usable routes.

Agent Extensibility (AgentX). A protocol used to implement Simple Network Management Protocol (SNMP) that defines communications between an SNMP agent and an SNMP client. AgentX does not directly communicate with an SNMP client, but relies on the agent to handle the protocol details of SNMP. Defined by RFC 2741.

aggregate route. A single entry in a routing table that represents a combination of groups of routes that have common addresses. See also route summarization.

alarm indication signal (AIS). A signal transmitted instead of the normal signal to maintain transmission continuity and to indicate to the receiving device that a transmission interruption (fault) has occurred either at the equipment originating the AIS signal or upstream of that equipment.

American National Standards Institute (ANSI). A voluntary organization of corporate, government, and other members that develops international and U.S. standards relating to, among other things, communications and networking. ANSI is a member of the International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO).

application-specific integrated circuit (ASIC). An integrated circuit that is designed for a specific application.

area. A logical division of devices that maintains detailed routing information about itself as well as routing information that allows it to reach other routing subdomains. An area divides a network into small, manageable pieces, reducing the amount of information each device must store and maintain about all other devices.

In Intermediate System to Intermediate System (IS-IS) and Open Shortest Path First (OSPF), an area is a set of contiguous networks and hosts within an autonomous system (AS) that have been administratively grouped together.

area border router (ABR). A router on the border of one or more Open Shortest Path First (OSPF) areas that connects those areas to the backbone network. An ABR is a member of both the OSPF backbone and its attached

areas. Therefore, an ABR maintains routing tables for both the backbone topology and the topology of the other areas. See also Not-So-Stubby-Area (NSSA), stub area.

authentication. A process that verifies that data is not altered during transmission and ensures that users are communicating with the individual or organization that they believe they are communicating with.

authentication, authorization, and accounting (AAA). A framework for controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services:

- Authentication determines who the user is and whether to grant that user access to the network
- Authorization determines what the user can do
- Accounting tracks the user's activities and provides an audit trail that can be used for billing or resource tracking

See also Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial In User Service (RADIUS), Terminal Access Controller Access Control System Plus (TACACS+).

Authentication Header (AH). An Internet Protocol Security (IPsec) protocol that authenticates either all or part of the contents of a packet by adding a header with a a hash message authentication code (HMAC) calculated based on the values in the packet. AH provides authentication but not confidentiality. See also Encapsulating Security Payload (ESP).

Automatic Protection Switching (APS). A means to detect a signal failure or signal degrade on a working channel and switch traffic to a protection channel. There are two types of APS:

- Ethernet Linear Protection Switching (ELPS) • Ethernet Ring Protection Switching (ERPS)

autonomous system (AS). A network controlled as a single administrative entity sharing a common routing strategy. An autonomous system is subdivided into areas. An AS runs an Interior Gateway Protocol (IGP) such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), or Intermediate System to Intermediate System (IS-IS) within its boundaries. An AS uses an Exterior Gateway Protocol (EGP) to exchange routing information with other ASs.

autonomous system border router (ASBR). An area border router (ABR) located between an Open Shortest Path First (OSPF) autonomous system (AS) and a non-OSPF network. ASBRs run both OSPF and another routing protocol, such as Routing Information Protocol (RIP).

An ASBR is a link between the OSPF autonomous system and the outside network. An ASBR exchanges routing information with routers in other ASes. The ASBR redistributes routing information received from other ASs throughout its own AS. An ASBR must reside in a standard OSPF area.

availability. The amount of time that a system is available during time periods when it is expected to be available. Availability is often measured as a percentage of an elapsed year. For example, 99.95% availability equates to 4.38 hours of downtime in a year (0.0005 * 365 * 24=4.38) for a system that is expected to be available all the time.

B

B-MAC. A source and destination backbone MAC address (B-AA and a B-DA) in a Provider Backbone Bridging (PBB) header.

B-TAG. See backbone VLAN (B-VLAN).

backbone. The part of a network used as the primary path for transporting traffic between network segments.

backbone core bridge (BCB). A device that bridges frames based on backbone VLAN (B-VLAN) and backbone MAC address (B-MAC) information in a Provider Backbone Bridging (PBB) network core.

backbone edge bridge (BEB). A device that encapsulates customer frames for transmission across a Provider Backbone Bridging (PBB) network. There are two types:

- B-BEB (B type BEB): Contains a B-component for bridging in the provider space based on backbone MAC address (B-MAC) and backbone VLAN (B-VLAN) information.
- I-BEB (I type BEB): Contains an I-component for bridging in the customer space based on customer MAC address (C-MAC) and service VLAN (S-VLAN) information.

backbone VLAN (B-VLAN). A field in a Provider Backbone Bridging (PBB) header that carries the backbone VLAN identifier information. The format is the same as a service VLAN (S-VLAN) tag. Also called B-VID tag, B-TAG.

backhaul. The part of a hierarchical network that connects small subnetworks at the edge of the network to the core or backbone network.

In wireless backhaul, the part of the network that transports traffic from a cellular base station to a core network that routes and switches voice and data traffic. **bandwidth.** A measure of the data transfer rate of a communications transport medium.

base station. An earth-based transmitting/receiving station for cellular phones and other wireless transmission systems.

Bellman-Ford algorithm. Used in distance-vector routing protocols such as Routing Information Protocol (RIP) to determine the best path to all routes in the network. Contrast with Dijkstra algorithm.

best effort. Traffic class in which the network forwards as many packets as possible in as reasonable a time as possible. By default, packets not explicitly assigned to a specific traffic class are assigned to the best-effort class.

BGP confederation. A method to solve scaling problems created by the iBGP full-mesh requirement. BGP confederations effectively break up a large autonomous system (AS) into subautonomous systems (sub-ASs). Each sub-AS must be uniquely identified within the confederation AS by a sub-AS number.

Within a sub-AS, the same iBGP full mesh requirement exists. Connections to other confederations are made with eBGP, and peers outside the sub-AS are treated as external. To avoid routing loops, a sub-AS uses a confederation sequence, which operates like an AS path but uses only the privately assigned sub-AS numbers.

BGP neighbor. Another device on the network that is running Border Gateway Protocol (BGP). There are two types of BGP neighbors: internal neighbors in the same autonomous system (AS) and external neighbors in different autonomous systems.

BGP peer. A remote Border Gateway Protocol (BGP) speaker that is an established neighbor of the local BGP speaker. BGP peers do not have to be directly connected to each other to share a BGP session.

BGP speaker. A router configured to run the Border Gateway Protocol (BGP) routing protocol. A BGP speaker must be explicitly configured with a set of BGP peers with which it exchanges routing information.

Bidirectional Forwarding Detection (BFD). Protocol that reduces the reliance upon the relatively slow hello mechanism in routing protocols to detect failures where no hardware signaling is available. BFD works with Border Gateway Protocol (BGP), Open Shortest Path First (OSPF) v2, and Intermediate System to Intermediate System (ISIS) to enable them to receive failure notifications. Defined in RFCs 5880 and 5881.

bit error rate (BER). The ratio of error bits to the total number of bits transmitted. A BER is generally shown as a negative exponent (for example, 10-7, which means one out of 10,000,000 bits is in error).

Border Gateway Protocol (BGP). An Exterior Gateway Protocol (EGP) that maintains a table of IP networks, or prefixes, which designate network reachability among autonomous system (AS) instances. BGP uses path-vector routing that makes decisions based on path, network policies, and/or rule sets. BGP is the primary protocol for the global Internet. First defined by RFC 1163.

BGP Version 4 (BGP4) defined in RFC 4271 supports Classless Interdomain Routing (CIDR) and route summarization.

BGP performs these tasks:

- Collects information about reachable networks from neighboring autonomous systems
- Advertises its reachable networks to routers inside the AS and to neighboring autonomous systems
- Selects routes if there are multiple routes available.

Each BGP device can have both external and internal connections to other BGP devices:

- Internal BGP (iBGP) connections are within the same autonomous system • External BGP (eBGP) connections are between different autonomous systems The configuration and behavior is slightly different between eBGP and iBGP.

You can use iBGP for multihomed BGP networks (with more than one connection to the same external autonomous system).

To avoid routing loops, iBGP does not advertise routes learned from an internal BGP peer to other internal BGP peers. Instead, BGP requires that all internal peers be fully meshed so that any route advertised by one router is advertised to all peers within the autonomous system (AS). As a network grows, the full-mesh requirement becomes difficult to manage. To combat scaling problems, BGP uses route reflection and BGP confederations.

Multiprotocol BGP (MP-BGP) allows different types of addresses (address families) to be distributed in parallel. MPBGP supports IPv4 and IPv6 addresses as well as unicast and multicast variants of each. Defined in RFC 4760. See also IPv6 Provider Edge (6PE).

See also community.

bridge. A device operating at Layer 1 (L1) and Layer 2 (L2) of the Open Systems Interconnection (OSI) Reference Model that forwards frames from one network segment to another based on the MAC address.

The term bridge also describes a device that connects collision domains. Collisions that appear on one side of a switch are not allowed to propagate to the other.

Originally, bridges only had two ports, with each one connected to a network segment. Later, bridges had multiple ports that could connect more than two network segments as well as directly connecting hosts. As bridges evolved, they were also able to filter frames, that is, forward only certain traffic from one network segment to another. This type of device is sometimes called an intelligent bridge, but the more modern term is switch. The term “bridge” is somewhat archaic but is still often used in standards documents.

bridge protocol data unit (BPDU). A protocol data unit (PDU) sent by switches running the Spanning Tree Protocol (STP) to learn about other switches in the network and maintain the spanning tree.

broadcast. The process of a single host simultaneously sending the same message to all nodes on a network. Compare to multicast, where a only a subset of the receivers are addressed. See also unicast.

bursty. The tendency of the bandwidth needed in a network to vary greatly from one moment to the next.

C

C-MAC. A source and destination customer MAC address (C-SA and a C-DA) in a Provider Backbone Bridging (PBB) header.

C-TAG. See customer VLAN (C-VLAN).

Carrier Ethernet. Extensions to Ethernet that enable network operators to provide Ethernet services to customers and to use Ethernet technology in their networks. See also Metro Ethernet Forum (MEF).

certificate. Electronic document that identifies a person or entity. Through the use of keys and certificates, the entities exchanging data can authenticate each other.

channel. A connecting path that carries information from a sending device to a receiving device. A channel can refer to a physical medium (such as a coaxial cable or fiber optic cable). **circuit.** A communications channel or path between two devices capable of carrying electrical current.

circuit switching. A network where a dedicated circuit must be opened between devices before they can communicate and, while the circuit is open, no other devices may use that circuit or parts of it. A circuit can remain open without any information transmission, and still be unusable by other devices; it must be closed before it is available to other users. Contrast with packet switching.

Class of Service (CoS). A way of managing traffic in a network by grouping similar types of traffic (for example, email, video, voice, file transfer) together and treating each type as a class with its own level of service priority. However, no guarantees are made that a given priority will meet any specified minimum level. See also Quality of Service (QoS).

classful IP addressing. An older addressing scheme for configuring the ratio of networks to hosts using fixed length prefixes. See Classless Interdomain Routing (CIDR).

Classless Interdomain Routing (CIDR). A notation for specifying an IP addresses and its network prefix which appends a slash character to the address and a decimal number indicating the leading bits in the network prefix. For example:

- In the IPv4 notation “192.168.0.0/16”:
- “192.168” (the first 16 bits) defines the network address.
- .0.0 up to .255.255 refer to the host addresses on that network. This leaves 16 bits to contain host addresses, enough for 65536 host addresses.
- In the IPv6 notation “2001:db8::/32”:
- “2001:db8” (the first 32 bits) defines the network address.
- :0:0:0:0:0:0 to:ffff:ffff:ffff:ffff:ffff:ffff refer to host addresses on that network. This leaves 96 bits to contains host addresses, enough for 7,922,816,251,426,433 host addresses.

The lower the number after the slash, the more hosts contained in that block.

CIDR uses variable length subnet masking (VLSM) based on arbitrary length prefixes. In VLSM, the number of network and host bits assigned to a subnet can vary based on the number of hosts the subnet needs to support.

CIDR replaced traditional classful IP addressing, in which address allocation was based on octet (8-bit) boundary segments of the IP address. In CIDR, the boundary between the network and host portions of an IP address can be on any bit boundary. The old classful A, B, and C network designations correspond to CIDR prefixes of /8, /16, or /24. 192.168.0.0/16 corresponds to an old class B network. With CIDR, finer grained division of networks are possible, down to individual IP addresses, such as 192.168.100.2/32.

CIDR routes can be carried by Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), and Routing Information Protocol (RIP).

Before CIDR notation, IPv4 networks were represented using dotted decimal notation for both the address and a subnet mask.

Also called route summarization or supernetting.

client/server architecture. A computing architecture that distributes processing between clients and servers on the network. A client program makes a service request from a server which fulfils the request.

collapsed core. Collapsing the core layer and the distribution layer into one layer (one device) in the network design model. A collapsed core design reduces cost, while maintaining most of the benefits of the network design model for small networks that do not grow significantly larger over time.

collision domain. A network segment where data frames can collide with one another when being sent on a shared medium such as Ethernet. Hosts in a collision domain arbitrate among themselves using an access control mechanism.

command-line interface (CLI). Environment for entering commands to configure and monitor routing and switching software and hardware.

committed information rate (CIR). The average rate at which packets are admitted to the network. Each packet is counted as it enters the network. Packets that do not exceed the CIR are marked green, which corresponds to low loss priority. Packets that exceed the CIR but are below the peak information rate (PIR) are marked yellow, which corresponds to medium loss priority.

common and internal spanning tree (CIST). A single topology connecting all Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP) switches into one active topology. In other words, an entire spanning tree fabric.

common spanning tree (CST). The topology connecting all Spanning Tree Protocol (STP)/Rapid Spanning Tree Protocol (RSTP) *switches* and multiple spanning-tree (MST) region *instances*. An MST region appears as a single switch to spanning tree configurations outside the region.

community. In Border Gateway Protocol (BGP), a logical group of prefixes or destinations that share a common attribute; used to simplify a routing policy. Community members can be on different networks and in different autonomous systems.

In Simple Network Management Protocol (SNMP), an authentication scheme that authorizes SNMP clients based on the source IP address of incoming SNMP packets, defines which Management Information Base (MIB) objects are available, and specifies the operations (read-only or read-write) allowed on those objects.

congestion. The state in which the network load exceeds the available resources such as link capacity or memory buffers.

connection-oriented. A packet switching technology where a virtual circuit between sending and receiving devices makes it seem like the devices are connected by a switched circuit with a fixed bandwidth without regard to their physical addresses. In a connection-oriented service, packets always reach their destination in the same order as they were sent. Transmission Control Protocol (TCP) is a connection-oriented transport service. See also connectionless.

Connection-oriented protocols can be used to send information that requires a constant delay and bandwidth such as voice and video.

connectionless. A packet switching technology where the source and destination addresses are included in each packet so that a direct connection or an established session between sender and receiver is not required for communications. In a connectionless service, each packet is handled independently of all others, and packets might not reach their destination in the same order in which they were sent. User Datagram Protocol (UDP) is a connectionless transport service. See also connection-oriented.

Connectivity Fault Management (CFM). An Operation, Administration, and Maintenance (OAM) protocol that can manage Ethernet services and detect, verify, and isolate connectivity failures in VLANs. CFM enables service providers to configure:

- Maintenance association End Point (MEP) on a per-port, per-VLAN, or per-domain basis
- Maintenance domain Intermediate Point (MIP) on a per-port and per-level basis

CFM can operate over a LAN segment, customer VLAN (C-VLAN), service VLAN (S-VLAN), backbone VLAN (BVLAN), or backbone identified by an I-SID (Service Instance Identifier). Defined by IEEE 802.1ag and 802.1ah.

Constrained Shortest Path First (CSPF). An extension of shortest path first (SPF). The path computed using CSPF is the shortest path that fulfills a set of constraints. After running the shortest path algorithm, the paths are pruned, removing those links that violate a given set of constraints. See also Resource Reservation Protocol— Traffic Engineering (RSVP-TE).

Content Addressable Memory (CAM). An integrated circuit in a device that stores a table used to make frame forwarding and classification decisions. CAM can perform a massively parallel search of entries in the table much faster than a serial search than in conventional Random Access Memory (RAM).

There are two types of CAM:

- Binary CAM: A binary lookup that returns either a 1 or 0. A MAC address in an Ethernet frame comes into a switch, the switch looks in its MAC address table and either finds that MAC address or does not (1 or 0).
- Ternary CAM (TCAM): A binary lookup that returns either a 1 or 0 but also has a “do not care” bit. TCAM can have multiple matches and can determine a best match. This is necessary because Classless Interdomain Routing (CIDR) lookups need a longest prefix match. For example, 192.168.1.7/32 matches both 192.168.1.0/24 and 192.168.1.0/25. The closest match to 192.168.1.7/32 is 192.168.1.0/25 which would be chosen.

Continuity Check Message (CCM). A multicast Connectivity Fault Management (CFM) protocol data unit (PDU) transmitted periodically by a Maintenance association End Point (MEP) in ensure continuity over the Maintenance Association (MA) to which the transmitting MEP belongs.

control plane. The part of switch or router architecture that makes decisions about where traffic is sent. Control plane processing is the “signalling” of the network. Anything that is needed to get routing and switching working on a device is considered part of the control plane. The control plane serves the data plane.

The control plane functions include the manual system configuration and management operations performed by a network administrator. The control plane functions also include dynamic routing protocols such as Routing Information

Protocol (RIP), Open Shortest Path First (OSPF), or Border Gateway Protocol (BGP) that exchange topology information with other routers and construct a Routing Information Base (RIB).

The control plane functions are not performed on each arriving individual packet, so they do not have a strict speed constraint and are not time-critical.

Control plane packets are sent to or are locally originated by the device itself.

convergence. The synchronization process that a network must go through immediately after a topology change. Convergence time is the time required to update all the devices on the network with the routing information changes. See also routing table.

core layer. In the network design model, the layer that provides a transit function to access the internal network and external networks. The core layer moves packets between distribution layer devices. The core layer also links to the devices at the enterprise edge to support Internet, virtual private networks (VPN), extranet, and WAN access.

The core layer uses Layer 3 (L3) routing protocols that scale well and converge quickly such as Open Shortest Path First (OSPF).

The core serves as the backbone for the network and is critical for connecting distribution layer devices, so it is important for the core to be fast with low-latency, reliable, and scalable.

Also called backbone or trunk.

count-to-infinity. A distance-vector routing problem where if A tells B that it has a path somewhere, there is no way for B to know if the path has B as a part of it.

The count-to-infinity problem is caused by a link failure that partitions the network into two or more segments. When the network is partitioned, devices in one part of the segment cannot reach devices in the other part of the segment. The distance-vector algorithm adjusts the distance value slowly upwards toward infinity.

The count-to-infinity problem can be solved through split horizon methods.

cryptography. Rendering information unintelligible and restoring encrypted information to an intelligible form.

customer edge (CE). A device that provides an interface between a Local Area Network (LAN) and an enterprise or service provider core network. Outbound packets from the LAN are forwarded from the CE to a provider edge (PE) device, and inbound packets are forwarded from the PE to the CE.

customer VLAN (C-VLAN). In a Provider Bridging (PB) frame, a field that identifies the customer VLAN. See also service VLAN (S-VLAN). Also called C-TAG.

D

daemon. A background program that runs unattended and is usually invisible to users and that provides important system services. Pronounced “dee-mon” or “day-mon”.

Data Center Bridging (DCB). A collection of extensions for Ethernet that allows LANs and Storage Area Networks (SANs) to use a single unified fabric in a data center. DCB can carry Fibre Channel, TCP/IP, and inter-process communication traffic over a single, converged Ethernet network. DCB features include:

- Priority-based Flow Control (PFC)
- Enhanced Transmission Selection (ETS)

- Quantized Congestion Notification (QCN)
- Data Center Bridging Capability Exchange (DCBX)

Data Center Bridging Capability Exchange (DCBX). Defined in IEEE 802.1Qaz, a protocol that uses Link Layer Discovery Protocol (LLDP) to convey configuration of Data Center Bridging (DCB) features between neighbors.

data communications equipment (DCE). The interface between data terminal equipment (DTE) and a network.

Data Encryption Standard (DES). A method of data encryption using a private (secret) key. There are 72 quadrillion or more possible encryption keys that can be used. For each given message, the key is chosen at random from among these. Both the sender and the receiver must know and use the same private key.

In triple DES (3DES), a symmetric-key block cipher applies the DES cipher algorithm three times to each data block.

data link layer. See Layer 2 (L2).

data plane. The part of switch or router architecture that forwards frames and packets arriving on an interface. Routers and switches use what the control plane has built to process incoming frames and packets. The data plane forwards traffic to the next hop along the path to the destination according to the control plane logic. Data plane frames or packets go *through* the device.

Also called forwarding plane.

data terminal equipment (DTE). Any device such as a host, router, or switch connected to a network. A DTE connects to a network through data communications equipment (DCE). **default gateway.** A router that connects hosts on a network segment to the Internet.

default route. A route used to forward Internet Protocol (IP) packets when a more specific route is not present in the Routing Information Base (RIB). Often represented as 0.0.0.0/0, the default route is sometimes called the “route of last resort”.

Differentiated Services (DiffServ). A mechanism to classify and manage network traffic and provide Quality of Service (QoS) guarantees for service providers. DiffServ extends the Resource Reservation Protocol—Traffic Engineering (RSVP-TE). DiffServ enables traffic to be prioritized by class, so that certain kinds of traffic, for example voice traffic, can take precedence over other types of traffic.

DiffServ redefines bits in the type of service (ToS) field of an IP packet header. DiffServ uses the Differentiated Services Code Point (DSCP) field for the QoS priority and supports 64 levels of classification.

Defined by RFC 2474; Multi-Protocol Label Switching (MPLS) support is defined in RFCs 3270 and 4124.

Differentiated Services Code Point (DSCP). A six-bit field in an IP header that enables service providers to allocate resources on a per-packet basis to meet customer requirements. See also Differentiated Services (DiffServ).

Diffie–Hellman. A method of securely exchanging cryptographic keys that allows two parties with no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

Digital Signature Algorithm (DSA). An asymmetric cryptographic algorithm that produces a digital signature in the form of a pair of large numbers. The signature is computed using rules and parameters such that the identity of the signer and the integrity of the signed data can be verified.

Dijkstra algorithm. An algorithm used by Intermediate System to Intermediate System (IS-IS) and Open Shortest Path First (OSPF) to make routing decisions based on link state. Also called shortest path first (SPF). Contrast with Bellman-Ford algorithm.

distance-vector routing. A family of routing algorithms that calculate the best route to use to send data based on information from adjacent (directly connected) routers on the network.

"Distance-vector" means that routes are advertised with two characteristics:

- Distance: How far it is to the destination based on a metric such as the number of hops, cost, bandwidth, or delay.
- Vector: The direction (exit interface) of the next hop router to reach the destination.

Each router sends its neighbors a list of networks it can reach and the distance to that network. For each network path, the receiving router picks the neighbor advertising the lowest metric, then adds this entry into its Routing Information Base (RIB). These best paths are advertised to each adjacent router.

Routing information is broadcast periodically rather than only when a change occurs, which makes the method compute- and bandwidth-intensive. For this reason, a distance-vector algorithm is best used in relatively small networks with few interrouter connections.

The Bellman-Ford algorithm is often used to determine the best path, which is used by the Routing Information Protocol (RIP).

Distance-vector routing can be prone to routing loops which are avoided through split horizon techniques.

Contrast with link-state routing and shortest-path routing.

distribution layer. In the network design model, the layer that aggregates the data received from the access layer and sends it to the core layer or to other segments of the local network. Routers or multilayer switches in the distribution layer performs many functions including:

- Routing between subnetworks and Virtual Local Area Network (VLAN) instances in the access layer
- Managing access control, routing, filtering, and QoS policies
- Managing firewalls and network address translation (NAT)
- Managing queues and prioritizing traffic
- Summarizing routes before advertising them to the core
- Isolating the core from access layer failures or disruptions

The distribution layer uses Layer 3 (L3) routing to connect to the core layer and Layer 2 (L2) switching to connect to the access layer.

Also called the aggregation layer or concentration layer.

domain. A representation of all or a subset of a network used for addressing and administrative purposes. Also refers to a collection of routers that use a common Interior Gateway Protocol (IGP). See also area and autonomous system (AS).

domain name. A meaningful and easy-to-remember name for an IP address. A domain name is a sequence of names (labels) separated by periods such as "example.com".

Domain Name Service (DNS). A service that translates a domain name into a numeric IP address needed to locate devices. The DNS database is hierarchical. When a client such as a Web browser gives a request that specifies a host name, the DNS resolver on the client first contacts a DNS server to determine the server's IP address. If the DNS server does not contain the needed mapping, it forwards the request to a different DNS server at

the next higher level in the hierarchy. After potentially several forwarding and delegation exchanges within the DNS hierarchy, the IP address for the given host eventually arrives at the client. Defined in RFCs 1034 and 1035.

dotted decimal. A method of representing an IPv4 address as four decimal numbers separated by dots, or periods; for example, 194.65.87.3. See also IP address.

double colon. A notation used to represent a consecutive block of zeroes in the middle of an IPv6 address. For example, given this address:

FE80:0000:0000:0000:0202:B3FF:FE1E:8329

With double colon notation, the address shown above becomes:

FE80::0202:B3FF:FE1E:8329

You can only use the double colon notation once in an address.

double tagged. See Provider Bridging (PB).

dynamic address. An address assigned to a device on a network with no regard to matching a specific address to that device. When a client device (such as a laptop) is given a dynamic address, it simply receives one from a pool of available addresses. It might or might not be allocated the same IP address as on previous connections. See also Dynamic Host Configuration Protocol (DHCP).

Dynamic Host Configuration Protocol (DHCP). A protocol where a client can obtain an IP address and other information such as default gateway, subnet mask, and Domain Name Service (DNS) servers, for the client to use to connect to a network. Defined in RFCs 2131 and 3315. See also Transmission Control Protocol/Internet Protocol (TCP/ IP).

A DHCP server “leases” an IP address for a predetermined period of time, and reclaims the address for reassignment at the expiration of that period. DHCP greatly simplifies the administration of large networks, and networks in which nodes such as laptops, tablets, and smart phones frequently join and leave.

dynamic routing. A technique used by routing protocols where devices send and receive messages about the network topology to and from other devices and update a local Routing Information Base (RIB) used to locate the best available path to a destination.

There are different forms of dynamic routing: distance-vector routing, link-state routing, and path-vector routing. Several protocols use dynamic routing such as Border Gateway Protocol (BGP), Intermediate System to Intermediate System (IS-IS), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).

Also called adaptive routing. Contrast with static routing.

E

east/west. The flow of traffic traversing a data center or cloud horizontally between servers. Contrast with north/south.

Edge Virtual Bridging (EVB). A mechanism that enables a virtual switch to send all traffic to an adjacent physical switch. This moves the forwarding decisions and network operations from the host CPU to the switch. EVB leverages the advanced management capabilities in access or aggregation layer switches. Defined by IEEE 802.1Qbg. **egress.** Outbound or outgoing, referring to a protocol data unit (PDU) exiting a device. See also ingress.

encapsulation. The technique used by layered protocols in which a layer adds its own header information to the protocol data unit (PDU) from the layer above. As an example, in the Open Systems Interconnection (OSI) Reference Model, a PDU can contain a header for Layer 1 (L1), followed by a header for Layer 2 (L2), followed by a header for the Layer 3 (L3), followed by a header for the transport layer (Transmission Control Protocol (TCP), followed by data for the higher layers.

encryption. The process of encoding information in an attempt to make it secure from unauthorized access, particularly during transmission. The reverse of this process is known as decryption. Two main encryption schemes are in common use:

- Private (symmetrical) key: Using a private encryption key known to both the sender and the receiver of the information.
- Public (asymmetrical) key: Using a public key to encrypt and a private key to decrypt.

See also Data Encryption Standard (DES).

end-of-row switch. A chassis-based switch in a rack or cabinet at either end of the server row in a data center that connects to hundreds of servers in that row. Each cabinet in the row has cabling connecting 48 (or more) servers to the end-of-row switch. An end-of-row switch typically has redundant supervisor engines, power supplies, and overall better high availability characteristics than a Top-of-Rack (ToR) switch.

An end-of-row switch extends Layer 1 (L1) cabling topology from the switch to each rack, resulting in a smaller Layer 2 (L2) footprint and fewer Spanning Tree Protocol (STP) nodes in the topology.

Enhanced Transmission Selection (ETS). A protocol for assigning bandwidth to frame priorities. Defined in IEEE 802.1Qaz.

equal-cost multipath (ECMP). A forwarding mechanism for routing traffic along multiple paths of equal cost that ensures load balancing. The link-state routing protocols that use a cost-based metric such as Intermediate System to Intermediate System (IS-IS) and Open Shortest Path First (OSPF) explicitly allow ECMP routing.

Encapsulating Security Payload (ESP). An Internet Protocol Security (IPsec) protocol that ensures confidentiality by encrypting IP packets. An encryption algorithm combines the data in a packet with a key to transform the packet into an encrypted form. At the destination, the packet is decrypted it using the same algorithm. ESP also ensures the integrity of a packet using a hash message authentication code (HMAC). ESP also supports an authentication scheme like that used in Authentication Header (AH), or can be used in conjunction with AH.

Ethernet. A specification for a LAN technology at Layer 1 (L1) and Layer 2 (L2) of the Open Systems Interconnection (OSI) Reference Model based on packetized transmissions between physical ports over a variety of electrical and optical media. Ethernet can transport several upper-layer protocols, the most popular of which is Transmission Control Protocol/Internet Protocol (TCP/IP). Ethernet standards are maintained by the IEEE 802.3 committee.

Ethernet uses a bus topology and CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to resolve contention when two devices try to access the network at exactly the same time. Transmission speeds range from 10 Mbps, to Fast Ethernet at 100 Mbps, to Gigabit Ethernet at 1000 Mbps.

Ethernet Linear Protection Switching (ELPS). A type of Automatic Protection Switching (APS) that specifies these techniques:

- Linear 1+1 (One-plus-One) operates with either uni-directional or bi-directional switching; normal traffic is copied and fed to both working and protection transport entities

- Linear 1:1 (One-to-One) operates with bi-directional switching; normal traffic is transported either on the working transport entity or on the protection transport entity, using a selector bridge at the source Defined by ITU-T G.8032.

Ethernet Local Management Interface (E-LMI). An Operation, Administration, and Maintenance (OAM) protocol for communications between two User-to-Network Interface (UNI) instances. E-LMI provides both UNI and Ethernet Virtual Connection (EVC) status information to customer edge devices. This information enables automatic configuration of customer edge operation based on the configuration. Defined by Metro Ethernet Forum (MEF) 16.

Ethernet Ring Protection Switching (ERPS). A type of Automatic Protection Switching (APS) that protects traffic in a ring topology by ensuring that no loops are within the ring. Loops are prevented by blocking traffic on either a predetermined link or a failed link. ERPS integrates Operation, Administration, and Maintenance (OAM) functions with a simple APS protocol. An Ethernet ring uses normal learning, forwarding, filtering, and flooding mechanisms and a forwarding database (FDB). Defined by ITU-T G.8032.

Ethernet to the First Mile (EFM). A set of extensions to the 802.3 MAC and MAC sub layer. EFM describes technologies and the physical layer specifications for subscriber access, including remote failure detection, remote loop back, and link monitoring. Defined by IEEE 802.3ah.

Ethernet Virtual Connection (EVC). An association of two or more instances of a User-to-Network Interface (UNI). There are three types of EVC:

- In a point-to-point EVC, exactly two UNIs are associated with one another.
- In a multipoint EVC, two or more UNIs are associated with one another.
- In a rooted-multipoint EVC, one or more of the UNIs must be designated as root and each of the other UNIs must be designated as a leaf. If root, the UNI can send service frames to all other points in the EVC; if leaf, the UNI can send and receive service frames to and from root only.

Explicit Route Object (ERO). An extension to Resource Reservation Protocol (RSVP) that allows a path message to traverse an explicit sequence of routers that is independent of conventional shortest-path IP routing.

Exterior Gateway Protocol (EGP). An interdomain protocol such as Border Gateway Protocol (BGP) used to exchange network reachability information between autonomous system (AS) instances. Contrast with Interior Gateway Protocol (IGP).

F

FEC-to-NHLFE (FTN) map. In Multi-Protocol Label Switching (MPLS), a mapping from the forwarding equivalence class (FEC) of incoming packets to the corresponding Next Hop Label Forwarding Entry (NHLFE).

filtering. The process of determining whether to forward a frame or packet through a port. The simplest form of filtering is to not forward frames out the same port on which they were received. A network administrator can configure filtering manually or a device can be “self-learning” and record the source addresses of devices on each segment of a network in a filtering database.

Filtering behavior is sometimes referred to as “drop, flood, or forward”:

- If the switch determines that the destination MAC is on the same port, it does not forward the frame, dropping it.
- If the switch determines that the destination MAC is on a different port, it forwards the frame on that port.

- If the switch does not know where to send the frame (or if it is multicast or broadcast), the frame is flooded out all ports (except the port it was received on).

filtering database. A data structure in a switch that maps addresses to ports, addresses to VLANs, and/or ports to VLANs. A switch learns the location of hosts by recording the source MAC address-port number association for each frame received at an incoming port. All future transmissions destined to a MAC address in the filtering database are only directed to the port associated with that MAC address unless the transmission originated on that port.

A switch can also be configured and act as several independent switches by creating VLAN associations to switch ports.

flapping. Condition of network instability when a route is announced and then withdrawn repeatedly, usually as the result of an intermittently failing link. Also called route flapping.

flooding. Forwarding a frame onto all ports except the port upon which it arrived. In Open Shortest Path First (OSPF), distributing and synchronizing the link-state database (LSDB) between routers. **flow control.** Any mechanism that prevents a source from sending faster than the destination is capable of receiving.

Forward Error Correction (FEC). A system of error control that allows the receiver to correct some errors without having to request a re-transmission of data. **forwarding.** Finding the output port to which a frame needs to go, and relaying the frame to that port.

forwarding equivalence class (FEC). A set of packets with similar characteristics that are forwarded in the same manner, on the same path, with the same forwarding treatment, and using the same Multi-Protocol Label Switching (MPLS) label. FECs are defined by the Label Distribution Protocol (LDP). FECs are also represented in other label distribution protocols.

Forwarding Information Base (FIB). A data structure used to find the interface to which to forward a packet. The FIB contains the minimum amount of information required to make a forwarding decision for a particular packet, such as destination prefix and nexthop. The FIB is an abbreviated form of the information in the Routing Information Base (RIB).

Also called forwarding table.

frame. A protocol data unit (PDU) at Layer 2 (L2) with addressing and protocol control information. A frame contains a header field and a trailer field that “frame” the user data. (Some control frames contain no data.) See also packet.

G

GARP Multicast Registration Protocol (GMRP). A Generic Attribute Registration Protocol (GARP) application that allows switches to exchange multicast group information with other GMRP switches, prune unnecessary broadcast traffic, and dynamically create and manage multicast groups. See also Multiple MAC Registration Protocol (MMRP).

GARP VLAN Registration Protocol (GVRP). A Generic Attribute Registration Protocol (GARP) application that provides VLAN registration services. A switch can exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs. Defined by 802.1Q. See also Multiple VLAN Registration Protocol (MVRP).

gateway. A device that understands and converts between two different networking models. Since Transmission Control Protocol/Internet Protocol (TCP/IP) has become the dominant model, gateways are not used much at this time.

See also default gateway.

Generic Attribute Registration Protocol (GARP). A generic framework for devices to register attributes, such as VLAN identifiers and multicast group membership. See also Multiple Registration Protocol (MRP).

generic routing encapsulation (GRE). A tunneling protocol that encapsulates Layer 3 (L3) packets inside IP packets. GRE provides a virtual point-to-point link over an IP network. GRE is completely insecure, but provides a fast and simple way to access a remote network.

graceful restart. A process that allows a router whose control plane is restarting to continue forwarding traffic while recovering its state from neighboring routers. Without graceful restart, a control plane restart disrupts services provided by the router. Also called nonstop forwarding.

gratuitous ARP. Broadcast request for a router's own IP address to check whether that address is being used by another node. Used to detect IP address duplication.

H

hash message authentication code (HMAC). A method of calculating a message authentication code (MAC) using a cryptographic hash function in combination with a secret cryptographic key. As with any MAC, it can be used to simultaneously verify both the data integrity and the authenticity of a message. Any cryptographic hash function, such as MD5 or SHA-2, can be used to calculate an HMAC.

header. The portion of a protocol data unit (PDU) that contains control information for the message such as destination address, source address, input sequence number, the type of message, and priority level.

hello packet. A multicast packet that is used by protocols for neighbor discovery and recovery. Hello packets also indicate that a client is still operating and network-ready.

high availability. The ability of a system or component to limit or avoid network disruption when a component fails. High availability provides both hardware and software methods to minimize downtime and improve the performance of a network.

hold down. A state that a route is placed into so that devices will neither advertise the route nor accept advertisements about the route for a specific length of time (the hold down period). A hold down is used to flush bad information about a route from all devices in a network. A route is placed into hold down when a link in that route fails.

hop. A single link between two computer systems that a protocol data unit (PDU) must cross on its way to its destination. See also hop count.

hop count. The number of links that must be crossed to get from a source to a destination. A protocol data unit (PDU) might pass over many hops to reach its destination. If it must pass between five computers, it is said to have taken four hops to reach its destination. Hop count is often used as a metric for evaluating a route in distance-vector routing. Routing Information Protocol (RIP) uses hop count as its sole metric.

host. A computer connected to a network that is assigned a Layer 3 (L3) address and that provides an access point to that network. Similar to a node, except that host usually implies a computer system, whereas node generally applies to any networked device such as a router or switch.

hypervisor. A thin operating system designed solely to provide virtualization. A hypervisor drives physical hardware, executes virtual machine (VM) instances, and dynamically shares the underlying hardware with the associated virtual hardware. A hypervisor does not serve as a general-purpose operating system, but instead provides the platform on which VMs can run.

I

I-SID (Service Instance Identifier). A field in an I-TAG that defines the service instance to which the Provider Backbone Bridging (PBB) frame is mapped.

I-TAG. Field in the Provider Backbone Bridging (PBB) header that carries the I-SID (Service Instance Identifier) associated with the frame.

Incoming Label Map (ILM). In Multi-Protocol Label Switching (MPLS), a mapping from incoming labels to corresponding Next Hop Label Forwarding Entry (NHLFE).

ingress. Inbound or incoming, referring to a protocol data unit (PDU) entering a device. See also egress.

Institute of Electrical and Electronics Engineers (IEEE). A coordinating body for computing and communications standards. The IEEE mainly covers Layer 1 (L1) and Layer 2 (L2) of the Open Systems Interconnection (OSI) Reference Model. (Pronounced “eye-triple-ee”.) See http://www.ieee.org.

interface. The point at which a connection is made between two devices. An interface describes the logical and physical connections and usually means the same thing as the term port.

Interior Gateway Protocol (IGP). An intradomain protocol used to exchange network reachability and routing information among devices within an autonomous system (AS), such as Intermediate System to Intermediate System (IS-IS), Open Shortest Path First (OSPF), or Routing Information Protocol (RIP). Contrast with Exterior Gateway Protocol (EGP).

Intermediate System to Intermediate System (IS-IS). An Interior Gateway Protocol (IGP) that floods link state information throughout a network of routers. Each IS-IS router independently builds a database of the network's topology, aggregating the flooded network information. A Routing Information Base (RIB) is calculated from the database by constructing a shortest path tree (SPT).

Like Open Shortest Path First (OSPF), IS-IS uses the Dijkstra algorithm to find the best path through a network. Packets are then forwarded, based on the computed ideal path, through the network to the destination.

Defined by International Organization for Standardization (ISO) 10589.

internal spanning tree (IST). A special type of multiple spanning-tree instance (MSTI) that runs in an multiple spanning-tree (MST) region. An IST connects all the switches in the MST region and appears as a subtree in the common and internal spanning tree (CIST) that encompasses the entire switched domain.

An IST is identified by the number zero (0) and exists on all ports; you cannot delete the IST. By default, all VLANs are assigned to the IST. The IST is the only spanning tree instance that sends and receives bridge protocol data unit (BPDU) messages.

Any other spanning tree instance within an MST region is called a multiple spanning-tree instance (MSTI).

International Organization for Standardization (ISO). An international standards body that establishes global standards for communications and information exchange. Voting members are designated standards bodies of participating nations; American National Standards Institute (ANSI) is the U.S. member of the ISO. The Open Systems Interconnection (OSI) Reference Model is one of the ISO's most widely accepted recommendations.

Sometimes mistakenly referred to as the "International Standards Organization". Because "International Organization for Standardization" has different acronyms in different languages (IOS in English, OIN in French for *Organisation internationale de normalisation*), the founders gave it the short form ISO. ISO is derived from the Greek *isos*, meaning "equal".

For more, see http://www.iso.org/iso/home.html.

International Telecommunication Union (ITU). An international organization that develops standards for telecommunications. Formerly known as the CCITT. See http://www.itu.int.

Internet. The world's largest computer network, serving universities, commercial interests, government agencies, and private individuals. The Internet uses Transmission Control Protocol/Internet Protocol (TCP/IP) protocols, and Internet computers and devices run many different operating systems.

No government agency, single person, or corporate entity controls the Internet. All decisions on methods and standards are made by standards groups based on input from users.

See also Internet Engineering Task Force (IETF); Request for Comments (RFC).

Internet Control Message Protocol (ICMP). An Internet Protocol (IP) that provides management and control functions. Routers send ICMP messages to respond to undeliverable datagrams by placing an ICMP message in an IP datagram and then sending the datagram back to the original source. ICMP is also used by the ping (packet internet groper) command and enables a host to discover addresses of operating routers on the subnet. Defined in RFC 792.

IPv6 makes greater use of ICMP (ICMPv6 defined in RFC 4443) than IPv4, including neighbor solicitation, neighbor advertisement, router solicitation, router advertisement, and redirect.

Internet Engineering Task Force (IETF). An international community of network designers, operators, vendors, and researchers that develops Request for Comments (RFC) documents that define protocols and specifications for the Internet. The IETF mainly covers Layer 2 (L2) and Layer 3 (L3) of the Open Systems Interconnection (OSI) Reference Model. See http://www.ietf.org.

Internet Group Management Protocol (IGMP). An IPv4 protocol that allows hosts to add or remove themselves from a multicast group. Defined by RFC 3376.

IGMP enables receivers to register that they want to receive a particular multicast transmission, but does not route multicast traffic from the source to receivers. That task is left to a multicast routing protocol, such as Protocol Independent Multicast (PIM).

See also Multicast Listener Discovery (MLD), multicast group, (S,G).

Internet Key Exchange (IKE or IKEv2). An Internet Protocol Security (IPsec) protocol used to set up a security association (SA) by negotiating keys in secret. IKE builds upon Internet Security Association and Key Management Protocol (ISAKMP) using X.509 certificates for authentication and a Diffie–Hellman key exchange to set up a shared session secret from which cryptographic keys are derived. In addition, a security policy for every peer which will connect must be manually maintained.

The IKE protocol runs in two phases. The first phase establishes a ISAKMP SA which is used in the second phase to negotiate and set up the IPsec SAs.

Internet Protocol (IP). A Layer 3 (L3) protocol that provides connectionless delivery of data across heterogeneous physical networks. IP provides features for addressing, type-of-service, fragmentation and reassembly, and security. Defined by RFCs 791 and 1349.

Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.

IP is best effort and provides no guarantees of reliability, so if packets are lost in transit, accidentally duplicated, arrive in the wrong order, or arrive corrupted, no effort is made to address the problem on the IP level—that is left to protocols a layer above, such as Transmission Control Protocol (TCP).

Internet Protocol Security (IPsec). A protocol suite for securing IP communications by authenticating and encrypting packets during a communication session. Authentication Header (AH) and Encapsulating Security Payload (ESP) are the main wire-level protocols used by IPsec. Before either AH or ESP can be used, however, the two devices must share a public key through Internet Key Exchange (IKE or IKEv2).

RFC 2401 specifies the base architecture for IPsec compliant systems. RFCs 2402, 2406, and 2407 provide more details about IPsec.

Internet Security Association and Key Management Protocol (ISAKMP). A framework for authentication and key exchange with actual authenticated keying material provided either by manual configuration with pre-shared keys or Internet Key Exchange (IKE or IKEv2). See also Internet Protocol Security (IPsec).

IP address. A unique number that identifies a device on an Internet Protocol (IP) network. IP addresses have two formats:

- An IPv4 address is 32 bits and is usually written in dotted decimal notation as four decimal numbers separated by periods. For example, 192.168.50.4 is an IPv4 address.
- An IPv6 address is 128 bits and is written in a hexadecimal notation of eight 16-bit parts separated by colons. For example, FE80:0000:0000:0000:0202:B3FF:FE1E:8329 is an IPv6 address. In the double colon address format, consecutive colons (“::”) represent successive 16-bit blocks that contain zeros: FE80::0202:B3FF:FE1E:8329. While a much larger address space is a feature, IPv6 also has other features such as multicast support, jumbograms (packets up to 4 GB in size), and stateless host auto-configuration.

Table 4-263 compares the IPv4 and IPv6 address formats.

Table 4-263: IPv6 and IPv4 Address Formats

Feature	IPv6	IPv4
Address space	128-bits = 3.4 x 1038 (340 unidecillion)	32-bits = 4.3 x 109 (4.2 billion)
Field separator	colon (:)	period (.)
Notation	hexadecimal	decimal
Example	db8:0:0:1	0.23.2.3

Each IP address contains a network part, an optional subnetwork part, and a host part. The network and subnetwork parts together are used for routing, while the host part is used to address an individual host within the network or

subnetwork. A subnet mask is used to extract network and subnetwork parts from the IP address. Classless Interdomain Routing (CIDR) provides a way to represent IP addresses and subnet masks.

IP addresses are difficult to remember, so people tend to refer to computers by their domain names instead.

IPv6 Provider Edge (6PE). A protocol that enables IPv6 domains to communicate with each other over an Multi-Protocol Label Switching (MPLS) IPv4 core network. V6PE routers are “dual stack” and run both IPv4 and IPv6. Multiprotocol Border Gateway Protocol (BGP) (MP-BGP) in the IPv4 network is used to exchange IPv6 reachability information along with a label for each IPv6 prefix announced. Defined in RFC 4798.

Also called V6PE.

K

keepalive message. A message sent between devices when no data traffic has been detected for a given period of time. This communication verifies that the virtual and physical connection between the devices is still active. **kernel.** The part of an operating system that performs basic functions such as allocating hardware resources.

KVM (Kernel-based Virtual Machine). A virtualization infrastructure for the Linux kernel that turns it into a hypervisor. KVM requires a processor with hardware virtualization technology extensions. By itself, KVM does not perform any emulation. Instead, KVM exposes an interface with which a user space host can then set up guest virtual machine (VM) instances.On Linux, QEMU (Quick EMUlator) is one such user space host.

L

Label Distribution Protocol (LDP). A protocol for distributing labels in non-traffic-engineered applications. LDP allows routers to create label-switched path (LSP) instances through a network by mapping network layer routing information directly to data-link layer switched paths.

A label is a short fixed-length, locally-significant identifier that identifies a forwarding equivalence class (FEC).

LDP works with other routing protocols such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP) to create LSPs.

See also Resource Reservation Protocol—Traffic Engineering (RSVP-TE).

label edge router (LER). A router that operates at the edge of an Multi-Protocol Label Switching (MPLS) network and acts as the entry and exit points for the network.

When forwarding IP packets into an MPLS domain, an LER makes the initial path selection, add the appropriate labels to the packet, and forwards the labelled packets into the MPLS domain. Likewise, upon receiving a labelled packet which is destined to exit the MPLS domain, the LER strips off the label and forwards the resulting IP packet using normal IP forwarding rules. (Under penultimate hop popping (PHP), the popping function might be performed by an label switch router (LSR) directly connected to the LER.) Also called an edge LSR.

label switch router (LSR). A Multi-Protocol Label Switching (MPLS) router located in the middle of a MPLS network. When an LSR receives a packet, it uses the label included in the packet header to determine the next hop on the label-switched path (LSP) and find a corresponding label for the packet from a lookup table. The old label is then removed from the header and replaced with the new label before the packet is forwarded.

Also called transit router.

label-switched path (LSP). A sequence of routers that cooperatively perform Multi-Protocol Label Switching (MPLS) operations for a packet stream. An LSP is a unidirectional, point-to-point, half-duplex connection carrying information downstream from the ingress (first) router to the egress (last) router. The ingress and egress routers cannot be the same device. **latency.** Delay in the transmission through a network from source to destination. See also line rate, wire speed.

Layer 1 (L1). The physical layer in the Open Systems Interconnection (OSI) Reference Model that conveys the bit stream through electrical impulse, light waves, or radio signals through the network. L1 represents the basic network hardware and specifies the type of medium used for transmission and the network topology.

Layer 2 (L2). The data link layer in the Open Systems Interconnection (OSI) Reference Model that provides reliable transit of data across a physical link between two directly connected devices. L2 refers to physical addressing, network topology, line discipline, error notification, sequenced delivery of frames, and flow control.

L2 transfers data between network entities by splitting data into frames to send on Layer 1 (L1) and receiving acknowledgment frames. The data link layer performs error checking and retransmits frames not received correctly. In general, the data link layer controls the flow of information across the link, providing an error-free virtual channel to Layer 3 (L3).

The data-link layer has two sublayers:

- logical link control (LLC)
- Media Access Control

(MAC)

Also called link layer.

Layer 3 (L3). The network layer in the Open Systems Interconnection (OSI) Reference Model that routes packets of data from source to destination across a network. L3 provides network-wide communication, including global addressing, lifetime control, fragmentation, and reassembly. Internet Protocol (IP) is an example.

Layer 4 (L4). The transport layer in the Open Systems Interconnection (OSI) Reference Model that provides logical communication between processes running on different hosts. L4 manages the end-to-end delivery of payload from a source to a destination within and between networks while maintaining the quality of service. Transmission Control Protocol (TCP) is an example.

Lightweight Directory Access Protocol (LDAP). A protocol used to locate organizations, individuals, and other resources in a network. Defined in RFC 4511. See also authentication, authorization, and accounting (AAA), Remote Authentication Dial In User Service (RADIUS), Terminal Access Controller Access Control System Plus (TACACS+). **line rate.** Total number of physically transferred bits per second, including useful data and protocol overhead, over a communication link. For example, if the line rate of a link is 10 Gbps, the link transmits 10 gigabits of data every second over its physical interface. Contrast with throughput. See also latency, wire speed.

link. Communication path between two neighbor nodes.

link aggregation. A method for using multiple parallel links between a pair of devices as if they were a single higherperformance channel. The aggregated interface is viewed as a single link to each device. Spanning Tree Protocol (STP) also views it as one interface. Link aggregation can also be used to increase availability so that when there is a failure in one physical link, the remaining links stay up, and there is no disruption. Defined by IEEE 802.1AX.

Also called link aggregation group (LAG), LAG bundle, and EtherChannel. See also Link Aggregation Control Protocol (LACP), Multi-Chassis Link Aggregation (MC-LAG).

Link Aggregation Control Protocol (LACP). Mechanism for exchanging port and system information to create and maintain link aggregation groups.

link cost. An arbitrary number configured on an Open Shortest Path First (OSPF) interface which is used in shortest path first calculations.

Link Layer Discovery Protocol (LLDP). A mechanism for the devices on a network to advertise their identity, capabilities, and neighbors to each other. Defined by IEEE 802.1AB.

link state. Information about a link and link cost to neighboring routers.

link-state advertisement (LSA). An Open Shortest Path First (OSPF) protocol data unit (PDU) to share information on the operating state of a link, link cost, and other OSPF neighbor information. LSAs are used by the receiving routers to update their Routing Information Base (RIB)s.

link-state database (LSDB). The data structure on a router that contains all routing knowledge in a link-state network. An LSDB stores all link-state advertisement (LSA) instances produced by a link-state routing protocol such as Open Shortest Path First (OSPF) or Intermediate System to Intermediate System (IS-IS). Each router runs shortest path first (SPF) algorithm against this database to locate the best network path to each destination in the network.

link-state routing. A routing technique used by Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (IS-IS) where each router shares information with other routers by flooding information about itself to every reachable router in the area. Link-state protocols use characteristics of the route such as speed and cost to determine the best path. Link-state information is transmitted only when something has changed in the network.

Every router constructs a map of the connectivity of the network, determining the interconnections between all routers. As a router receives an advertisement, it stores this information in a link-state database (LSDB). Each router then independently calculates the best next hop from it to every possible destination in the network using the shortest path first (SPF) algorithm to build a shortest path tree (SPT) with itself as the center of that tree. The shortest path to each reachable destination within the network is found by traversing the tree. The collection of best next hops forms the router's Routing Information Base (RIB).

Link-state algorithms create a consistent view of the network and are therefore not prone to routing loops, but they achieve this at the cost of more computing cycles and more traffic compared to distance-vector routing.

See also Dijkstra algorithm.

Linktrace Message (LTM). A Connectivity Fault Management (CFM) protocol data unit (PDU) initiated by a Maintenance association End Point (MEP) to trace a path to a target MAC address, forwarded from Maintenance domain Intermediate Point (MIP) to MIP, up to the point at which the LTM reaches its target MEP.

Linux. A Unix-like computer operating system assembled under the model of free and open source software development and distribution. The defining component of Linux is the kernel, the central part of the operating system that manages system services. Many people use the name “Linux” to refer to the complete operating system package which is called a Linux distribution which is made up of a collection of software based around the Linux kernel.

Linux has since been ported to more computer hardware platforms than any other operating system and is available for a wide variety of systems from small embedded systems up to supercomputers. In particular, networking devices such as switches and routers almost universally run some Linux distribution.

As an open operating system, Linux is developed collaboratively, meaning no one organization is solely responsible for its development or ongoing support. Companies participating in the Linux community share research and development costs with their partners and competitors.

Local Area Network (LAN). A group of computers and devices connected by a communications channel, capable of sharing resources among several users. LANs are based on a small physical area such as a building, floor, or department. LANs can connect to a wide area network (WAN). Ethernet is the most popular LAN technology.

logical link control (LLC). The higher sublayer of Layer 2 (L2) in the Open Systems Interconnection (OSI) Reference Model. The LLC sublayer provides the interface for Layer 3 (L3) and handles error control, flow control, framing, and MAC-sublayer addressing. The most prevalent LLC protocol is IEEE 802.2, which includes both connectionless and connection-oriented variants. See also Media Access Control (MAC).

loopback. A troubleshooting test in which a signal is transmitted from a source to a destination and then back to the source again so that the signal can be measured and evaluated.

M

MAC address. A permanent, unique serial number that uniquely identifies a network device among all other network devices in the world. MAC addresses are 12-digit numbers, 48 bits in length. MAC addresses are usually written as six groups of two hexadecimal digits, separated by hyphens (“-”) or colons (“:”):

MM:MM:MM:SS:SS:SS

MM-MM-MM-SS-SS-SS

Each pair of hexadecimal digits represents one byte of the 6-byte (48-bit) address.

An example of a MAC address is 68:A3:C4:3B:8D:24:

- The first three parts (68:A3:C4) identify the manufacturer (Liteon Technologies)
- The second three parts (3B:8D:24) is the serial number assigned by the manufacturer

At Layer 2 (L2), other devices use MAC addresses to locate specific ports in a network, and to create and update a Routing Information Base (RIB). A MAC address maps to an IP address through the Address Resolution Protocol (ARP).

Also called physical address, Ethernet address, or hardware address.

MAC-in-MAC. See Provider Backbone Bridging (PBB).

Maintenance Association (MA). In Connectivity Fault Management (CFM), a set of Maintenance association End Point (MEP) instances, each configured with the same MAID (Maintenance Association Identifier) and Maintenance Domain (MD) Level, established to verify the integrity of a single service instance.

Maintenance association End Point (MEP). A Connectivity Fault Management (CFM) entity at the edge of a Maintenance Domain (MD) that confines CFM messages within the domain via the MD level. MEPs periodically transmit and receive Continuity Check Message (CCM) instances from other MEPs within the domain. MEPs are either “Up” (toward the switch) or “Down” (toward the wire).

Maintenance Domain (MD). In Connectivity Fault Management (CFM), the network or the part of the network for which faults in connectivity can be managed.

Maintenance domain Intermediate Point (MIP). A Connectivity Fault Management (CFM) entity that catalogs and forwards information received from Maintenance association End Point (MEP) instances. MIPs are passive points that respond only to CFM Linktrace Message (LTM) and loopback messages.

Management Information Base (MIB). A specification of objects used by Simple Network Management Protocol (SNMP) to monitor or change network settings. MIBs provides a logical naming scheme for resources on a network. A MIB contains information about a device such as settings, usage statistics, performance data, or physical properties (such as temperature or fan speed). MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches. Standard MIBs are defined by the IETF.

Maximum Transmission Unit (MTU). The maximum number of bytes in a packet or frame. For Ethernet, the default MTU is 1500 bytes (data payload), but each media has different sizes. The Ethernet MTU is defined in RFC 894.

Media Access Control (MAC). The lower sublayer of Layer 2 (L2) in the Open Systems Interconnection (OSI) Reference Model. The MAC sublayer provides addressing and channel access control mechanisms that make it possible for several network nodes to communicate within a multiple-access network that uses a shared medium such as Ethernet. The MAC sublayer is the interface between the logical link control (LLC) sublayer and Layer 1 (L1).

mesh. A physical or logical network topology in which devices have many redundant interconnections. A full mesh is when all devices in a network have a connection to all other devices, a partial mesh is when some devices have a connection to all other devices.

Metro Ethernet Forum (MEF). A defining body for Carrier Ethernet with many participating organizations including service providers, and network hardware and software manufacturers. The MEF's mission is to accelerate the worldwide adoption of carrier-class Ethernet networks and services. For more, see http://metroethernetforum.org/.

Multi-Chassis Link Aggregation (MC-LAG). A technique that extends the link aggregation concept. At either one or both ends of a link aggregation group, a single aggregation system is replaced by a *portal* that is a collection of one to three portal systems. Defined by IEEE 802.1AX.

Also called MLAG and Distributed Resilient Network Interconnect (DRNI).

Multi-Protocol Label Switching (MPLS). A method for forwarding packets through a network. MPLS operates between the traditional definitions of Layer 2 (L2) and Layer 3 (L3).

In a traditional IP network, each router performs an IP lookup to determine a next hop based on its routing table, and forwards the packet to that next hop. Every router in the path repeats this process, making its own independent routing decisions, until the final destination is reached.

In an MPLS network, the first device does a routing lookup, but instead of finding a next hop, it finds the final destination router and finds a pre-determined path from the source to the destination. The router applies a "label" based on this information. Other routers in the path use the label to route the traffic without needing to perform any additional IP lookups.

At each incoming (ingress) point of the network, packets are assigned a label by a label edge router (LER). Packets are forwarded along an label-switched path (LSP) where each label switch router (LSR) makes forwarding decisions based on the label information. At each hop, an LSR swaps the existing label for a new label that tells the next hop how to forward the packet. At the outgoing (egress) point, an LER removes the label, and forwards the packet to its destination via IP routing.

MPLS enables these applications: Virtual Private Network (VPN), traffic engineering (TE), and Quality of Service (QoS).

See also Label Distribution Protocol (LDP), Resource Reservation Protocol—Traffic Engineering (RSVP-TE).

Multi-Protocol Label Switching - Transport Profile (MPLS-TP). A subset of Multi-Protocol Label Switching (MPLS) with extensions that address transport network requirements. The extensions provide the same QoS, protection and restoration, and Operation, Administration, and Maintenance (OAM) as in SONET/SDH. In MPLS-TP, some of the MPLS functions are turned off, such as penultimate hop popping (PHP), label-switched path (LSP) merge, and equal-cost multipath (ECMP).

The use of a control plane protocol is optional in MPLS-TP. The control plane can set up an LSP automatically across a packet-switched network domain. However, some network operators might prefer to configure the LSPs statically without using an IP or routing protocol.

multicast. The process of a single host sending messages to a selected group of receivers. See also broadcast, unicast.

multicast group. A collection of hosts receiving packets from a host that is transmitting multicast packets. Only hosts that need to hear a particular multicast declare that requirement. A multicast group restricts traffic to just those paths between the sources and destinations associated with the multicast address. Membership is dynamic; when a host joins a group, it starts receiving the datastream, and when a host leaves a group, it stops receiving the datastream. When there are no more members, the group simply ceases to exist.

See also GARP Multicast Registration Protocol (GMRP), Internet Group Management Protocol (IGMP), Multicast Listener Discovery (MLD), Multiple MAC Registration Protocol (MMRP), (S,G).

Multicast Listener Discovery (MLD). An IPv6 protocol that allows hosts to add or remove themselves from a multicast group. Defined by RFC 3810.

See also Internet Group Management Protocol (IGMP), multicast group, (S,G).

Multiple MAC Registration Protocol (MMRP). A protocol that manages multicast group MAC addresses. In addition, MMRP improves the convergence time of GARP Multicast Registration Protocol (GMRP). Defined by 802.1ak.

Multiple Registration Protocol (MRP). A generic registration framework with protocols, procedures, and managed objects for switches to register attributes with other switches in a LAN. Defined by 802.1ak. MRP replaces Generic Attribute Registration Protocol (GARP)

Multiple Spanning Tree Protocol (MSTP). An enhancement to the Rapid Spanning Tree Protocol (RSTP) where a separate spanning tree for can be configured for a VLAN group. Each VLAN group belongs to a multiple spanningtree instance (MSTI). Several MSTIs can run in an multiple spanning-tree (MST) region, with each region interconnected in a common and internal spanning tree (CIST).

MSTP is backward compatible with both RSTP and Spanning Tree Protocol (STP).

Originally defined in IEEE 802.1s and later merged into 802.1Q.

multiple spanning-tree (MST) region. A collection of interconnected switches that have the same Multiple Spanning Tree Protocol (MSTP) configuration which includes region name, revision number, and VLAN-to-instance map. Each MST region can contain multiple instances of spanning trees. The network administrator must properly configure participating switches throughout the region. All regions are bound together using a common and internal spanning tree (CIST), which creates a loop-free topology across regions. An MST region appears as a single switch to spanning tree configurations outside the region.

multiple spanning-tree instance (MSTI). A group of VLANs in a spanning-tree instance managed by Multiple Spanning Tree Protocol (MSTP) within an multiple spanning-tree (MST) region. Within each MST region, MSTP maintains multiple spanning-tree instances. Each instance has a spanning-tree topology independent of other

spanning-tree instances. An MSTI provides a fully connected active topology for frames belonging to a VLAN. You can assign a VLAN to only one spanning-tree instance at a time.

An internal spanning tree (IST) is a special type of MTSI.

Multiple VLAN Registration Protocol (MVRP). A protocol that manages registration of VLANs, tracking which routers are members of which VLANs and which router interfaces are in which VLAN. MVRP removes routers and interfaces from the VLAN information when they become unavailable. MVRP improves the convergence time of GARP VLAN Registration Protocol (GVRP). Defined by 802.1ak.

N

name resolution. The process of translating an IP address to a name that is easily remembered by a person. In a TCP/IP environment, a name such as www.example.com is translated into its IP equivalent by the Domain Name Service (DNS).

neighbor. An adjacent system reachable by traversing a single subnetwork; an immediately adjacent device. Also called peer. See also adjacency.

Neighbor Discovery Protocol (NDP). An IPv6 protocol that nodes on the same link use to discover each other's presence, determine each other's Link Layer addresses, find routers, and maintain reachability information about the paths to active neighbors. NDP is defined in RFC 2461 and is equivalent to the Address Resolution Protocol (ARP) used with IPv4.

NETCONF (Network Configuration Protocol). A mechanism to install, manipulate, and delete the configuration of network devices. The operations, notifications, and the database contents supported by a particular NETCONF server are extensible, and defined with a modeling language called YANG. The database is used to store YANG data structures which represent the configuration of the device containing the NETCONF server. This configuration can be saved in non-volatile storage so the configuration can be restored upon reboot. Defined in RFC 6241.

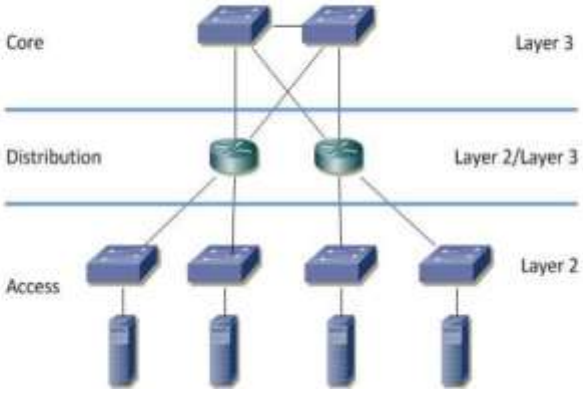
network. A group of computers and related devices connected by a communications channel capable of sharing resources among several users. A network consists of transmission media, devices such as routers or switches, and protocols that make message sequences meaningful.

A network can range from a peer-to-peer network connecting a small number of users in an office or department, to a Local Area Network (LAN) connecting many users, to a wide area network (WAN) connecting users on several networks spread over a wide geographic area.

network address translation (NAT). A method to use one set of IP addresses for an internal inetwork and a second set of addresses for the public Internet. This allows an organization to shield internal addresses from the public Internet. NAT is configured on the router at the border of an internal network and the Internet. NAT translates the internal local addresses to globally unique IP addresses before sending packets to the Internet and vice versa. Defined by RFC 1631.

network administrator. The person responsible for the day-to-day operation and management of a network.

network design model. A hierarchical model originally defined by Cisco that divides a network into three functional areas, or layers. This model optimizes network hardware and software to perform specific roles.



The roles that each layer performs are:

- The access layer provides local user access to the network
- The distribution layer connects network services to the access layer, and implements policies regarding security, traffic loading, and routing
- The core layer provides high-speed transport for the distribution layer See also collapsed core.

Network Element (NE). Any device in a network such as a host, router, switch, or firewall that performs a service or function for the network.

Network Functions Virtualization (NFV). The ability to decouple network services from dedicated hardware devices to be hosted on a virtual machine (VM). Once the network services are under the control of a hypervisor, the services can be performed on standard x86 servers.

network layer. See Layer 3 (L3).

network segment. A portion of a computer network that is separated from the rest of the network by a device such as a router or switch. Each segment can contain one or more hosts.

Network Services Module (NSM). The base module in SWMRE that communicates with every SWMRE routing and switching process. The protocol components use APIs exposed by the NSM client, which act as conduits to transfer data between the protocol modules and NSM.

Network Time Protocol (NTP). A protocol used to synchronize the system clocks of hosts on a network to Universal Coordinated Time (UTC). A device can update its clock automatically by configuring itself as an NTP client. Using NTP enables the device to record accurate times of events. Defined by RFC 5905.

Neutron. The networking component of OpenStack that provides “networking as a service” between virtual NICs managed by other OpenStack services.

Neutron provides a “plug-in” mechanism that lets network operators enable different technologies. It also lets tenants create multiple private networks and control their IP addressing. Organizations have control over security and compliance policies, Quality of Service (QoS), monitoring and troubleshooting, as well as the ability to deploy network services, such as a firewall, intrusion detection, and Virtual Private Network (VPN) instances. **next hop.** The next device to which a protocol data unit (PDU) is sent on its way to its destination.

Next Hop Label Forwarding Entry (NHLFE). An Multi-Protocol Label Switching (MPLS) entry containing next hop information (interface and next hop address) and label manipulation instructions; it can also include label encoding, L2 encapsulation information, and other information to process packets in the associated stream.

node. An addressable device such as a host, router, or switch, attached to a network, that transmits and receives data.

north/south. The flow of traffic traversing between users and a data center (spanning-tree). Contrast with east/west.

northbound. An interface that allows a network component to communicate with a higher-level component. A northbound interface hides complex details of operations. Northbound flow can be thought of as going upward. In architectural diagrams, northbound interfaces are drawn at the top of the component. See also southbound.

Not-So-Stubby-Area (NSSA). An extension of a Open Shortest Path First (OSPF) stub area. OSPF uses an NSSA as a transit to send external routes to other areas or to domains that are not part of the OSPF autonomous system. OSPF does not flood external routes from other areas into an NSSA, but does translate and flood route information from the NSSA into other areas such as the backbone. Defined by RFC 1587.

O

Open Network Foundation (ONF). A non-profit organization responsible for the development and standardization of a software architecture that supports Software-Defined Networking (SDN). ONF is also responsible for the commercialization and promotion of SDN as a concept and its underlying technologies. For more, see: https://www.opennetworking.org/.

Open Shortest Path First (OSPF). An Interior Gateway Protocol (IGP) based on link-state routing. OSPF is widely deployed in large networks because of its efficient use of network bandwidth and its rapid convergence after changes in topology. Defined in RFCs 2328 and RFC 5340.

OSPF advertises the states of local network links within an autonomous system (AS) and makes routing decisions based on the shortest path first (SPF) algorithm. Each OSPF router maintains an identical database describing the autonomous system's topology. From this database, a Routing Information Base (RIB) is calculated by constructing a shortest path tree (SPT).

OSPF features include least-cost routing, multipath routing, and load balancing. OSPF includes explicit support for Classless Interdomain Routing (CIDR) and the tagging of externally derived routing information.

OSPF version 2 supports IPv4 and OSPF version 3 supports IPv6.

OSPF divides an autonomous system into contiguous groups of networks called areas.

- In a standard area, intra-area routes, inter-area routes, and external routes (learned from other routing protocols such as RIP and BGP) are distributed. Inter-area routes and external routes are distributed as summary addresses.
- A backbone area is essentially a standard area which has been designated as the central point to which all other areas connect. A backbone area combines a set of independent areas into an AS and acts as a hub for inter-area transit traffic and routing information distribution. Each non-backbone area is directly connected to the backbone area.
- OSPF uses stub area instances and Not-So-Stubby-Area (NSSA) instances to limit distribution of inter-area routes and external routes.

See also area border router (ABR), autonomous system border router (ASBR).

Open Systems Interconnection (OSI) Reference Model. A conceptual model defined by the International Organization for Standardization (ISO) that organizes the computer-to-computer communications process into seven layers. Each layer provides services to the layer above and receives services from the layer below. Such a set of layers is called a protocol stack.

Layers seven through five manage end-to-end communications between the message source and destination, while layers one through four manage network access:

- Layer 4 (L4) ensures the end-to-end delivery from a source to a destination
- Layer 3 (L3) routes packets of data from source to destination across a network
- Layer 2 (L2) reliably transports data across the physical link between two directly connected nodes
- Layer 1 (L1) conveys the bit stream at the electrical and mechanical level

The OSI Reference Model is often compared to the more descriptive (versus prescriptive) Transmission Control Protocol/Internet Protocol (TCP/IP) model.

Open vSwitch (OVS). A software switch used in virtualized server environments that forwards traffic between different virtual machine (VM) instances on the same physical host and between VMs and the physical network. OVS enables network automation through programmatic extension, while still supporting standard management interfaces and protocols. For more, see http://openvswitch.org/.

OpenFlow. An open standard for forwarding plane operations that enables researchers to run experimental protocols. OpenFlow is developed, specified, and sponsored by the Open Network Foundation (ONF). OpenFlow provides a protocol that enables a controller to dynamically program internal flow-tables in devices. Network vendors have added OpenFlow features to routers and switches.

OpenStack. A cloud operating system that controls pools of compute, storage, and networking resources in a data center which users manage through a Web-based dashboard, command-line tools, or a RESTful API. See also Neutron.

Operation, Administration, and Maintenance (OAM). A set of Ethernet specifications that provide connectivity monitoring, fault detection and notification, fault verification, fault isolation, loopback, and remote defect identification. The primary specifications are 802.3ah link-fault management (LFM) and 802.1ag Connectivity Fault Management (CFM).

P

packet. A protocol data unit (PDU) at Layer 3 (L3) of the Open Systems Interconnection (OSI) Reference Model. A packet contains source and destination addresses, user data, and control information such as the length of the packet, the header checksum, and flags indicating whether the packet has been fragmented. The user data in a packet is often referred to as the payload. The actual format of a packet depends on the protocol that creates the packet.

A packet sent through a connectionless protocol such as User Datagram Protocol (UDP) is sometimes called a datagram.

See also frame, packet switching.

packet switching. A data-transmission method that transmits information over one of several routes. Information is sent to the destination through the best route, determined by a routing algorithm.

A packet switched network breaks information to be transmitted into discrete packets. Related packets might not all follow the same path to their destination. Packet sequence numbers are used to reassemble the original message at the destination.

A packet-switched network is connectionless because each packet contains its destination address and does not require a dedicated path to reach that destination. Multiple users may transmit packets over the same connection at the same time, independent of one another.

The Internet is an example of a packet-switched network.

Contrast with circuit switching.

paravirtualized. A software component that is aware that it is running in a virtual machine (VM). For example, a paravirtualized virtual device driver runs in a VM that communicates with the underlying host OS. Typically, a paravirtualized driver is optimized to share queues, buffers, or other data items with the underlying host OS to improve throughput and reduce latency.

path computation element (PCE). An entity (component, application, or server) that can compute a network path or route based on a network graph and constraints (see RFC 4655).

path-vector routing. A routing technique that advertises a network as a destination address and a complete path to reach that destination. Each entry in the Routing Information Base (RIB) contains the destination network, the next router, and the path to reach the destination.

A path vector protocol guarantees loop-free paths by recording each hop the routing advertisement traverses through the network. A node can easily detect a loop by looking for its own node identifier in the path. This technique is sometimes used in Bellman-Ford algorithm to avoid count-to-infinity problems.

Border Gateway Protocol (BGP) is an example of a prefix-based path-vector protocol where the Routing Information Base (RIB) maintains the autonomous systems to traverse to reach a destination.

peer. Immediately adjacent device with which a protocol relationship has been established. Also called neighbor.

penultimate hop popping (PHP). A technique where the outermost label of an Multi-Protocol Label Switching (MPLS) packet is removed by a label switch router (LSR) before the packet is passed to an adjacent label edge router (LER). **physical layer.** See Layer 1 (L1).

ping (packet internet groper). A command used to test network connectivity by transmitting an Internet Control Message Protocol (ICMP) diagnostic packet to a specific node on the network, forcing the node to acknowledge that the packet reached the correct destination. If the node responds, the link is operating; if not, something is wrong. The word ping is often used as a verb, as in “ping that workstation to see if it is alive.” **policing.**

Applying rate limits on bandwidth and burst size for traffic for a particular interface.

policy-based routing (PBR). Classifying packets to determine their forwarding path within a device. PBR is used to redirect traffic for analysis. Also called filter-based forwarding (FBF).

port. The point at which a communications circuit terminates on a network. A port can be logical, physical or both. Examples include:

- The physical interface between a device and a communications circuit, usually identified by a number or name.
- The logical interface between a TCP/IP applications and a communications facility which use well-known port numbers such as FTP: 20, HTTP: 80, and NFS: 2049.
- The logical interface between a process and a communications facility that allows more than one logical port to be associated with one physical port. For example, Ethernet uses multiple MAC addresses to distinguish between separate logical channels connecting two ports on the same physical transport network interface.

Also called interface.

port authentication. A mechanism for port-based user authentication and network access control for LAN devices. Defined by IEEE 802.1X.

Precision Time Protocol (PTP). A protocol that synchronizes clocks throughout a computer network. On a LAN, PTP achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control systems. The time synchronization is achieved through packets that are transmitted and received in a session between a master clock and a slave clock. Defined by IEEE 1588v2.

Priority-based Flow Control (PFC). A flow control mechanism that can be set independently for each frame priority on full-duplex links. Defined by IEEE 802.1Qbb.

private VLAN (PVLAN). A switch with ports that cannot communicate with each other, but can access other networks. A PVLAN has at least one private port and a trunk port. All traffic received on a private port is forwarded out the trunk port. All traffic received on a trunk port is handled as normal switch traffic. No traffic communication occurs between the private ports.

protocol. A set of rules that end points in a network connection must follow when they communicate. A protocol includes data representation, data item ordering, message formats, message and response sequencing rules, block data transmission conventions, and timing requirements.

The Open Systems Interconnection (OSI) Reference Model and Transmission Control Protocol/Internet Protocol (TCP/ IP) are both used as a model for many protocols. There are one or more protocols at each layer in the models that both ends of the connection must recognize and observe.

protocol data unit (PDU). A unit of data transmitted as a composite by a protocol.

In the Open Systems Interconnection (OSI) Reference Model, the actual name used for a PDU depends on the layer:

- Layer 4 (L4): segment
- Layer 3 (L3): packet
- Layer 2 (L2): frame
- Layer 1 (L1): stream, symbol stream, or bit stream

See also bridge protocol data unit (BPDU). Sometimes called datagram.

Protocol Independent Multicast (PIM). A method to determine the best paths for distributing a multicast transmission. PIM uses unicast routing tables (such as those used by Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP)) and static routes to perform multicasting. Each host must be registered using IGMP to receive the transmission.

PIM has these variations:

- PIM dense mode (PIM-DM: RFC 3973) uses a push model. PIM-DM initially floods multicast traffic throughout the network. Routers that have no downstream neighbors prune back the unwanted traffic. This process repeats periodically.
- PIM sparse mode (PIM-SM: RFC 4601) uses a pull model. PIM-SM uses a shortest path tree (SPT) where sources forward multicast packets to a designated router which unicasts the packets to an assigned rendezvous point router, which then forwards the packets to members of multicast groups.
- PIM source-specific multicast (PIM-SSM: RFC 3569) uses PIM-SM functionality to create a SPT between the client and the source without using a rendezvous point.
- Bidirectional PIM (Bidir-PIM: RFC 5015) uses PIM-SM functionality to route traffic only along a bidirectional SPT that is rooted at the rendezvous point for a group.

protocol stack. The layers of software used in network communications.

Provider Backbone Bridge-Traffic Engineering (PBB-TE) . An extension to Provider Backbone Bridging (PBB) that removes features such as flooding, dynamically created forwarding tables, and spanning tree protocols. PBB-TE also covers Connectivity Fault Management (CFM) and Ethernet Linear Protection Switching (ELPS).

In PBB-TE, a network administrator configures the forwarding tables in the backbone switches with static routes to ensure that frames take predetermined paths within the network. Frames with destination MAC addresses not in a forwarding table are dropped. Broadcast frames are not supported and are also dropped by backbone switches.

Defined in IEEE 802.1Qay.

Provider Backbone Bridging (PBB). A technique to create Ethernet backbones for service access networks. Defined in IEEE 802.1ah, PBB extends Provider Bridging (PB) defined in 802.1ad in these ways:

- The 802.1ah header adds an I-SID (Service Instance Identifier) which is a label that maps to a customer VLAN identifier. An I-SID virtualizes VLANs across a network. VLANs are mapped into I-SIDs by configuring only the edge of the network at a backbone edge bridge (BEB). This makes the maximum number of service instances 16 million.
- The 802.1ah header encapsulates backbone source and destination MAC addresses (B-MAC) along with the customer source and destination MAC addresses (C-MAC). The B-MAC contains MAC addresses of the service provider's PBB edge switches. The 802.1ah format is sometimes called “MAC-in-MAC” because of this MAC address encapsulation. The encapsulation of customer MAC addresses in backbone MAC addresses means that the backbone does not need to learn customer MAC addresses. Customer MAC addresses are learned at BEB ports only.

Provider Bridging (PB). A technique that enables a service provider to use the architecture and protocols of 802.Q to offer the equivalent of separate LANs, bridged LANs, or VLANs to multiple customers. Provider bridging requires no active cooperation between customers and requires minimal cooperation between an individual customer and the service provider.

When VLANs were originally defined in 802.1Q, the number of unique VLAN identifiers was limited to 4096. In large provider networks, each subscriber needs a separate address, so this limit could prevent a provider from having more than 4096 subscribers.

To overcome this limit, 802.1ad inserts an additional VLAN tag into a single 802.1Q Ethernet frame. Frames passing through the provider network are doubly tagged with:

- customer VLAN (C-VLAN) tag which identifies the customer network VLAN
- service VLAN (S-VLAN) tag which identifies the service provider network VLAN

With two VLAN identifiers in combination for each provider-customer pair, it is possible to define up to 16,777,216 VLANs.

The frame format for 802.1ad is also called Q-in-Q, double tagged, stacked VLANs, or VLAN stacking.

provider edge (PE). A device at the edge of an enterprise or service provider core network. A PE offers an initial, first level of network traffic aggregation for many customer edge (CE) devices.

pseudowire (PW). An emulation of a point-to-point connection over a packet-switching network. A pseudowire is a way to transport legacy services such as TDM over a packet-switched network:

- Structure-aware TDM circuit emulation service over packet-switched network (CESoPSN)
- Structure-agnostic TDM over packet (SAToP)

A pseudowire that both originates and terminates on the edge of a single packet-switched network (autonomous system or carrier network) is called a single-segment pseudowire (SS-PW). A pseudowire that extends through multiple autonomous systems or carrier networks is called a multi-segment pseudowire (MS-PW).

Q

Q-in-Q. See Provider Bridging (PB).

QEMU (Quick EMUlator). A hosted hypervisor that performs hardware virtualization. QEMU emulates CPUs through dynamic binary translation and provides a set of device models enabling it to run a variety of unmodified guest operating systems. QEMU also can be used together with KVM (Kernel-based Virtual Machine) to run virtual machines at near-native speed (requiring hardware virtualization extensions on x86 machines). QEMU can also be used purely for CPU emulation for user-level processes, allowing applications compiled for one architecture to be run on another.

Quality of Service (QoS). The ability to *guarantee* the delivery, control the bandwidth, set priorities for specific network traffic, and provide an appropriate level of security. QoS provides a level of predictability and control beyond the best effort delivery that a device provides by default.

See also Class of Service (CoS).

Quantized Congestion Notification (QCN). An end-to-end congestion management scheme for protocols capable of transmission rate limiting. Defined by IEEE 802.1Qau.

R

radio access network (RAN). The air interface and base station technology in a cellular network. In addition to the RAN, the entire cellular system includes the core network, which provides the backbone and services, as well as the cellphones.

Rapid Per-VLAN Spanning Tree Plus (RPVST+). A version of Cisco Per VLAN Spanning Tree Plus (PVST+) that uses the Rapid Spanning Tree Protocol (RSTP) state machine. PVST+ runs a spanning tree instance for each VLAN in the network. PVST+ is not scalable when there are many VLANs in a network. A compromise between RSTP and R-PVST+ is Multiple Spanning Tree Protocol (MSTP) which runs multiple instances of spanning tree that are independent of VLANs. MSTP maps a set of VLANs to each spanning tree instance.

Rapid Spanning Tree Protocol (RSTP). An enhancement to the Spanning Tree Protocol (STP) that re-configures quickly after a topology change. RSTP can verify if a port can change to a forwarding state safely without waiting for timers to start convergence. RSTP is not aware of VLANs and blocks ports at the physical level. Defined by IEEE 802.1D. See also Multiple Spanning Tree Protocol (MSTP).

Remote Authentication Dial In User Service (RADIUS). An authentication and accounting protocol to authenticate users and authorize their access to the requested system or service.

Defined in RFCs 2058, 2059, and 2865. See also authentication, authorization, and accounting (AAA), Lightweight Directory Access Protocol (LDAP), Terminal Access Controller Access Control System Plus (TACACS+).

remote monitoring (RMON). A Management Information Base (MIB) specification that defines functions for remotely monitoring networked devices. The RMON specification provides many problem detection and reporting capabilities. Defined by RFC 2819.

Request for Comments (RFC). Proposals and standards that define protocols for communications over the Internet. RFCs are developed and published by the Internet Engineering Task Force (IETF).

Resource Reservation Protocol (RSVP). A signalling protocol for reserving resources across a network. RSVP is rarely used by itself, but Resource Reservation Protocol—Traffic Engineering (RSVP-TE) is widely used.

Resource Reservation Protocol—Traffic Engineering (RSVP-TE). RSVP with traffic engineering extensions, as defined by RFC 5101, that allows RSVP to establish label-switched path (LSP) instances in Multi-Protocol Label Switching (MPLS) networks, using Constrained Shortest Path First (CSPF), taking into consideration constraints such as available bandwidth and explicit hops. The LSPs might not agree with the route suggested by the Open Shortest Path First (OSPF) or Intermediate System to Intermediate System (IS-IS).

reverse path forwarding (RPF). An algorithm that checks the unicast Routing Information Base (RIB) to determine whether there is a shortest path back to the source address of an incoming multicast packet. Unicast RPF helps determine the source of denial-of-service attacks and rejects packets from unexpected source addresses.

Rivest-Shamir-Adleman (RSA). A public key, or asymmetric, encryption scheme. The oretical background to RSA is that it is difficult to find the factors of a very large number that is the product of two prime numbers. RSA is considered very secure provided a sufficiently long key is used. **route.** The path from source to destination through a network.

route flap damping. Method for minimizing instability caused by route flapping. The router stores a penalty value for each route. Each time the route flaps, the router increases this value. If the penalty for a route reaches a configured suppress value, the router does not include the route as a forwarding entry and does not advertise the route to peers.

route redistribution. One protocol learning routes from another protocol running on the same device. Also called redistribution or route leakage.

route reflection. A method of allowing iBGP routers to accept and propagate iBGP routes to their clients.

To avoid routing loops, Border Gateway Protocol (BGP) does not advertise routes learned from an internal BGP peer to other internal BGP peers. Instead, BGP requires that all internal peers be fully meshed so that any route advertised by one router is advertised to all peers within the autonomous system (AS). As a network grows, the full mesh requirement becomes difficult to manage. To handle scaling problems, BGP uses route reflection and BGP confederations.

Route reflection allows you to designate one or more routers as route reflectors. BGP relaxes the re-advertising restriction on route reflectors, allowing them to accept and propagate iBGP routes to their clients.

route summarization. Consolidating multiple routes into a single route advertisement, in contrast to flat routing where a Routing Information Base (RIB) contains a unique entry for each route.

Classless Interdomain Routing (CIDR) is used to implement route summarization. All IP addresses in the route advertisement must have identical high-order bits. Also called route aggregation. See also subnet mask.

router. A Layer 3 (L3) device that makes decisions about the paths over which network traffic will flow. Routers use dynamic routing protocols to learn about the network and to find the best route to forward packets toward their final destination:

1. Find a matching destination address in the Routing Information Base (RIB)
2. Find the MAC address for the packet from the Address Resolution Protocol (ARP) cache
3. Write the new MAC address in the IP packet
4. Send the packet on the port associated with the MAC address

routing. The process of finding a path to a destination to use to transmit a protocol data unit (PDU) over a network. Routing is usually controlled by a Routing Information Base (RIB) which defines where a PDU should go. Each router only needs to know where a PDU should be sent on its next hop, and does not know nor care what happens afterward; the next hop plus one is the responsibility of the next router, and so on through the network until a PDU reaches its destination.

Routing Information Base (RIB). A data structure in a device that lists the routes to destinations and metrics (distances) associated with those routes. A RIB contains information about the topology of the network immediately around it. Maintaining a RIB by discovering network topology is the primary purpose of dynamic routing protocols such as Border Gateway Protocol (BGP), Routing Information Protocol (RIP), and Open Shortest Path First (OSPF). Network administrators can also add fixed routes to the RIB for static routing.

Also called a routing table. Contrast with Forwarding Information Base (FIB).

Routing Information Protocol (RIP). An Interior Gateway Protocol (IGP) that implements a distributed variant of the Bellman-Ford algorithm to provide distance-vector routing capabilities. RIP uses the hop count of a destination to detect the best path to route packets, but limits the maximum number of hops to 15 to prevent routing loops. RIP implements split horizon techniques. Defined in RFC 1058.

RIP is easy to configure and has low processing requirements. However, the hop count limit restricts the size of the network that RIP can support. Also, RIP can be slow to converge.

RIPv2 defined in RFC 2453 also supports subnet information, allowing Classless Interdomain Routing (CIDR).

RIPng (next generation), an extension of RIPv2 defined in RFC 2080, supports IPv6.

routing protocol. A set of processes, algorithms, and messages that are used to exchange routing information and populate the local Routing Information Base (RIB) with the best path between a source and destination.

The term “routing protocol” usually implies dynamic routing, where a device reports changes and shares information with other devices in the network. Each router starts with knowledge of only the devices to which it is directly attached. The routing protocol shares this information first with its immediate neighbors, and then throughout the network. This way, routers learn the topology of the network.

A primary benefit of dynamic routing protocols over static routing is that routers exchange information when there is a topology change. This exchange allows routers to automatically learn about new devices and networks and also to find alternate paths when there is a link failure in the current network.

Table 4-264 summarizes the characteristics of the dynamic routing protocols supported by SWMRE:

Table 4-264: Dynamic routing protocols

	Border Gateway Protocol (BGP)	Routing Information Protocol (RIP)	Open Shortest Path First (OSPF)	Intermediate System to Intermediate System (ISIS)
Algorithm	path-vector routing	distance-vector routing	link-state routing	link-state routing

Type	Exterior Gateway Protocol (EGP)	Interior Gateway Protocol (IGP)	Interior Gateway Protocol (IGP)	Interior Gateway Protocol (IGP)
Classless Interdomain Routing (CIDR)	Yes	RIP v1: No RIP v2: Yes	Yes	Yes
Scalable	Yes	No	Yes	Yes
Speed of convergence	Moderate	Slow	Fast	Fast

Table 4-264: Dynamic routing protocols

	Border Gateway Protocol (BGP)	Routing Information Protocol (RIP)	Open Shortest Path First (OSPF)	Intermediate System to Intermediate System (ISIS)
Resource Use	High	Low	High	High
Configuration ease	Complex	Simple	Complex	Complex

routing table. See Routing Information Base (RIB).

S

S-TAG. See service VLAN (S-VLAN).

(S,G). A notation used in multicast that enumerates a shortest path tree (SPT) where:

- S is the IP address of the source
- G is the multicast group address that identifies the receivers

If the IP address of the source is 192.1.1.1, and the IP address of the multicast group is 224.1.1.1, the source group is written as (192.1.1.1, 224.1.1.1).

Secure Shell (SSH). A protocol that allows the opening of a secure, encrypted channel between two computers with secure authentication. SSH is most often used to provide a secure shell to log in to a remote machine, but also supports file transfers, TCP, and other functions.

segment routing. A form of source routing where nodes and links are represented as segments. The path that a particular protocol data unit (PDU) needs to traverse is represented by one or more segments.

server. A system entity that provides a service to other entities called clients.

service VLAN (S-VLAN). In a Provider Bridging (PB) frame, a tag that identifies the service provider network VLAN. See also customer VLAN (C-VLAN). Also called an S-TAG or S-VID tag.

Shortest Path Bridging (SPB). A control plane protocol that combines an Ethernet data path with an Intermediate System to Intermediate System (IS-IS) link state protocol running between switches. SPB does not depend on spanning tree protocols to provide a loop-free topology, but instead uses IS-IS link-state packets to discover and advertise the network topology and compute the shortest path tree (SPT) instances from all bridges in the SPB area. SPB only requires provisioning at the edge of the network. Defined by IEEE 802.1aq, with RFC 6329 describing the ISIS extensions to support SPB.

There are two types of SPB depending on the type of Ethernet data path:

- Shortest Path Bridging - VID (SPBV) uses a Provider Bridging (PB) (802.1ad) data path
- Shortest Path Bridging - MAC (SPBM) uses a Provider Backbone Bridging (PBB) (802.1ah) data path

shortest path first (SPF). Algorithm used by Intermediate System to Intermediate System (IS-IS) and Open Shortest Path First (OSPF) to make routing decisions based on the state of network links. Also called the Dijkstra algorithm.

shortest path tree (SPT). A Routing Information Base (RIB) formed by using the shortest path first (SPF) algorithm.

shortest-path routing. A routing algorithm in which paths to all network destinations are calculated. The

shortest path is then determined by a cost assigned to each link. **signalling.** The ability to transfer information

within a network or between different networks.

Simple Network Management Protocol (SNMP). A standardized framework for monitoring and managing devices in a network. The SNMP framework consists of three parts:

- SNMP manager: The system used to control and monitor the activities of network devices.
- SNMP agent: The component within a managed device that maintains the data for the device and reports the data SNMP managers.
- Management Information Base (MIB): How SNMP exposes data as variables which describe the system configuration. These variables can be queried (and sometimes set) by SNMP managers.

SNMP uses User Datagram Protocol (UDP) to send and receive messages on the network.

Single Root I/O Virtualization (SR-IOV). A specification that allows a single Peripheral Component Interconnect Express (PCIe) physical device under a single root port to appear to be multiple separate physical devices to the hypervisor or the guest operating system.

SR-IOV uses physical functions (PFs) and virtual functions (VFs) to manage global functions for the SR-IOV devices:

- PFs are used to configure and manage the SR-IOV functionality
- VFs are lightweight and contain all the resources necessary for data movement but have a minimal set of configuration resources

SR-IOV enables network traffic to bypass the software switch layer of a virtualization stack. The I/O overhead in the software emulation layer is nearly the same as in nonvirtualized environments.

Software-Defined Networking (SDN). An approach to designing, building, and operating networks that decouples the control plane from the data plane. The control plane is centralized in the form of a controller system.

Communication between the controller system and the network device uses a standard protocol such as OpenFlow or other agents. The controller system can consist of multiple, domain specific, clustered controllers. An SDN architecture usually includes APIs that developers use to control the underlying network. These APIs can be standards-based, or they can be vendor-specific.

source routing. A technique where the sender of a protocol data unit (PDU) can partially or completely specify the route that the PDU should take through the network. See also segment routing.

southbound. An interface that allows a network component to communicate with a lower-level component. A southbound interface breaks down the concepts into smaller technical details that are specifically geared toward the lower-layer component within the architecture. Southbound flow can be thought of as going downward. In architectural diagrams, southbound interfaces are drawn at the bottom of the component. See also northbound.

spanning tree algorithm. A technique that finds the best path between segments of a multilooped, mesh network. If multiple paths exist in the network, the spanning tree algorithm finds the most efficient path and limits the link between the two networks to this single active path. If this path fails because of a cable failure or other problem, the algorithm reconfigures the network to use another path.

From the point of view of an individual switch, a spanning tree has a root node and one path that connects all the other switches.

Spanning Tree Protocol (STP). A protocol that creates spanning trees within mesh networks of connected devices, disabling any links that are not a part of the tree and leaving a single active connection between any two unique network nodes. Defined by 802.1D.

STP devices exchange bridge protocol data unit (BPDU) messages. The spanning tree algorithm calculates the best path and prevents multiple paths between network segments. STP elects a root bridge, finds paths and determines the least cost path to the root bridge, then disables all other paths.

Network managers can set up redundant links as backups in case active links fails. Automatic backup takes place without the pitfalls of bridge loops or the need to manually enable or disable backup links. See also Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP).

split horizon. A technique where routes learned from an interface are not advertised on that same interface, preventing the router from seeing its own route updates.

In split horizon with poison reverse, routes learned from an interface are set as unreachable and advertised on that same interface which also prevents the router from seeing its own route updates. **stacked VLAN.** See Provider Bridging (PB).

static address. An address permanently assigned to a device. Contrast with a dynamic address.

static routing. A method where a network administrator programs connecting paths between networks into a router. If a connection fails, the administrator must reprogram the router to use a new path. Static routes have precedence over routes chosen by dynamic routing protocols.

stub area. A type of Open Shortest Path First (OSPF) area where external routes are distributed as a single default route (address 0.0.0.0). Inter-area routes are distributed in a stub area as summary addresses.

In a *totally stubby area*, a single default route is distributed for all external *and* inter-area routes. Addresses from both other areas and external networks are distributed as the default route (address 0.0.0.0).

See also Not-So-Stubby-Area (NSSA).

subnet mask. A bit pattern that shows how an Internet address is divided into network, subnetwork, and host parts. The mask has ones in the bit positions to be used for the network and subnet parts, and zeros for the host part. The mask should contain at least the standard network portion, and the subnet field should be contiguous with the network portion.

This is an example is this IPv4 address and subnet mask:

192.168.100.12 with subnet mask of 255.255.255.0

The first 24 bits of the address is the network address (192.168.100.0) and the last 8 bits are the hosts (12). The entire subnet spans the address range 192.168.100.0 to 192.168.100.255.

The addresses on a given subnet are always contiguous and can all be derived from the network address. Bit masks are always with respect to binary digits, so the number of IP addresses on a given subnet is always some power of two.

A mask gives the first address in the block (the network address) when ANDed with an address in the block.

Classless Interdomain Routing (CIDR) represents the equivalent of a subnet mask by adding a prefix length to an IP address that is the number of bits in the network portion. For example, the subnet mask above can be written as:

192.168.100.12/24 where 192.168.100.12 is the IP address and /24 is the number of bits

in the subnet mask.

A subnet mask represents the same information as a prefix length, but predates the use of CIDR.

Also called address mask, network mask.

subnetwork. A group of related IP addresses that all begin with the same network portion and end with a unique portion identifying the host within the subnet.

Also called subnet. See also subnet mask.

subsequent address family identifier (SAFI). Number that further identifies an address family.

supernetting. The process of taking several discrete network addresses and advertising them as one route. For example, if an organization is using 192.10.1.0/24 to 192.10.254.0/24, instead of advertising 254 separate networks, the organization can advertise only the single route 192.10.0.0/16.

switch. A Layer 2 (L2) device that forwards frames based on a destination MAC address. A switch finds a destination address in its filtering database and transmits the frame on the port associated with the destination address. The filtering database is populated through a self-learning process, where each incoming frame is used to update the entries in the filtering database.

A switch that is VLAN-aware can also forward frames based on VLAN identifiers. A network administrator can configure this mapping manually or a switch can dynamically learn mappings via GARP VLAN Registration Protocol (GVRP).

Basic switch behavior is defined in IEEE 802.1D and 802.1Q.

See also bridge. Contrast with router.

Synchronous Ethernet (SyncE). SONET/SDH/PDH-based synchronization that is used to synchronize and send frequency information to devices on an Ethernet network. Synchronous Ethernet provides only frequency synchronization, not time or phase synchronization.

T

telnet. A client/server protocol that establishes a session between a user terminal and a remote host:

- The telnet client software takes input from the user and sends it to the server's operating system
- The telnet server takes output from the host and sends it to the client to display to the user

While telnet is most often used to implement remote login capability, the protocol is general enough to allow it to be used for a variety of purposes.

Terminal Access Controller Access Control System Plus (TACACS+). An authentication method that provides access control for networked devices using one or more centralized servers. TACACS+ provides separate authentication, authorization, and accounting (AAA) services. (Usually pronounced like tack-axe.)

See also Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial In User Service (RADIUS).

throughput. Average rate of successful delivery of data packets over a communication link. Throughput is measured in bits per second, data packets per second, or sometimes data packets per time slot. See also line rate, latency, wire speed.

time to live (TTL). A limit on how long a piece of information can exist before it should be discarded. TTL is a field in an IP header that is (usually) decremented by 1 for each hop through which the packet passes. If the field reaches zero, the packet is discarded, and a corresponding error message is sent to the source of the packet.

Top-of-Rack (ToR) switch. In a data center, an access layer switch that connects to servers installed in the same rack. A ToR switch is usually low profile (one or two rack units in height) with a low port count (typically 48 ports). All cabling for servers stays within the rack as relatively short cables from the servers to the switch. The switch connects the rack to the data center network with one fiber uplink to a distribution layer switch. There is no need to run cabling between racks and each rack can be managed as a modular unit.

A ToR switch extends the Layer 2 (L2) topology from the aggregation switch to each individual rack resulting in a larger Layer 2 footprint.

See also end-of-row switch.

topology. The physical or logical layout of a network.

topology change notification (TCN). In Spanning Tree Protocol (STP), a bridge protocol data unit (BPDU) that a switch sends to signal a topology change.

traffic engineering (TE). The ability to control the path taken through a network based on a set of traffic parameters. Traffic engineering optimizes the performance of networks and their resources by balancing traffic load across links, routers, and switches in the network. See also Resource Reservation Protocol—Traffic Engineering (RSVP-TE).

Transmission Control Protocol (TCP). A Layer 4 (L4) protocol that works above Internet Protocol (IP) and provides reliable data delivery over connection-oriented links.

TCP splits the stream of data into packets with a sequence number, and sends the packets over an IP-based network. At the destination, TCP acknowledges packets that have been received (so that missing packets can be resent) and reassembles received packets in the correct order to provide an in-order data stream to the remote application. If TCP detects a missing, corrupted, or out of order packet, it requests it be resent from the source. See also Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP).

Transmission Control Protocol/Internet Protocol (TCP/IP). A family of Internet protocols that describe how data should be formatted, addressed, transmitted, routed, and received to enable computers to communicate over a network.

The Open Systems Interconnection (OSI) Reference Model is a more prescriptive (versus descriptive) approach to network design. TCP/IP does not map cleanly to the OSI model because it was developed before the OSI model and was designed to solve a specific set of problems, not to be a general description for all network communications.

TCP/IP is a widely published open standard and is supported by many vendors and is available on many different computers running many different operating systems. TCP/IP is separated from the network hardware and will run over Ethernet and other connections.

TCP/ IP also refers to the specific functionality at layers 4 and 3:

- Transmission Control Protocol (TCP) at Layer 4 (L4) splits a message into packets that are transmitted over the Internet and reassembles the packets into the original message at the destination
- Internet Protocol (IP) at Layer 3 (L3) addresses and routes each packet so that it gets to its destination

TRansparent Interconnection of Lots of Links (TRILL). Layer 2 (L2) bridging using Intermediate System to Intermediate System (IS-IS) link-state routing. TRILL encapsulates native frames in a transport header that contains a hop count, routes the encapsulated frames using IS-IS, and decapsulates the native frame before delivery.

Spanning tree protocols restrict all traffic to a loop-free tree and in doing so creates blocking conditions that require the over provisioning of links. With TRILL, you can create a fully meshed network where all links are available on all paths, eliminating the need to over-provision links and improving the utilization of data center networking equipment.

transport layer. See Layer 4 (L4).

tunneling. A method of transporting data in one protocol by encapsulating it in another protocol. Tunneling is used for reasons of incompatibility, implementation simplification, or security. For example, a tunnel lets a remote VPN client have encrypted access to a private network.

type of service (ToS). A field in the IPv4 header used to differentiate packet flows. See also Differentiated Services (DiffServ).

type-length-value (TLV). A data structure used to encode optional information in a data communications protocol:

- Type: the kind of field that this part of the message represents
- Length: the size of the value field, usually in bytes
- Value: a variable-sized set of bytes that contains the data of the message

U

unicast. The process of a single host sending messages to one destination.See also broadcast, multicast.

User Datagram Protocol (UDP). A connectionless transport layer protocol that exchanges datagrams without acknowledgments or guaranteed delivery and which requires other protocols to handle error processing and retransmission. Defined in RFC 768.

Multicast applications that deliver audio and video streams use UDP as their delivery mechanism because the acknowledgment and retransmission services offered by Transmission Control Protocol (TCP) are not needed and add too much overhead.

User-to-Network Interface (UNI). The physical interface/demarcation between a service provider and a subscriber, the service start or end point. There are two types of UNI:

- UNI-C: customer-side processes
- UNI-N: network-side processes

V

VirNOS. AnSymanitron Networks product based on Network Functions Virtualization (NFV) that helps network operators deploy and manage networking services. Many core networking services, including switching, routing, load balancing and VPN can be performed by software either running directly on x86-64 servers or running as virtual machine (VM) instances instead of requiring expensive networking equipment. Therefore, organizations are migrating networking functions to standard, high-volume server environments and replacing dedicated network hardware with virtualization software that runs on commodity servers. Carriers, service providers, enterprises and network equipment manufacturers can run VirNOS as-is, on top of a standard server platform. Symanitron Networks customers can integrate VirNOS into their software offering and thereby add services and features quickly.

Virtual Ethernet Bridge (VEB). A virtual switch implemented in a virtualized server environment. A VEB mimics a traditional external Layer 2 (L2) switch for connecting to a virtual machine (VM). VEBs can communicate between VMs on a single physical server, or they can connect VMs to the external network. The most common implementations of VEBs are software-based vSwitches built into hypervisors.

Virtual Local Area Network (VLAN). A logical group of network devices that appear to be on the same LAN, regardless of their physical location. VLANs enable multiple bridged LANs to transparently share the same physical network link while maintaining isolation between networks. Traffic between VLANs is restricted to devices that forward unicast, multicast, or broadcast traffic only on the LAN segments that serve the VLAN to which the traffic belongs.

VLANs make it easy to administer logical groups of hosts that can communicate as if they were on the same LAN.

Membership in a particular VLAN can be by port, MAC address, protocol, or subnet.

VLANs are configured as unique Layer 2 (L2) broadcast domains. VLANs allow network administrators to resegment their networks without physically rearranging the devices or network connections. VLANs span one or more ports on multiple devices and several VLANs can co-exist on a single physical switch. By default, each VLAN maintains its own filtering database containing MAC addresses learned from frames received on ports belonging to the VLAN.

IEEE 802.1Q provides for tagging Ethernet frames with VLAN identifiers. 802.1Q only supports up to 4094 VLANs, which is a scaling constraint for service providers.

virtual machine (VM). An operating system or application environment installed on emulated hardware and not physically installed on dedicated hardware. The virtual machine's guest operating system does not have to be modified to run in a virtualized environment. A VM behaves like a traditional, physical server and runs a traditional operating system such as Windows or Linux.

A hypervisor emulates the computer's CPU, memory, hard disk, network and other hardware resources completely, enabling virtual machines to share the resources. The hypervisor can emulate multiple virtual hardware platforms that are isolated from each other. For example, virtual machines can run Linux and Windows operating systems and share the same underlying physical host. An operating sysem is unaware that it is running in a VM.

See also paravirtualized, virtualization.

virtual port. A port on a vSwitch (Virtual Switch) where virtual Ethernet adapters or physical uplinks can be attached. During their creation, virtual switches are typically configured with a specific number of virtual ports.

virtual private LAN service (VPLS). Multipoint-to-multipoint Layer 2 (L2) VPN service used to interconnect multiple Ethernet LANs across an Multi-Protocol Label Switching (MPLS) backbone.

VPLS evolved as a logical extension of Virtual Private Wire Service (VPWS) based on RFC 4447.

VPLS can be defined as several instances of a virtual switch instance (VSI) that are interconnected to form a single logical bridge domain.

Virtual Private Network (VPN). A network service which uses encryption and tunneling to provide a subscriber with a secure private network that runs over the public network infrastructure.

Virtual Private Wire Service (VPWS). Point-to-point Layer 2 (L2) VPN service used to interconnect multiple Ethernet LANs across an Multi-Protocol Label Switching (MPLS) backbone. Also called Virtual Leased Line (VLL) or Ethernet over MPLS (EoMPLS).

virtual router (VR). A SWMRE proprietary abstraction where multiple distinct logical routers exist within a single device. Each virtual router executes separate instances of the routing protocol and network management software. A virtual router provides support for multiple Routing Information Base (RIB) instances and multiple Forwarding Information Base (FIB) instances per physical router. Each VR might consist of an Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), or Routing Information Protocol (RIP) routing process, each with its own Routing Information Base (RIB) and Forwarding Information Base (FIB). Applications include segregating traffic dedicated to different customers, enterprise Virtual Private Network (VPN) users, or a specific traffic type such as streaming video.

Do not confuse a Virtual Router Redundancy Protocol (VRRP) virtual router with a SWMRE virtual router. They are two different things.

Virtual Router Redundancy Protocol (VRRP). A protocol that uses a *virtual router*, an abstract representation of multiple routers (master and backup routers) that act as a group. VRRP advertises a virtual router as the default gateway instead of one physical router. Two or more physical routers are configured, with only one doing the actual routing at any given time. If the current physical router that is routing on behalf of the virtual router fails, the other physical router automatically takes over. Defined by RFC 5798.

Do not confuse a VRRP virtual router with an SWMRE virtual router (VR). They are two different things.

Virtual Routing and Forwarding (VRF). A technology that allows multiple instances of a Routing Information Base (RIB) to co-exist within the same router at the same time. Multiple VRFs inside a virtual router (VR) logically subdivide the RIBs. Service providers can use VRF technology to create a separate Virtual Private Network (VPN) for each of their customers. Therefore, the technology is also called VPN routing and forwarding.

virtual switch instance (VSI). A mechanism for VLANs to pass packets to other VLANs without sending the packets through a router. With a VSI, the switch recognizes packet destinations that are local to the sending VLAN and bridges (switches) those packets. Only packets destined for another VLAN are routed.

A VSI is similar to the bridging defined in IEEE 802.1Q; a frame is switched, based on the destination MAC and membership in a Layer 2 (L2) VPN. A VSI floods unknown, broadcast, or multicast frames to all ports associated with the VSI.

virtualization. A technology that abstracts the physical characteristics of a machine, creating a logical version of it, including creating logical versions of entities such as operating systems and network resources. See also hypervisor, virtual machine (VM).

vNIC (Virtual Network Interface Card). Software that behaves like a Ethernet hardware adapter. It has a MAC address, and it sends and receives Ethernet frames.

VPN routing and forwarding. See Virtual Routing and Forwarding (VRF).

vSwitch (Virtual Switch). Software that behaves like a physical Ethernet switch. A vSwitch connects virtual machine (VM) instances in a virtual network at layer 2:

- Connects vNIC (Virtual Network Interface Card) instances from multiple VMs to virtual ports
- Connects physical network interface cards to virtual ports
- Uplinks to the physical network

A vSwitch maintains a MAC address table and routes traffic to specific ports, rather than repeating traffic on all ports. A vSwitch can include other features found in physical Ethernet switches, such as VLANs.

See also Open vSwitch (OVS).

W

weighted fair queuing (WFQ). Queue scheduling discipline where each queue has a weight and is assigned a different percentage of output port bandwidth. WFQ supports variable-length packets so that flows with larger packets are not allocated more bandwidth than flows with smaller packets.

WFQ classifies traffic as high- or low-bandwidth with low-bandwidth traffic getting priority and high-bandwidth traffic sharing what is left over. If traffic bursts ahead of the rate at which the interface can transmit, new high-bandwidth traffic is discarded after a congestive-messages threshold has been reached.

WFQ provides preferential treatment for higher priority traffic while preventing total starvation of lower priority traffic under sustained overload conditions.

weighted random early detection (WRED). Congestion avoidance mechanism which prevents an output queue from ever filling to capacity. WRED provides separate thresholds and weights for different IP precedences, allowing you to provide different qualities of service in regard to packet dropping for different traffic types. Standard traffic may be dropped more frequently than premium traffic during periods of congestion.

weighted round-robin queuing (WRR). Queue scheduling discipline that supports flows with significantly different bandwidth requirements. Each queue can be assigned a weight that is relative to other queues. WRR ensures that lower-priority queues are not denied access to buffer space and output port bandwidth. At least one packet is removed from each queue during each service round.

white box switch. In computer hardware, a white box is a server without a well-known brand name made from commonly available parts. White box switches are like white box servers, offering low cost without the brand name or tight integration of silicon and network software features.

Traditional black box switches are built with vertically integrated hardware and software. Some vendors use custom application-specific integrated circuit (ASIC) components to boost performance and add features, which adds to the cost. A white box switch decouples the software from the switching hardware. By decoupling software and hardware, customers have more flexibility and can potentially change software without changing hardware.

A white box switch runs a network operating system on generic x86 hardware with “merchant silicon” chipsets from manufacturers such as Broadcom, Centec, Intel, Marvell, and Mellanox. White box switches rely on an operating system such as Linux to integrate the Layer 2 (L2)/Layer 3 (L3) networking functions.

White box switches do not have the same complex features as black box switches because most interact with Software-Defined Networking (SDN) controllers to make forwarding and control plane decisions from a centralized point for all switches in the network. The SDN controller uses OpenFlow (or another southbound API) to program the forwarding table of the white box switches.

Some vendors sell a complete white box solution with the operating system already installed, while others supply just the “bare-metal” switch and you buy the operating system direct from the software vendor.

wide area network (WAN). A network that provides communication services to a geographic area larger than that served by a Local Area Network (LAN) and that may use or provide public communication facilities.

wire speed. The ability of a device to achieve throughput equal to the maximum throughput of a communication standard.

Y

YANG. A data modeling language that specifies the syntax and semantics for NETCONF (Network Configuration Protocol) operations, notification events, and database content. YANG tools can automate behavior within the NETCONF protocol for clients and servers.

YANG can model both configuration and state data of network elements. YANG structures the data definitions into tree structures and provides many modeling features, including an extensible type system, formal separation of state and configuration data and a variety of syntactic and semantic constraints. YANG data definitions provide a strong set of features for extensibility and reuse. Defined in RFC 6020.

SECTION 17 Master Command Index

Symanitron

Master Command Index

g8031 configure vlan 3334 disable 4224 enable 4225 ethernet cfm pbb-te ais interval 3404 ethernet cfm pbb-te cc multicast 3406 ethernet cfm pbb-te cc unicast 3407 ethernet cfm pbb-te throughput-measurement reception 3416 g8031 configure switching 3333 g8031 force 3337 g8031 local-lockout 3339 g8031 manual 3341 g8031 mode 3342 g8031 set-nr 3344 g8031 timer 3345 g8031 vlan 3347 preempt-mode 4226 priority 4227
1dm 3217 1dm receive 3218 aaa accounting details 423 aaa authentication login 422 aaa authentication login console 424 aaa authentication login console fallback error 426 aaa authentication login default 425 aaa authentication login default fallback error 427 aaa group server 428 aaa local authentication attempts max-fail 429 aaa local authentication unlock-timeout 430 abr-type 2377 accept-lifetime 2593 accept-lifetime 2485 accept-mode 4200 accept-non-adj 3977 access-list logging cache-size 855 access-list logging rate-limit 856 add policy 452 add static fdb neighbor-nickname 3978 add static l2-unicast-trill-fdb 3979 add static multicast-fdb d-tree ingress-nickname 3980 add static multicast-fdb d-tree neighbor-nickname 3981 add static multicast-trill-fdb ingress-d-tree 3982 add static multicast-trill-fdb multicast-listener 3983 add static unicast-trill 3984 add vid 3219 address 979 address-family 1993 address-family ipv4 unicast 2378

address-family ipv4 vrf 2668 adjacency-check 2487 admin-group 753 advertisement-interval 4201 advertisement-interval 4222 aggregate-address 1995 aggregate-address 2642 aggregate-address X:X::X:X/M 2144 ais interval 3220 ais status 3221 allocate interface 4374 announce interval 4436 announce timeout-interval 4437 application-priority advertise-local-config 3486 application-priority enable (interface) 3487 application-priority enable (switch) 3488 area authentication 2252 area default-cost 2253 area default-cost 2379 area filter-list 2254 area nssa 2255 area nssa 2380 area range 2257 area range 2382 area stub 2258 area stub 2384 area virtual-link 2259 area virtual-link 2385 area virtual-link 4330 area-password 2488 arp-ageing-timeout 5038 arp-cache disable 4948 arp-nd flood-suppress 4949 arp-nd refresh timer 4950 arp-reachable-time 5039 authentication 980 authentication key-chain 2489 authentication mode 2490 authentication send-only 2491 auth-mac auth-fail-action 1416 auth-mac disable 1417 auth-mac dynamic-vlan-creation 1418 auth-mac enable 1419 auth-mac mac-aging 1420 auth-mac system-auth-ctrl 1421 auto-cost reference bandwidth 2261 auto-cost reference bandwidth 2387 automatic-router-id-selection enable 672

auto-summary 1997 bandwidth 4745 bandwidth 754 bandwidth remaining 4746 bandwidth-percentage 3489 banner motd 567 bfd 4301 bfd all-interfaces 4331 bfd all-interfaces 2262 bfd all-interfaces 2492 bfd auth type 4300 bfd echo 4302 bfd echo interval 4303 bfd interval 4305 bfd multihop-peer 4306 bfd multihop-peer A.B.C.D interval 4307 bfd multihop-peer X:X::X:X interval 4308 bfd notification 4309 bfd slow-timer 4310 bfd-firmware 4304 bgp additional-paths 1998 bgp additional-paths select 1999 bgp aggregate-nexthop-check 2000 bgp always-compare-med 2001 bgp as-local-count 2002 bgp bestpath as-path ignore 2003 bgp bestpath as-path multipath-relax 2004 bgp bestpath compare-confed-aspath 2005 bgp bestpath compare-routerid 2006 bgp bestpath dont-compare-originator-id 2007 bgp bestpath med 2008 bgp bestpath tie-break-on-age 2010 bgp client-to-client reflection 2011 bgp cluster-id 2012 bgp confederation identifier 2013 bgp confederation peers 2014 bgp config-type 2015 bgp dampening 2016 bgp default ipv4-unicast 2018 bgp default local-preference 2019 bgp deterministic-med 2020 bgp enforce-first-as 2021 bgp extended-asn-cap 2022 bgp fast-external-failover 2023 bgp graceful-restart 2024 bgp g-shut 2026 bgp g-shut-capable 2027 bgp g-shut-local-preference 2028 bgp inbound-route-filter 2160 bgp log-neighbor-changes 2029 bgp multiple-instance 2031 bgp nexthop-trigger delay 2032 bgp nexthop-trigger enable 2033 bgp rfc1771-path-select 2034

bgp rfc1771-strict 2035 bgp router-id 2036 bgp scan-time 2037 bgp update-delay 2040 bridge acquire 1188 bridge address 1189 bridge ageing 1190 bridge agreement convention 3692 bridge cisco-interoperability 1217 bridge forward-time 1191 bridge g8031 eps-id 3332 bridge g8032 ring-id 3352 bridge hello-time 1192 bridge instance 1218 bridge instance priority 1219 bridge instance vlan 1220 bridge instance vlan 3693 bridge loop-mitigation 3694 bridge loop-prevention 3695 bridge mac-priority-override 1193 bridge max-age 1194 bridge max-hops 1195 bridge multiple-spanning-tree 1222 bridge priority 1196 bridge protocol 3544 bridge protocol 3696 bridge protocol ieee 1223 bridge protocol mstp 1224 bridge protocol provider-mstp 3190 bridge protocol provider-rstp 3191 bridge protocol rpvst+ 1285 bridge protocol rstp 1225 bridge rapid-pervlan-spanning-tree 1286 bridge rapid-spanning-tree 1226 bridge region 1227 bridge revision 1228 bridge shutdown 1197 bridge spanning-tree 1229 bridge spanning-tree errdisable-timeout 1230 bridge spanning-tree force-version 1231 bridge spanning-tree pathcost 1232 bridge spanning-tree portfast 1233 bridge spb enable 3697 bridge spbv bvlan group-mac 3698 bridge spbv bvlan spvid 3699 bridge spbv mode 3700 bridge spsourceid 3703 bridge spvid (alloc|dealloc) 3701 bridge spvid-pool 3702 bridge te-msti 1234 bridge te-msti vlan 1235 bridge transmit-holdcount 1198 bridge vlan 1282 bridge vlan priority 1283

bridge-group 1199 bridge-group instance 1236 bridge-group instance path-cost 1237 bridge-group instance priority 1238 bridge-group path-cost 1200 bridge-group path-cost 1239 bridge-group priority 1201 bridge-group priority 1240 bridge-group spanning-tree 1241 bridge-group spb path-cost 3704 bridge-group vlan 1284 capability cspf 2263 capability cspf 2388 capability lls 2264 capability opaque 2265 capability restart 2266 capability restart 2389 capability te 2468 capability te/traffic-engineering 2267 capability vrf-lite 2268 capability vrf-lite 2464 cc 3222 cc interval 3223 cc multicast 3224 cc unicast 3225 channel-group mode 1296 channel-protocol 4100 circuit-failover 4202 circuit-failover 4223 cisco-metric-behavior 2595 cisco-metric-behavior 2643 class 4563 class type qos 4749 class type queuing 4750 class-map name 4564 class-map type qos 4747 class-map type queuing 4748 clear 3226 clear aaa local user lockout username 330 clear access-list log-cache 857 clear access-list 858 clear allowed-ethertype 1202 clear arp 5040 clear bgp (A.B.C.D|X:X::X:X) 2041 clear bgp * 2042 clear bgp * ipv6 2146 clear bgp * l2vpn vpls 2161 clear bgp <1-4294967295> 2044 clear bgp <1-4294967295> l2vpn vpls 2163 clear bgp A.B.C.D l2vpn vpls 2165 clear bgp dampening 2046 clear bgp external 2047 clear bgp flap-statistics 2049 clear bgp ipv6 (A.B.C.D|X:X::X:X) 2147 clear bgp ipv6 <1-4294967295> 2148 clear bgp ipv6 external 2149 clear bgp ipv6 peer-group 2150 clear bgp ipv6 unicast dampening 2151 clear bgp ipv6 unicast flap-statistics 2152 clear bgp peer-group 2050 clear bgp statistics 2052 clear bgp view 2053 clear clns is-neighbors 2494 clear clns neighbors 2493 clear crypto isakmp 981 clear crypto sa 982 clear crypto sa entry 983 clear crypto sa map 984 clear crypto sa peer 985 clear ddm transceiver alarm 1032 clear ethernet cfm errors 3228 clear ethernet cfm maintenance-

points 3229 clear ethernet cfm traceroute-cache 3230 clear ethernet lmi statistics 3444 clear gmrp 1448 clear gvrp 1464 clear interface counters 755 clear interface cpu counters 756 clear interface fec 644 clear ip access-list 859 clear ip bgp * vpnv4 2162 clear ip bgp <1-4294967295> vpnv4 2164 clear ip bgp A.B.C.D 2055 clear ip bgp A.B.C.D vpnv4 2166 clear ip bgp A.B.C.D vrf 2057 clear ip bgp table-map 2058 clear ip bpg ipv6 unicast table-map 2155 clear ip dhcp snooping binding 1398 clear ip igmp 2774 clear ip isis route 2495 clear ip mroute 2760 clear ip mroute 2861 clear ip msdp peer 2863 clear ip msdp sa-cache 2864 clear ip ospf 2269 clear ip pim sparse-mode 2865 clear ip prefix-list 757 clear ip rip route 2596 clear ip rip route vrf NAME 2597 clear ip rip statistics 2598 clear ip route 2575 clear ip route kernel 2574 clear ip route vrf NAME 2576 clear ipv6 access-list 860 clear ipv6 bgp * vrf 2153 clear ipv6 bgp X:X::X:X vrf 2154 clear ipv6 mld 2808 clear ipv6 mroute 2931 clear ipv6 neighbors 5041 clear ipv6 neighbors 758 clear ipv6 ospf process 2390 clear ipv6 pim sparse-mode bsr 2933 clear ipv6 prefix-list 759 clear ipv6 rip route 2644 clear isis adjacency 2496 clear isis counter 2497 clear isis interface counter 2498 clear isis process 2499 clear lacp 1298 clear ldap-server statistics 472 clear lldp counters 3156 clear mac access-list 861 clear mac address table dynamic vxlan 4951 clear mac address-table 1203 clear mls qos cosq-stat 4565 clear mmrp 1480 clear mvrp 1494 clear ntp statistics 336 clear nvo vxlan counters 4952 clear nvo vxlan mac-stale-entries 4953 clear qos statistics 4751 clear rbridge trill 3985 clear rbridge trill counter 3986 clear rbridge trill interface counter 3987 clear rbridge trill mac 3988 clear router-id 673 clear sflow statistics 4514 clear snmp hostconfig 277 clear spanning-tree detected protocols 1242 clear spanning-tree statistics 1243 clear ssh hosts 256 clear switch-source 4484 clear tfo counter 3766 clock timezone 674 clock-port 4438 clock-selection mode 4485 cnpv 3512 compatible rfc1583 2270 confidence 3989 configuration file 4358 configure terminal 568 configure terminal force 569 continue 707 control-adjacency 944 control-channel 936 copy empty-config startup-config 645 copy file running-config 399 copy ftp running-config 380 copy ftp startup-config (interactive) 393 copy ftp startup-config 379 copy http running-config (interactive) 392 copy http running-config 388 copy http startup-config (interactive) 397 copy http startup-config 387 copy running-config (interactive) 374 copy running-config 373 copy running-config startup-config 570 copy scp running-config (interactive) 389 copy scp running-config 382 copy scp startup-config (interactive) 394 copy scp startup-config 381 copy sftp running-config (interactive) 390 copy sftp running-config 384 copy sftp startup-config (interactive) 395 copy sftp startup-config 383 copy startup-config (interactive) 376 copy startup-config 375 copy startup-config running-config 398 copy system file (interactive) 378 copy system file 377 copy tftp running-config (interactive) 391 copy tftp running-config 386 copy tftp startup-config (interactive) 396 copy tftp startup-config 385 cos 4954 cos queue 4955 cp enable 3513 crypto ipsec security-association lifetime 986 crypto ipsec transform-set 987 crypto isakmp enable 989 crypto isakmp policy 990 crypto key generate rsa 991 crypto map (Configure Mode) 992 crypto map (Interface Mode) 993 crypto map local-address 994 cspf default-retry-interval 2469 cspf tie-break 2470 customer-spanning-tree customer-edge path-cost 1244 customer-spanning-tree customer-edge priority 1245 customer-spanning-tree forward-time 1246 customer-spanning-tree hello-time 1247 customer-spanning-tree max-age 1248 customer-spanning-tree priority 1249 customer-spanning-tree provider-edge path-cost 1250 customer-spanning-tree provider-edge priority 1251 customer-spanning-tree transmit-holdcount 1252 cvlan registration table 3192 cvlan svlan 3193 data-center-bridging 3490 data-link 924 dcbx enable 3491 ddm monitor 1033 ddm monitor all 1034 ddm monitor interval 1035

debug aaa 431 debug
bfd 4311
debug bgp 2059 debug bgp bfd 4332 debug bgp
mpls 2167 debug cmm 1020 debug cspf 2471
debug ddm 1036 debug dns client 246 debug
dot1x 1422 debug ecp 3545 debug elmi 3445
debug gmrp 1449 debug gvrp 1465 debug ip arp
5042 debug ip dhcp snooping 1399 debug ip igmp
2775 debug ip mrib 2761 debug ip ospf graceful-
restart 2276 debug ip ospf lfa 2277 debug ip ospf
redist 2278 debug ip ospf retransmission 2279
debug ip pim 2866 debug ip pim packet 2867
debug ip pim timer assert 2869 debug ip pim timer
bsr 2870 debug ip pim timer hello 2871 debug ip
pim timer joinprune 2873 debug ip pim timer
register 2875 debug ipv6 mld 2809 debug ipv6 nd
5043 debug ipv6 ospf 2391 debug ipv6 ospf bfd
2392 debug ipv6 ospf events 2393 debug ipv6
ospf ifsm 2394 debug ipv6 ospf lfa 2395 debug
ipv6 ospf lsa 2396 debug ipv6 ospf nfsm 2397
debug ipv6 ospf nsm 2398 debug ipv6 ospf packet
2399 debug ipv6 ospf retransmission 2400 debug
ipv6 ospf rib 2401 debug ipv6 ospf route 2402
debug ipv6 pim 2934 debug ipv6 pim packet 2935
debug ipv6 pim timer assert 2936 debug ipv6 pim
timer bsr 2937 debug ipv6 pim timer hello 2938
debug ipv6 pim timer joinprune 2939 debug ipv6
pim timer register 2941 debug ipv6 rip 2645 debug
isis 2500 debug isis bfd 4333 debug isis-spb 3705
debug lacp 1299 debug ldap 473 debug logging
311 debug mcec 1327 debug mstp 1253 debug
nsm all 646 debug nsm bfd 647 debug nsm
events 648 debug nsm hal 649 debug nsm packet
650 debug ntp 337 debug ospf bfd 4334 debug
ospf database-timer rate-limit 2273 debug ospf
events 2274 debug ospf ifsm 2275 debug ospf lsa
2280 debug ospf nfsm 2281 debug ospf nsm 2282
debug ospf packet 2283 debug ospf rib 2284
debug ospf route 2285 debug ospf 2271 debug
pim all 2868 debug ptp all 4439 debug ptp event
4440 debug ptp packet rx 4441 debug ptp packet
tx 4442 debug ptp protocol 4443 debug ptp timer
4444 debug radius 440 debug rib 2577 debug rip
2599 debug rip bfd 4335 debug sflow 4515 debug
snmp-server 278 debug spb 3706 debug ssh
server 257 debug tacacs+ 453 debug telnet server
298 debug trill all 4041 debug trill esadi 4043
debug trill events 4042 debug trill ifsm 4044 debug
trill l2mrib 4046 debug trill lsp 4045 debug trill
nfsm 4047 debug trill nsm 4048 debug trill oam
4049 debug trill pdu 4050 debug
trill spf 4051 debug user-mgmt 331 debug vrrp
4203 default 454 default-information originate
2286 default-information originate 2403 default-
information originate 2502 default-information
originate 2601 default-information originate 2647
default-metric 2288 default-metric 2405 default-
metric 2602 default-metric 2648 defense-mode
cnpv 3514 delay-req-interval 4445 delete vid
bridge 3231 deny 455 description 1352
description 2579 description 4359 description
4956 description 760 description 925 description
937 description 945 destination port 1348 disable
4204 disable 571 disable l3-protocols-cpu vxlan
4957 distance (IPv6) 2503 distance 2289 distance
2406 distance 2603 distance 2649 distance bgp
2061 distribute-list 2290 distribute-list 2407
distribute-list 2604 distribute-list 2650
dmm 3232 do 610 domain hello timeout 1328
domain priority 1329 domain system number
1330 domain-address 1326 domain-password
2504 dot1x initialize 1423 dot1x keytxenabled
1424 dot1x port-control 1425 dot1x protocol-
version 1426 dot1x quiet-period 1427 dot1x
reauthentication 1429 dot1x reauthMax 1428
dot1x system-auth-ctrl 1430 dot1x timeout re-
authperiod 1431 dot1x timeout server-timeout
1432 dot1x timeout supp-timeout 1433 dot1x
timeout tx-period 1434 dscp 4958 dscp queue
4959 dtree-in-use 3990 dtree-nickname-to-
compute 3991 duplex 761 dvm 3233 dynamic-
learning disable 4960 enable 4205 enable 572
enable db-summary-opt 2292 enable db-
summary-opt 2409 enable password 573
encapsulation 4961 encryption 995 end 574
enhanced-transmission-selection (interface)
3495 enhanced-transmission-selection (switch)
3494 enhanced-transmission-selection accept-
peer-config
3492
enhanced-transmission-selection advertise-
local-config
3493 errdisable cause 675 errdisable
link-flap-setting 676 errdisable timeout
677 esadi confidence 4014 esadi csnp-
timer 4015 esadi disable 4016 esadi
enable 4017 esadi instance 4018 esadi
l2-learning 4019 esadi lsp-gen-interval
4020 esadi priority 4021 ethernet cfm
1dm mepid 3363 ethernet cfm 1dm
receive 3364 ethernet cfm ais interval
3365 ethernet cfm ais status 3366

ethernet cfm automatic bridge 3234 ethernet cfm automatic mep 3235 ethernet cfm cc multicast 3367 ethernet cfm cc unicast 3368 ethernet cfm configure default-md-level 3236 ethernet cfm configure vlan 3237 ethernet cfm debug 3238 ethernet cfm default-domain-level 3239 ethernet cfm default-md-level entry isid 3240 ethernet cfm default-md-level entry vid 3241 ethernet cfm default-mepid 3242 ethernet cfm dmm mepid 3375 ethernet cfm domain-name 3243 ethernet cfm dvm mepid 3376 ethernet cfm enable 3245 ethernet cfm exm 3377 ethernet cfm in-service 3378 ethernet cfm lmm counter 3246 ethernet cfm lmm frame count simulator 3247 ethernet cfm lmm mpid 3379 ethernet cfm mcc 3380 ethernet cfm mep 3248 ethernet cfm mep 3381 ethernet cfm mep clear 3369 ethernet cfm mep domain 3371 ethernet cfm mep domain tx-lbm-messages 3373 ethernet cfm mep domain tx-lbm-status 3374 ethernet cfm out-of-service 3382 ethernet cfm pbb 1dm 3383 ethernet cfm pbb 1dm receive 3384 ethernet cfm pbb ais interval 3385 ethernet cfm pbb ais status 3386 ethernet cfm pbb cc domain-name 3387 ethernet cfm pbb cc multicast 3388 ethernet cfm pbb cc unicast 3389 ethernet cfm pbb dmm 3390 ethernet cfm pbb dvm 3391 ethernet cfm pbb exm 3392 ethernet cfm pbb in-service 3393 ethernet cfm pbb lmm 3394 ethernet cfm pbb mcc 3395 ethernet cfm pbb mep 3396 ethernet cfm pbb out-of-service 3397 ethernet cfm pbb throughput-measurement 3398

ethernet cfm pbb tst 3399 ethernet cfm pbb vsm 3401 ethernet cfm pbb-te 1dm mepid 3402 ethernet cfm pbb-te 1dm receive 3403 ethernet cfm pbb-te ais status 3405 ethernet cfm pbb-te dmm 3408 ethernet cfm pbb-te dvm 3409 ethernet cfm pbb-te exm 3410 ethernet cfm pbb-te in-service 3411 ethernet cfm pbb-te lmm 3412 ethernet cfm pbb-te mcc 3413 ethernet cfm pbb-te mep 3414 ethernet cfm pbb-te out-of-service 3415 ethernet cfm pbb-te throughput-measurement unicast 3417 ethernet cfm pbb-te tst mep 3418 ethernet cfm pbb-te vsm 3420 ethernet cfm server-ais 3249 ethernet cfm throughput-measurement reception 3421 ethernet cfm throughput-measurement unicast 3422 ethernet cfm traceroute cache 3250 ethernet cfm traceroute cache size 3251 ethernet cfm tst 3423 ethernet cfm vid 3252 ethernet cfm vsm 3425 ethernet lmi async-msg-interval 3446 ethernet lmi global 3448 ethernet lmi interface 3447 ethernet lmi n391 3449 ethernet lmi n393 3450 ethernet lmi t391 3451 ethernet lmi t392 3452 ethernet oam debug 3286 ethernet oam disable 3287 ethernet oam enable 3288 ethernet oam link-monitor {symbol-period|frame-period} 3289 ethernet oam link-monitor event-log-size 3290 ethernet oam link-monitor frame {frame-seconds|frame} 3291 ethernet oam link-monitor frame 3292 ethernet oam link-monitor frame-period 3293 ethernet oam link-monitor frame-seconds 3294 ethernet oam link-monitor high 3295 ethernet oam link-monitor on 3296 ethernet oam link-monitor supported 3297 ethernet oam link-monitor symbol-period 3298 ethernet oam local-event 3299 ethernet oam max-rate 3300 ethernet oam min-rate 3301 ethernet oam mode 3302 ethernet oam remote-failure 3303 ethernet oam remote-loopback (start|stop) 3304 ethernet oam remote-loopback {supported|timeout} 3305 ethernet oam timeout 3306 ethernet oam unidirectional-link 3307 ethertype 3496 evb bridge cdcp channel-capacity 3546 evb bridge cdcp svid-pool-range 3547 evb bridge ecp-acktimer 3548 evb bridge ecp-max-retry 3549 evb bridge resource-wait-delay 3550 evb bridge tlv-mode 3551 evb bridge vdp-keep-alive 3552 evb cdcp 3553 evb reflective-relay 3554 evb-station 3555 evpn esi holdtime 4962 evpn irb1 4967 evpn irb-forwarding anycast-gateway-mac 4965 evpn irb-if-forwarding anycast-gateway-mac 4966

evpn multi-homed 4964
evpn multi-homing enable 4963 exec-timeout 575
exit 576 exit-address-family 2062 exit-address-family 2413 exit-address-family 2669 exit-interface-eth-cfm-mep 3253 exm tx 3254 fast-reroute keep-all-paths 2293 fast-reroute keep-all-paths 2410 fast-reroute tie-break 2294 fast-reroute tie-break 2411 fault-recover 4446
feature daemon 4376 feature dhcp 242 feature dynamic-rbac enable 456 feature ldap 474 feature ntp 338 feature rsyslog 310 feature sflow 4516 feature software-watchdog 402 feature ssh 258 feature tacacs+ 457 feature telnet 299 fec 762 fib retain 2580 filter 1351 flowcontrol 1178 fog 3767 fog tfc 3768 fog type 3769 forward-delay 3992 forwarding custom-profile 678 forwarding profile 680 g8031 ethernet 3335 g8031 exercise 3336 g8031 local-freeze 3338 g8031 lockout 3340 g8031 near 3343 g8031 signal-sync 3346 g8032 configure switching 3353 g8032 md-name 3354 g8032 mep 3355 g8032 rpl 3356 g8032 shared-link 3357 g8032 timer 3358 group 996 hardware register get 1180 hardware register set 1181 hardware-profile filter (Qumran) 682 hardware-profile filter 681 hardware-profile portmode 763 hardware-profile portmode bundle 764 hardware-profile statistics (Qumran) 683
hash 997 help 577
history 578 hold-off 4486
host area 2296
hostname 579
if-arbiter 765 igmp snooping 2834 igmp snooping fast-leave 2835 igmp snooping mrouter 2836 igmp snooping querier 2837 igmp snooping report-suppression 2838 igmp snooping static-group 2839 ignore-lsp-errors 2505 ignore-lsp-errors 3993 ike-version 998 import map 2168 input-source 4487 in-service testing 3255 interactive ping 615 interface 766 Interface irb 4968 interface po 1300 interface sa 1301 interface tunnel 950 intra-domain-link 1331 ip access-group 862 ip access-list default 864 ip access-list filter 870 ip access-list fragments 873 ip access-list icmp 865 ip access-list remark 874 ip access-list resequence 875 ip access-list tcp|udp 876 ip access-list WORD 882 ip address 926 ip address A.B.C.D/M 767 ip address dhcp 243 ip address dhcp 768 ip arp 5044 ip arp vrf 5045 ip as-path access-list 2063 ip bfd static all-interfaces 4340 ip community-list <100-500> 2065 ip community-list <1-99> 2064 ip community-list expanded 2066 ip community-list standard 2067 ip community-list WORD 2068 ip dhcp client request 244 ip dhcp packet strict-validation 1400 ip dhcp relay 360 ip dhcp relay address 361 ip dhcp relay information option 362 ip dhcp snooping 1401 ip dhcp snooping binding 1402 ip dhcp snooping database 1403 ip dhcp snooping information option 1404 ip dhcp snooping ratelimit 1405 ip dhcp snooping trust 1406 ip dhcp snooping verify mac-address 1407 ip dhcp snooping vlan 1408 ip domain-list 247 ip domain-lookup 248 ip domain-name 249 ip evpn prefix route 4969 ip extcommunity-list <100-500> 2070 ip extcommunity-list <1-99> 2069
ip extcommunity-list expanded 2071
ip extcommunity-list standard 2072
ip forwarding 769
ip host 250
ip ospf retransmit-interval 2314
ip ospf transmit-delay 2315
ip pim 2886
ip pim accept-register 2881
ip pim anycast-rp 2882
ip pim bsr-border 2883
ip pim bsr-candidate 2884
ip pim cisco-register-checksum 2885
ip pim dr-priority 2888
ip pim exclude-genid 2889
ip pim hello-holdtime 2890
ip pim hello-interval 2891
ip pim ignore-rp-set-priority 2892
ip pim jp-timer 2893
ip pim neighbor-filter 2894
ip pim passive 2887
ip pim propagation-delay 2895
ip pim register-rate-limit 2896
ip pim register-source 2898
ip igmp 2777
ip igmp access-group 2778
ip igmp immediate-leave 2779
ip igmp join-group 2780
ip igmp last-member-query-count 2781
ip igmp last-member-query-interval 2782
ip igmp limit 2783
ip igmp mroute-proxy 2784
ip igmp offlink 2785
ip igmp proxy unsolicited-report-interval 2787
ip igmp proxy-service 2786
ip igmp querier-timeout 2788
ip igmp query-interval 2789
ip igmp query-max-response-time 2790
ip igmp ra-option 2791
ip igmp robustness-variable 2792

igmp ssm-map enable 2793 ip pim register-suppression 2899 ip igmp ssm-map static 2794
ip pim router-id 2900 ip igmp startup-query-count 2796 ip pim rp-address 2901 ip igmp startup-
query-interval 2797 ip pim rp-candidate 2903 ip igmp static-group 2795 ip pim rp-
register-kat 2904 ip igmp version 2798 ip pim spt-threshold 2905 ip local-proxy-arp 770 ip pim
ssm 2906
ip mroute 686 ip pim state-refresh origination-interval 2907 ip msdp default-peer 2876 ip pim unicast-
bsm 2908 ip msdp mesh-group 2877 ip prefix-list 771 ip msdp originator-id 2878 ip proxy-arp
5046 ip msdp password 2879 ip proxy-arp 774 ip msdp peer 2880 ip radius source-interface 1435
ip multicast route-limit 2762 ip remote-address 775 ip multicast ttl-threshold 2763 ip rip
authentication key-chain 2605 ip multicast-routing 2764 ip rip authentication mode 2606 ip name-server
251 ip rip authentication string 2607 ip ospf authentication 2297 ip rip receive version 2609 ip
ospf authentication-key 2298 ip rip receive-packet 2608
ip ospf bfd 4336 ip rip send version 2611 ip ospf bfd 2299 ip rip send-packet 2610
ip ospf cost 2300 ip rip split-horizon 2612 ip ospf database-filter 2301 ip route
2581 ip ospf dead-interval 2302 Ip route vrf <vrfname> 4972 ip ospf disable 2303
ip router isis 2506
ip ospf fast-reroute per-prefix candidate disable 2304 ip static bfd 4342
ip ospf flood-reduction 2305 ip static fall-over bfd 4341 ip ospf hello-interval 2306
ip unnumbered 776 ip ospf message-digest-key 2308 ip urpf allow-default 685
ip ospf mtu 2310 ip urpf enable 684
ip ospf mtu-ignore 2311 ip verify unicast source reachable-via 974 ip ospf multi-area 2307 ip vrf
2169 ip ospf network 2312 ip vrf 2583 ip ospf priority 2313 ip vrf 4360
ip vrf forwarding 4971 ip vrf forwarding 777 ip mld version 2826 ipv6 mroute 688 ipv6 nd current-
vrf isid 3707 ip6-access-list (extended named) hoplimit 780 ipv6 nd link-mtu 781 ipv6 nd
4574 ip6-access-list (extended numbered) managed-config-flag 782 ipv6 nd minimum-ra-
4576 ip6-access-list (standard named) 4578 interval 783 ipv6 nd other-config-flag 784 ipv6 nd
ip6-access-list (standard numbered) 4579 ip- prefix 785 ipv6 nd ra-interval 787 ipv6 nd ra-
access-list (extended named) 4566 ip-access- lifetime 788 ipv6 nd reachable-time 789 ipv6 nd
list (extended numbered) 4569 ip-access-list retransmission-time 790
(standard named) 4572 ip-access-list ipv6 nd suppress-ra 791 ipv6 neighbor 5047 ipv6
(standard numbered) 4573 ipv6 access-group ospf cost 2414 ipv6 ospf dead-interval 2415 ipv6
888 ipv6 access-list default 883 ipv6 access- ospf demand-circuit 2416 ipv6 ospf display route
list filter 884 ipv6 access-list fragments 887 single-line 2417 ipv6 ospf hello-interval 2418 ipv6
ipv6 access-list icmpv6 889 ipv6 access-list ospf link-lsa-suppression 2419 ipv6 ospf mtu-
remark 893 ipv6 access-list resequence 894 ignore 2420 ipv6 ospf neighbor 2421 ipv6 ospf
ipv6 access-list sctp 895 ipv6 access-list network 2423 ipv6 ospf priority 2424 ipv6 ospf
tcp|udp 898 ipv6 access-list WORD 904 ipv6 restart grace-period 2425 ipv6 ospf restart helper
address 778 ipv6 bfd static all-interfaces 4343 2426 ipv6 ospf retransmit-interval 2428 ipv6 ospf
ipv6 dhcp relay 363 ipv6 dhcp relay address transmit-delay 2429 ipv6 pim 2949 ipv6 pim
364 Ipv6 evpn prefix route 4970 ipv6 accept-register 2942 ipv6 pim anycast-rp 2943
forwarding 779 ipv6 mld 2811 ipv6 mld ipv6 pim bind ecmp-bundle 2944 ipv6 pim bsr-
access-group 2812 ipv6 mld immediate-leave border 2945 ipv6 pim bsr-candidate 2946 ipv6 pim
2813 ipv6 mld last-member-query-count 2814 cisco-register-checksum 2947 ipv6 pim crp-cisco-
ipv6 mld last-member-query-interval 2815 prefix 2948 ipv6 pim dense-group 2951 ipv6 pim
ipv6 mld limit 2816 ipv6 mld mroute-proxy dr-priority 2952 ipv6 pim ecmp-bundle 2953 ipv6
2817 ipv6 mld proxy-service 2818 ipv6 mld pim exclude-genid 2955 ipv6 pim hello-holdtime
querier-timeout 2819 ipv6 mld query-interval 2956 ipv6 pim hello-interval 2957 ipv6 pim ignore-
2820 ipv6 mld query-max-response-time 2821 rp-set-priority 2958 ipv6 pim jp-timer 2959 ipv6
ipv6 mld robustness-variable 2822 ipv6 mld pim neighbor-filter 2960 ipv6 pim passive 2950
ssm-map enable 2823 ipv6 mld ssm-map ipv6 pim propagation-delay 2961 ipv6 pim register-
static 2824 ipv6 mld static-group 2825 ipv6 rate-limit 2962 ipv6 pim register-rp-reachability

2963 ipv6 pim register-source 2964 ipv6 pim register-suppression 2965 ipv6 pim router-id 2966 ipv6 pim rp embedded 2954 ipv6 pim rp-address 2967 ipv6 pim rp-candidate 2969 ipv6 pim rp-register-kat 2970 ipv6 pim spt-threshold 2971 ipv6 pim ssm 2972 ipv6 pim state-refresh origination-interval 2973 ipv6 pim unicast-bsm 2974 ipv6 prefix-list 792 ipv6 rip metric-offset 2651 ipv6 rip split-horizon 2652 Ipv6 route vrf <vrfname> 4973 ipv6 router ospf 2430 ipv6 router rip 2653 ipv6 static bfd 4345 ipv6 static fall-over bfd 4344 ipv6 te-metric 2432 ipv6 unnumbered 794 ipv6 verify unicast source reachable-via 975
ipv6-address 999 ipvpn 3708 isis authentication key-chain 2507 isis authentication mode md5 2508 isis authentication send-only 2509 isis bfd 4337 isis bfd 2510 isis circuit-type 2511 isis csnp-interval 2512 isis hello padding 2515 isis hello-interval 2513 isis hello-multiplier 2514 isis lsp-interval 2516 isis metric 2517 isis network 2518 isis password 2519 isis priority 2520 isis retransmit-interval 2521 isis wait-timer 2523 isis-spb configuration bridge 3709 isis-spb hello-interval 3710 isis-spb hello-multiplier 3711 isis-spb hostname 3712 isis-spb ignore-lsp-errors 3713 isis-spb lsp-gen-interval 3714 isis-spb lsp-interval 3715 isis-spb lsp-refresh-interval 3716 isis-spb max-lsp-lifetime 3717 isis-spb multi-topology-id 3718 isis-spb retransmit-interval 3719 isis-spb set-overload-bit 3720 isis-spb spf-interval-exp 3721 isis-spb system-id 3722 ispf 2522 is-type 2524 key chain 2525 key chain 2614 key chain 4313 key 2526 key 2613 key 4312 key-string 2527 key-string 2615 l3vni 4976 label-switching 927 lacp destination-mac
1302 lacp discard wrong conversation 1303 lacp port-priority 1304 lacp system-priority 1305
lacp timeout 1306 ldap-server deadtime 475 ldap-server host 476 ldap-server port 478 ldap-server timeout 479 leave lsr 4379 license get 634 lifetime 1000 line console 580 line vty 581 link-flap errdisable 795 link-type 3770 lldp debug 3158 lldp debug 3316 lldp ip 3317 lldp run 3159 lldp tlv 3318 lldp tlv-select 3173 lldp tlv-select basic-mgmt 3175 lldp tlv-select ieee-8021-org-specific 3176 lldp tlv-select ieee-8023-org-specific 3177 lldp tlv-select med 3174 lldp-agent 3157 lmm 3256 load 4361 load interval 796 load IPv6 4362 load-balance rtag7 690 load-balance rtag7 hash 693 load-balance rtag7 macro-flow 694 load-balance rtag7 vxlan inner-l2 4974 load-balance rtag7 vxlan inner-l3 4975 Local Proxy ARP Overview 499 local-address 938 locator led 1021 lockout 4488 log syslog 312 log-adjacency-changes 2316 logging cli 582 logging console 313 logging level 314 logging logfile 316 logging monitor 317 logging server 318 logging timestamp 320 login local 611 login virtual-router 4363 logout 583 logout 612 lsp-gen-interval 2528 lsp-gen-interval 3994 lsp-mtu 2529 lsp-refresh-interval 2530 lsp-refresh-interval 3995
lsr name 4375 lsr-move 4377 mac 4977 mac access-group 905 mac access-list default 907 mac access-list filter 908 mac access-list remark 910 mac access-list resequence 911 mac access-list WORD 912 mac vrf 4978 mac-access-list 4580 mac-address 4378 mac-holdtime 4979 map qos-profile 4980 map vnid 4981 match access-group 4582 match access-group 4752 match address 1001 match as-path 709 match community 710 match cos 4583 match cos 4753 match cos inner 4584 match cos inner 4754 match dscp 4755 match ethertype 4585 match extcommunity 711 match interface 712 match ip address 713 match ip address prefix-list 714 match ip next-hop 715 match ip next-hop prefix-list 716 match ip peer 2073 match ip peer 717 match ip rtp 4757 match ip6-dscp 4587 match ip6-precedence 4589 match ip-dscp 4586 match ip-precedence 4588 match ipv6 address 718 match ipv6 address prefix-list 719 match ipv6 next-hop 720 match ipv6 next-hop prefix-list 721 match ipv6 peer 722 match layer4 4590 match layer4-range 4591 match mac 4758 match metric 723 match origin 724 match precedence 4759 match protocol 4760 match qos-group 4761 match route-type 725 match tag 726 match traffic-type 4762 match vlan 4592 match vlan 4763 match vlan inner 4593 match vlan inner 4764 match vlan-range 4594 max-area-address 2531 max-concurrent-dd 2317 max-concurrent-dd 2433 max-ecmp-path 4052 max-fib-routes 2585 maximum-area 2318 maximum-paths 2584 maximum-prefix 2616 max-lsp-lifetime 2532 max-lsp-lifetime 3996 max-nickname 3997 max-paths

2074 max-static-routes 2586 max-traffic-class-group 3498 mcast-pruning 3998 mcc tx 3257 mcec domain configuration 1333 mep attributes 3258 mep crosscheck 3261 mep mpid 3262 mlag 1332 mld snooping 2848 mld snooping fast-leave 2849 mld snooping mrouter 2850 mld snooping querier 2851 mld snooping report-suppression 2852 mls qos aggregate-police 4595 mls qos cos 4596 mls qos cos-cos 4597 mls qos cos-queue 4598 mls qos dscp 4599 mls qos dscp-dscp 4600 mls qos dscp-queue 4601 mls qos enable 4602 mls qos strict-queue 4603 mls qos trust 4604 mls qos wrr-weight 4605 mode 1002 mode 1334 mode 4489 mode 4606 monitor session 1344 monitor session shut 1345 mtu 797 mtu-probe 3999 multicast 798 multipath 4000 mv 630

nd-ageing-timeout 5048 nd-cache disable 4982 nd-reachable-time 5049 neighbor 2319 neighbor 2617 neighbor 2654 neighbor activate 2077 neighbor additional-paths 2075 neighbor advertise additional-paths 2076 neighbor advertisement-interval 2078 neighbor allowas-in 2079 neighbor allow-ebgp-vpn 2170 neighbor as-origination-interval 2081 neighbor as-override 2171 neighbor attribute-unchanged 2082 neighbor capability dynamic 2083 neighbor capability graceful-restart 2084 neighbor capability orf prefix-list 2085 neighbor capability route-refresh 2086 neighbor collide-established 2087 neighbor connection-retry-time 2088 neighbor default-originate 2089 neighbor description 2090 neighbor disallow-infinite-holdtime 2091 neighbor distribute-list 2092 neighbor dont-capability-negotiate 2093 neighbor ebgp-multihop 2094 neighbor enforce-multihop 2095 neighbor fall-over bfd (RIP) 4338 neighbor filter-list 2096 neighbor g-shut 2097 neighbor g-shut-timer 2098 neighbor limit 2099 neighbor local-as 2100 neighbor maximum-prefix 2101 neighbor next-hop-self 2102 neighbor optional-as 2103 neighbor override-capability 2104 neighbor passive 2105 neighbor password 2106 neighbor peer-group 2107 neighbor peer-group range 2108 neighbor port 2109 neighbor prefix-list 2110 neighbor remote-as 2111 neighbor remove-private-AS 2113 neighbor restart-time 2114 neighbor route-map 2115 neighbor route-reflector-client 2116 neighbor route-server-client 2117 neighbor send-community 2118 neighbor send-community 2172 neighbor send-label explicit-null 2119 neighbor shutdown 2120

neighbor soft-reconfiguration inbound 2121 neighbor soo 2173 neighbor strict-capability-match 2122 neighbor timers 2123 neighbor transparent-as 2124 neighbor transparent-nexthop 2125 neighbor unsuppress-map 2126 neighbor update-source 2127 neighbor version 2128 neighbor weight 2129 neighbor WORD peer-group 2130 net 2533 network 2131 network 2320 network 2618 network synchronization 2133 network X:X::X:X 2156 nickname 4001 nickname-priority 4002 no debug all 5050 no nvo vxlan 4983 no shut 1349 ntp authenticate 339 ntp authentication-key 340 ntp enable 341 ntp logging 342 ntp peer 343 ntp server 345 ntp sync-retry 347 ntp trusted-key 348 number-of-dtrees-to-compute 4003 number-of-d-trees-to-use 4004 number-of-mtu-probes 4005 nvo vxlan 4984 nvo vxlan access-if 4985 nvo vxlan id 4986 nvo vxlan irb 4989 nvo vxlan mac-ageing-time 4987 nvo vxlan max-cache-disable 4988 nvo vxlan tunnel qos-map-mode 4990 nvo vxlan vtep-ip-global 4991 oam-protocol 4101 offset-list 2619 offset-list 2655 operational-ip 4206 ospf abr-type 2322 ospf flood-reduction 2323 ospf restart grace-period 2324 ospf restart helper 2325 ospf router-id 2326 out-of-service testing 3263 output-source 4490 overflow database 2327 overflow database external 2328 passive-interface 2329 passive-interface 2434 passive-interface 2620 passive-interface 2656 peer 1003 peer public-key 1004 permit 458 PIM-SM Configuration 2699 ping 613 ping ethernet 3264 ping ethernet mac 3266 poe debug level 549 poe enable/disable 548 police 4607 police 4765 police-aggregate 4609 policy 459 policy-map 4610 policy-map 4767 port breakout enable 799 Port Bundle Configuration 534 port bundle enable 802 port-channel load-balance 1307 port-channel min-bandwidth 1308 port-channel min-links 1309 prc-interval-exp 2534 preempt-mode 4207 prefix-sid value 4162 priority 4768 priority level 4769 priority1 4447 priority2 4448 priority-flow-control accept-peer-config 3524 priority-flow-control advertise-local-config 3525 priority-flow-control cap 3527 priority-flow-control enable 3526 priority-flow-control enable priority 3528 priority-flow-control link-delay-allowance 3529 priority-flow-control mode 3530 private-vlan association 1360 private-vlan community 1361

private-vlan isolated 1362 private-vlan primary 1363 privilege level 617 psk key 1005 ptp global 4449 ptp-clk 4450 ptp-unicast 4451 pwd 631 qcn enable 3516 qos (enable | disable) 4770 qos cos-queue-profile 4992 qos dscp-queue-profile 4993 qos map 4771 qos remark dei 4772 qos statistics 4773 qualification timer 4452 quality-level 4491 queue-limit 4774 quit 584 radius-server dot1x deadtime 1436 radius-server dot1x host 1437 radius-server dot1x key 1439 radius-server dot1x retransmit 1440 radius-server dot1x timeout 1441 radius-server login host 441 radius-server login host acct-port 442 radius-server login host auth-port 443 radius-server login host key 444 radius-server login key 446 radius-server login timeout 447 random-detect 4775 rbridge trill 4006 rbridge trill bridge 4007 rbridge-mping 4110 rbridge-mtraceroute 4111 rbridge-ping 4102 rbridge-ping count 4103 rbridge-ping count ping-interval 4104 rbridge-ping count ping-interval timeout 4105 rbridge-ping-interval 4106 rbridge-ping-timeout 4107 rbridge-traceroute 4108 rbridge-traceroute timeout 4109 rd (route distinguisher) 2174 recv-buffer-size 2621 recv-buffer-size 2657 redistribute 2134 redistribute 2330 redistribute 2435 redistribute 2535 redistribute 2622 redistribute 2658 redistribute isis 2537 reload 585 remote destination 1353 remote ip address 928 remote-link-id 929 renew ip dhcp snooping binding database 1409 reservable-bandwidth 930 restart bgp graceful 2136 restart ipv6 ospf graceful 2437 restart ospf graceful 2332 restore-clock-setting 4453 rmon alarm 962 rmon clear 963 rmon collection history 964 rmon collection stats 965

rmon debug 966 rmon event 967 role 460 root-priority 4008 route 2624 route 2659 route-map 2660 route-map 727 router bgp 2137 router ipv6 ospf 2439 router ipv6 rip 2661 router ipv6 vrrp 4228 router ipv6 vrrp vlan 4229 router isis 2538 router ospf 2333 router ospf vrf 2465 router rip 2625 router vrrp 4208 router-id 2438 router-id 695 route-target 2175 rsa key 1006 segment-routing mpls
4163 send-lifetime 2539 send-lifetime 2626 send-lifetime 4314 server 432 service advanced-vty 586 service ma-name 3267 service ma-name 3453 service ma-type 3268 service password-encryption 587 service terminal-length 588 service unsupported-transceiver 1037 service-policy 4776 service-policy input 4611 service-policy type qos 4777 service-policy type queuing 4778 set aggregator 728 set as-path 729 set atomic-aggregate 730 set bridge cos 4779 set bridge dscp 4780 set comm-list 731 set community 732 set cos 4612 set cos 4782 set dampening 734 set dscp 4783 set ecp 3556 set extcommunity 735 set gmrp disable 1450 set gmrp enable 1451 set gmrp extended-filtering 1452
set gmrp fwdall 1453 set gmrp registration 1454 set gmrp timer 1455 set gvrp applicant 1466 set gvrp disable 1467 set gvrp dynamic-vlan-creation 1468 set gvrp enable 1469 set gvrp registration 1470 set gvrp timer 1471 set interface null0 737 set ip next-hop 738 set ip6-dscp 4614 set ip6-precedence 4616 set ip-dscp 4613 set ip-precedence 4615 set ipv6 next-hop 739 set ipv6 peer 1007 set level 740 set lldp agt-circuit-id 3160 set lldp chassis locally-assigned 3163 set lldp chassis-id-tlv 3162 set lldp chassis-id-tlv 3319 set lldp disable 3164 set lldp disable 3320 set lldp enable 3161 set lldp enable 3321 set lldp locally-assigned 3165 set lldp locally-assigned 3322 set lldp management-address-tlv 3166 set lldp management-address-tlv 3323 set lldp med-devtype 3167 set lldp msg-tx-hold 3168 set lldp msg-tx-hold 3324 set lldp port-id-tlv 3169 set lldp system-description 3178 set lldp system-description 3325 set lldp system-name 3179 set lldp system-name 3326 set lldp timer 3170 set lldp timer 3327 set lldp too-many-neighbors 3172 set lldp too-many-neighbors 3328 set lldp tx-fast-init 3180 set lldp tx-max-credit 3181 set local-preference 741 set metric 742 set metric-type 743 set mirror-to-port 4617 set mmrp disable 1481 set mmrp enable 1482 set mmrp extended-filtering 1483 set mmrp fwdall 1484 set mmrp pointtopoint 1485 set mmrp registration 1486
set mmrp timer 1487 set mpls class 4785 set mvrp applicant 1495 set mvrp disable 1496 set mvrp dynamic-vlan-creation 1497 set mvrp enable 1498 set mvrp pointtopoint 1499 set mvrp registration 1500 set mvrp timer 1501 set origin 744 set originator-id 745 set peer 1008 set poe admin-state 551 set poe high-power 556 set poe max-power 557 set poe mdi-state 552 set poe power-pair 553 set poe priority 555 set poe source 554 set poe total-power 550 set port gmrp 1456 set port gvrp 1472 set port mmrp 1488 set port mvrp

1502 set precedence 4786 set qos queue scheduler 4788 set qos-group 4787 set redirect-to-port 4618 set security-association lifetime 1009 set session-key 1010 set tag 746 set transform-set 1012 set vlan 4619 set vpnv4 next-hop 747 set weight 748 set-overload-bit 2541 sflow collector 4517 sflow poll-interval 4518 sflow sampling enable 4519 sflow sampling-rate 4520 shape 4789 show aaa accounting 436 show aaa authentication 433 show aaa authentication login 434 show aaa groups 435 show access-list log-cache 915 show access-lists 913 show allowed-ethertype 1205 show application-priority bridge 3499 show application-priority interface 3500 show arp 5051 show bfd 4316 show bfd interface 4317 show bfd session 4319
show bfd session A.B.C.D 4323 show bfd session ipv6 4325 show bgp 2179 show bgp A.B.C.D 2180 show bgp A.B.C.D/M 2182 show bgp client 2183 show bgp community 2184 show bgp community-list 2186 show bgp dampening dampened-paths 2187 show bgp dampening flap-statistics 2188 show bgp dampening parameters 2191 show bgp filter-list 2192 show bgp inconsistent-as 2193 show bgp ipv6 2194 show bgp l2vpn evpn 4994 show bgp l2vpn evpn prefix-route 5024 show bgp l2vpn evpn summary 4998 show bgp l2vpn vpls 2197 show bgp neighbors 2200 show bgp neighbors advertised-routes 2204 show bgp neighbors received prefix-filter
2205 show bgp neighbors received-routes 2206 show bgp neighbors routes 2207 show bgp nexthop-tracking 2209 show bgp nexthop-tree-details 2211 show bgp paths 2212 show bgp prefix-list 2213 show bgp quote-regexp 2214 show bgp regexp 2215 show bgp route-map 2216 show bgp statistics 2217 show bgp summary 2218 show bgp view 2221 show bgp X:X::X:X 2223 show bgp X:X::X:X/M longer prefixes 2224 show bootup-parameters 403 show bridge 1206 show bridge eps-id 3348 show bridge g8031 3349 show bridge g8032 3359 show bridge spb 3728 show bridge trill 4053 show class-map 4790 show class-map name 4620 show cli 651 show cli history 590 show clns is-neighbors 2546 show clns neighbors 2548 show clock 589 show control-adjacency 946 show control-channel 939 show controller details 1038 show cores 404 show crypto ipsec transform-set 1013
show crypto isakmp policy 1014 show crypto-map interface 1015 show cspf ipv6 lsp 2473 show cspf lsp 2474 show cvlan registration table 3194 show data-center-bridging 3501 show debug ldap 480 show debug radius 448 show debug ssh-server 259 show debug tacacs+ 461 show debug telnet-server 300 show debug trill 4054 show debugging bfd 4327 show debugging bgp 2225 show debugging cspf 2475 show debugging dot1x 1442 show debugging elmi 3454 show debugging gmrp 1457 show debugging gvrp 1473 show debugging ip arp 5053 show debugging ip dhcp snooping 1410 show debugging ip igmp 2799 show debugging ip mrib 2765 show debugging ip pim 2909 show debugging ipv6 cspf 2476 show debugging ipv6 mld 2827 show debugging ipv6 nd 5054 show debugging ipv6 ospf 2440 show debugging ipv6 pim 2975 show debugging ipv6 rip 2662 show debugging isis 2550 show debugging lacp 1310 show debugging lldp 3182 show debugging mld 2853 show debugging mstp 1255 show debugging nsm 652 show debugging ospf 2334 show debugging pim 2910 show debugging ptp 4454 show debugging rib 2587 show debugging rip 2628 show debugging vrrp 4209 show dot1x 1443 show dot1X 653 show dtag vlan 1364 show enhanced-transmission-selection bridge 3503 show enhanced-transmission-selection interface 3505 show errdisable details 696 show esmc counters 4500 show etherchannel 1311 show ethernet cfm active-levels 3269 show ethernet cfm ais 3270 show ethernet cfm dual-ended lmm 3271 show ethernet cfm errors 3272 show ethernet cfm ma status 3273 show ethernet cfm maintenance-points local 3274 show ethernet cfm maintenance-points

remote 3275 show ethernet cfm mep 3276 show ethernet cfm traceroute-cache 3277 show ethernet lmi evc 3455 show ethernet lmi evc detail EVC ID 3457 show ethernet lmi evc detail evc-ref-id 3456 show ethernet lmi evc interface 3458 show ethernet lmi evc map 3459 show ethernet lmi parameters 3460 show ethernet lmi statistics 3461 show ethernet lmi uni 3462 show ethernet oam 3308 show ethernet oam discovery 3310 show ethernet oam eventlog 3311 show ethernet oam statistics 3312 show ethernet oam status 3313 show evb ecp statistics

3557 show evb interface 3558 show evb vdp vsi-info 3559 show evb-bridge 3560 show evpn multi-homing all 5016 show evpn multihoming-status 5017 show filter 1357 show flowcontrol 1182 show forwarding profile limit 697 show gmrp configuration 1458 show gmrp machine 1459 show gmrp statistics 1460 show gmrp timer 1461 show gvrp configuration 1474 show gvrp machine 1475 show gvrp statistics 1476 show gvrp timer 1477 show hardware-information 1022 show hardware-profile filters 699 show hosts 252 show hosts 840 show igmp snooping groups 2842 show igmp snooping interface 2840 show igmp snooping mrouter 2845 show igmp snooping statistics 2846 show interface 804 show interface capabilities 1183 show interface counters (indiscard-stats|outdiscard-stats) 812 show interface counters 806 show interface counters drop-stats 808 show interface counters error-stats 811 show interface counters protocol 815 show interface counters queue-drop-stats 816 show interface counters queue-stats 817 show interface counters rate 819 show interface counters summary 821 show interface errdisable status 700 show interface fec 656 show interface irb 5023 show interface switchport 1207 show interface transceiver details 1040 show ip access-lists 916 show ip bgp 2226 show ip bgp attribute-info 2229 show ip bgp cidr-only 2230 show ip bgp community-info 2231 show ip bgp peer-group 2232 show ip bgp peer-group vrf all 2233 show ip bgp rtfilter all 2234 show ip bgp scan 2235 show ip bgp vpnv4 2236 show ip dhcp arp-inspection statistics 1414 show ip dhcp relay 365 show ip dhcp relay address 366 show ip dhcp snooping 1411 show ip dhcp snooping binding 1412 show ip extcommunity-list 2240 show ip forwarding 823 show ip igmp groups 2800 show ip igmp interface 2802 show ip igmp proxy 2804 show ip igmp ssm-map 2806 show ip interface 824 show ip isis igp-shortcut-lsp 2551 show ip isis route 2552 show ip isis route igp-shortcut 2554 show ip mroute 2766 show ip msdp peer 2911 show ip msdp sa-cache 2912 show ip mvif 2769 show ip ospf 2335 show ip ospf border-routers 2339 show ip ospf database brief 2340 show ip ospf database detail 2342 show ip ospf igp-shortcut-lsp 2349 show ip ospf igp-shortcut-route 2350 show ip ospf interface 2351 show ip ospf multi-area-adjacencies 2354 show ip ospf neighbor 2356 show ip ospf route 2360 show ip ospf segment-routing announce-list 4164 show ip ospf segment-routing capability 4165 show ip ospf segment-routing prefix-sid 4167 show ip ospf te-database 2477 show ip ospf virtual-links 2363 show ip ospf valid 2362 show ip pim bsr-router 2922 show ip pim interface 2914 show ip pim local-members 2924 show ip pim mroute 2916 show ip pim neighbor 2918 show ip pim nexthop 2921 show ip pim rp mapping 2926 show ip pim rp-hash 2925 show ip prefix-list 826 show ip protocols 2241 show ip protocols 2365 show ip protocols 2556 show ip protocols rip 2629 show ip rip 2631 show ip rip interface 2633 show ip rip interface vrf 2670 show ip rip statistics 2635 show ip rip vrf 2672 show ip route 827 show ip route fast-reroute 2367 show ip route virtual-router 4364 show ip rpf 657 show ip vrf 2243 show ip vrf 2674 show ip vrf 833 show ipsec status 1016 show ipv6 access-lists 917 show ipv6 dhcp relay 367 show ipv6 dhcp relay address 368 show ipv6 dhcp relay address interface 369 show ipv6 forwarding 834 show ipv6 interface brief 835 show ipv6 mld groups 2828 show ipv6 mld interface 2830 show ipv6 mld ssm-map 2832 show ipv6 neighbors 5055 show ipv6 ospf 2441 show ipv6 ospf database 2442 show ipv6 ospf interface 2446 show ipv6 ospf neighbor 2448 show ipv6 ospf route 2451 show ipv6 ospf te-database 2479 show ipv6 ospf virtual-links 2456 show ipv6 ospfv3 topology 2454 show ipv6 pim bsr-router 2984 show ipv6 pim interface 2976

show ipv6 pim local-members 2986 show ipv6 pim mroute 2978 show ipv6 pim neighbor 2981 show ipv6 pim nexthop 2983 show ipv6 pim rp mapping 2988 show ipv6 pim rp-hash 2987 show ipv6 prefix-list 839 show ipv6 protocols rip 2663 show ipv6 rip 2664 show ipv6 rip interface 2665 show ipv6 route 837 show ipv6 route fast-reroute 2453 show ipv6 rpf 658 show ipv6 vrf 2458 show isis counter 2557 show isis database 2558 show isis interface 2561 show isis tag database 2564 show isis topology 2566 show isis-spb configuration 3729 show isis-spb fdb 3730 show isis-spb interface 3731 show isis-spb lsp 3732 show isis-spb neighbors 3733 show isis-spb topology 3734 show lacp sys-id 1314 show lacp-counter 1315 show ldap-server 481 show license 635 show list 660 show lldp 3329 show lldp interface 3186 show lldp neighbors 3183 show logging 321 show logging cli 591 show logging last 323 show logging logfile 324 show logging logfile last-index 325 show logging logfile start-seqn end-seqn 326 show logging logfile start-time end-time 327
show lsr 4381 show lsr membership 4383 show lsr process-list 4382 show mac access-lists 918 show mac address-table bridge 1210 show mac address-table count bridge 1209 show mcec statistics 1340 show mlag detail 1335 show mlag summary 1337 show mld snooping mrouter 2854 show mld snooping statistics 2855 show mls qos 4621 show mls qos aggregate-policer 4622 show mls qos cosq-stat 4623 show mls qos interface 4624 show mmrp configuration 1489 show mmrp machine 1490 show mmrp statistics 1491 show mmrp timer 1492 show monitor 1354 show monitor running configuration 1358 show monitor session 1355 show mvrp configuration 1503 show mvrp machine 1504 show mvrp statistics 1505
show mvrp timer 1506 show nsm client 661 show nsm trill adjacency 4055 show nsm trill appointed-forwarder 4056 show nsm trill detail 4057 show nsm trill l2-table 4058 show nsm trill mfdb 4059 show nsm trill multicast-pruning 4060 show nsm trill portinfo 4061 show nsm trill rpf 4062 show nsm trill ufdb 4063 show nsm trill vlan-pruning 4064 show nsm virtual-router 4365 show ntp authentication-keys 349 show ntp authentication-status 350 show ntp logging-status 351 show ntp peers 353 show ntp peer-status 352 show ntp statistics 354 show ntp trusted-keys 356 show nvo vxlan 5000 show nvo vxlan access-if-config 5002 show nvo vxlan arp-cache 5003 show nvo vxlan counters access-port 5004 show nvo vxlan counters network-port 5005 show nvo vxlan interface counters 5006 show nvo vxlan irb-status 5021 show nvo vxlan mac-table 5008 show nvo vxlan nd-cache 5010 show nvo vxlan route-count 5018 show nvo vxlan static host state 5011 show nvo vxlan tunnel 5013 show nvo vxlan vni-name 5020 show poe port 562 show poe power-configuration 559 show poe power-management 560 show poe power-status 561 show poe pse 558 show policy 462 show policy-map interface 4792 show policy-map name 4625 show policy-map 4791 show port etherchannel 1316 show priority-flow-control details 3531 show priority-flow-control statistics 3533 show privilege 618 show process 593 show process 662 show ptp data 4455 show ptp forign-master 4456 show ptp port 4457 show ptp time-properties 4458 show ptp unicast-neighbors 4459 show qcn cnpv 3519
show qcn configuration 3517 show qcn cp 3521 show qos-access-list 4626 show queuing interface 4795 show radius-server 449 show rbac-role 463 show rmon alarm 968 show rmon event 969 show rmon history 970 show rmon statistics 971 show route-map 749 show router-id 701 show running-config 594 show running-config aaa 437 show running-config access-list 595 show running-config access-list 920 show running-config aclmgr 919 show running-config as-path access-list 596 show running-config community-list 597 show running-config control-adjacency 947 show running-config control-channel 940 show running-config dhcp 370 show running-config dns 253 show running-config interface 841 show running-config interface igmp 598 show running-config interface ip 843 show running-config interface ipv6 844 show running-config interface irb 5022 show running-config interface isis 2568 show running-config interface multicast 599 show running-config ip 845 show running-config ipv6 846 show running-config ipv6 access-list 921 show running-config ldap 482 show running-config logging 328 show running-config ntp 357 show running-config nvo vxlan 5014 show running-config prefix-list 600 show

running-config qos 4796 show running-config radius 450 show running-config rbridge 4009 show running-config route-map 750 show running-config router 663 show running-config router ipv6 vrrp 4230 show running-config router isis 2569 show running-config router vrrp 4210 show running-config router-id 702 show running-config snmp 279 show running-config ssh server 260 show running-config switch 664 show running-config switch udld 3753 show running-config tacacs+ 464 show running-config te-link 931 show running-config telnet server 301
show running-config urpf 666 show running-config virtual-router 4366 show running-config vrf 601 show sflow 4521 show sflow interface 4523 show sflow statistics 4524 show snmp 280 show snmp community 281 show snmp engine-id 282 show snmp group 283 show snmp host 284 show snmp user 285 show snmp view 286 show software-watchdog status 405 show spanning-tree 1256 show spanning-tree mst 1260 show spanning-tree rpvst+ 1287 show spanning-tree statistics 1262 show spb adjacency 3735 show spb bridge vlan 3736 show spb service bridge 3737 show spbv bridge vid-translation-table 3738 show ssh key 261 show ssh server 262 show startup-config 667 show static-channel load-balance 1320 show static-channel-group 1319 show supported-transceiver 1039 show synce details 4501 show synce input-sources 4502 show synce output-sources 4503 show system log 408 show system login 410 show system reboot-history 411 show system resources 412 show system uptime 414 show system-information 1026 show sys-update details 636 show tacacs-server 465 show tcp 602 show techsupport 415 show te-link 932 show telnet-server 302 show tfo 3771 show trill detail 4065 show trill dtree 4068 show trill esadi-instance 4022 show trill esadi-lsp 4023 show trill esadi-native-l2-table 4025 show trill esadi-remote-l2-table 4026 show trill esadi-statistics 4027 show trill fdb 4070 show trill interface 4072 show trill l2mcast 4075 show trill neighbor 4076 show trill nicknamedatabase 4078 show trill pruning 4079 show trill rpfinfo 4080 show trill statistics 4081 show trill topology 4082 show trill vlantable 4083 show udld 3751 show udld interface 3752 show user-account 332 show username 263 show users 604 show version 668 show virtual-router ip 4368 show vlan 1366 show vlan access-map 1365 show vlan brief 1368 show vlan classifier 1369 show vlog all 624 show vlog clients 625 show vlog terminals 626 show vlog virtual-routers 4369 show vlog virtual-routers 627 show VR and VRF 4367 show vrrp <1-255> 4213 show vrrp 4211 show vrrp statistics 4214 shut 1350 shutdown 2368 shutdown 5025 shutdown 847 shutdown 933 shutdown 941 slave-only 4460 snmp restart 703 snmp restart auth 1446 snmp restart bfd 4328 snmp restart bgp 2138 snmp restart cfm 3278 snmp restart cfm_v1 3426 snmp restart efm 3314 snmp restart isis 2542 snmp restart lacp 1321 snmp restart lldp 3188 snmp restart lldp 3330 snmp restart mribd 2771 snmp restart mstp 1185 snmp restart ospf 2369 snmp restart ospf6 2459 snmp restart pim 2927 snmp restart rib 2588 snmp restart rip 2637 snmp restart rmon 972 snmp restart trill 4085
snmp restart vrrp 4215 snmp-server community 287 snmp-server contact 288 snmp-server enable snmp 289 snmp-server enable traps 290 snmp-server host 291 snmp-server location 293 snmp-server tcp-session 294 snmp-server user 295 snmp-server view 296 software-watchdog 416 software-watchdog keep-alive-time 418 source port 1346 source vlan 1347 spanning-tree autoedge 1265 spanning-tree bpdu-filter 1272 spanning-tree bpdu-guard 1273 spanning-tree edgeport 1266 spanning-tree guard 1267 spanning-tree instance restricted-role 1268 spanning-tree instance restricted-tcn 1269 spanning-tree link-type 1270 spanning-tree mst configuration 1271 spanning-tree restricted-domain-role 1274 spanning-tree restricted-role 1275 spanning-tree restricted-tcn 1276 spanning-tree rpvst+ configuration 1291 spanning-tree te-msti configuration 1277 spanning-tree vlan restricted-role 1292 spanning-tree vlan restricted-tcn 1293 spb configuration 3723 spb enable 3724 speed 848 spf-interval-exp 2543 spf-interval-exp 4010 ssh 264 ssh algorithm encryption 267 ssh key 269 ssh login-attempts 270 ssh server port 271 ssh6 265 static-channel-group 1322 storm-control 1278 storm-control 4799 strict-queue 4627 summary-address 2370 summary-address 2460 summary-address 2544 switch lsr 4380 switch-back-delay 4216 switchover type 1341 switchport 1212 switchport 850 switchport access 1371

switchport allowed ethertype 1213 switchport allowed ethertype 851 switchport beb customer-backbone 3725 switchport customer-edge 3195 switchport customer-edge default-svlan 3196 switchport customer-edge hybrid 3197 switchport customer-edge trunk 3198 switchport customer-edge vlan registration 3199 switchport customer-edge vlan translation 3200 switchport customer-network vlan 3201 switchport customer-network vlan translation 3202 switchport ethertype 3204 switchport hybrid 1372 switchport mode 1374 switchport mode 3205 switchport mode access ingress-filter 1375 switchport mode customer-edge 3207 switchport mode customer-edge hybrid acceptableframe-type 3208 switchport mode hybrid acceptable-frame-type 1376 switchport mode hybrid ingress-filter 1377 switchport mode ingress-filter 3206 switchport mode private-vlan 1383 switchport mode sbp 3561 switchport mode trunk ingress-filter 1378 switchport mode uap 3562 switchport private-vlan host-association 1384 switchport private-vlan mapping 1385 switchport provider-edge 3209 switchport provider-network vlan translation 3210 switchport trunk allowed

1379 switchport trunk allowed vlan dtag 1381 switchport trunk native 1382 switch-source 4493 sync interval 4461 synce (configure mode) 4494 synce (interface mode) 4495 synce debug 4496 synchronization 2139 synchronization option 4497 syntonization 4462 Syslog Severities 308 systemid 4011 sys-update commit 637 sys-update install 638 sys-update list-version 639 sys-update rollback 640 tacacs-server login host 467 tacacs-server login key 469 tail-drop threshold 4628 tcp 3507 te-link 934 te-link 948 telnet 303
telnet 619 telnet server port 305 telnet6 304 terminal length 606 terminal monitor 607 tfo 3772 throughput-measurement reception 3279 throughput-measurement unicast 3280 timers basic 2638 timers basic 2666 timers bgp 2140 timers lsa arrival 2371 timers spf exp 2372 timers throttle lsa 2373 traceroute
620 traceroute ethernet 3281 traffic-class-group 3508 traffic-shape rate 4629 trill access-port 4086 trill announcing-vlan 4087 trill bpdu-handling 4088 trill designated-vlan

4089 trill disable-port 4090 trill end-station-service-vlan 4091 trill instance 4092 trill link-type 4093 trill max-neighbor 4094 trill overload-flag 4095 trill pseudonode 4096 trill root-inhibition-time 4097 trill trunk-port 4098 trill-isis csnp-interval 4030 trill-isis hello-interval 4031 trill-isis hello-interval minimal 4032 trill-isis hello-multiplier 4033 trill-isis lsp-interval 4034 trill-isis metric 4035 trill-isis port-priority 4036 trill-isis retransmit-interval 4037 trust dscp 4801 tst 3282 tunnel checksum 951 tunnel destination 952 tunnel dmac 953 tunnel mode 954 tunnel mode ipv6ip 955 tunnel path-mtu-discovery 956 tunnel source 957 tunnel tos 958 tunnel ttl 959 TYPE-5 EVPN 4872 udld 3748 udld message-time 3749 udld
mode 3750
udp 3509 undebug all ip pim 2928 undebug all ipv6 pim 2989 undebug bgp 2141 undebug vrrp 4217 unicast-neighbor 4463 username 333 username 4370 username keypair 273 username sshkey 272 version 2639 virtual-ip 4218 virtual-ipv6 4231 virtual-router 4371 virtual-router forwarding 4372 vlan classifier activate 1386 vlan classifier group 1387 vlan classifier rule ipv4 1388 vlan classifier rule mac 1389 vlan classifier rule proto 1390 vlan database 1392 vlan dtag 1393 vlan state 1394 vlan type 3213 vlan type customer 3211 vlan type service 3212 vlan VLAN_RANGE bridge 1395 vlan-pruning 4012 vrrp compatible-v2 4219 vrrp vmac 4220 vsm tx 3283

vxlan host-reachability-protocol evpn-bgp 5026 vxlan static-entry host-mac 5027 wait-to-restore 4498 watch static-mac-movement 704 write 608 write terminal 621 wrr-queue queue-id 4630 wrr-queue random-detect 4631 wrr-queue weight 4802

SECTION 18 Index

Index

Numerics

6to4 automatic tunnel 1870
6to4 relay 1872
802.1x Commands
auth-mac auth-fail-action 1416 auth-mac dynamic-vlan-creation disable 1418 auth-mac enable 1419 auth-mac system-auth-ctrl 1421 debug dot1x 1422 dot1x initialize interface 1423 dot1x port-control 1425 dot1x protocol-version 1426 dot1x quiet-period 1427 dot1x reauthentication 1429 dot1x reauthMax 1428 dot1x system-auth-ctrl 1430 dot1x timeout re-authperiod 1431 dot1x timeout server-timeout 1432 dot1x timeout supp-timeout 1433 dot1x timeout tx-period 1434 ip radius source-interface 1435 radius-server deadtime 1436 radius-server host 1437 radius-server key 1439 radius-server retransmit 1440 radius-server timeout 1441 show debugging dot1x 1442 show dot1x 1443

A

aaa accounting default 422 aaa accounting details 423 aaa authentication attempts login 422 aaa authentication login 422 aaa authentication login console 424 aaa authentication login default 425 aaa authentication login default fallback error 427 aaa authorization config-commands default 428 aaa group server 428 aaa local authentication attempts max-fail 429 ABRs 2382
accept-lifetime 2485, 2593
Access Lists 209
ACTIVE_SEND_LOCAL 3064
adding IP addresses to VLAN interface 1860, 1898
adding multiple instances of same AS to administer route
selection 1579
address 979
Address Resolution Protocol 5033 address-family ipv4 unicast 2378 address-family ipv4 vrf command 2668 adjacency checks 3981
advantages
offload IP traffic from backbone routers 513
reduced system cost 513 simplified maintenance 513 simplified network design 513
advantages of hybrid switch 513 advertisement interval, VRRP Commands
advertisement-interval 4222
Aggregate Policing 4543
aggregate-address 2642
aggregate-address command 2144
aggregate-nexthop-check 2000 ais status 3221 area
authentication 2252
area authentication 2252
Area Border Router
configuring 1672
Area Border Router in OSPFv3 1718
Area Border Routers 2382 area default cost 2253 area default-cost 2379
area filter-list 2254 area nssa 2255, 2380 area range 2257, 2382 area stub 2258, 2384 area virtual-link 2259, 2385 area-password 2488 area-password command 2488 arp A.B.C.D MAC 573 arp-cache disable 4948 arp-nd flood-suppress 4949 Authentication 210
authentication 980, 1107, 4279
authentication BGP 1543
authentication commands
accept-lifetime 2593 ip rip authentication key-chain 2605 ip rip authentication mode md5 2606 ip rip authentication string 2607 key chain 2614 send-lifetime 2626
authentication key-chain 2489
authentication mode md5 2490
authentication OSPF 1685
authentication rip multiple keys 1930
authentication rip-multiple keys 1937
authentication send-only 2491
Authentication, Authorization and Accounting Command Reference 419 auth-mac auth-fail-action 1416 auth-mac dynamic-vlan-creation disable 1418

auth-mac enable 1419 auth-mac system-auth-ctrl 1421 auth-mac-aging 1166 auth-mac-fail-action 1165 auto-cost reference bandwidth 2261 auto-cost reference-bandwidth 2387 auto-summary 1997

B

backward compatibility 4186
Bandwidth Configuration 4675
banner 567 basic configuration 2720
Basic VR configuration 1885 basic VR configuration 1886 begin modifier 90 bfd 4301 bfd all-interfaces 2262 bfd auth type 4300
BFD Configuration 4237
Echo Function 4237
Echo Interval 4244
Multi-hop Peer Timer 4240
Single-hop Session Timer 4242
Slow Timer 4239
Topology 4237, 4279 bfd echo 4302 bfd echo interval 4303 BFD for LDP LSP 4269
BFD for MPLS LSPs 4269
BFD for RSVP LSP 4271
BFD for Static LSP 4274 BFD for Static LSP with Explicit Null 4276 bfd interval 4305 bfd multihop-peer 4306 bfd multihop-peer A.B.C.D interval 4307
bfd multihop-peer X
X
X
X
X interval 4308 bfd notification 4309
BFD protocol commands 4329 debug ospf bfd 4334
IS-IS isis bfd 4337 BFD Protocol Configurations 4247 bfd slow-timer 4310
BFD Static Configurations 4265
Topology 4265 bfd-firmware 4304
BGP 1949
BGP Commands
address-family 1993 aggregate-address 1995 auto-summary 1997 bgp aggregate-nexthop-check 2000 bgp always-compare-med 2001

bgp bestpath as-path ignore 2003 bgp bestpath compare-confed-aspath 2005 bgp bestpath compare-routerid 2006 bgp bestpath med 2008 bgp client-to-client reflection 2011 bgp cluster-id 2012 bgp confederation identifier 2013 bgp confederation peer 2014 bgp config-type 2015 bgp dampening 2016 bgp default ipv4-unicast 2018 bgp default local-preference 2019 bgp deterministic med 2020 bgp enforce-first-as 2021 bgp extended-asn-cap 2022 bgp fast-external-failover 2023 bgp g-shut 2026 bgp g-shut-capable 2027 bgp g-shut-local-preference 2028 bgp log-neighbor-changes 2029 bgp multiple-instance 2031 bgp nexthop delay 2032 bgp nexthop enable 2033 bgp rfc1771-path-select 2034 bgp rfc1771-strict 2035 bgp router-id 2036 bgp scan-time 2037 bgp update-delay 2040 clear bgp * 2042 clear bgp A.B.C.D| X:X::X:X 2041, 2147 clear bgp external 2047 clear bgp peer-group 2050, 2150 clear ip bgp A.B.C.D

clear ip bgp A.B.C.D 2055 clear ip bgp ASN 2044, 2046 clear ip bgp dampening 2046 clear ip bgp flap-statistics 2049 clear ip bgp view 2053 debug bgp 2059 distance 2061 exit address family mode 2062 ip as-path access-list 2063 ip community-list 2064, 2068 ip community-list expanded 2066 ip community-list standard 2067

ip extcommunity-list
expanded 2071
extended 2070 standard 2069, 2072
neighbor
activate 2077 advertisement-interval 2078 capability dynamic 2083 capability graceful-restart 2084 capability orf prefix-list 2085 capability route-refresh 2086 collide-established 2087 default-originate 2089 distribute-list 2092 dont-capability-negotiate 2093 ebgp-multihop 2094 enforce-multihop 2095 fall-over bfd 2096 filter-list 2096 maximum-prefix 2101 next-hop-self 2102 peer-group add 2107 port 2108 remote-as 2111 remove private-as 2113 restart-time 2114 route-map 2115 route-reflector-client 2116 send-community 2118 shutdown 2120 soft-reconfiguration 2121 strict-

capability-match 2122
timers 2123 transparent-as
2124 transparent-nexthop
2125 unsuppress-map 2126
update-source 2127 version
2128 weight 2129
neighbor attribute-unchanged 2082
neighbor connection-retry-time 2088
neighbor disallow-infinite-holdtime 2091
neighbor g-shut 2097 neighbor g-shut-timer 2098 neighbor passive 2105
neighbor prefix-list 2110 network 2131
network and network backdoor 2156
redistribute 2134 restart bgp graceful 2136
router bgp 2137
show
ip bgp attribute-info 2229 ip bgp cidr-only 2230 ip bgp community 2184 ip bgp community-info 2231 ip bgp community-list 2186 ip bgp filter-list 2192 ip bgp view 2221 ip protocols bgp 2241
show bgp neighbors received prefix-filter 2205
show bgp neighbors received-routes 2206
show bgp neighbors routes 2207 show bgp paths 2212 show bgp prefix-list 2213 show bgp quote-regexp 2214 show bgp route-map 2216 show bgp summary 2218 show ip bgp inconsistent-as 2193
show ip extcommunity-list 2240 synchronization 2139 timers 2140
BGP community value
command syntax 88
BGP configuration 1513 adding multiple instances of same AS to administer
route selection 1579
configuring BGP Confederation 1531 configuring BGP distance 1611 configuring BGP Extended Community attributes 1585 configuring BGP Four-Byte AS 1582 configuring BGP weight per peer basis 1614 configuring Next-hop Tracking 1598 configuring Next-hop Tracking delay timer 1600 enabling BGP 1513
enabling BGP- different autonomous systems 1514 enabling EBGP Multihop 1545 enabling peer groups 1574 removing Multi-Exit Disc attribute from update messages 1581 route
reflector 1518
route-map 1516
bgp dampening 2016
bgp g-shut 2026 bgp g-shut-capable 2027 bgp g-shut-local-preference 2028 bgp inbound-route-filter 2160
BGP VPN Commands
bgp inbound-route-filter 2160
clear ip bgp * vpnv4 2162 clear ip bgp <1-4294967295> vpnv4 2164 clear ip bgp A.B.C.D vpnv4 2166 debug bgp mpls 2167 import map 2168 ip vrf 2169 neighbor send-community 2172
neighbor allow-egbp-vpn 2170 neighbor as-override 2171
neighbor send-community 2172
neighbor soo 2173 rd (route distinguisher) 2174 route-target 2175
show ip vrf 2243 site-of-origin 2173
BGP4+ Commands
aggregate-address 2144
network and network backdoor 2156
BGP4+ configuration 1647 confederations 1655 enable eBGP peering 1649 enable iBGP peering 1647 enable iBGP peering-link-local address 1648 graceful restart 1657 route reflector 1653 route-map 1651
Bidirectional Forwarding Commands 4299 bind the interface 4092
binding an interface to the VR 1886, 2720 Bootstrap Router 2696
bootstrap router 2922, 2984 Border Gateway BC Protocol (BGP) 1949
Border Gateway Protocol 117
boundary clock 4397
Ethernet 4397
UDP 4402
braces
command syntax 88
bridge acquire 1188 bridge address 1189 bridge ageing-time 1190 bridge agreement convention 3692

bridge cisco-interoperability 1217
Bridge commands bridge acquire 1188 bridge address 1189 bridge ageing-time 1190 bridge protocol mstp 1224 bridge protocol rstp 1225 clear mac address-table 1203 show interface switchport bridge 1207 switchport 1212
bridge forward-time 1191 bridge instance priority 1219 bridge loop-mitigation 3694 bridge max-age 1194 bridge max-hops 1195 bridge multiple-spanning-tree enable 1222 bridge priority 1196 bridge protocol 3544 bridge protocol mstp 1224 bridge protocol provider-rstp 3191 bridge protocol rpvst+ 1285 bridge protocol rstp 1225 bridge rapid-spanning-tree enable 1226 bridge region 1227 bridge revision 1228 bridge shutdown 1197 bridge spanning-tree enable 1229 bridge spanning-tree errdisable-timeout enable 1230 bridge spanning-tree portfast bpdu-filter 1233 bridge spb enable 3697 bridge spsourceid 3703 bridge te-msti 1235 bridge transmit-holdcount 1198 bridge-group instance 1236 bridge-group instance path-cost 1237 bridge-group path-cost 1200 bridge-group priority 1201 bridge-group spb path-cost 3704 bridge-group vlan 1284 Broadcast Storm Suppression 110
BSR 2696, 2922, 2984
BSR validation 2706
Bundling in UNI 1139

C

candidate status 2903, 2969 capability opaque 2265
capability restart 2266
capability restart graceful 2389
capabilit y te 2468 C-API 104
cc interval 3223 cc multicast 3224 cc unicast 3225
CFM configuration 3047
CFM commands ais interval 3220 ais status 3221 cc interval 3223 cc multicast 3224 cc unicast 3225 clear ethernet cfm errors 3228 clear ethernet cfm maintenance-points remote 3229 clear ethernet cfm traceroute-cache 3230 ethernet cfm ais interval 3365 ethernet cfm ais status 3366, 3405 ethernet cfm cc multicast state 3367 ethernet cfm cc unicast state 3368 ethernet cfm enable 3245 ethernet cfm exm|vsm 3425 ethernet cfm in-service|out-of-service 3382 ethernet cfm lmm frame count simulator 3247 ethernet cfm lmm unicast|multicast 3379 ethernet cfm mcc tx 3380 ethernet cfm server-ais status 3249 ethernet cfm throughput-measurement 3422 ethernet cfm throughput-measurement reception 3421 ethernet cfm traceroute cache 3250 ethernet cfm tst mep 3423 exit-interface-eth-cfm-mep 3253 exm tx 3254 in-service testing 3255 mcc tx 3257 mep crosscheck mpid 3261 mep mpid 3262 out-of-service testing 3263 show ethernet cfm ma status 3273 tst 3282 vsm tx 3283
CFM over PBB 3055
Chassis Management Module Commands 1019 Chassis Monitoring Module Command Reference 1017 circuit-failover 4202, 4223 cisco-metric-behavior 2595, 2643 class 4563 class map 4637 criteria 4637
class type qos 4749 class type queuing 4750
classification 4636 classify traffic per-port-per-VLAN basis 4530 using ACLs 4529
class-map 4564 clear bgp * 2042 A.B.C.D|X:X::X:X 2041, 2147 external 2047 peer-group 2050, 2150
clear bgp ipv6 A.B.C.D| X:X::X:X 2041, 2147 external 2047 peer-group 2050, 2150
clear clns is-neighbors 2494 clear clns neighbors 2493 clear commands

clear rbridge trill counter 3986 clear rbridge trill interface counter 3987
clear crypto isakmp 981 clear crypto sa 982 clear crypto sa entry 983 clear crypto sa map 984 clear crypto sa peer 985 clear data from RIPng routing table 2644 clear ethernet lmi statistics bridge 3444
clear gmrp statistics 1448 clear gvrp statistics 1464
clear ip bgp ASN 2044, 2046 view 2053
clear ip bgp * vpnv4 2162 clear ip bgp <1-4294967295> vpnv4 2164 clear ip bgp A.B.C.D vpnv4 2166 clear ip igmp 2774 clear ip mroute 2760, 2861, 2931 clear ip msdp peer 2863 clear ip msdp sa-cache 2864 clear ip ospf process 2269 clear ip pim sparse-mode bsr 2865 clear ip pim sparse-mode bsrt 2933 clear ip prefix-list 757 clear ip rip route 2596 clear ip route kernel 2574 clear ipv6 mld 2808 clear ipv6 neighbors 758 clear ipv6 ospf process 2390 clear ipv6 rip route 2644 clear isis interface counter 2498 clear isis process 2499 clear isis route 2495 clear ldap-server statistics 472 clear mac address table dynamic vxlan 4950 clear mac address-table 1203 clear mmrp statistics 1480 clear ntp statistics 336 clear nvo vxlan counters 4952 clear snmp hostconfig 277 clear spanning-tree detected protocols 1242 clear ssh hosts 256

clear switch-source 4484 clear tfo counter 3766 Client 209 clock timezone 674 clock-selection mode 4485 collide-established 2087 command abbreviations 86 command completion 86 command line errors 86 help 85 keyboard operations 89
command modes 92
configure 93 exec 92 interface 93 privileged exec 92 router 93
command negation 87 command syntax
? 88
. 88
() 87 {} 88
| 87
A.B.C.D/M 88 AA:NN 88 BGP community value 88 braces 88 conventions 87 curly brackets 88 HH:MM:SS 88 IFNAME 88 interface name 88 IPv4 address 88 IPv6 address 88 LINE 88 lowercase 87 MAC address 89 monospaced font 87 numeric range 89 parantheses 87 parentheses 87 period 88 question mark 88 square brackets 88 time 88 uppercase 87 variable placeholders 88 vertical bars 87 WORD 88 X:X::X:X 88 X:X::X:X/M 88 XX:XX:XX:XX:XX:XX 89 common commands 643, 671, 705
banner 567 clear ip prefix-list 757 configure terminal 568 copy running-config startup-config 646 description 937 disable 571, 651 enable 572 enable password 573 end 574 errdisable 675 errdisable timeout 677 exit 576 ip prefix-list 771 ip remote-address 775 ip unnumbered 776 ipv6 prefix-list 792 ipv6 unnumbered 794 log file 693 log syslog 312 match as-path 709 match community 710 match interface 712 match ip address 713 match ip address prefix-list 714 match ip next-hop 715 match ip next-hop prefix-list 716 match ipv6 address 718 match ipv6 address prefix-list 719 match ipv6 next-hop 720 match metric 723 match origin 724 match route-type 725 match tag 726 reload 585 route-map 727 service advanced-vty 586 service password-encryption 587 service terminal-length 588 set as-path 729 set atomic-aggregate 730 set comm-list delete 731 set community 732 set dampening 734 set extcommunity 735 set ip next-hop 738 set ipv6 next-hop 739 set level 740 set metric 742 set metric-type 743 set origin 744 set originator-id 745 set tag 746 set vpnv4 next-hop 747 set weight 748 show access-list 651 show cli 651 show ip prefix-list 839 show list 660 show startup-config 667 show version 668 write terminal 621
Common Configure Mode Commands 671
Common NSM Layer 2 commands flowcontrol off 1178 hardware register get 1180 show

flowcontrol interface 1182 storm-control level 1278, 4799
compatible rfc1583 2270
confederations 1655
Configuration
BFD Configuration in BGP 4257
BFD Configuration in IS-IS 4255
BFD Configuration in RIP 4261
OSPF—BFD Multi-hop Session 4251 configuration 3759 Automated Protection Switching 3092 disable spanning tree 1081 DOT1.X Tunneling in UNI 1135
Ethernet Switched Path 3087
Multicast Connectivity Fault Management 3107
PBB-TE 3087
Unicast Connectivity Fault Management 3102 configuration file 4358 Configuration Storage 134 configurations
Ethernet CFM 3047
PBB-TE 3087
configure
802.1x authentication 1107
Area Border Router for OSPFv3 1718
BGP 1513
BGP authentication 1543
BGP4+ 1647
configuring overload bit 1801
customer edge 3432, 3434
distance 1799
EFM OAM
Ethernet to the First Mile 3063 GMRP 1161, 1171
graceful restart 1799
GVRP 1169
IGMP snooping 2715
IP address on VLAN 1860, 1898
IS-IS 1785
IS-IS-IPv6 1809
LACP 1109
LLDP 2995
MAC authentication 1163 metric 1789 MSTP 1067
OSPF 1663
OSPFv3 1711
passive interface 1804
Provider Bridging 3017
provider Ethernet bridge 1 3431 provider Ethernet bridge 2 3432
QoS 4529, 4635 RIPng 1945 route leaking 1797
route summarization 1798 route-map 1516
RSTP 1057
STP 1047
VLAN interfaces 1859, 1897 configure hybrid switch 517 configure hybrid switch as a layer-2 switch 514 configure hybrid switch as port-based VLAN 515 configure hybrid switch to work as a router or switch 514 configure hybrid switch to work as l-3 router 515 configure l-2 and l-3 protocols 514 configure mode 93 Configure Multipath eBGP 1623 Configure Multipath iBPG 1632 configure OSPFv3 graceful restart 1747 configure static RIPng routes 2660 configure terminal 568 configured tunnel 1865 configuring BGP Confederation 1531 configuring BGP Extended Community attributes 1585 configuring BGP Four-Byte AS 1582 configuring BSR BSR topology 2705 validation commands 2706 configuring CFM over PBB
validation commands 3060 configuring Layer-2 interfaces 517
configuring Layer-3 interfaces 518
configuring OSPF
redistributing routes into OSPF 1676 configuring overload bit in IS-IS 1801 Configuring PoE through SNMP 543 Configuring port Breakout 530 Configuring port Breakout(100G to 4x10G) 530 configuring preempt mode 4207, 4226 configuring RIPng
enable RIPng 1945
configuring RP dynamically 2703
configuring RP statically 2700, 2748 configuring sFlow 4509
Configuring
VRRP one
virtual router 4175 two
backup routers 4180 two virtual routers 4177
configuring VRRP IPv6 4191
connectivity fault management
provider backbone bridging 3055
Connectivity Fault Management (CFM) configuration 3145 Control

Port Group 3759, 3767, 3769 copy 381 copy file running-config 399 copy ftp binary file 398 copy ftp running-config 380, 384, 386 copy ftp running-config (interactive) 387 copy ftp startup-config 379 copy ftp startup-config (interactive) 392, 393 copy ftp system file 398 copy http running-config 388 copy http startup-config 387 copy http startup-config (interactive) 397 copy running-config 373 copy running-config (interactive) 374 copy running-config start-config 646 copy scp (startup-config|running-config) 381 copy scp running-config 382 copy scp running-config (interactive) 389 copy scp startup-config 381 copy scp startup-config (interactive) 394 copy scp system file 398 copy sftp (startup-config|running-config) 383 copy sftp running-config 384 copy sftp running-config (interactive) 390 copy sftp startup-config 383 copy sftp startup-config (interactive) 395 copy sftp system file 398 copy startup-config 375 copy startup-config (interactive) 376 copy startup-config running-config 398 copy system file 377 copy system file (interactive) 378 copy tftp running-config 386 copy tftp running-config (interactive 391 copy tftp running-config (interactive) 392 copy tftp startup-config 385 copy tftp startup-config (interactive) 396 copy tftp system file 398 CoS to Queue Map Configuration 4645 CoS value 4635 cost
  OSPF 1678
create a user 1885, 2719 create aggregate policer 4531 create policy map 4530 creating a VLAN interface 1859, 1897 creating tunnel interface
  between PIM-DM routers 2755
  between PIM-SM routers 2755
crypto ipsec security-association lifetime 986 crypto ipsec transform-set 987 crypto isakmp enable 989 crypto isakmp policy 990 crypto key generate rsa 991 crypto map (Configure Mode) 992 crypto map (Interface Mode) 993 crypto map local-address 994 cspf default-retry-interval 2469 cspf tie-break 2470
CSPF-TE Commands capability te 2468 cspf default-retry-interval 2469 cspf tie-break 2470 debug cspf events 2471 show cspf ipv6 lsp 2473 show cspf lsp 2474 show debugging cspf 2475 show debugging ipv6 cspf 2476 show ip ospf te-database 2477 show ipv6 ospf te-database 2479
curly brackets
  command syntax 88
customer-spanning-tree customer-edge path-cost 1244 customer-spanning-tree customer-edge priority 1245 customer-spanning-tree forward-time 1246 customer-spanning-tree hello-time 1247 customer-spanning-tree max-age 1248 customer-spanning-tree priority 1249 customer-spanning-tree provider-edge path-cost 1250 customer-spanning-tree provider-edge priority 1251 customer-spanning-tree transmit-holdcount 1252 cvlan registration table 3192 cvlan svlan 3193

D

Daemons 134
damped route 2227
data flow
  PIM-SM 2696
data-link 924 ddm monitor 1032 debug bfd all 4311 debug bgp events 2059 debug bgp filters 2059 debug bgp fsm 2059 debug bgp keepalives 2059 debug bgp mpls 2167 debug bgp updates 2059
debug cmm 1020
debug commands
  debug trill all 4041 debug trill events 4042 debug trill ifsm 4044 debug trill nfsm 4047 debug trill nsm 4048 debug trill spf 4051 elmi 3445
debug cspf events 2471 debug ddm 1034, 1037 debug dns client 246 debug dot1x 1422 debug ecp 3545 debug gmrp 1449 debug gvrp 1465 debug igmp 2775, 2833 debug ip ospf graceful-restart 2276 debug ip pim timer joinprune 2873, 2875 debug ipv6 ospf 2391

ifsm 2394
packet 2399
debug ipv6 ospf lsa 2395, 2396 debug ipv6 ospf nfsm 2397 debug ipv6 ospf nsm 2398 debug ipv6 ospf packet 2399 debug ipv6 ospf route 2402 debug ipv6 rip 2645 debug isis 2500 debug isis-spb 3705 debug lacp command 1299 debug ldap 473
debug logging 311
debug mcec 1327 debug mld 2809
debug mstp 1253 debug nsm packet 650 debug ntp 338
debug ospf 2271 packet 2283
debug ospf database-timer rate-limit 2273 debug ospf events 2274 debug ospf ifsm 2275 debug ospf lsa 2280 debug ospf nfsm 2281 debug ospf nsm 2282 debug ospf packet 2283 debug ospf route 2285 debug ospf6 packet 2399 debug pim packet 2867, 2935 debug pim sm sparse-mode timer assert 2936 debug pim sparse-mode timer hello 2938 debug pim sparse-mode timer register 2875, 2941 debug radius 440 debug rib 2577 debug sflow 4515 debug snmp-server 278 debug spb 3706 debug ssh server 257 debug tacacs+ 453 debug telnet server 298 debug trill esadi 4043 debug trill l2mrib 4046 debug trill oam 4049 debug user-mgmt 330 debug vrrp 4203
default-information originate 2286, 2403, 2502, 2601, 2647 default-metric 2288, 2405, 2602, 2648 default-metric command 2405 description 925, 937, 2579, 4359 designated router election 4036 designated router priority 2888, 2952 DiffServ architecture 4635 disable 571, 651 disable spanning tree configuration 1081 spanning-tree te-msti configuration 1277
disable VRRP session 4204, 4224 displaying VLAN interface 1860 distance 2061, 2289, 2406, 2603, 2649
distance (OSPF command) 2289 distance in IS-IS 1799
distribute-list 1776, 2407, 2604, 2650
do 610 domain hello timeout 1328
Domain Name System 5033
domain priority 1329 domain system number 1330 domain-address 1326
domain-name, ip 249 domain-password 2504
dot1x initialize interface 1423 dot1x port-control 1425 dot1x protocol-version 1426 dot1x quiet-period1427dot1x reauthentication 1429
dot1x reauthMax 1428
dot1x system-auth-control 1430 dot1x timeout re-authperiod 1431 dot1x timeout server-timeout 1432 dot1x timeout supp-timeout 1433 dot1x timeout tx-period 1434 downstream 2696,2711,2733
downstream multicast listener 3983 DRNI 1111
DSCP to Queue Map Configuration 4643
DSCP value Differentiated Services Code Point 4636
Dual-ended LMM configuration 3141 dynamic-learning disable 4960

E

eBGP peering 1649
EFM OAM configuration Link Monitoring Events 3066 remote failure detection 3067 remote loopback 3065

validation 3064
validation commands 3064
embedded RP
configuration 2709
EMF OAM configuration validation commands 3064
enable 572 enable BGP 1513 enable db-summary-opt 2292, 2409 enable eBGP peering 1649 enable IS-IS 1785 enable multiple OSPF instances 1689 enable multiple OSPFv3 instances 1736 enable OSPFv3 1711 enable password 573 enable QoS 4529 enable RIPng 2653
enable routing between VLAN and routed port 516 enable VRRP sessions 4205, 4225
Enable/Disable Configuration 4639
enabling IS-IS 1809 enabling Load Balancing 1857 encapsulation 4807 encryption 995 end 574 enhanced-transmission-selection advertise-local-config 3493
EPS commands
bridge g8031 eps-id working-port protection-port 3332 g8031 configure switching eps-id bridge 3333 g8031 configure vlan eps_id 3334
g8031 ethernet domain-name service-id ma-name 3335
g8031 exercise 3336 g8031 force 3337 g8031 local-freeze 3338 g8031 local-lockout 3339 g8031 lockout 3340 g8031 manual 3341 g8031 mode bridging restoration 3342 g8031 set-nr 3344 g8031 timer 3345 g8031 vlan VID 3347 show bridge eps-id 3348 show bridge g8031 3349
ERPS commands
g8032 configure switching ring-id 3353 g8032 rpl 3356 g8032 shared 3357 g8032 timer 3358 show bridge g8032 3359
errdisable 675
errdisable timeout 677
Ethernet 4389, 4397 Ethernet address 5033 ethernet cfm 1dm receive 3384 ethernet cfm ais interval 3385 ethernet cfm pbb cc 3387 ethernet cfm pbb cc multicast state 3388 ethernet cfm pbb cc unicast state 3389 ethernet cfm pbb lmm 3394 ethernet cfm pbb mcc tx 3395 ethernet cfm pbb mep 3396 ethernet cfm pbb throughput-measurement reception 3398
ethernet cfm pbb traceroute-cache 3250 ethernet cfm server-ais status 3249 ethernet cfm traceroute cache 3250 ethernet lmi commands
global 3448
Ethernet OAM CLI ethernet oam disable 3287
ethernet oam enable 3288 ethernet oam link-monitor frame 3291, 3292 ethernet oam link-monitor frame-period threshold 3293 ethernet oam link-monitor high threshold 3295 ethernet oam link-monitor on 3296 ethernet oam link-monitor remote-failure 3303 ethernet oam link-monitor supported 3297 ethernet oam link-monitor symbol-period threshold 3298 ethernet oam max-rate 3300 ethernet oam remote-loopback 3304 show ethernet oam discovery interface 3310 show ethernet oam IFNAME 3308 show ethernet oam interface statistics 3312 show ethernet oam status interface 3313
ethernet oam disable 3287
ethernet oam enable 3288
ethernet oam link-monitor frame 3291, 3292 ethernet oam link-monitor frame-period threshold 3293 ethernet oam link-monitor high threshold 3295 ethernet oam link-monitor on 3296 ethernet oam link-monitor remote-failure 3303 ethernet oam link-monitor supported 3297 ethernet oam link-monitor symbol-period threshold 3298 ethernet oam max-rate 3300 ethernet oam remote-loopback 3304

Ethernet Ring Protection Switching (ERPS)
configuration 3121
ETS
configuration 3467
ETS commands
application-priority advertise-local-config 3486 application-priority enable (interface) 3487 application-priority enable (switch) 3488 bandwidth-percentage 3489 data-center-bridging 3490 dcbx enable 3491 enhanced-transmission-selection 3494 enhanced-transmission-selection accept-peerconfig 3492 enhanced-transmission-selection advertise-localconfig 3493 enhanced-transmission-selection enable 3495 ethertype 3496 max-traffic-class-group 3498 show application-priority interface 3500 tcp 3507 traffic-class-group add 3508
evb bridge cdcp channel-capacity 3546 evb bridge cdcp svid-pool-range 3547 evb bridge ecp-acktimer 3548 evb bridge ecp-max-retry 3549 evb bridge resource-wait-delay 3550 evb bridge tlv-mode 3551 evb bridge vdp-keep-alive 3552 evb cdcp 3553 evb reflective-relay 3554 evb-station 3555 evpn esi holdtime 4962 evpn irb1 4967
evpn irb-forwarding anycast-gateway-mac 4965 evpn irb-if-forwarding anycast-gateway-mac 4966 evpn multi-homing enable 4963 exec command mode 92 exit 576 exit-address-family 2413 exit-address-family command 2062, 2669 exit-interface-eth-cfm-mep 3253 ext tx 3254 Extended Prefix opaque LSA 4119

F

Fail Over Group 3759 fast-external-failover 2023
FAULT 3064

feature dhcp 242
feature ldap 474
feature ntp 338
feature sflow 4516
feature ssh 258
feature tacacs+ 457 feature telnet 299 fec 762 fib retain 2580
flowcontrol off 1178 fog tfc 3768
fog type 3769
FTN/ILM 4117, 4119

G

GARP Multicast Registration Protocol 1161, 1171
GARP VLAN Registration Protocol 1169
Generic Routing Encapsulation 1863
GMRP
configuring 1161, 1171
GMRP commands
clear gmrp statistics 1448 debug gmrp 1449 set gmrp 1450, 1451 set gmrp extended-filtering bridge 1452 set gmrp fwdall 1453 set gmrp registration 1454 set gmrp timer 1455 set port gmrp 1456 show debugging gmrp configuration 1457 show gmrp configuration 1458, 1474 show gmrp machine 1459, 1475 show gmrp statistics 1460 show gmrp timer 1461

graceful restart commands neighbor capability graceful-restart 2084 restart bgp graceful 2136
graceful restart in IS-IS 1799
GRE 1863 GRE tunnel 1867 group 996 group-to-RP mappings 2705
GVRP 1169
configuring 1169
GVRP commands
clear gvrp statistics 1464 debug gvrp 1465 set gvrp 1467, 1469 set gvrp applicant 1466 set gvrp dynamic-vlan-creation 1468 set gvrp registration 1470 set gvrp timer 1471 set port gvrp 1472 show debugging gvrp 1473 show gvrp statistics 1476, 1491 show gvrp timer 1477

H

Hardware Abstraction Layer (HAL) 134 hardware register get 1180 Hardware Services Layer (HSL) 136 hardware-profile portmode 681, 763 hardware-profile portmode bundle 764 hash 997

Hierarchical Queuing Configuration 4711 High Level Architecture 100 history 2227 hold-off 4486 host area 2296 how l-2 switches are used 513 how l-3 routers are used 513 how to bind an interface to the VR 1886, 2720 how to disable VRRP session 4204, 4224 how to enable
authentication on an area 1685
authentication on an interface 1685
BGP 1513 iBGP peering 1647 IS-IS 1785

IS-IS IPv6 1809 Load Balancing 1857 multiple OSPF instances 1689 multiple OSPFv3 instances 1736
OSPF on an interface 1663
OSPFv3 1711
RIP 1917 how to enable VRRP session 4205, 4225 how to enable/disable Virtual MAC 4220 how to enter router mode 4228 how to log in as GA 1885, 2719 how to log in as VR administrator 1887, 2721 how to redistribute routes 1721 how to redistribute routes into OSPF 1676 how to save configuration on a VR 1887, 2721 how to set priority in OSPF 1666 how to set priority in OSPFv3 1714 how to set priority-IS-IS 1786 how to set the Virtual IP address 4218 how to set the Virtual IPv6 address 4231 how to specify RIP version 1922 hybrid L-2/ L-3 switch router 513 hybrid switch configuration 517

I

iBGP peering 1647 IEEE 802.1x 1107 if-arbiter 765
IFNAME 88
IFSM debug 4044
IGMP 1971
IGMP Commands
clear ip igmp 2774 debug igmp 2775, 2833 ip igmp 2777 ip igmp access-group 2778 ip igmp immediate-leave 2779 ip igmp last-member-query-count 2781 ip igmp last-member-query-interval 2782
ip igmp limit 2783 ip igmp mroute-proxy 2784 ip igmp proxy-service 2786 ip igmp querier-timeout 2788 ip igmp query-interval 2789 ip igmp query-max-response-time 2790 ip igmp robustness-variable 2792 ip igmp snooping 2834 ip igmp snooping fast-leave 2835 ip igmp snooping mrouter 2836 ip igmp snooping querier 2837 ip igmp snooping report-suppression 2838 ip igmp ssm-map enable 2793 ip igmp ssm-map static 2794 ip igmp static-group 2795 ip igmp version 2798 show ip igmp groups 2800 show ip igmp interface 2802 show ip igmp snooping mrouter 2840 show ip igmp snooping statistics 2846
IGMP snooping configuration 2715
ignore-lsp-errors 2505 IGP 4117 ike-version 998 import map 2168 ingress DTree 3982 input-source 4487 in-service testing 3255 integrated solution 513 inter-area 4131 interface 766 bind to TRILL instance 4092
Interface Add 517 Interface Commands 751 Interface Delete 517 Interface irb 4968 interface mode 93 interface po 1300 interface sa 1301 interface tunnel 950 Interior Gateway Protocol (IGP) 1949 Intermediate System to Intermediate System 119
Intermediate System to Intermediate System (IS-IS) 1957
Internet Group Management Protocol (IGMP) 1971 Internet Protocol Version 6 5033 interval
link state PDU 4034
intra-domain-link 1331 intra-site automatic tunnel address protocol 1874 ip address 767, 926 ip address dhcp 243, 768 ip bfd static all-interfaces 4340
ip dhcp client request 244 ip dhcp relay 360 ip dhcp relay address 361 ip dhcp relay information option 362 ip domain-list 247 ip domain-lookup 248 ip domain-name 249
ipextcommunity-list
expanded2071
extended 2070
standard 2072
ip extcommunity-list standard 2069 ip forwarding 769 ip host 250 ip igmp 2777 ip igmp access-group 2778 ip igmp immediate-leave

2779 ip igmp last-member-query-count 2781 ip igmp last-member-query-interval 2782 ip igmp limit 2783 ip igmp mroute-proxy 2784 ip igmp proxy-service 2786 ip igmp querier-timeout 2788 ip igmp query-interval 2789 ip igmp query-max-response-time 2790 ip igmp robustness-variable 2792 ip igmp snooping 2834 ip igmp snooping fast-leave 2835 ip igmp snooping mrouter 2836 ip igmp snooping querier 2837 ip igmp snooping report-suppression 2838 ip igmp ssm-map enable 2793 ip igmp ssm-map static 2794 ip igmp static-group 2795 ip igmp version 2798 ip mroute 686 ip msdp default-peer 2876 ip msdp mesh-group 2877 ip msdp originator-id 2878 ip msdp password 2879 ip msdp peer 2880 ip multicast route-limit command 2762 ip multicast ttl-threshold 2763 ip multicast-routing 2764 ip name-server 251 ip ospf authentication 2297 ip ospf authentication-key 2298 ip ospf bfd 2299 ip ospf cost 2300 ip ospf database-filter 2301 ip ospf dead-interval 2302 ip ospf disable all 2303, 2305 ip ospf hello-interval 2306 ip ospf message-digest-key 2308 ip ospf mtu 2310 ip ospf mtu-ignore 2311 ip ospf network 2312 ip ospf priority 2313 ip ospf retransmit-interval 2314

ip ospf transmit-delay 2315 ip pim accept-register list 2881, 2942 ip pim anycast-rp 2882, 2943 ip pim bsr-border 2883, 2945 ip pim bsr-candidate 2884, 2946 ip pim cisco-register-checksum 2885, 2947 ip pim dr-priority 2888, 2952 ip pim exclude-genid 2889, 2955 ip pim hello-holdtime 2890, 2956 ip pim hello-interval 2891, 2957 ip pim ignore-rp-set-priority 2892, 2958 ip pim jp-timer 2893, 2959 ip pim neighbor-filter 2894, 2960 ip pim register-candidate 2903, 2969 ip pim register-candidate group-list 2969 ip pim register-rate limit 2896, 2962 ip pim register-rp-reachability 2897, 2963 ip pim register-source 2898, 2964 ip pim rp-address 2901, 2967 ip pim rp-register-kat 2970 ip pim spt-threshold 2905, 2971 ip pim ssm 2906, 2972 ip pim unicast-bsm 2908, 2974 ip prefix-list 771 ip proxy-arp 774 ip radius source-interface 1435 ip remote-address 775 ip rip authentication key-chain 2605 ip rip authentication mode md5 2606 ip rip authentication string 2607 ip rip receive version 2609 ip rip receive-packet 2608 ip rip send version 2611 ip rip send-packet 2610 ip rip split-horizon 2612 ip route 2581 ip router isis 2506 ip static bfd 4342 ip static fall-over bfd 4341 IP telephones 541 ip unnumbered 776
ip vrf 777, 2169, 2583 ip vrf forwarding 777 ip vrf isid 3707

ip-access-list 4569, 4573 IP-IP tunneling 1863
IPv4 address command syntax 88
IPv4 Tunneling 1863 IPv6 5033
ipv6 access-list filter 884
IPv6 address command syntax 88
ipv6 address 778 ipv6 bfd static all-interfaces 4343 IPv6 configuration 4191 ipv6 dhcp relay 363 ipv6 dhcp relay address 364 Ipv6 evpn prefix route 4970
ipv6 forwarding 779 ipv6 mld 2811 ipv6 mld access-group 2812 ipv6 mld immediate-leave 2813 ipv6 mld last-member-query-count 2814 ipv6 mld last-member-query-interval 2815 ipv6 mld limit 2816 ipv6 mld mroute-proxy 2817 ipv6 mld proxy-service 2818 ipv6 mld querier-timeout 2819 ipv6 mld query-interval 2820 ipv6 mld query-max-response-time 2821 ipv6 mld robustness-variable 2822 ipv6 mld ssm-map enable 2823 ipv6 mld ssm-map static 2824 ipv6 mld static-group 2825 ipv6 mld version 2826 ipv6 mroute 688 ipv6 nd current-hoplimit 780 ipv6 nd link-mtu 781 ipv6 nd managed-config-flag 782 ipv6 nd other-config-flag 784 ipv6 nd prefix 785 ipv6 nd ra-interval 787 ipv6 nd reachable-time 789 ipv6 nd retransmission-time 790 ipv6 nd suppress-ra 791 ipv6 ospf cost 2414 ipv6 ospf dead-interval 2415 ipv6 ospf display route single-line 2417 ipv6 ospf link-lsa-suppression 2419 ipv6 ospf mtu-ignore 2420 ipv6 ospf neighbor 2421 ipv6 ospf network 2423 ipv6 ospf priority 2424 ipv6 ospf restart grace-period 2425 ipv6 ospf restart helper 2426 ipv6 ospf retransmit-interval 2428 ipv6 ospf6 transmit-delay 2429 ipv6 prefix-list 792 ipv6 rip split-horizon 2652 Ipv6 route vrf 4973 ipv6 router mode 4228 ipv6 router ospf 2430 ipv6 router rip 2653 ipv6 static bfd 4345 ipv6 static fall-over bfd 4344 ipv6 te-metric 2432 IPv6 transition

6to4 automatic tunnel 1870 6to4 relay 1872 configured tunnel 1865 GRE tunnel 1867
ISATAP automatic tunnel 1874 IPv6 Transition Software 120 ipv6 unnumbered 794 ipv6-address 999 ipvpn 3708 ISATAP automatic tunnel 1874 isis authentication key-chain 2507 isis authentication mode md5 2508 isis authentication send-only 2509
isis circuit-type 2511

IS-IS Commands
trill instance 4092 trill link-type 4093
IS-IS commands 2499 accept-lifetime 2485 area-password 2488 authentication key-chain 2489 authentication mode md5 2490 authentication send-only 2491 clear clns is-neighbors 2494 clear clns neighbors 2493 clear isis interface counter 2498 clear isis route 2495 default-information originate 2502 distance (IPv4) 2503 isis authentication key-chain 2507 isis authentication mode md5 2508 isis authentication send-only 2509 isis csnp-interval 2512 isis hello-interval 2513 isis hello-multiplier 2514 isis metric 2517 isis network 2518 isis password 2519 isis priority 2520 isis retransmit-interval 2521 key 2526, 2613 key chain 2525 key-string 2527 max-area-address 2531 redistribute 2535 redistribute isis 2537 send-lifetime 2539, 2542 set-overload-bit 2541 show clns is-neighbors 2546 show clns neighbors 2548 show cspf lsp 2550 show debugging isis 2550 show ip protocols 2556 show isis counter 2557 show isis counter command 2557 show isis database 2558 show isis interface 2561 show isis tag database 2564 show isis topology 2566 show running-config interface isis 2568 show running-config router isis 2569 summary-address 2544

ISIS Configuration 1957
IS-IS configuration 1785 configuring distance 1799 configuring metric 1789 configuring overload bit 1801 configuring passive interface 1804 enabling IS-IS on an interface 1785 graceful restart 1799
L1 L2 area routing with multiple instances 1794 L1 L2 area routing with single instance 1792 redistributing routes into IS-IS 1788 route leaking 1797 route summarization 1798 setting priority 1786
IS-IS configuration-IPv6 1809
configuring IS-IS IPv6 distance 1819 enabling IS-IS on an interface 1809
L1 L2 area routing 1815
L1 L2 area routing with multiple instances 1817
metric 1812
redistributing routes 1811 setting priority 1810
isis csnp-interval 2512 isis csnp-interval command 2512 isis hello-interval 2513 isis hello-interval command 2513 isis hello-multiplier 2514, 3711 isis hello-multiplier command 2514 isis metric 2517 isis metric command 2517 isis network command 2518 isis password 2519
isis password command 2519 isis priority 2520 isis priority command 2520 isis retransmit-interval 2521, 3719 isis retransmit-interval command 2521 isis-spb configuration bridge 3709 isis-spb hello-interval 3710 isis-spb hello-multiplier 3711 isis-spb hostname 3712 isis-spb ignore-lsp-errors 3713 isis-spb lsp-gen-interval 3714 isis-spb lsp-interval 3715 isis-spb lsp-refresh-interval 3716 isis-spb max-lsp-lifetime 3717 isis-spb retransmit-interval 3719 isis-spb set-overload-bit 3720 isis-spb spf-interval-exp 3721 isis-spb system-id 3722 is-type 2524

K

kernel patch MD5 authentication 1543 key chain 2525, 2614, 4313 key command 2526, 2613 key 4312 key-string 2527, 2615

L

L1L2 area routing 1792, 1794, 1815 L1L2 area routing multiple instance 1817 L-2 and L-3 Integration overview 513
L3_LAG Configuration 1893

label 4117
label range 4117 label switching 4131
LACP
configuring 1109
LACP Commands
debug lacp 1299 lacp port-priority 1304 lacp system-priority 1305 lacp timeout 1306 show debugging lacp 1310 show lacp-counter 1315 show

port etherchannel 1316
static-channel-group 1322
LACP commands
port-channel load-balance 1307
lacp destination-mac 1302
lacp discard wrong conversation 1303
LACP peering configuration 1129 in MEF UNI 1129 Validation Commands 1131 verification 1134
lacp port-priority command 1304 lacp system-priority command 1305 lacp timeout command 1306 LAN Access Points 541
LAN segments 4807
Layer 2 Multicast Routing Information Base Daemon 121 Layer 3 Multicast Routing Information Base Daemon 122 ldap-server deadtime 475 ldap-server host 476 ldap-server port 478
ldap-server timeout 479 LDP 4117
lifetime 1000
LINE 88
Link aggregation 1111 link Monitoring validation 3067
link monitoring events 3066 link-local address 1648 link-type 3770 listener
downstream multicast 3983
LLDP commands
lldp system-name 3179, 3326
set lldp disable 3161, 3320
set lldp enable 3161, 3321 set lldp locally-assigned 3167, 3322 set lldp msg-tx-hold 3168, 3324 set lldp msg-tx-interval 3170, 3180 set lldp too-many-neighbors 3181, 3328 show lldp port 3182, 3329
LLDP configuration validation 542
lldp system-name 3179, 3326 load-balance 690 load-balance rtag7 690 load-balance rtag7 hash 693 load-balance rtag7 vxlan inner-l2 4965, 4974 load-balance rtag7 vxlan inner-l3 4975 locator led 1021 lockout 4488 log file 693 log in as a GA 1885, 2719 log syslog 312
Logging 134 Logging Console Configuration 171 logging in as VR administrator 1887, 2721 logging level 314 logging logfile 316 logging server 318 logging source-interface 320 logging timestamp 320 Logical Switch Router 4373 login virtual-router 4363 log-neighbor-changes command 2029 logout 612 lsp-gen-interval 2528 lsp-refresh-interval 2530

M

mac 4977
MAC address 5033 command syntax 89
MAC address authentication 1163
MAC addresses 4807
MAC authentication auth-mac 1167 auth-mac-aging
auth-mac-fail-action 1165
configuring 1163
initial configuration 1163
MAC address authentication 1163 multiple PCs 1163 RADIUS server configuration 1164 MAC headers 513 mac vrf 4978 mac-access-list 4580 mac-holdtime 4979 map vnid 4981 Marking/Remarking Configuration 4653 match access-group 4582 match address 1001
Match and Set Commands match as-path 709 match community 710 match interface 712 match ip address 713 match ip address prefix-list 714 match ip next-hop 715 match ip next-hop prefix-list 716 match ipv6 address 718 match ipv6 address

prefix-list 719 match ipv6 next-hop 720 match metric 723
match origin 724 match route-type 725 match tag 726 set as-path 729 set atomic-aggregate 730 set comm-list delete 731 set community 732 set dampening 734 set extcommunity 735 set ip next-hop 738 set ipv6 next-hop 739 set level 740 set metric 742 set metric-type 743 set origin 744 set originator-id 745 set tag 746 set vpnv4 next-hop 747 set weight 748
match as-path 709
match command origin 724
match community 710 match cos 4763 match dscp 4760 match interface 712 match ip address 713 match ip address prefix-list 714 match ip next-hop 715 match ip next-hop prefix-list 716 match ip rtp 4760 match ip-dscp 4586 match ip-precedence 4588 match ipv6 address 718 match ipv6 address prefix-list 719 match ipv6 next-hop 720 match layer4 4590 match mac 4758 match metric 723 match origin 724 match protocol 4760 match route-type 725 match tag 726 match vlan 4592, 4763 match vlan-range 4594 max-area-address 2531 max-concurrent-dd 2317, 2433 max-fib-routes 2585 maximum-area 2318 maximum-paths 2584 maximum-prefix 2616 max-lsp-lifetime 2532 Maxpoll and Minpoll Configuration 211 max-static-routes 2586
mcec domain configuration 1333 MC-LAG 1111
MC-LAG Configuration 1111
MD5 authentication on BGP 1543
MD5 libraries 1543
MED 2001 Memory Management 133
metric in IS-IS 1789
metric-IS-IS 1812
metrics 117 mlag 1332
MLD Commands
clear ipv6 mld 2808 debug mld 2809 ipv6 mld 2811 ipv6 mld access-group 2812 ipv6 mld immediate-leave 2813 ipv6 mld last-member-query-count 2814 ipv6 mld last-member-query-interval 2815 ipv6 mld limit 2816 ipv6 mld mroute-proxy 2817 ipv6 mld proxy-service 2818 ipv6 mld querier-timeout 2819 ipv6 mld query-interval 2820 ipv6 mld query-max-response-time 2821 ipv6 mld robustness-variable 2822 ipv6 mld ssm-map enable 2823 ipv6 mld ssm-map static 2824 ipv6 mld static-group 2825 ipv6 mld version 2826 mld snooping 2848 mld snooping fast-leave 2849 mld snooping mrouter 2850 mld snooping querier 2851 mld snooping report-suppression 2852 show ipv6 mld groups 2828 show ipv6 mld interface 2830 show mld snooping mrouter 2854 show mld snooping statistics 2855
mld snooping 2848 mld snooping fast-leave 2849 mld snooping mrouter 2850 mld snooping querier 2851 mld snooping report-suppression 2852 mls qos 4596 mls qos aggregate-police 4595 mls qos enable 4602
MMRP commands
clear mmrp statistics 1480 set mmrp 1481, 1482 set mmrp extended-filtering 1483 set mmrp fwdall disable 1484 set mmrp timer join 1487 show mmrp configuration 1489 show mmrp machine 1490 show mmrp timer 1492
mode 1002, 4489 Module Compatibility 134
Monitor Port Group 3759, 3767, 3768, 3769
Monitor Port Groups 3768
MPLS 4117
MRIB 2695
MSDP 2741
MSTP
configuring 1067 Multi Exit Discriminator 2001 multicast 798
downstream listener 3983
Multicast Commands
clear ip mroute 2760 debug ip mrib debug ip mrib 2761 ip mroute 686 ip multicast route-limit 2762 ip multicast ttl-threshold 2763 ip multicast-routing 2764 multicast 798 show ip mroute 2766 show ip mvif 2769 show ip rpf 656 show ipv6 rpf 658
multicast routing 2764 multicast routing table, displaying 2916, 2978 multicast routing table, displaying based on address 2978
Multicast VR configuration 2719
Multiple Spanning Tree Protocol 110
multiple-instance 2031 MVRP commands
set mvrp 1496, 1498 set mvrp applicant state active 1495 set mvrp dynamic-vlan-creation 1497 set mvrp registration

fixed 1500 set mvrp timer join 1501 set port mvrp disable 1502 show mvrp configuration 1503 show mvrp machine bridge 1504 show mvrp statistics 1505 show mvrp timer 1506

N

NBMA 1874
nd-cache disable 5004
neighbor 2319, 2617 passive 2105 peer-group add 2107 remove-private-AS 2113 unsuppress-map 2126
neighbor allow-egbp-vpn 2170
neighbor as-override 2171 neighbor attribute-unchanged 2082 neighbor command 2654 advertisement-interval 2078 capability dynamic 2083 capability graceful-restart 2084 capability orf prefix-list 2085 enforce-multihop 2095
neighbor connection-retry-time 2088
neighbor disallow-infinite-holdtime 2091
Neighbor Discovery protocol 5033
neighbor g-shut 2097 neighbor g-shut-timer 2098

neighbor send-community 2172 neighbor soo 2173 net 2533 network 2618 network area 2320 network backdoor 2156 network command 2131 Network Services Manager 105 nexthop 2711 no nvo vxlan 4983
NSM Commands
arp A.B.C.D MAC 573 clear ipv6 neighbors 758 debug nsm packet 650 if-arbiter 765 interface 766 ip address 767 ip address dhcp 768 ip forwarding 769 ip proxy-arp 774 ipv6 address 778 ipv6 forwarding 779 ipv6 nd managed-config-flag 782 ipv6 nd other-config-flag 784 ipv6 nd prefix 785 ipv6 nd ra-interval 787 ipv6 nd ra-lifetime 788 ipv6 nd reachable-time 789 ipv6 nd suppress-ra 791 multicast 798 show debugging nsm 652 show ip forwarding 823 show ip interface brief 824 show ipv6 forwarding 834 show ipv6 interface brief 835 show ipv6 route 837 show nsm client 661 show router-id 696, 701 shutdown 941
ntp access-group 339 ntp authenticate 339 NTP Authentication 212 ntp authentication-key 340 NTP Configuration 210 ntp enable 341 ntp logging 342 ntp master 343 ntp peer 343 ntp server 345 ntp trusted-key 348 nvo vxlan 4984
nvo vxlan access-if 4985 nvo vxlan id 4986 nvo vxlan irb 4989 nvo vxlan mac-ageing-time 5011 nvo vxlan max-cache-disable 4988 nvo vxlan tunnel qos-map-mode 4990 nvo vxlan vtep-ip-global 4991

O

OAM discovery state 3064
ACTIVE_SEND_LOCAL 3064
FAULT 3064
PASSIVE_WAIT 3064
SEND_ANY 3064
SEND_LOCAL_REMOTE 3064
SEND_LOCAL_REMOTE_OK 3064
offset-list 2619, 2655
Open Shortest Path First 118 Open Shortest Path First (OSPF) 1955 ordinary clock 4389
Ethernet 4389
UDP 4391, 4392 origin codes 2227 OSPF 4117, 4119, 4131 ospf abr-type 2322
OSPF commands
area authentication 2252 area default-cost 2253 area filter-list 2254 area nssa 2380 area range 2257 area stub 2258 area virtual-link 2259 auto-cost reference-bandwidth 2261 bfd all-interfaces 2262 capability opaque 2265 capability restart 2266 clear ip ospf process 2269 compatible rfc1583 2270 debug ospf 2271 debug ospf database-timer rate-limit 2273 debug ospf events 2274 debug ospf ifsm 2275 debug ospf ism 2275 debug ospf lsa 2280 debug ospf nfsm 2281 debug ospf nsm 2282 debug ospf packet 2283 debug ospf route 2285 default-information originate 2286, 2403 default-metric 2288, 2405 distance 2289, 2406 distribute-list 2290 enable db-summary-opt 2292 host area 2296 ip ospf authentication 2297 ip ospf authentication-key 2298 ip ospf bfd 2299 ip ospf cost 2300 ip ospf database-filter 2301 ip ospf dead-interval 2302 ip ospf disable all 2303, 2305 ip ospf hello-interval 2306 ip ospf message-digest-key 2308 ip ospf mtu 2310 ip ospf mtu-ignore 2311

ip ospf network 2312 ip ospf priority 2313 ip ospf retransmit-interval command 2314 ip ospf transmit-delay 2315 ipv6 ospf mtu-ignore 2420 max-concurrent-dd 2317 maximum-area 2318 neighbor 2319 network area 2320 ospf abr-type 2322 ospf router-id 2326

overflow database 2327 overflow database external 2328 passive-interface 2329, 2434 redistribute 2330 restart helper 2325 restart ospf graceful 2332 router ospf 2333 show debugging ospf 2334 show ip ospf 2335 show ip ospf brder-routers 2339 show ip ospf igp-shortcut-lsp 2349 show ip ospf igp-shortcut-route 2350 show ip ospf interface 2351 show ip ospf neighbor 2356 show ip ospf route 2360 show ip ospf virtual-links 2363 show ip protocols ospf 2365 summary-address 2370 timers lsa arrival 2371 timers throttle lsa 2373
OSPF Configuration 1955
OSPF configuration 1663 Area Border Router 1672 configuring multiple OSPF instances on same subnet 1696
configuring OSPF as PE-CE protocol for VPNs 1618 configuring virtual links 1683 enable multiple OSPF instances 1689 enabling authentication 1685 enabling OSPF on an interface 1663 OSPF cost 1678 redistributing routes into OSPF 1676 setting priority 1666
ospf router-id 2326
OSPF VPN
Commands router
ospf vrf 2465
OSPFv3 commands abr-type 2377 address-family ipv4 unicast 2378 area default-cost 2379 area nssa 2380 area range 2382 area stub 2384 area virtual-link 2385 auto-cost reference bandwidth 2387 capability restart graceful 2389 clear ipv6 ospf process 2390 debug ipv6 ospf 2391
debug ipv6 ospf ifsm 2394 debug ipv6 ospf lsa 2395, 2396 debug ipv6 ospf nfsm 2397 debug ipv6 ospf nsm 2398 debug ipv6 ospf packet 2399 debug ipv6 ospf route 2402 default-metric 2405 distribute-list 2407 enable db-summary-opt 2409 exit-address-family 2413 ipv6 ospf cost 2414 ipv6 ospf dead-interval 2415 ipv6 ospf display route single-line 2417 ipv6 ospf link-lsa-suppression 2419 ipv6 ospf neighbor 2421 ipv6 ospf network 2423 ipv6 ospf priority 2424 ipv6 ospf restart grace-period 2425 ipv6 ospf restart helper
2426 ipv6 ospf retransmit-interval 2428 ipv6 ospf transmit-delay 2429 ipv6 ospf6 transmit-delay 2429 ipv6 router ospf 2430 ipv6 te-metric 2432 max-concurrent-dd 2433 passive-interface 2434 redistribute 2435 restart ipv6 ospf graceful 2437 router ipv6 ospf 2439 router-id 2438 show debugging ipv6 ospf 2440 show ipv6 ospf database 2442 show ipv6 ospf interface 2446 show ipv6 ospf neighbor 2448 show ipv6 ospf route 2451 show ipv6 ospf topology 2454 show ipv6 ospf virtual-links 2456 show ipv6 ospf6 interface 2446 show ipv6 vrf 2458 summary-address 2460

OSPFv3 configuration 1711 configuring Area Border Router 1718 cost 1723 enable multiple OSPFv3 instances 1736 enable OSPFv3 on an interface 1711 OSPFv3 graceful restart 1747 redistribute routes into OSPFv3 1721 setting priority 1714 virtual links 1733
output-source 4490 overflow database 2327 overflow database external 2328

P

parantheses command syntax 87
parentheses command syntax 87

passive interface in IS-IS 1804
PASSIVE_WAIT 3064 passive-interface 2329, 2434, 2620, 2656 PBB CFM commands
ethernet cfm pbb 1dm receive 3384 ethernet cfm pbb ais interval 3385 ethernet cfm pbb cc 3387 ethernet cfm pbb cc multicast state 3388 ethernet cfm pbb cc unicast state 3389 ethernet cfm pbb lmm 3394 ethernet cfm pbb mcc tx 3395 ethernet cfm pbb mep 3396 ethernet cfm pbb throughput-measurement reception 3398
ethernet cfm pbb traceroute-cache 3250
PBB-TE CFM commands
ethernet cfm pbb-te 1dm receive 3403 ethernet cfm pbb-te ais interval 3404 ethernet cfm pbb-te cc enable 3406 ethernet cfm pbb-te cc unicast 3407 ethernet cfm pbb-te in-service|out-of-service 3415 ethernet cfm pbb-te lmm unicast|multicast 3412 ethernet cfm pbb-te mep 3414 ethernet cfm pbb-te

throughput-measurement 3417 ethernet cfm pbb-te throughput-measurement reception 3416
PBB-TE configurations 3087
Automatic Protection Switching 3092
Ethernet Switched Path 3087
Multicast Connectivity Fault Management 3107
Unicast Connectivity Fault Management 3102
Peer 209 peer 1003 peer public-key 1004 period
command syntax 88
PFC commands
priority-flow-control accept-peer-config 3524 priority-flow-control link-delay-allowance 3529 priority-flow-control mode 3530 show priority-flow-control details 3531
PFC priority-flow-control advertise-local-config 3525
PIM 1965
PIM-DM 2689 configuration 2711 downstream 2711, 2733 forwarding multicast packets 2711 nexthop 2711 Reverse Path Forwarding 2711 terminology 2733 upstream 2711, 2733
PIM-SM commands
clear ip mroute 2861, 2931 clear ip msdp peer 2863 clear ip msdp sa-cache 2864 clear ip pim sparse-mode bsr 2865, 2933 debug ip pim timer joinprune 2873, 2875 debug pim packet 2867, 2935 debug pim sparse-mode timer assert 2936 debug pim sparse-mode timer hello 2938 debug pim sparse-mode timer register 2875, 2941 ip msdp default-peer 2876 ip msdp mesh-group 2877 ip msdp originator-id 2878 ip msdp password 2879 ip msdp peer 2880 ip pim accept-register list 2881, 2942 ip pim anycast-rp 2882, 2943 ip pim bsr-border 2883, 2945 ip pim bsr-candidate 2884, 2946 ip pim cisco-register-checksum 2885, 2947 ip pim dr-priority 2888, 2952 ip pim exclude-genid 2889, 2955 ip pim hello-holdtime 2890, 2956 ip pim hello-interval 2891, 2957 ip pim ignore-rp-set-priority 2892, 2958 ip pim jp-timer 2893, 2959 ip pim neighbor-filter 2894, 2960 ip pim register-rate limit 2896, 2962 ip pim register-rp-reachability 2897, 2963 ip pim register-source 2898, 2964 ip pim rp-address 2901, 2967 ip pim rp-candidate 2903, 2969 ip pim rp-candidate group-list 2969 ip pim rp-register-kat 2970 ip pim ssm 2906, 2972 ip pim unicast-bsm 2908, 2974 show debugging pim 2909, 2975 show ip msdp peer 2911 show ip msdp sa-cache 2912 show ip pim bsr-router 2914 show ip pim rp mapping 2988 show ip pim rp-hash 2925, 2987 undebug all pim sparse-mode 2928
PIM-SM configuration 2695 bootstrap router 2696 configuring RP dynamically 2703 configuring RP statically 2700, 2748 data flow from source to receivers 2696 determining the RP 2697 downstream 2696 electing a designated router 2697 forwarding multicast packets 2698 group-to-RP mappings 2705 joining the shared tree 2697 Multicast Routing Information Base 2695 pruning the interface 2697 references 2695 registering with the RP 2697 rendezvous point 2695 reverse path forwarding 2695, 2733 sending out Hello messages 2696 sending Register-Stop messages 2697 shared trees 2696 source-based trees 2696 tree information base 2695 upstream 2696
PIM-SM on VR configuration 2721
PIM-SMv6 on VR configuration 2729 PIMv4 Commands 2859 ping 613 Platform Abstraction Layer 133
poe debug level 549 poe enable 548 police 4607 police-aggregate 4609 policer attributes 4636 types aggregate 4636 individual 4636
policing 4636 Policing Configuration 4667
Policing Configuration for MLS 4537 Policy Based Routing Configuration 521, 4351

policy traffic-type 4773
policy-map 4610, 4767
Port 521 port 1309
Port Breakout Configuration 521
port breakout enable 799 port bundle enable 802 Port Mapping 4809 portal-system-number 1335
portal-topology 1335 port-channel load-balance 1307 port-channel min-links 1309 port-conv-id 1335 Power over Ethernet (PoE) 541
Power over Ethernet Commands 547
Power over Ethernet Configuration 541
Power Sourcing Device (PSE) 541
power threshold 543 Powered Devices (PDs) 541 Power-pair value 543
preempt-mode 4207, 4226 prefix segments 4117 prefix SID 4119 prefix-list 771 prefix-sid value 4162 priority 4227, 4769 Priority Configuration 4691
priority-delta 4184
Private-VLAN commands switchport private-vlan host-association 1384
switchport private-vlan mapping 1385
privilege 617
Privileged Exec mode show ip pim rp mapping 2988
privileged exec mode 92 Protocol-Independent Multicast (PIM) 1965
Provider Bridging commands bridge protocol provider-rstp 3191 cvlan registration table 3192 cvlan svlan 3193 switchport customer-edge 3195 switchport customer-edge default-svlan 3196 switchport customer-edge hybrid allowed vlan 3197 switchport customer-edge vlan registration 3199 switchport customer-network vlan translation 3202 switchport mode 3206 switchport mode customer-edge access 3207 switchport mode customer-edge hybrid 3208 switchport mode ingress-filter 3206 switchport provider-edge vlan 3209 switchport provider-network vlan translation 3210
vlan type 3211
PSE admin control 543
pseudonode flag 4096 psk key 1005 Pv4 5033

Q

QoS
enable 4529
functionality 4635
terminology 4635
QoS commands class 4563 class-map 4564 ip-access-list 4569, 4573 mac-access-list 4580 match access-group 4582 match ip-dscp 4586 match ip-precedence 4588 match layer4 4590 match vlan 4592 match vlan-range 4594 mls qos 4596 mls qos aggregate-police 4595 mls qos enable 4602 police 4607 police-aggregate 4609 policy-map 4610 service-policy input 4611 set ip-dscp 4613 set ip-precedence 4615 show class-map 4620 show mls qos 4621 show mls qos aggregator-policer 4622 show mls qos interface 4624 show policy-map 4625 show qos-access-list 4626 wrr-queue dscp-map 4631 wrr-queue queue-limit 4631 wrr-queue random-detect max-threshold 4631

qos statistics 4773 QoS Statistics Configuration 4641 quality-level 4491 Query-only 210 question mark command syntax 88 queue-limit 4774

R

RADIUS Server Accounting 204 RADIUS Server Authentication 193 radius-server deadtime 441, 1436 radius-server directed-request 441 radius-server host 441, 1437 radius-server host acct-port 442 radius-server host auth-port 443 radius-server host key 446 radius-server key 446, 1439 radius-server retransmit 447, 1440 radius-server timeout 447, 1441 Rapid Spanning Tree Protocol 110
RBridge commands add static fdb neighbor-nickname 3978 add static l2-unicast-trill-fdb 3979 add static multicast-fdb d-tree ingress-nickname 3980 add static multicast-fdb d-tree neighbor-nickname 3981 add static multicast-trill-fdb 3982, 3983 add static multicast-trill-fdb ingress-d-tree 3982 add static multicast-trill-fdb multicast-listener 3983 add static unicast-

trill 3984 rbridge trill bridge 4007 systemid 4011
rd (route distinguisher) 2174
recv-buffer-size 2621, 2657
redistribute 2435, 2535, 2622, 2658 redistribute command 2330
redistribute isis 2537 redistribute routes 1676 redistribute routes in OSPFv3 1721 redistributing routes into IS-IS 1788
redistributing routes into IS-IS IPv6 1811 redistributing routes into OSPF 1676 redundancy using VRRP and OSPF 4188
references
PIM-SM 2695 reload 585 remote failure detection 3067, 3068
remote loopback 3065
validation 3066
remote-link-id 929
Remove MPLS LSPs BFD 4278
removing Multi-Exit Disc attribute from update messages 1581
Rendezvous Point 2695 rendezvous point candidate status 2903, 2969
mappings 2926
reservable-bandwidth 930 reset log file 624 restart bgp graceful 2136
restart helper 2325
restart ipv6 ospf graceful 2437 restart ospf graceful 2332
restart-time 2114
Reverse Path Forwarding 2695, 2711, 2733
rfc1771-path-select 2034 rfc1771-strict 2035
RIB 4119
Ring Protection Switching Configuration
ring protection switching timers 3128
ring protection switching timers 3128 RIP Commands
accept-lifetime 2593 cisco-metric-behavior 2595 clear ip rip route 2596 debug rip 2599 default-information originate 2601 default-metric 2602 distance 2603 distribute-list 2604 ip rip authentication key-chain 2605 ip rip authentication mode md5 2606 ip rip authentication string 2607 ip rip receive packet 2608 ip rip receive version 2609 ip rip send packet 2610 ip rip send version 2611 ip rip send-packet 2610 ip rip split-horizon 2612 key chain 2614 key-string 2615 maximum-prefix 2616 neighbor 2617 network 2618
offset-list 2619 passive-interface 2620 recv-buffer-size 2621 redistribute 2622, 2658 route 2624 router rip 2625 send-lifetime 2626 show debugging rip 2628 show ip protocols rip 2629 show ip rip 2631 show ip rip interface 2633 timers 2638 version 2639
RIP configuration enabling RIP 1917 RIPv2 md5 authentication 1937 RIPv2 text authentication-multiple keys 1930 specifying the RIP version 1922
RIP PE-CE Commands
address-family ipv4 vrf 2668 exit-address-family 2669 show ip rip database vrf 2672
RIP version 1922
RIP VPN commands
address-family ipv4 vrf 2668 exit-address-family 2669 show ip rip database vrf 2672
RIPng commands aggregate-address 2642 cisco-metric-behavior 2643 clear ipv6 rip route 2644 debug ipv6 rip 2645 default-information-originate 2647 default-metric 2648 distance 2649 distribute-list 2650 ipv6 rip split-horizon 2652 ipv6 router rip 2653 neighbor 2654 offset-list 2655 passive-interface 2656 recv-buffer-size 2657 route 2659 route-map 2660 router ivp6 rip 2661 show debugging ipv6 rip 2662 show ipv6 protocols rip 2663 show ipv6 rip interface 2665 show ipv6 rip show ipv6 rip 2664 timers basic 2666 RIPng configuration 1945 rmon alarm 962 rmon collection history 964 rmon collection stats 965
RMON Commands 961 rmon alarm 962 rmon collection

history 964 rmon collection stats 965 rmon event 967 show rmon alarm 968 show rmon event 969 show rmon history 970 show rmon statistics 971
rmon event 967 root of the tree 2696 route 2624, 2659 route leaking in IS-IS 1797 route reflector 1653 route summarization in IS-IS 1798 route-map 727, 2660 route-map-BGP 1651
Router Advertised Commands iipv6 nd current-hoplimit 780 iipv6 nd link-mtu 781 ipv6 nd managed-config-flag 782 ipv6 nd other-config-flag 784 ipv6 nd prefix 785 ipv6 nd ra-interval 787 ipv6 nd ra-lifetime ipv6 nd ra-lifetime 788 ipv6 nd reachable-time 789 ipv6 nd retransmission time 790 ipv6 nd suppress-ra 791
Router Advertisement 1874 Router Information opaque LSA 4119 router ipv6 ospf 2439 router ipv6 rip 2661 router isis 2538 router mode 93 router ospf 2333 router ospf vrf 2465
router rip 2625 router vrrp 4208 route-reflector 1518 router-id 2438 route-target 2175
Routing Information Base Daemon 116
Routing Information Protocol 118
Routing Information Protocol (RIP) 1981
routing, switching or both 513
RP 2695
RPF 2695, 2711, 2733, 2741
RPVST+ commands
bridge protocol rpvst+ 1285 bridge-group vlan 1284 spanning-tree rpvst+ configuration 1291 spanning-tree vlan path-cost 1292 spanning-tree vlan restricted-role 1292 spanning-tree vlan restricted-tcn 1293
rsa key 1006 RSVP 4117

S

saving configuration on a VR 1887, 2721
scan-time 2037 scheduling SP 4637 WRR 4637 WRR with SP 4637 segment routing 4117 segment-routing mpls 4163
SEND_ANY 3064
SEND_LOCAL_REMOT 3064
SEND_LOCAL_REMOTE_OK 3064 send-lifetime 2539, 2542, 2626 send-lifetime 4314
Serve-only 210 Server 209, 210 server 432
service advanced-vty 586 service password-encryption 587 service terminal-length 588 service-policy 4776 service-policy input 4611 service-policy type qos 4777 set administrative distance 2649 set as-path 729 set atomic-aggregate 730 set bridge cos 4779 set comm-list delete 731 set community 732 set dampening 734 set ecp 3556 set extcommunity 735 set gmrp 1450, 1451 set gmrp extended-filtering bridge 1452 set gmrp fwdall 1453 set gmrp registration 1454 set gmrp timer 1455
set gvrp 1467, 1469 set gvrp applicant 1466 set gvrp dynamic-vlan-creation 1468 set gvrp registration 1470 set gvrp timer 1471 set interface null0 737 set ip next-hop 738 set ip-dscp 4613 set ip-precedence 4615 set ipv6 next-hop 739 set ipv6 peer 1007 set level 740 set lldp disable 3161 set lldp enable 3161, 3321 set lldp locally-assigned 3167, 3322 set lldp msg-tx-hold 3168, 3324 set lldp msg-tx-interval 3170, 3180 set lldp too-many-neighbors 3181, 3328 set metric 742 set metric-type 743 set mmrp 1481, 1482 set mmrp extended-filtering 1483 set mmrp fwdall disable 1484 set mmrp timer join 1487 set mvrp 1496, 1498 set mvrp applicant state active 1495 set mvrp dynamic-vlan-creation 1497 set mvrp registration fixed 1500 set mvrp timer join 1501 set origin 744 set originator-id 745 set peer 1008 set poe admin-state 551 set poe high-power 556 set poe max-power 557 set poe mdi-state 552 set poe power-pair 553 set poe priority 555 set poe source 554 set poe total-power 550 set port gmrp 1456 set port gvrp 1472 set port mvrp disable 1502 set precedence 4786 set security-association lifetime 1009 set session-key 1010 set tag 746 set transform-set 1012 set vpnv4 next-hop 747 set weight 748 set-overload-bit 2541 setting priority 1714 setting priority for IS-IS IPv6 1810 setting router priority 4227 setting-priority 1786 sFlow 4516
sflow collector 4517 Shaping Configuration 4683
Shaping Configuration for MLS 4547 shared trees 2696 show 5021 show aaa accounting 433 show aaa authentication 433 show aaa authentication login 434 show access-list 651 show access-lists 913 show bfd 4316 show bfd interface 4317 show bfd session 4319 show bfd session A.B.C.D 4323 show bfd session ipv6 4325 show bgp ipv6 2194 show bgp l2vpn evpn 4994 show bgp l2vpn evpn prefix-route 5024 show bgp l2vpn evpn summary 4998 show bgp neighbors received prefix-filter 2205 show bgp

neighbors received-routes 2206 show bgp neighbors routes 2207 show bgp paths command 2212 show bgp prefix-list command 2213 show bgp quote-regexp command 2214 show bgp route-map command 2216 show bridge spb 3728 show class-map 4620 show cli 651 show clns is-neighbors 2546 show clns is-neighbors command 2546 show clns neighbors command 2548 show commands 90
exclude modifier 91
include modifier 91 redirect modifier 92
show crypto ipsec transform-set 1013 show crypto isakmp policy 1014 show crypto-map interface 1015 show cspf ipv6 lsp 2473 show cspf lsp 2474, 2550 show debug ldap 480 show debug radius 448 show debug ssh server 259 show debug tacacs+ 461 show debug telnet server 300 show debugging bfd 4327 show debugging cspf 2475 show debugging dot1x 1442 show debugging elmi 3454 show debugging gmrp 1457 show debugging gvrp 1473 show debugging ipv6 cspf 2476 show debugging ipv6 ospf 2440 show debugging ipv6 rip 2662 show debugging isis 2550 show debugging lacp command 1310 show debugging mstp 1255 show debugging nsm 652 show debugging ospf 2334 show debugging pim 2909, 2975 show debugging rib 2587 show debugging rip 2628 show debugging vrrp 4209 show dot1x 1443 show errdisable details 696 show esmc counters 4500 show ethernet lmi evc bridge 3455 show ethernet lmi evc detail 3456, 3457 show ethernet lmi parameters 3460 show ethernet lmi statistics bridge 3461 show ethernet lmi uni interface 3462 show ethernet oam discovery interface 3310 show ethernet oam IFNAME 3308 show ethernet oam interface statistics 3312 show ethernet oam status interface 3313 show evb ecp statistics 3557 show evb interface 3558 show evb vdp vsi-info 3559 show evb-bridge 3560 show flowcontrol interface 1182 show gmrp configuration 1458, 1474 show gmrp machine 1459, 1475 show gmrp statistics 1460 show gmrp timer 1461 show gvrp statistics 1476, 1491 show gvrp timer 1477 show hardware-information 1022 show hosts 252 show interface errdisable status 700 show interface irb 5023 show interface switchport bridge 1207 show ip bgp rtfilter all 2234 show ip dhcp relay 365 show ip dhcp relay address interface 366 show ip extcommunity-list 2240 show ip forwarding 823 show ip igmp groups 2800 show ip igmp interface 2802 show ip igmp snooping mrouter 2840 show ip igmp snooping statistics 2846 show ip interface brief 824 show ip mroute 2766 show ip msdp peer 2911 show ip msdp sa-cache 2912 show ip mvif 2769 show ip ospf 2335
border routers 2339
show ip ospf border-routers 2339 show ip ospf igp-shortcut-lsp 2349 show ip ospf igp-shortcut-route 2350 show ip ospf interface 2351 show ip ospf neighbor 2356 show ip ospf route 2360 show ip ospf segment-routing announce-list 4164 show ip ospf segment-routing capability 4165 show ip ospf segment-routing prefix-sid 4167 show ip ospf te-database 2477 show ip ospf virtual-links 2363 show ip pim bsr-router 2914 show ip pim rp mapping 2988 show ip pim rp-hash 2925, 2987 show ip prefix-list 839 show ip protocols 2556 show ip protocols bgp 2241 show ip protocols ospf 2365 show ip protocols rip 2629 show ip rip command 2631 show ip rip database vrf 2672 show ip rip interface 2633 show ip vrf 833 show ipsec status 1016 show ipv6 dhcp relay 367 show ipv6 dhcp relay address 368 show ipv6 dhcp relay address interface 369 show ipv6 forwarding 834 show ipv6 interface brief 835 show ipv6 isis route 2557 show ipv6 mld groups 2828 show ipv6 mld interface 2830 show ipv6 ospf database 2442 show ipv6 ospf database, router 2437 show ipv6 ospf interface 2446 show ipv6 ospf neighbor 2448 show ipv6 ospf route 2451 show ipv6 ospf te-database 2479 show ipv6 ospf topology 2454 show ipv6 ospf virtual-links 2456 show ipv6 ospf6 interface 2446 show ipv6 rip interface 2665 show ipv6 route 837 show ipv6 rpf 658 show ipv6 vrf 2458 show isis counter 2557 show isis database command 2558 show isis interface 2561 show isis tag database command 2564 show isis topology 2566 show isis-spb configuration 3729 show isis-spb fdb 3730 show isis-spb interface 3731 show isis-spb lsp 3732 show isis-spb neighbors 3733 show isis-spb topology 3734 show lacp-counter command 1315 show ldap-server 481 show list 660 show lldp interface 3186 show lldp port 3182, 3329 show logging 321 show logging

last 323 show logging logfile 324 show logging logfile last-index 325 show logging logfile start-seqn end-seqn 326 show logging logfile start-time end-time 327 show mac address-table count bridge 1209 show mcec statistics 1340 show mlag conversation-id 1335 show mlag detail 1335
show mlag summary 1337 show mld snooping mrouter 2854 show mld snooping statistics 2855 show mls qos 4621 show mls qos aggregator-policer 4622 show mls qos interface 4624 show mmrp configuration 1489 show mmrp machine 1490 show mmrp timer 1492 show mvrp configuration 1503 show mvrp machine bridge 1504 show mvrp statistics 1505 show mvrp timer 1506 show nsm client 661 show ntp
authentication-keys 349 show ntp authentication-status 350 show ntp client 351 show ntp logging-status 351 show ntp peers
353 show ntp peer-status 352 show ntp statistics 354 show ntp status 356 show ntp trusted-keys 356 show nvo vxlan 5000 show nvo vxlan arp-cache 5003 show nvo vxlan counters access-port 5004 show nvo vxlan counters network-port 5005 show nvo vxlan interface counters 5006 show nvo vxlan irb-status 5021 show nvo vxlan mac-table 5008 show nvo vxlan nd-cache 5010 show nvo vxlan static host state 5011 show nvo vxlan tunnel 5013 show poe port 562 show poe power-configuration 559 show poe power-management 560 show poe power-status 561 show poe pse 558 show policy-map 4625, 4791 show policy-map interface 4792 show port etherchannel command 1316 show priority-flow-control details 1037 show privilege 618 show process 593 show qos-access-list 4626 show radius-server 449 show rmon alarm 968 show rmon event 969 show rmon history 970 show rmon statistics 971 show role name 332 show router-id 696, 701 show running-config
594 show running-config aaa 437 show running-config access-list 595 show running-config as-path access-list 596 show running-config community-list 597 show running-config control-adjacency 947 show running-config dhcp 370

show running-config dns 253 show running-config interface 841 show running-config interface igmp 598 show running-config interface ip 843 show running-config interface ipv6 844 show running-config interface irb 5022 show running-config interface isis 2568 show running-config interface multicast 599 show running-config ipv6 access-list 846 show running-config ldap 482 show running-config ntp 357 show running-config nvo vxlan 5014 show running-config prefix-list 600 show running-config radius 450 show running-config route-map 750 show running-config router isis 2569 show running-config router vrrp 4210 show running-config router-id 702 show running-config snmp 279 show running-config ssh server 260 show running-config switch 664 show running-config syslog 328 show running-config tacacs+ 464 show running-config telnet server 301 show running-config vrf 601 show sflow 4521 show sflow interface 4523 show snmp 280 show snmp community 281 show snmp engine-id 282 show snmp group 283 show snmp host 284 show snmp user 285 show snmp view 286 show spanning-tree 1256 show spanning-tree mst 1260 show spanning-tree statistics 1262 show spb adjacency 3735 show spb bridge vlan 3736 show spb service bridge 3737 show ssh key 261 show ssh server 262 show startup-config 667 show synce details 4501 show synce input-sources 4502 show synce output-sources 4503 show system-information 1026 show tacacs-server 465 show te-link 932 show telnet server 302 show tfo 3771 show transceivers details 1039 show user-account 332 show username 263 show users 604 show version 668 show vlan access-map 1365 show vlan all 1366 show vlan auto 1368

show vlan brief 1368 show vlan classifier 1369 show vlog all 624 show vlog clients 625 show vlog terminals 626 show vlog virtual-routers 627 shutdown 941, 4979, 5023, 5025
SID 4117
Simple Network Management Protocol 213
SMUX 104
snmp restart bfd 4328 snmp restart mstp 1185 snmp-server community 287 snmp-server contact 288 snmp-server enable snmp 289 snmp-server enable traps 290 snmp-server group 291 snmp-server host 291 snmp-server location 293 snmp-server tcp-session 294 snmp-server user 295 snmp-server view 296 Sockets 133 soft-reconfiguration 2121 Source
134 source routing 4117 source-based trees 2696 Spanning Tree Protocol 110 spanning-tree autoedge 1265 spanning-tree edgeport 1266 spanning-tree guard root 1267 spanning-tree hello-time 1268 spanning-tree instance restricted-role 1268 spanning-tree instance restricted-tcn 1269 spanning-tree link-type 1270

spanning-tree mst configuration 1271 spanning-tree restricted-role 1275 spanning-tree restricted-tcn 1276 spanning-tree spvts+ configuration 1291 spanning-tree te-msti configuration 1277 spanning-tree vlan path-cost 1292 spanning-tree vlan restricted-role 1292 spanning-tree vlan restricted-tcn 1293 spb configuration 3723
spb enable 3724
SPF
debug 4051
square brackets command
syntax 88
SRGB 4117
SSH Client session 165 ssh key 269 SSH Keys 164 ssh login-attempts 270 ssh server port 271 stale route 2227 static neighbor table 3978 static-channel-group 1322 storm-control level 1278, 4799
STP
configuring 1047
STP commands
bridge cisco-interoperability 1217 bridge forward-time 1191 bridge instance priority 1219 bridge max-age 1194 bridge max-hops 1195 bridge multiple-spanning-tree enable 1222 bridge priority 1196 bridge rapid-spanning-tree enable 1226 bridge region 1227 bridge revision 1228 bridge shutdown 1197 bridge spanning-tree enable 1229 bridge spanning-tree errdisable-timeout enable 1230 bridge spanning-tree portfast bpdu-filter 1233 bridge transmit-holdcount 1198 bridge-group path-cost 1200 bridge-group priority 1201 clear spanning-tree detected protocols 1242 customer-spanning-tree customer-edge path-cost 1244 customer-spanning-tree customer-edge priority 1245 customer-spanning-tree forward-time 1246 customer-spanning-tree hello-time 1247 customer-spanning-tree max-age 1248 customer-spanning-tree priority 1249 customer-spanning-tree provider-edge path-cost 1250 customer-spanning-tree provider-edge priority 1251 customer-spanning-tree transmit-holdcount 1252 debug mstp 1253 show debugging mstp 1255 show spanning-tree 1256 show spanning-tree mst 1260 show spanning-tree statistics 1262 spanning-tree autoedge 1265 spanning-tree edgeport 1266 spanning-tree guard root 1267 spanning-tree hello-time 1268 spanning-tree instance restricted-role 1268 spanning-tree instance restricted-tcn 1269 spanning-tree link-type 1270 spanning-tree mst configuration 1271 spanning-tree restricted-role 1275 spanning-tree restricted-tcn 1276 String 133 summary-address 2370, 2460, 2544 suppressed route 2227 SVI 1961 switch virtual interface (SVI) 1961 switchport 1212 switchport access vlan 1371 switchport beb customer-backbone 3725 switchport customer-edge 3195 switchport customer-edge default-svlan 3196 switchport customer-edge hybrid allowed vlan 3197 switchport customer-edge vlan registration 3199 switchport customer-network vlan translation 3202 switchport hybrid allowed vlan 1372 switchport mode 3206 switchport mode access 1375 switchport mode customer-edge access 3207 switchport mode customer-edge hybrid 3208 switchport mode hybrid 1376, 1377 switchport mode ingress-filter 3206 switchport mode sbp 3561 switchport mode trunk 1378 switchport mode uap 3562 switchport private-vlan host-association 1384 switchport private-vlan mapping 1385 switchport provider-edge vlan 3209 switchport provider-network vlan translation 3210 switchport trunk allowed vlan 1379 switchport trunk native vlan 1382 switch-source 4493

SYN PTP commands
announceinterval4436
announce timeout-interval 4437 clock-port 4438 fault-recover 4446 show ptp foreign-master 4456
synce (configure mode) 4494
synce (interface mode) 4495
syncedebug4496
synchronization4427
synchronization command 2139 synchronization option 4497

T

tacacs-server deadtime 467 tacacs-server directed-request 467 tacacs-server host 467 tacacs-server key 469 Tail-Drop Configuration 4701 tail-drop threshold 4628 Telnet 297 telnet server port 305 tenant 4807 terminology
PIM-DM 2733 TIB 2695
time
command syntax 88

timers 2638 timers basic 2666
timers lsa arrival 2371 timers
throttle lsa 2373 Topology
1111 traceroute 620 Traffic
Engineering 126 transmit
delay 2351 transmit-delay
2429 transparent clock 4413
trap notification on the PSE
543 Tree Information Base
2695 trigger failover 3772
Trigger Failover Commands 3765

TRILL IS-IS commands trill
pseudonode 4096 trill-isis
csnp-interval 4030 trill-isis
hello-interval 4031 trill-isis
hello-interval minimal 4032
trill-isis hello-multiplier 4033
trill-isis lsp-interval 4034 trill-
isis metric 4035 trill-isis port-
priority 4036
trill-isis retransmit-interval 4037
Trust DSCP on Layer 2 Interface
Configuration 4647 tunnel checksum 951 tunnel
destination 952, 1874 Tunnel End Point 4807
tunnel interface, creating
between PIM-DM routers 2755
between PIM-SM routers 2755
tunnel mode 954, 955
tunnel path-mtu-
discovery 956 tunnel
source 957 tunnel tos 958
tunnel ttl 959
Tunneling 1863
Tunneling and Transitioning 1863
Tunneling Commands 949
interface tunnel 950
tunnel checksum 951
tunnel destination 952
tunnel mode 954, 955
tunnel path-mtu-
discovery 956 tunnel
source 957 tunnel tos 958
tunnel ttl 959

U

UDLD configuration 3743
UDP 4391, 4392, 4402
unconfiguration of auth-mac
1167 undebug all pim sparse-
mode 2928 unicast
configuration 4809 unicast
tunnel 4817 update-delay
2040 username 333 username
keypair 273 username sshkey
272

V

valid route 2227 validation 3068
validation commands 3060, 3064
verifying PIM-SM on VR configuration
2724 verifying PIM-SMv6 on VR
configuration 2732 version 2639 vertical
bars

command syntax 87
Virtual eXtensible Local Area Network
(VXLAN) 4807 virtual IP address 4218

virtual IPv6 address 4231
virtual links 1683 Virtual
Local Area Network 107
Virtual MAC command 4220
Virtual Router Redundancy Protocol (VRRP)
1969 Virtual routing and forwarding (VRF) 1953
virtual-ip 4218 virtual-ip command 4231 vlan
classifier ipv4 1390
VLAN commands show vlan
access-map 1365 show vlan all
1366 show vlan auto 1368 show
vlan brief 1368 show vlan
classifier 1369 switchport access
vlan 1371 switchport hybrid
allowed vlan 1372 switchport
mode access 1375 switchport
mode hybrid 1376, 1377
switchport mode trunk 1378
switchport trunk allowed vlan
1379 switchport trunk native vlan
1382 vlan classifier ipv4 1390 vlan
database 1392 vlan state 1394
vlan database command
1392 VLAN interfaces 1859,
1897 vlan state 1394 vlan
type 3211
VLOG commands 623 reset
log file 624 show vlog all
624 show vlog clients 625
show vlog terminals 626
show vlog virtual-routers
627
VPN Commands ip
vrf 777 ip vrf
forwarding 777
show ip vrf 833
VR Commands
configuration file 4358
description 4359
login virtual-router 4363

VRF 2465
VRF Configuration 1953
VRRP 119
VRRP Commands 4199, 4221 circuit-failover 4223 debug vrrp 4203 disable 4204, 4224 enable 4205, 4225 preempt-mode 4207, 4226 priority 4227 show debugging vrrp 4209 show running-config router vrrp 4210 virtual-ip 4218 vrrp vmac 4220
VRRP process 4173
VRRPv6 Commands
router ipv6 vrrp 4228 virtual-ip 4231
VXLAN Architecture 4807 VXLAN Commands 4945
vxlan host-reachability-protocol evpn-bgp 5026
VXLAN Multicast Configuration 4817
VXLAN Network Identifier (VNI) 4807
VXLAN Tunnel EndPoints 4807
VXLAN Unicast Configuration 4809

W

wait-to-restore 4498 Weights for Queues Configuration 4649
WORD 88
WRED Configuration 4693 WRED Configuration for MLS 4555 write terminal 621 wrr-queue dscp-map 4631 wrr-queue queue-limit 4631 wrr-queue random-detect max-threshold 4631