SYMANITRON

Инновационные
промышленные сети

Руководство по настройке линейки промышленных коммутаторов на DIN-рейку

Управление через WEB-интерфейс

WEB-интерфейс

Оглавление

Введение

В руководстве описаны программные функции промышленного коммутатора XXX1, а также приводится детальная информация по его настройке при помощи веб-интерфейса.

Условные обозначения

1. Условные обозначения в тексте

Формат	Описание
< >	Скобки < > обозначают «кнопки». Например, нажмите кнопку <Apply>
[ ]	Скобки [ ] обозначают имя окна или имя меню. Например, нажмите пункт меню [File]
→	Мультиуровневое меню разделяется посредством знака «→». Например, [Start] → [All Programs] → [Accessories]. Нажмите меню [Start], войдите в подменю [All programs], затем войдите в подменю [Accessories]
/	Выбор одной, двух или более опций при помощи символа «/». Например, «Add/Subtract» означает добавить или удалить

2. Условные обозначения CLI

Формат	Описание
Bold	Означает команды и ключевые слова. Например, **show version** будет показываться с использованием шрифта **Bold**
{*Italic*}	Указывает на значение параметра, которое необходимо ввести. Например, для команды **show vlan** {*vlan id*} вместо {*vlan id*} следует вводить актуальный идентификатор VLAN

3. Условные символы

Символ	Описание
 **Заметка**	Необходимые пояснения к содержимому выполняемых операций с устройством

1. Базовая конфигурация

1.1 Настройка HTTP

Коммутаторы могут быть настроены не только через интерфейс командной строки (CLI) и SNMP-протокол, но и через веб-интерфейс. Они поддерживают настройку порта службы HTTP, настройку времени передачи сообщения об аномальном состоянии и другие функции.

1.1.1 Выбор языка

Выбор языка системы осуществляется в режиме глобальной конфигурации через командную строку, как показано ниже.

Команда	Описание
[no] **ip http language** {english}	Установка английского языка для веб-интерфейса

1.1.2 Настройка порта HTTP

Обычно HTTP-портом по умолчанию является порт 80, и пользователи могут получить доступ к коммутатору, введя IP-адрес напрямую; однако коммутаторы также позволяют изменять сервисный порт, после чего для доступа необходимо будет указывать не только IP-адрес, но и измененный номер порта.

Например, если вы настроили IP-адрес и порт службы HTTP как 192.168.2.1 и 1234 соответственно, адрес доступа по HTTP должен быть изменен на http:// 192.168.2.1:1234. Лучше не использовать порты других распространенных протоколов, чтобы не произошло коллизии доступа. Например, FTP – 20, TELNET – 23, DNS – 53, SNMP – 161. Поскольку порты, используемые многими протоколами, трудно запомнить, лучше использовать для идентификаторов портов номера больше 1024.

Команда	Описание
ip http port {*portNumber*}	Настройка служебного порта HTTP

1.1.3 Включение службы HTTP

Коммутаторы поддерживают управления доступом при помощи HTTP. Только когда служба включена, может происходить обмен данными HTTP между коммутатором и ПК. Когда служба отключена, обмен прекращается. Настройте глобальную службу HTTP с помощью следующей команды:

Команда	Описание
ip http server	Включает службу HTTP

1.1.4 Настройка режима доступа HTTP

Вы можете получить доступ к коммутатору в двух режимах: HTTP и HTTPS. Используйте следующую команду, чтобы установить режим доступа HTTP:

Команда	Описание
ip http http-access enable	Устанавливает режим доступа HTTP

1.1.5 Настройка максимального количества VLAN для отображения на веб-странице

Коммутатор позволяет установить значение от 1 до 4094 в режиме глобальной конфигурации (4094 — максимальное значение, значение max-vlan по умолчанию — 100).

Команда	Описание
ip http web max-vlan {*max-vlan*}	Устанавливает максимальное число VLAN, отображаемых на веб-странице

1.1.6 Настройка максимального количества IGMP-групп для отображения на веб-странице

Коммутатор позволяет установить значение от 1 до 100 в режиме глобальной конфигурации (100 — максимальное значение, значение max-vlan по умолчанию — 15).

Команда	Описание
ip http web igmp-groups {*igmp-groups*}	Устанавливает максимальное число IGMP-групп, отображаемых на веб-странице

1.2 Настройка HTTPS

Чтобы повысить безопасность связи, коммутаторы поддерживают не только протокол HTTP, но и HTTPS. HTTPS – это HTTP-канал, предназначенный для обеспечения безопасности, и он использует протокол SSL для создания защищенной связи между клиентом и сервером.

1.2.1 Настройка режима доступа HTTPS

Запустите следующую команду, чтобы установить режим доступа HTTPS:

Команда	Описание
ip http ssl-access enable	Устанавливает режим доступа HTTPS

1.2.2 Настройка порта HTTPS

Аналогично HTTP, HTTPS имеет свой служебный порт по умолчанию – порт 443. Вы также можете запустить следующую команду, чтобы изменить служебный порт HTTPS. Рекомендуется использовать значение ID выше 1024, чтобы избежать конфликтов с портами других протоколов.

Команда	Описание
ip http secure-port {*portNumber*}	Устанавливает HTTPS-порт

2. Доступ к коммутатору

2.1 Доступ к коммутатору через HTTP

При доступе к коммутатору с помощью Web убедитесь, что используемый браузер соответствует следующим требованиям:

- HTML не ниже версии 4.0
- HTTP не ниже версии 1.1
- JavaScriptTM не ниже версии 1.5

Кроме того, убедитесь, что основной программный файл, работающий на коммутаторе, поддерживает доступ в Интернет, а ваш компьютер уже подключен к сети, в которой находится коммутатор.

2.1.1 Первоначальный доступ к коммутатору

При первоначальном доступе к коммутатору вы можете использовать веб-интерфейс без каких-либо дополнительных настроек:

1. Измените IP-адрес сетевого адаптера и маску подсети вашего компьютера на 192.168.2.2 и 255.255.255.0 соответственно.
2. Откройте веб-браузер и введите 192.168.2.1 в адресную строку. Этот адрес является адресом управления коммутатором по умолчанию.
3. Введите в диалоговом окне имя пользователя и пароль «admin». Данные аутентификации являются регистрозависимыми.

4. После успешной аутентификации систематизированная информация о коммутаторе появится в браузере.

2.1.2 Обновление до веб-версии

После обновления прошивки до версии, поддерживающей веб-интерфейс, если у коммутатора уже были сохранены рабочие файлы конфигурации, прямой доступ к нему через веб-интерфейс становится невозможным. Для исправления этой ситуации выполните следующие шаги один за другим:

1. Подключитесь с помощью вспомогательного кабеля к консольному порту коммутатора или по telnet к адресу управления коммутатором через компьютер.
2. Войдите в режим глобальной настройки коммутатора через командную строку (приглашение DOS – «Switch_config#»).
3. Если адрес управления коммутатором не настроен, создайте интерфейс VLAN и настройте IP-адрес.
4. Введите команду **ip http server** в режиме глобальной настройки и запустите веб-службу.
5. Запустите **username**, чтобы установить имя пользователя и пароль для коммутатора. После выполнения вышеуказанных операций вы можете ввести адрес коммутатора в веб-браузере и получить доступ к коммутатору.
6. Выполните **write**, чтобы сохранить текущие настройки в файле конфигурации.

2.2 Доступ к коммутатору через безопасное соединение

Данные между веб-браузером и коммутатором не будут зашифрованы, если вы получаете доступ к коммутатору через обычный HTTP. Чтобы зашифровать эти данные, вы можете использовать безопасное соединение, основанное на протоколе SSL.

Для этого следует выполнить следующие шаги:

1. Подключитесь с помощью вспомогательного кабеля к консольному порту коммутатора или по telnet к адресу управления коммутатором через компьютер.
2. Войдите в режим глобальной настройки коммутатора через командную строку (приглашение DOS – «Switch_config#»).
3. Если адрес управления коммутатором не настроен, создайте интерфейс VLAN и настройте IP-адрес.
4. Введите команду **ip http server** в режиме глобальной настройки и запустите веб-службу.
5. Запустите **username**, чтобы установить имя пользователя и пароль для коммутатора.
6. Запустите **ip http ssl-access enable**, чтобы включить безопасный доступ к коммутатору.

7. Запустите **no ip http http-access enable**, чтобы запретить доступ к коммутатору через небезопасное соединение HTTP.
8. Выполните **write**, чтобы сохранить текущие настройки в файле конфигурации.
9. Откройте веб-браузер на ПК, к которому подключается коммутатор, введите https://192.168.2.1 в адресной строке (192.168.2.1 — это IP-адрес управления коммутатором) и нажмите клавишу Enter. После выполнения вышеуказанных операций к коммутатору можно получить доступ через безопасное соединение.

2.3 Введение в веб-интерфейс

Домашняя страница интерфейса появляется после входа в систему. Вся домашняя страница состоит из верхней панели управления, панели навигации, области отображения конфигурации и нижней панели управления.

2.3.1 Верхняя панель управления

Рисунок 1 – Верхняя панель управления

Save	Запись текущих настроек в файл конфигурации устройства. Эта функция эквивалентна выполнению команды **write**. Конфигурация, выполненная через веб-интерфейс, не будет сразу же записана в файл конфигурации после проверки. Если нажать «Save», несохраненные настройки будут утеряны после перезагрузки
English	Переключает интерфейс на английскую версию

2.3.2 Панель навигации

Рисунок 2 – Панель навигации

Содержимое панели навигации отображается в виде списка и классифицируется по типам. По умолчанию список расположен в разделе [System]. Если необходимо настроить определенный элемент, выберите имя группы, а затем подпункт. Например, чтобы просмотреть поток трафика текущего порта, вам нужно нажать [Diagnostics] → [Ports] → [Statistics Table].

Пользователь с ограниченными правами может только просматривать состояние устройства и не может изменять конфигурацию. Если вы входите в веб-интерфейс с ограниченными правами, появится только пункт [System].

2.3.3 Область отображения конфигурации

Рисунок 3 – Область отображения конфигурации

Область отображения конфигурации показывает состояние и конфигурацию устройства. Содержимое этой области можно изменить, нажав элементы на панели навигации.

2.3.4 Нижняя панель управления

Рисунок 4 – Нижняя панель управления

В нижней части области конфигурации всегда содержится панель с одной или несколькими кнопками. Их функции перечислены в следующей таблице:

Set	Применяет измененную конфигурацию к устройству. Применение конфигурации не означает, что настройки сохраняются в файле конфигурации. Чтобы сохранить конфигурацию, необходимо нажать «Save» на верхней панели управления.
Reload	Обновляет содержимое, отображаемое в текущей области конфигурации
Create	Создает элемент списка. Например, вы можете создать VLAN или нового пользователя
Delete	Удаляет элемент в списке
Go back	Возвращает на страницу настроек предыдущего уровня
Clear	Очищает содержимое текущей конфигурации, например, статистику порта

3. Основные настройки

Рисунок 5 – Меню основных настроек на панели навигации

3.1 Информация о системе

Если нажать [Basic Settings] → [System] на панели навигации, появится страница, показанная на рисунке:

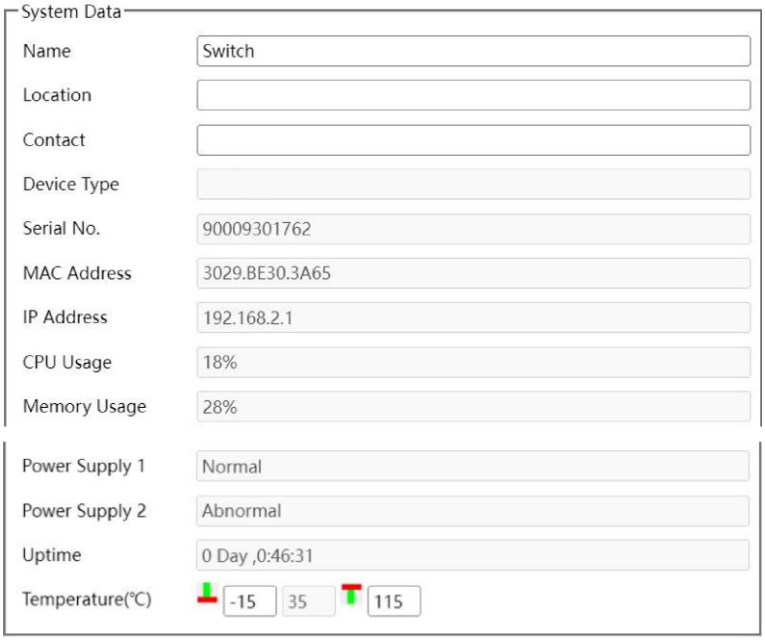


Рисунок 6 – Информация о системе

В диалоговом окне отобразится информация о системе. Имя устройства по умолчанию – «Switch». Вы можете ввести новое имя хоста в текстовое поле и затем нажать <Set>.

3.2 Режим глобальной конфигурации (интерфейс управления)

Если нажать [Basic Setting] → [Global Network Config] на панели навигации, появится страница, показанная на рисунке:

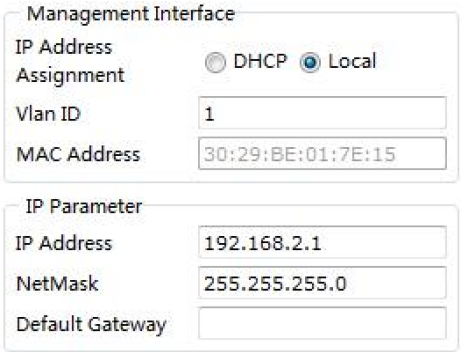


Рисунок 7 – Настройка IP-адреса интерфейса VLAN 1 для доступа к коммутатору

Эта страница используется для настройки IP-адреса порта Vlan 1 на интерфейсе управления. В исходных условиях на этой странице появятся MAC-адрес устройства, IP-адрес, маска и шлюз интерфейса.

3.3 Конфигурация портов

Для настройки портов нажмите [Basic Setting] → [Port Configuration] на панели навигации.

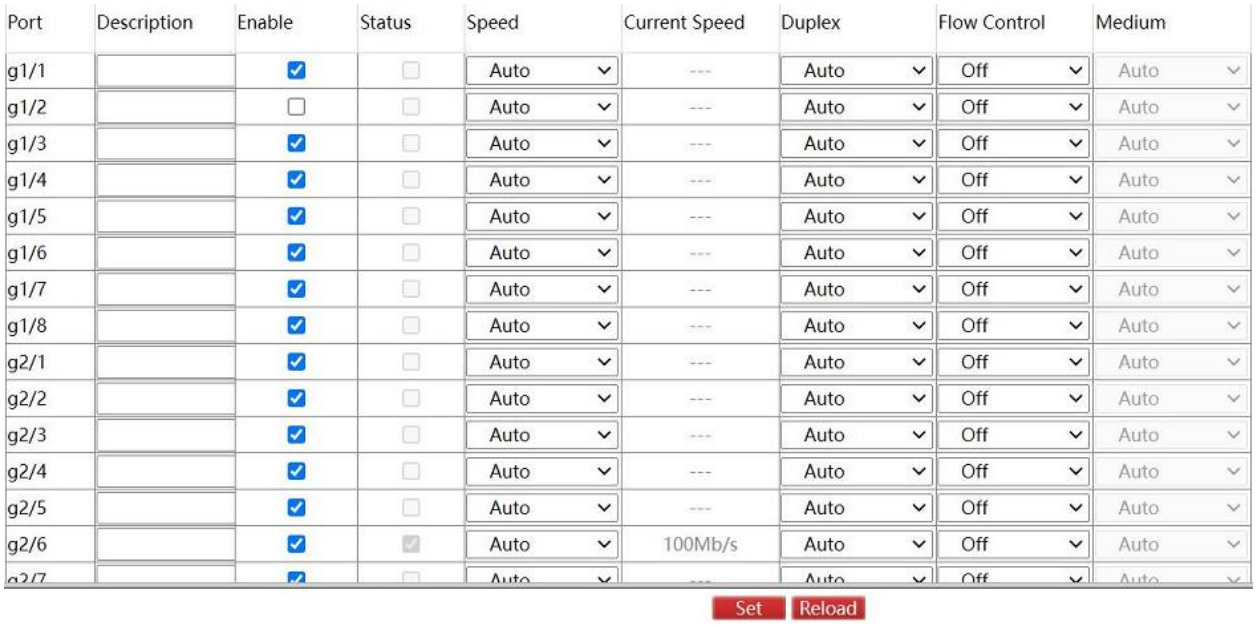


Рисунок 8 – Конфигурация портов

На этой странице вы можете изменить статус, скорость, дуплексный режим и управление потоком порта.

При изменении скорости или дуплексного режима может произойти переключение порта. В таком случае сетевая связь будет нарушена.

3.4 Автоматическое отключение

Нажмите [Basic Setting] → [auto-shutdown] на панели навигации, появится страница, показанная на следующем рисунке:

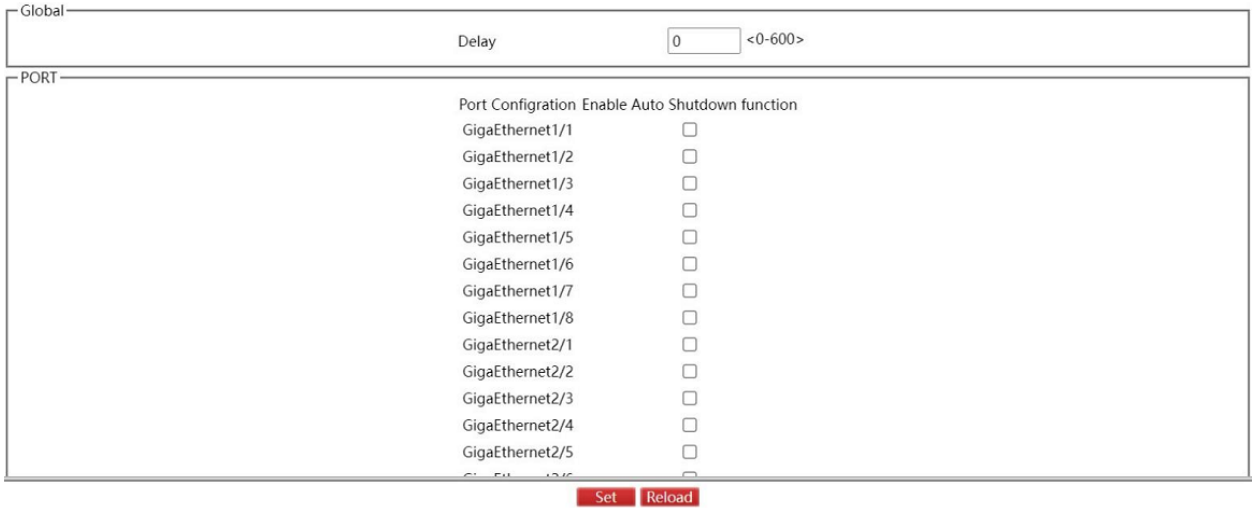


Рисунок 9 – Автоматическое отключение портов

На этой странице активируется функция автоматического выключения порта и задается время задержки выключения. Нажмите <Set> на нижней панели управления, чтобы завершить настройку, и нажмите <Save> вверху. Соответствующий порт будет отключен через заданное время после включения коммутатора.

3.5 Программное обеспечение

Если нажать [Basic Setting] → [Software] на панели навигации, появится страница, показанная на рисунке:

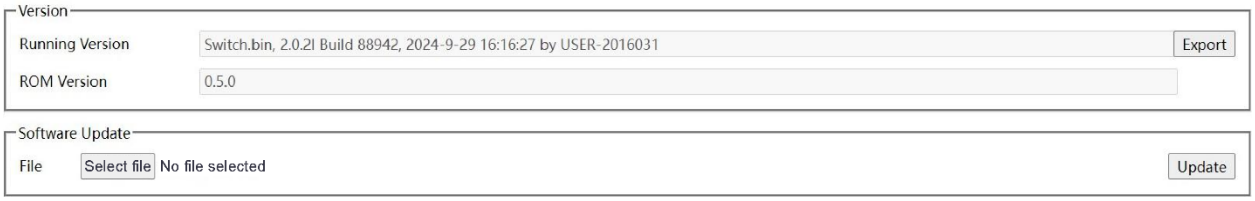


Рисунок 10 – Программное обеспечение

На этой странице можно проверить текущую рабочую версию и версию прошивки. Нажмите <Export>, чтобы экспортировать текущую версию на компьютер. В поле «Software Update» выберите файл с версией программного обеспечения, которую вы хотите установить, и нажмите <Update> для установки.

Программное обеспечение обновленной системы вступит в силу только после перезагрузки устройства.

3.6 Сохранение/загрузка

Если нажать [Basic Setting] → [Save/Load] на панели навигации, появится страница, показанная на рисунке:

Рисунок 11 – Сохранение/загрузка

Нажмите <Export>, после чего текущая конфигурация системы будет экспортирована на компьютер. Если вы нажмете <Import>, соответствующий файл конфигурации будет импортирован на коммутатор.

3.7 Перезапуск

Если нажать [Basic Setting] → [Restart] на панели навигации, появится страница, показанная на следующем рисунке:

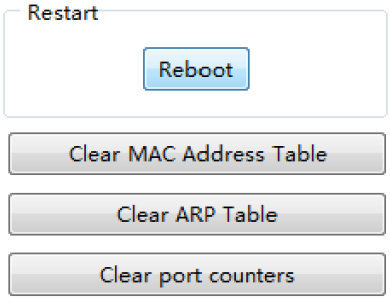


Рисунок 12 – Перезапуск

Чтобы перезагрузить коммутатор нажмите <Reboot>. Также данное меню позволяет очистить таблицу MAC-адресов, таблицу ARP, счетчики портов.

3.8 Заводские настройки

Рисунок 13 – Сброс до заводских настроек

На этой странице вы можете восстановить заводские настройки оборудования. Нажмите кнопку <Restore>, чтобы сбросить настройки до заводских.

4. Безопасность

Рисунок 14 – Меню безопасности на панели навигации

4.1 Управление пользователями

4.1.1 Управление пользователями

Если нажать [Security] → [User Management] на панели навигации, появится страница, показанная на рисунке:

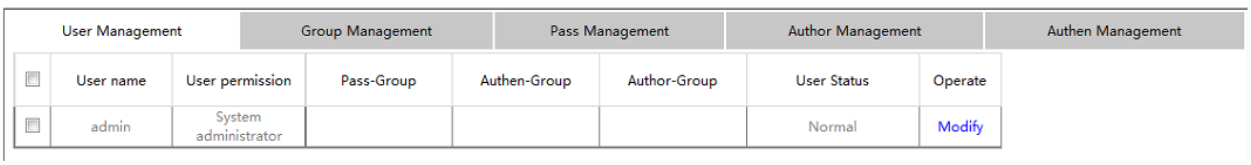


Рисунок 15 – Управление пользователями

Нажмите <Modify>, чтобы изменить конфигурацию пользователя. Для удаления выбранного пользователя нажмите <Delete> на нижней панели.

Нажмите <Create> на нижней панели, чтобы перейти на следующую страницу:

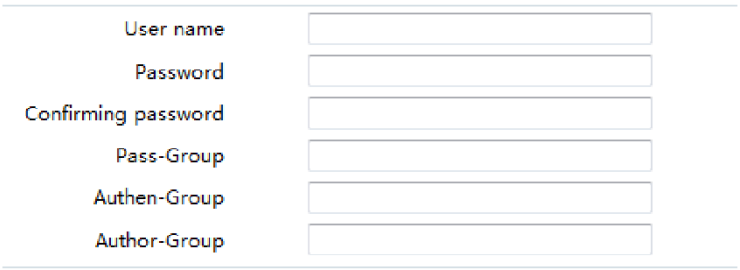


Рисунок 16 – Настройка нового пользователя

Заполните параметры в каждом поле конфигурации и нажмите <Set> на нижней панели, чтобы создать нового пользователя. Нажмите <Reload>, чтобы обновить информацию о пользователе. Нажмите <Go back>, чтобы вернуться на страницу предыдущего уровня.

4.1.2 Управление группами

Нажмите [Security] → [User Management] → [Group Management] чтобы открыть страницу настройки управления группами.

Рисунок 17 – Управление группами

Нажмите <Modify>, чтобы изменить конфигурацию группы пользователей. Выберите группу и нажмите <Delete> на нижней панели, чтобы удалить ее. Нажмите <Detail>, чтобы проверить и настроить параметры членов группы:

Рисунок 18 – Члены группы

Нажмите <Create> на нижней панели страницы управления группой, чтобы перейти на следующую страницу:

Рисунок 19 – Настройка новой группы

Заполните параметры в каждом поле конфигурации и нажмите <Set> на нижней панели, чтобы создать новую группу.

4.1.3 Управление политикой паролей

Нажмите [Security] → [User Management] и выберите вкладку [Pass Management], чтобы открыть страницу настройки правил политики паролей.

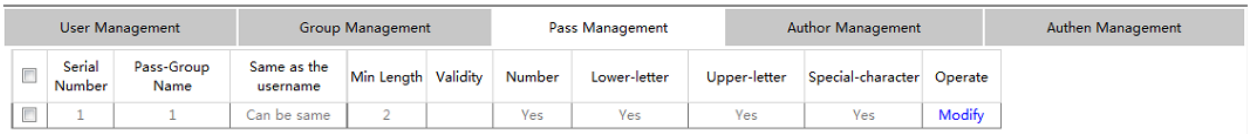


Рисунок 20 – Политики паролей

Нажмите <Modify>, чтобы изменить правила политики. Выберите политику и нажмите <Delete> на нижней панели, чтобы удалить ее.

Нажмите <Create> на нижней панели страницы управления группой, чтобы перейти на следующую страницу:

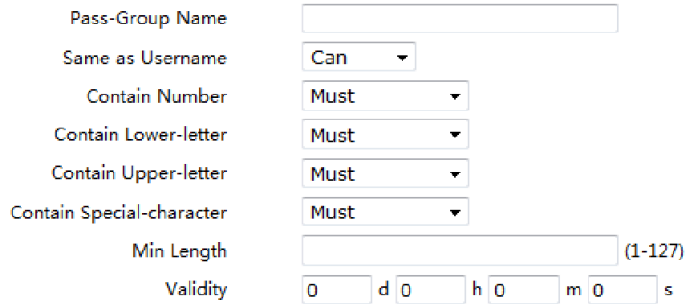


Рисунок 21 – Настройка правил политики паролей

Заполните параметры в каждом поле конфигурации и нажмите <Set> на нижней панели, чтобы создать новую политику.

4.1.4 Управление политикой авторизации

Нажмите [Security] → [User Management] и выберите вкладку [Author Management], чтобы открыть страницу настройки политики авторизации.

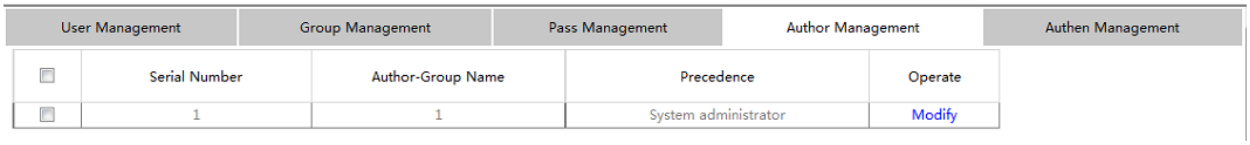


Рисунок 22 – Политики авторизации

Нажмите <Modify>, чтобы изменить правила политики. Выберите политику и нажмите <Delete> на нижней панели, чтобы удалить ее.

Нажмите <Create> на нижней панели страницы управления группой, чтобы перейти на следующую страницу:

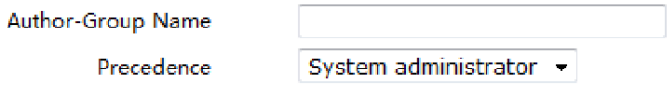


Рисунок 23 – Настройка правил политики авторизации

Заполните параметры в каждом поле конфигурации и нажмите <Set> на нижней панели, чтобы создать новую политику.

4.1.5 Управление политикой аутентификации

Нажмите [Security] → [User Management] и выберите вкладку [Authen Management], чтобы открыть страницу настройки политики аутентификации.

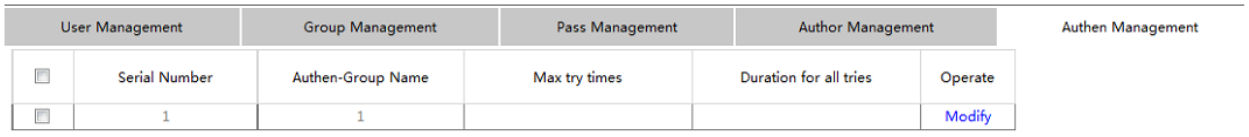


Рисунок 24 – Политики аутентификации

Нажмите <Modify>, чтобы изменить правила политики. Выберите политику и нажмите <Delete> на нижней панели, чтобы удалить ее.

Нажмите <Create> на нижней панели страницы управления группой, чтобы перейти на следующую страницу:

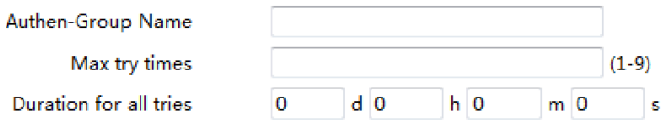


Рисунок 25 – Настройка правил политики аутентификации

Заполните параметры в каждом поле конфигурации и нажмите <Set> на нижней панели, чтобы создать новую политику.

4.2 Управление доступом

4.2.1 Службы

На этой странице можно настроить службы HTTP, HTTPS, SSH и SNMP. Нажмите [Security] → [Management Access] → [Server] на панели навигации, чтобы войти на страницу настройки. Выберите вкладку [HTTP] на этой странице, чтобы открыть раздел настройки HTTP.

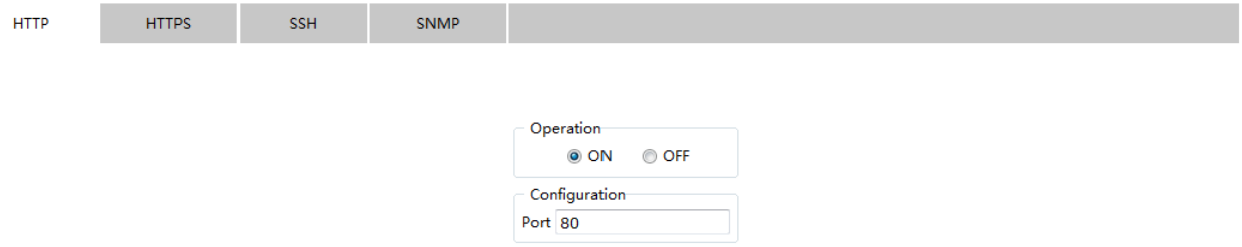


Рисунок 26 – Настройка HTTP

Для настройки HTTPS Выберите вкладку [HTTPS]:

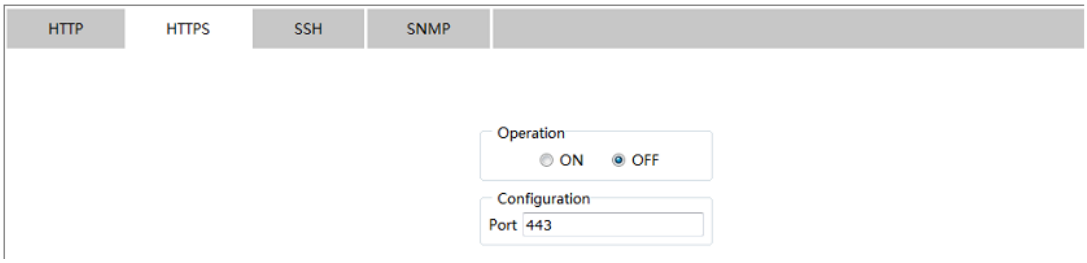


Рисунок 27 – Настройка HTTPS

Для настройки SSH выберите вкладку [SSH]:

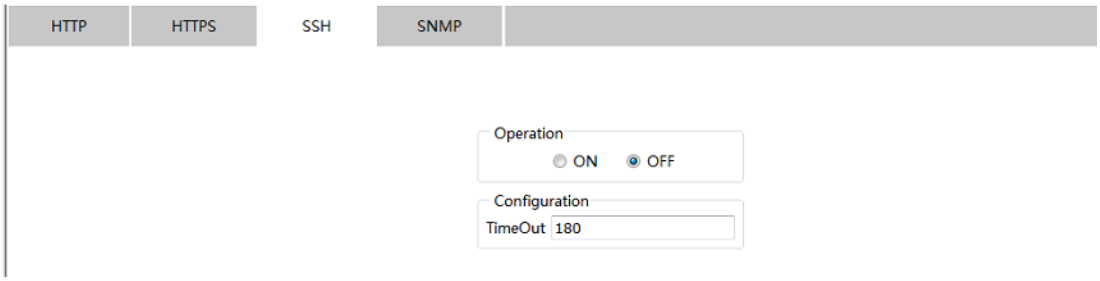


Рисунок 28 – Настройка SSH

Для настройки SNMP выберите вкладку [SNMP]:

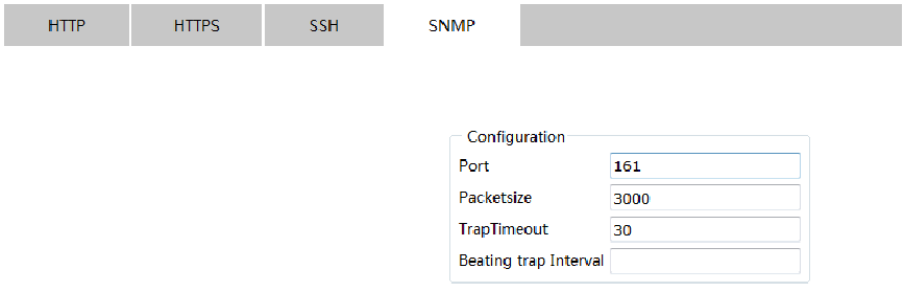


Рисунок 29 – Настройка SNMP

4.2.2 Настройка комьюнити SNMPv1/v2

Нажмите [Security] → [Management Access] → [SNMPv1/v2 Community] на панели навигации, чтобы войти на страницу настройки.

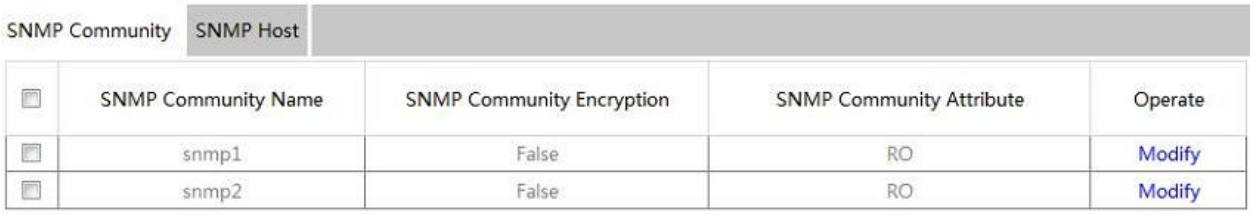


Рисунок 30 – SNMP-комьюнити

Для изменения параметров нажмите <Modify>. Для создания нового комьюнити нажмите <Create>:

Рисунок 31 – Создание SNMP-комьюнити

Для удаления комьюнити нажмите <Delete>.

Чтобы перейти в раздел конфигурации хостов выберите вкладку [SNMP Host]:

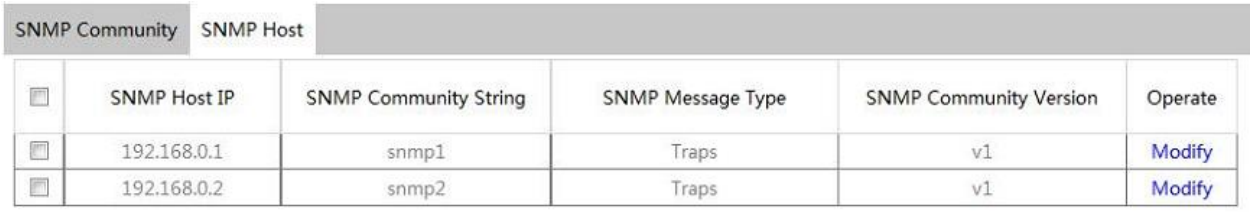


Рисунок 32 – Хосты SNMP

Для создания нового SNMP-хоста нажмите <Create>:

Рисунок 33 – Настройка SNMP-хоста

Для изменения параметров SNMP-хоста нажмите <Modify>, для удаления выбранного хоста нажмите <Delete>.

4.2.3 Настройка SNMPv3

Нажмите [Security] → [Management Access] → [SNMPv3 Configuration] на панели навигации, чтобы войти на страницу настройки.

Рисунок 34 – Группы SNMPv3

Нажмите <Modify>, чтобы изменить параметры группы SNMPv3.

Нажмите кнопку <Reload> на нижней панели управления, чтобы обновить информацию о конфигурации группы SNMPv3.

Нажмите <Create>, чтобы создать новую группе SNMPv3:

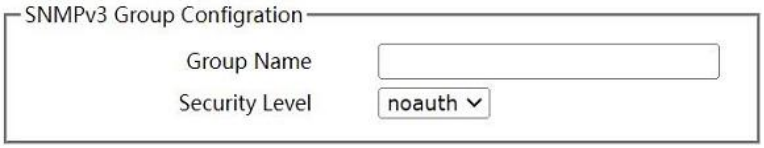


Рисунок 35 – Настройка группы SNMPv3

Чтобы перейти в раздел настройки пользователей SNMPv3 выберите вкладку [SNMPv3 User Config]:

Рисунок 36 – Пользователи SNMPv3

Нажмите <Modify>, чтобы изменить параметры пользователя SNMPv3.

Нажмите кнопку <Reload> на нижней панели управления, чтобы обновить информацию о настройках пользователя SNMPv3.

Нажмите <Create>, чтобы создать нового пользователя SNMPv3:

Рисунок 37 – Настройка нового пользователя SNMPv3

Нажмите <Delete> на нижней панели управления, чтобы удалить выбранную запись группы SNMPv3.

4.2.4 Интерфейс командной строки

Нажмите [Security] → [Management Access] → [CLI] на панели навигации, чтобы войти на страницу глобальной настройки интерфейса командной строки.

Рисунок 38 – Настройка времени терминальной сессии

На данной странице для коммутатора можно настроить время сеанса терминала. Если установить значение 0, это означает, что сеанс никогда не будет автоматически завершаться из-за превышения времени.

Чтобы настроить баннер, появляющийся при входе в терминал, нажмите [Login Banner]:

Рисунок 39 – Настройка сообщения баннера терминала

4.3 Безопасность интерфейсов

4.3.1 Настройка привязки IP-MAC на интерфейсах

Нажмите [Security] → [Port Security] на панели навигации и откройте раздел [IP MAC Binding]:

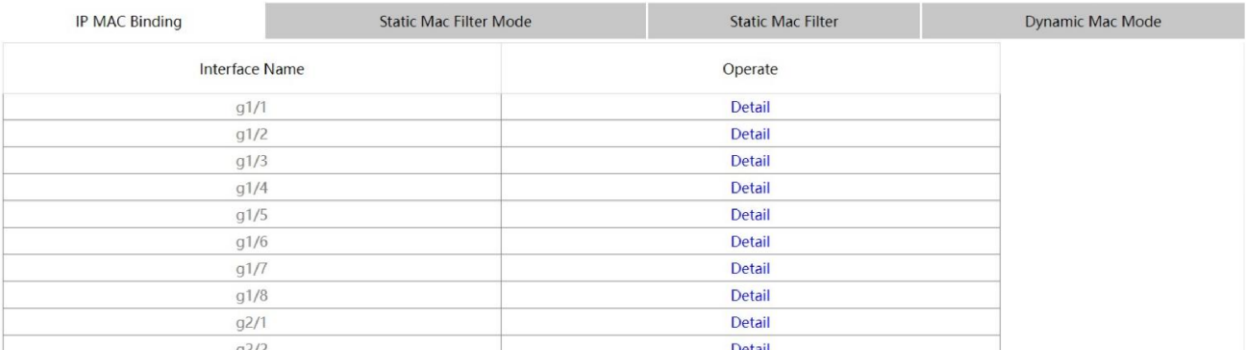


Рисунок 40 – Список интерфейсов

Нажмите <Detail>, чтобы проверить информацию о привязке для выбранного порта.

	Serial number	IP Address	MAC Address	Operate
☐	1	192.168.0.1	1001.1002.1003	Modify
☐	2	192.168.0.2	0002.0003.0004	Modify

Рисунок 41 – Информация о привязке IP-MAC

Для изменения параметров привязки IP-MAC нажмите <Modify>, для обновления информации нажмите <Reload>. Чтобы создать новый элемент привязки IP-MAC нажмите <Create>:

Enter a new IP address
Enter a new MAC

Рисунок 42 – Создание привязки IP-MAC

Для удаления выбранного элемента привязки нажмите <Delete> на нижней панели управления.

4.3.2 Статический режим фильтрации MAC-адресов

Выберите [Static MAC Filter Mode], чтобы прейти на страницу настройки.

IP MAC Binding | Static Mac Filter Mode | Static Mac Filter | Dynamic Mac Mode

Interface Name	Port Mode	Static MAC Filtration Mode
g1/1	Access	Disable
g1/2	Access	Disable
g1/3	Access	Disable
g1/4	Access	Disable
g1/5	Access	Disable
g1/6	Access	Disable
g1/7	Access	Disable
g1/8	Access	Disable
g2/1	Access	Disable
g2/2	Access	Disable
g2/3	Access	Disable
g2/4	Access	Disable
g2/5	Access	Disable
g2/6	Access	Disable
g2/7	Access	Disable
g2/8	Access	Disable

Set Reload

Рисунок 43 – Режим статической фильтрации MAC-адресов

На этой странице можно настроить статический режим фильтрации MAC-адресов для каждого интерфейса.

4.3.3 Настройка статической фильтрации MAC-адресов

Выберите [Static MAC Filter], чтобы прейти на страницу настройки.

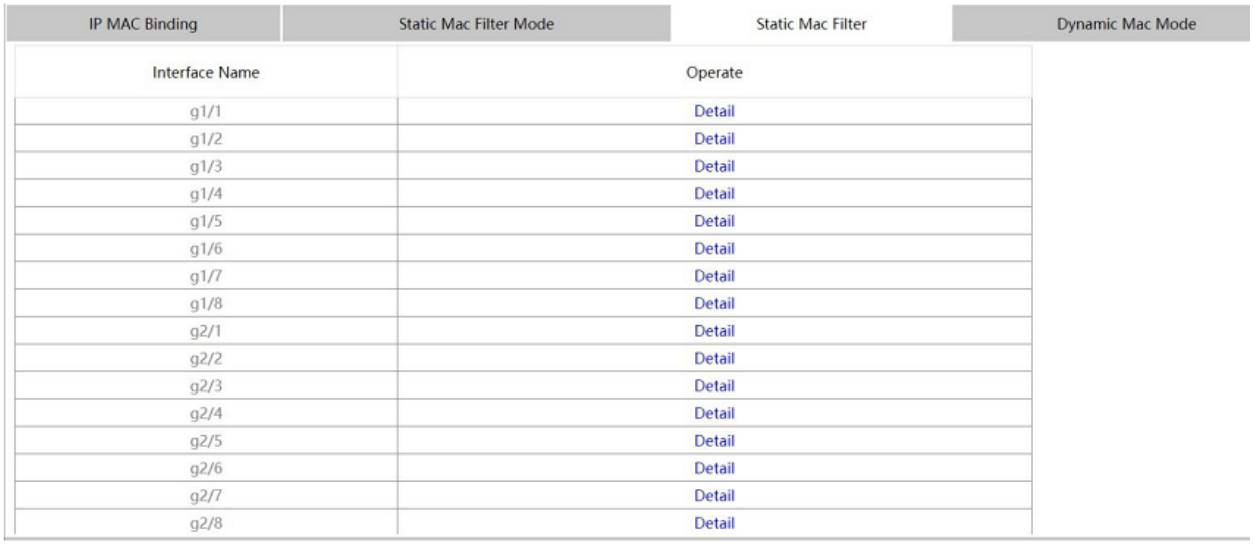


Рисунок 44 – Статическая фильтрация MAC-адресов

Нажмите <Detail>, чтобы проверить информацию таблицы MAC-адресов.

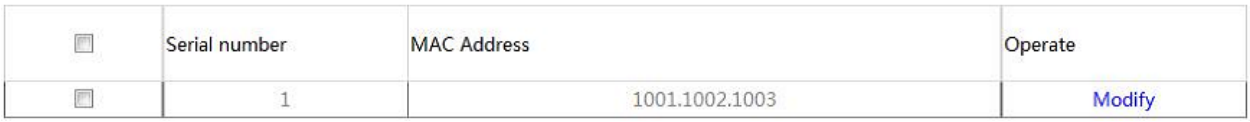


Рисунок 45 – Список MAC-адресов

Для изменения элементов фильтрации нажмите <Modify>. Нажмите <Create>, чтобы создать новую запись MAC-адреса:

Рисунок 46 – Создание нового элемента статической фильтрации

Для удаления выбранной записи нажмите <Delete> на нижней панели управления.

4.3.4 Динамический режим фильтрации MAC-адресов

Выберите [Dynamic MAC Mode], чтобы прейти на страницу настройки.

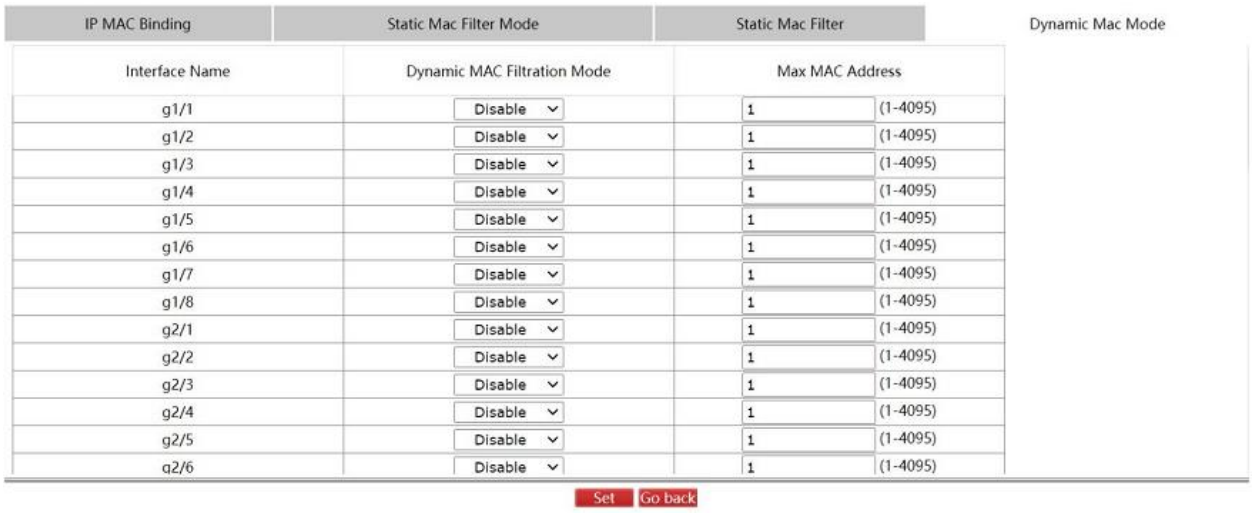


Рисунок 47 – Динамический режим фильтрации MAC-адресов

На этой странице можно настроить динамический режим фильтрации MAC-адресов для каждого интерфейса.

4.4 Switchport Protect

Нажмите [Security] → [Switchport Protect] на панели навигации, чтобы прейти на страницу настройки.

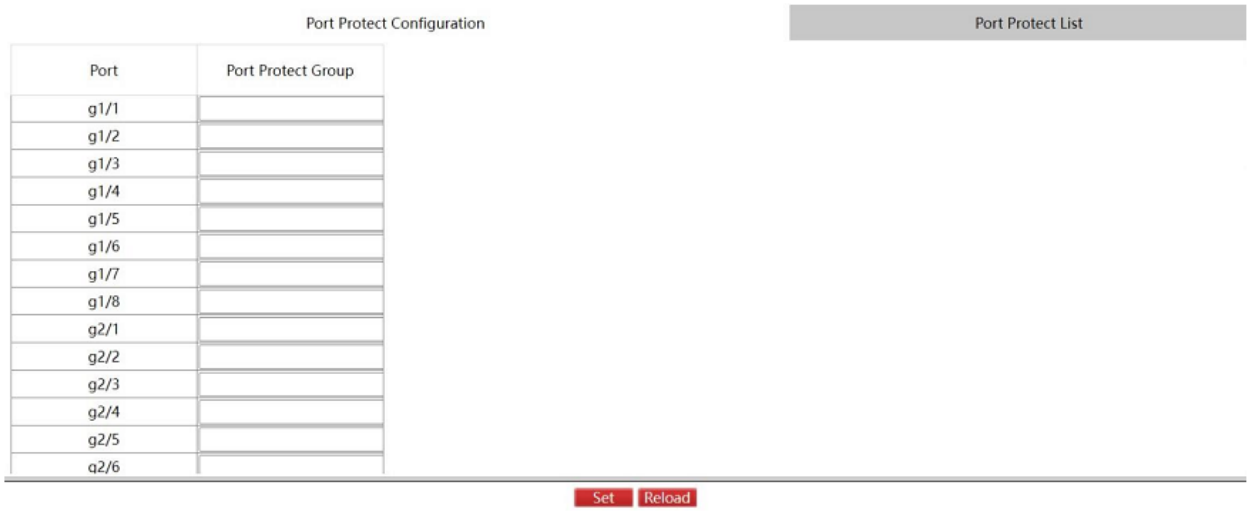


Рисунок 48 – Список защищаемых портов

Укажите группу Switchport Protect на этой странице и нажмите <Set> на нижней панели управления, чтобы завершить настройку.

Нажмите <Reload>, чтобы обновить информацию.

Нажмите [Port Protect list], перейдите на страницу настройки группы Switchport Protect:

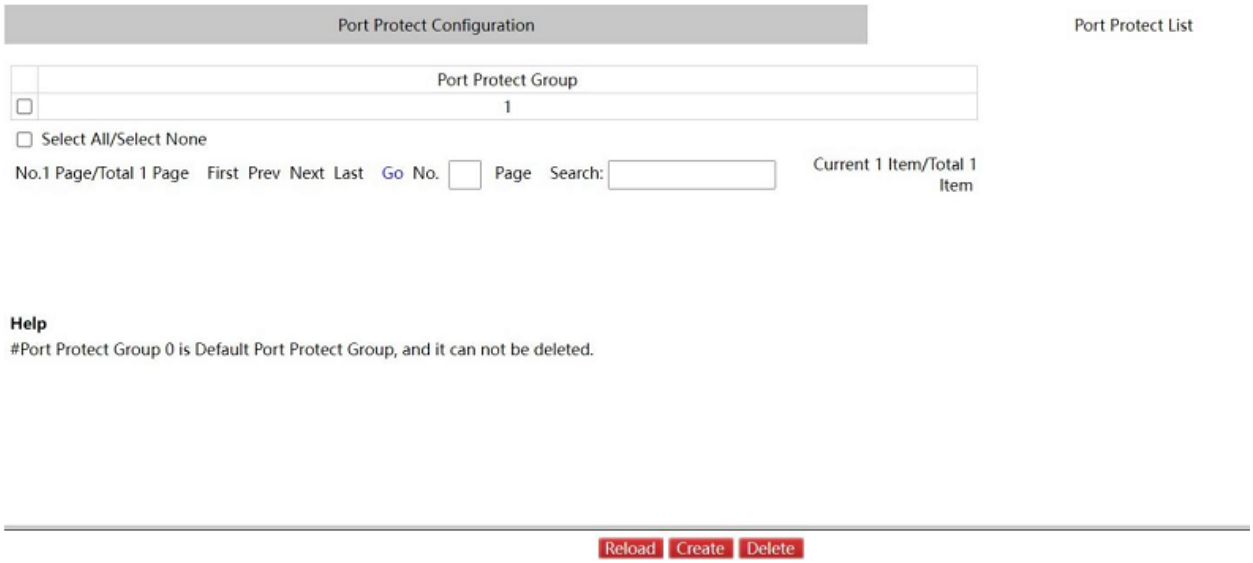


Рисунок 49 – Список групп Switchport Protect

Нажмите <Reload> на нижней панели управления, чтобы обновить информацию о группе.

Нажмите <Delete> на нижней панели управления, удалите выбранную группу.

Нажмите <Create> на нижней панели управления и перейдите на страницу создания группы Switchport Protect:

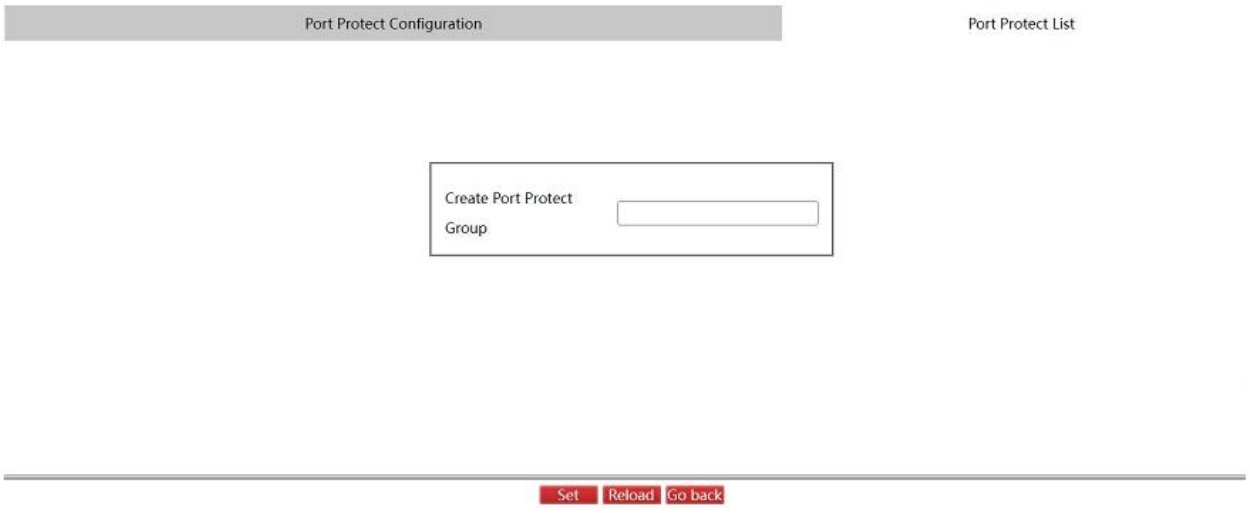


Рисунок 50 – Создание группы Switchport Protect

Нажмите <Set> на нижней панели управления, чтобы завершить настройку.

Нажмите <Reload>, чтобы обновить информацию Switchport Protect.

Нажмите <Go back>, чтобы вернуться в раздел [Port Protect list].

4.5 Keepalive

Нажмите [Security] → [Keepalive] на панели навигации, чтобы прейти на страницу настройки.

Рисунок 51 – Настройка Keepalive

После настройки нажмите <Set> на нижней панели управления, чтобы подтвердить изменения. Нажмите <Reload>, чтобы обновить информацию о настройках на портах.

4.6 Аутентификация 802.1X

4.6.1 Глобальная настройка

Нажмите [Security] → [802.1X Port Authentication] → [Global] на панели навигации, чтобы войти на страницу глобальной настройки 802.1X.

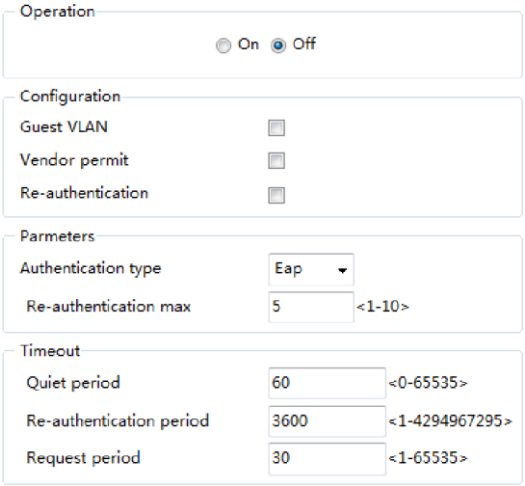


Рисунок 52 – Глобальная конфигурация 802.1X

На этой странице можно настроить параметры аутентификации 802.1X на интерфейсах коммутатора.

4.6.2 Список правил аутентификации

Нажмите [Security] → [802.1X Port Authentication] → [Authentication List] на панели навигации, чтобы войти на страницу настройки.

	Name	Method 1	Method 2	Method 3	Method 4
☐	zx	local			
☐	scc	group radius	group tacacs+	group 1	

Рисунок 53 – Список правил аутентификации

Нажмите <Reload> на нижней панели управления, чтобы обновить список.

Нажмите <Delete> на нижней панели управления, чтобы удалить выбранное правило аутентификации.

Нажмите <Create>, чтобы создать новую запись:

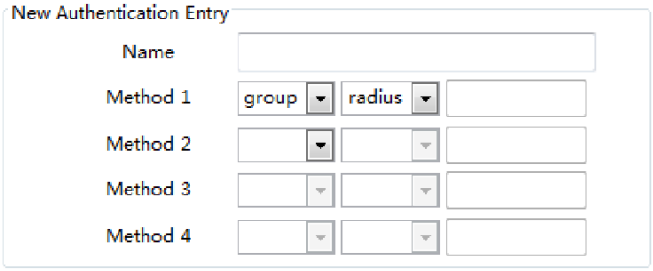


Рисунок 54 – Создание правила аутентификации

4.6.3 Настройка интерфейсов

Нажмите [Security] → [802.1X Port Authentication] → [Port Configuration] на панели навигации, чтобы перейти на страницу настройки.

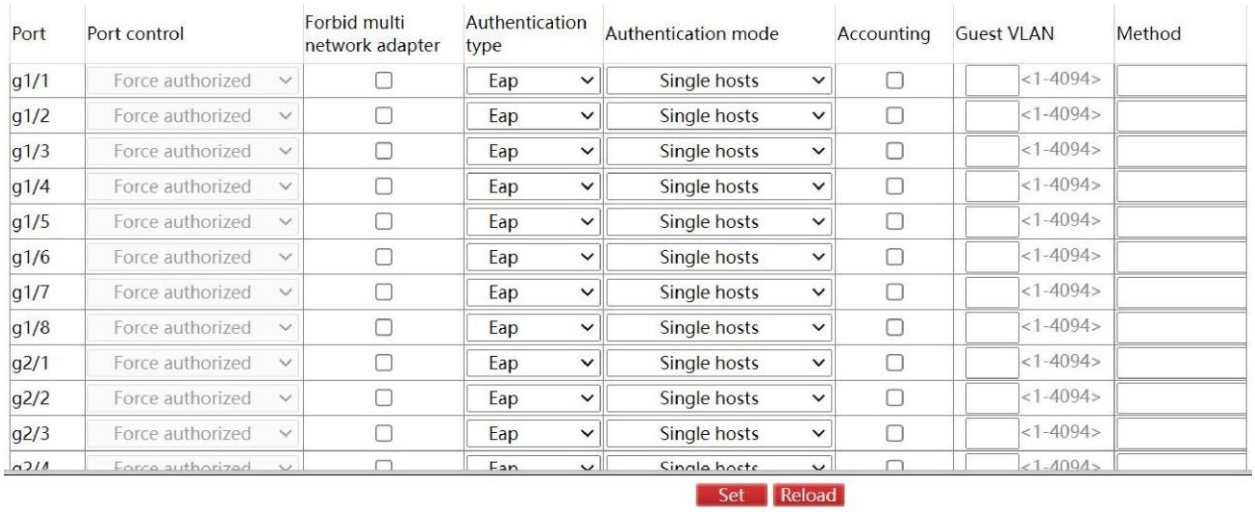


Рисунок 55 – Настройка интерфейсов

На этой странице для каждого интерфейса можно включить или выключить функцию аутентификации 802.1X, настроить тип, режим, метод аутентификации и т. д.

Некоторые настройки возможны только при условии, что функция аутентификации 802.1X на порту включена.

4.6.4 Статистика

Нажмите [Security] → [802.1X Port Authentication] → [Statistics] на панели навигации, чтобы перейти на страницу статистики 802.1X.

Port	EAPOL Start	EAPOL Logoff	EAPOL Invalid	Received EAPOL Total	EAP Response Id	EAP Response Other	EAP Length Error	Transmitted EAPOL Total	EAP Request Id	EAP Other
g0/1	---	---	---	---	---	---	---	---	---	---
g0/2	---	---	---	---	---	---	---	---	---	---
g0/3	---	---	---	---	---	---	---	---	---	---
g0/4	---	---	---	---	---	---	---	---	---	---

Рисунок 56 – Статистика 802.1X

На этой странице можно проверить статистическую информацию о сообщениях 802.1X на всех интерфейсах.

4.7 RADIUS

4.7.1 Глобальная настройка

Нажмите [Security] → [RADIUS] → [Global] на панели навигации, чтобы перейти на страницу настройки.

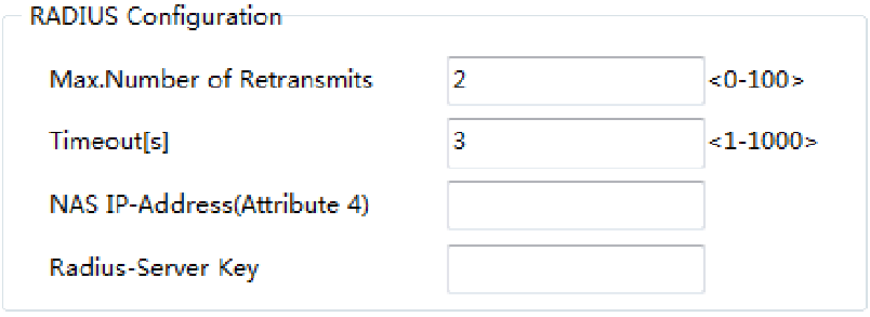


Рисунок 57 – Глобальная настройка RADIUS

На этой странице можно настроить максимальное количество повторных передач, время сеанса, NAS и ключ сервера RADIUS.

4.7.2 Настройка службы

Нажмите [Security] → [RADIUS] → [Service] на панели навигации, чтобы перейти на страницу настройки.

Рисунок 58 – Настройка портов RADIUS

На данной странице на коммутаторе можно настроить порты аутентификации и учета для сервера RADIUS.

Нажмите <Set> на нижней панели управления, чтобы завершить настройку.

Нажмите <Reload>, чтобы обновить информацию о портах аутентификации и учета.

Нажмите <Delete>, чтобы удалить выбранную запись.

Нажмите <Create>, чтобы создать новые элементы аутентификации RADIUS:

Рисунок 59 – Создание нового элемента RADIUS

5. Системное время

Рисунок 60 – Меню времени на панели навигации

5.1 Основные настройки

Нажмите [Time] → [Basic Setting] на панели навигации, чтобы перейти на страницу настройки.

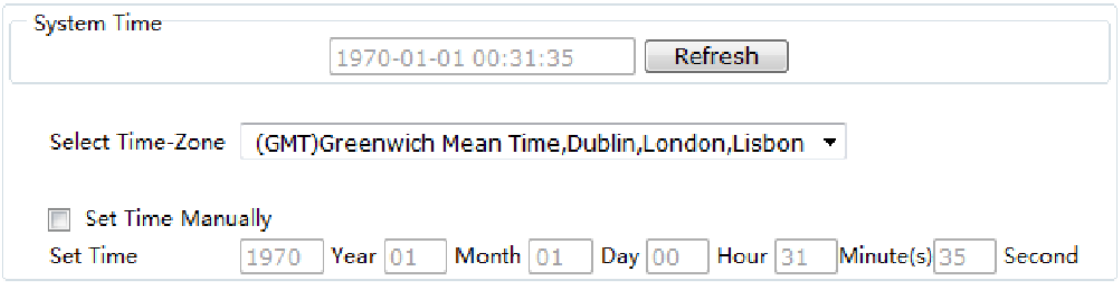


Рисунок 61 – Настройка системного времени

Нажмите <Reload>, чтобы обновить текущее отображаемое системное время. На этой странице можно настроить часовой пояс системы. Выберите «Set Time Manually», чтобы установить системное время вручную.

5.2 NTP

Нажмите [Time] → [NTP] на панели навигации, чтобы перейти на страницу настройки синхронизации времени.

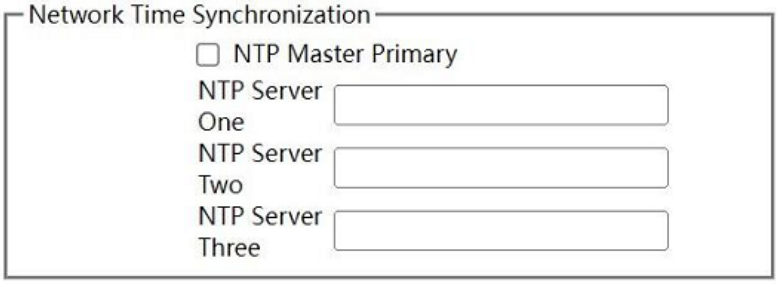


Рисунок 62 – Настройка синхронизации времени

На этой странице можно настроить IP-адрес NTP-сервера для синхронизации времени по сети.

5.3 PTP

5.3.1 Глобальная настройка

Нажмите [Time] → [PTP] → [Global] на панели навигации, чтобы перейти на страницу настройки протокола точного времени.

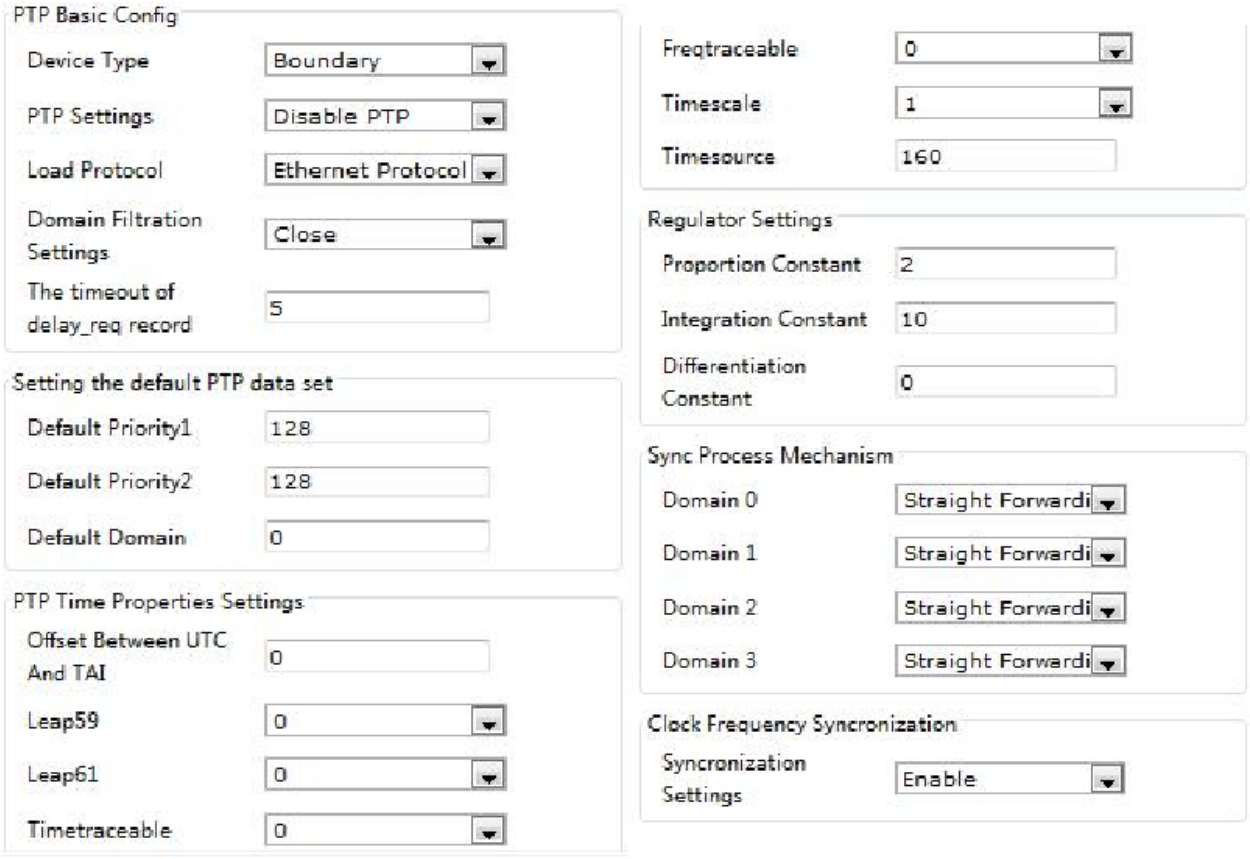


Рисунок 63 – Глобальная настройка PTP

На этой странице можно включить или отключить протокол PTP, а также настроить параметры по умолчанию, свойства времени PTP, механизм процесса синхронизации и т.д. Нажмите <Set> на нижней панели управления, чтобы завершить настройку. Нажмите <Reload>, чтобы обновить глобальную конфигурацию PTP.

5.3.2 Настройка на портах

Нажмите [Time] → [PTP] → [Port Configuration] на панели навигации, чтобы перейти на страницу настройки.

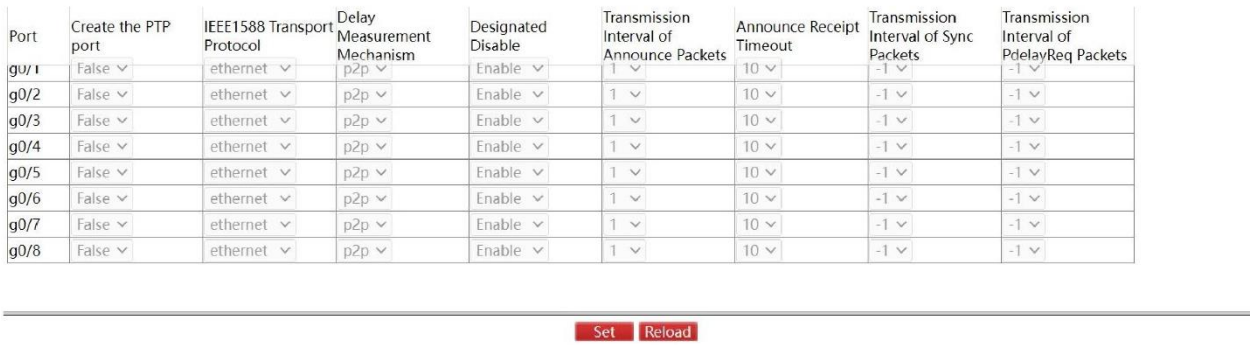


Рисунок 64 – Конфигурация PTP-портов

На этой странице доступны такие настройки как создание порта PTP, тип транспортного протокола IEEE1588, механизм измерения задержки и другие функции, выполняемые на порту. Нажмите <Reload> на нижней панели управления, чтобы обновить текущую конфигурацию каждого порта.

Настройки на этой странице доступны только при условии, что протокол PTP включен.

5.3.3 Одноадресная передача

Нажмите [Time] → [PTP] → [Unicast] на панели навигации, чтобы перейти на страницу настройки.

Рисунок 65 – Настройка одноадресной передачи на портах

На этой странице можно проверить и изменить статус одноадресной рассылки для каждого порта.

6. Сетевая безопасность

Рисунок 66 – Сетевая безопасность на панели навигации

6.1 Защита от DOS-атак

6.1.1 Глобальная настройка

Нажмите [Network Security] → [DOS] → [Global] на панели навигации, чтобы перейти на страницу настройки.

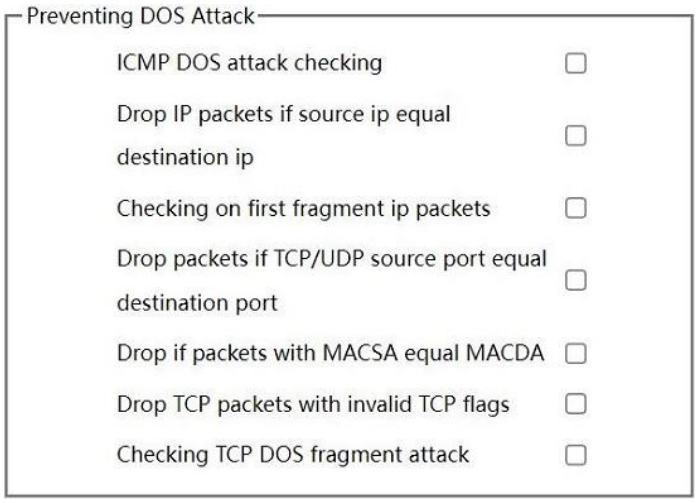


Рисунок 67 – Настройка защиты от DOS-атак

Вы можете включить или выключить необходимую функцию защиты в соответствии с текущими задачами. Нажмите <Set>, чтобы сохранить конфигурацию.

6.2 DHCP Snooping

6.2.1 Глобальная настройка

Нажмите [Network Security] → [DHCP Snooping] → [Global] на панели навигации, чтобы перейти на страницу настройки.

Рисунок 68 – Глобальная настройка DHCP Snooping

Включите протокол DHCP Snooping в глобальном режиме для обнаружения всех сообщений DHCP. Коммутатор будет проверять и подтверждать IP-адреса, предоставляемые DHCP-сервером, чтобы защитить сеть от атак на основе поддельных IP-адресов. Если клиент получал адреса от коммутатора до того, как функция была активирована, коммутатор не сможет добавить эти адреса в таблицу привязки DHCP Snooping.

После сохранения конфигурации на коммутаторе необходимо перезагрузить его. Все предыдущие настроенные отношения привязки интерфейсов будут удалены. После этого интерфейсы не будут иметь привязок, и коммутатор будет отклонять пересылку всех IP-сообщений, если активирована функция мониторинга исходного IP-адреса. Затем необходимо настроить резервное хранилище для списка привязки интерфейсов на TFTP-сервере. Далее привязки будут скопированы на сервер с помощью TFTP-протокола. После перезагрузки коммутатора он автоматически загрузит список с TFTP-сервера, чтобы обеспечить нормальную работу сети.

При настройке резервного копирования списка привязок сохраните файл с уникальным именем на TFTP-сервере. Таким образом, разные коммутаторы могут копировать свой список отношений привязки интерфейсов на один и тот же сервер.

Таблица привязки MAC-адреса и IP-адреса интерфейсов является динамической. Требуется проверить, не была ли обновлена запись. Если да (например, добавлены или удалены элементы привязки), резервное копирование следует выполнить заново. Временной интервал копирования по умолчанию составляет 30 минут.

6.2.2 Настройка для VLAN

Нажмите [Network Security] → [DHCP Snooping] → [VLAN Config] на панели навигации, чтобы перейти на страницу настройки.

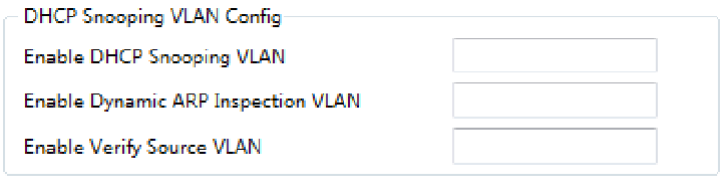


Рисунок 69 – Настройка DHCP Snooping в VLAN

После включения функции DHCP Snooping в VLAN сообщения DHCP, полученные всеми недоверенными физическими портами во всей VLAN, будут проверяться на соответствие настройкам DHCP Snooping. Ошибочные или подозрительные сообщения могут быть отброшены или проигнорированы, чтобы предотвратить возможные атаки или неправильное назначение адресов DHCP-сервером. Что касается запросов DHCP от ненадежных портов, если MAC-адрес не соответствует полю аппаратного адреса в сообщениях, запросы будут рассматриваться как сообщения, подделанные пользователем с целью атаки DHCP-DOS (отказ в обслуживании), и пользователь будет отключен.

DHCP Snooping отслеживает динамику ARP всех физических портов VLAN. Если исходные MAC и IP-адреса сообщений ARP, полученных портами, не соответствуют отношениям привязки, настроенным для портов, сообщения не смогут быть обработаны. Отношения привязки, настроенные для портов, могут быть динамическими (полученными при помощи DHCP) или настроенными вручную. Если для физического порта не настроены отношения привязки MAC и IP-адресов, коммутатор откажется пересылать все сообщения ARP.

В VLAN, где отслеживаются исходные IP-адреса, если исходные MAC и IP-адреса IP-сообщений, полученных всеми физическими портами в VLAN, не соответствуют отношениям привязки MAC и IP-адресов, настроенным для портов, сообщения не смогут быть обработаны. Отношения привязки, настроенные для портов, могут быть динамическими (полученными при помощи DHCP) или настроенными вручную. Если для физического порта не настроены отношения привязки MAC и IP-адресов, коммутатор откажется пересылать все IP-сообщения, полученные всеми портами.

6.2.3 Настройка на интерфейсах

Нажмите [Network Security] → [DHCP Snooping] → [Interface Config] на панели навигации, чтобы перейти на страницу настройки.

Port	DHCP Trust Port	ARP Inspection Trust Port	IP Source Trust Port
g0/1	Distrust	Distrust	Distrust
g0/2	Distrust	Distrust	Distrust
g0/3	Distrust	Distrust	Distrust
g0/4	Distrust	Distrust	Distrust
f1/1	Distrust	Distrust	Distrust
f1/2	Distrust	Distrust	Distrust
f1/3	Distrust	Distrust	Distrust
f1/4	Distrust	Distrust	Distrust
f2/1	Distrust	Distrust	Distrust
f2/2	Distrust	Distrust	Distrust
f2/3	Distrust	Distrust	Distrust
f2/4	Distrust	Distrust	Distrust

Рисунок 70 – Настройка DHCP Snooping на интерфейсах

Если порт настроен как DHCP-доверенный, сообщения DHCP, полученные этим портом, не будут проверяться. Функция мониторинга ARP не будет включена для ARP-доверенных портов. По умолчанию порты не являются доверенными. Функция проверки адреса источника DHCP-сообщений не включена для портов, которым можно доверять по исходным IP-адресам.

6.2.4 Настройка привязки

Нажмите [Network Security] → [DHCP Snooping] → [Bindings] на панели навигации, чтобы перейти на страницу настройки.

	MAC Address	IP Address	Interface Name	VLAN
☐	00:00:00:00:00:00	192.168.2.6	GigaEthernet1/1	2

Рисунок 71 – Таблица привязки

Для хостов, которые не используют DHCP для получения адресов, пользователи могут вручную добавлять записи привязки на портах коммутатора, чтобы хост беспрепятственно получал доступ к сети. Команда **«no»** может использоваться для удаления связанных записей.

Записи, привязанные вручную, имеют приоритет по отношению к записям, привязанным посредством динамической конфигурации. Если MAC-адрес статически настроенной записи совпадает с MAC-адресом динамически настроенной записи, последний будет обновлен на основе первого. MAC-адрес – единственный индекс для связанных записей порта.

Нажмите <Create>, чтобы создать записи привязки для настроенных вручную портов DHCP Snooping.

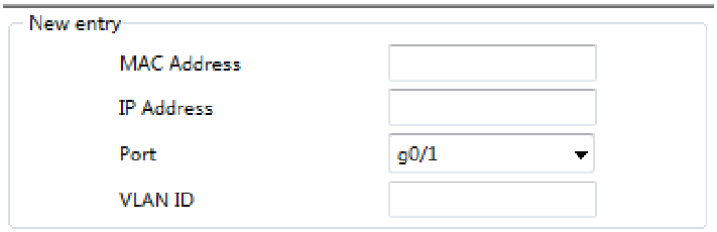


Рисунок 72 – Создание новой записи

Создание новых записей возможно только при условии, что протокол DHCP Snooping включен.

6.3 Список управления доступом (ACL)

6.3.1 Правила IPv4

Нажмите [Network Security] → [Access Control List] → [IPv4 Rules] на панели навигации, чтобы перейти на страницу настройки.

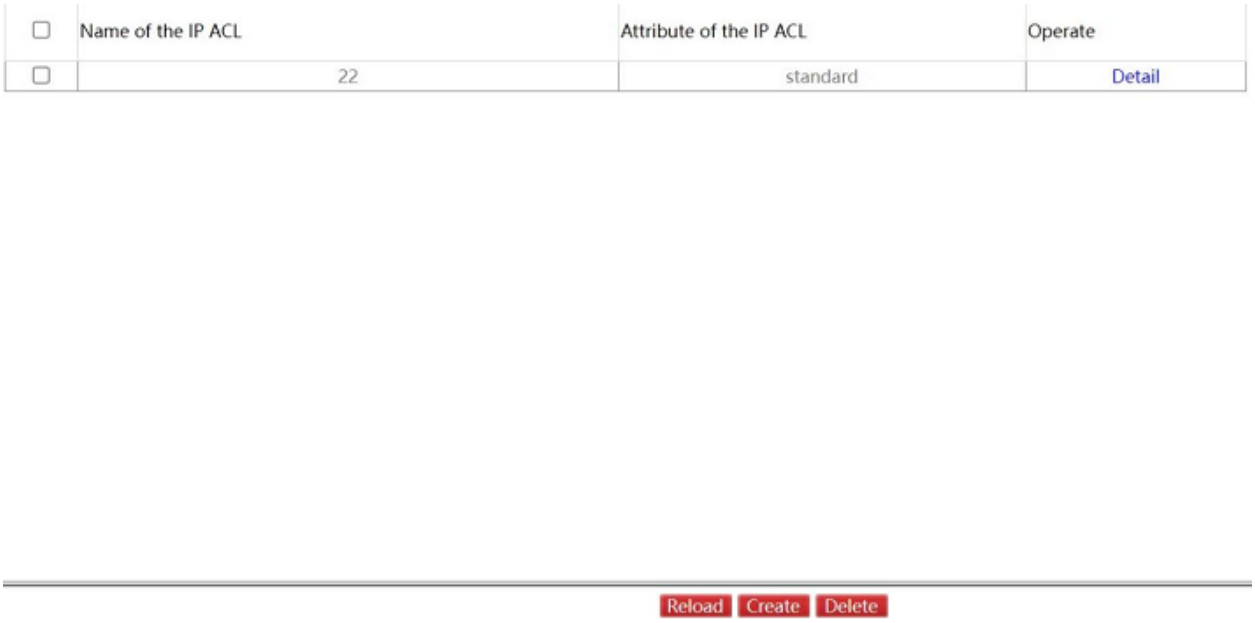


Рисунок 73 – IP ACL

Нажмите <Detail> справа от записи, чтобы перейти на страницу настройки выбранного списка.

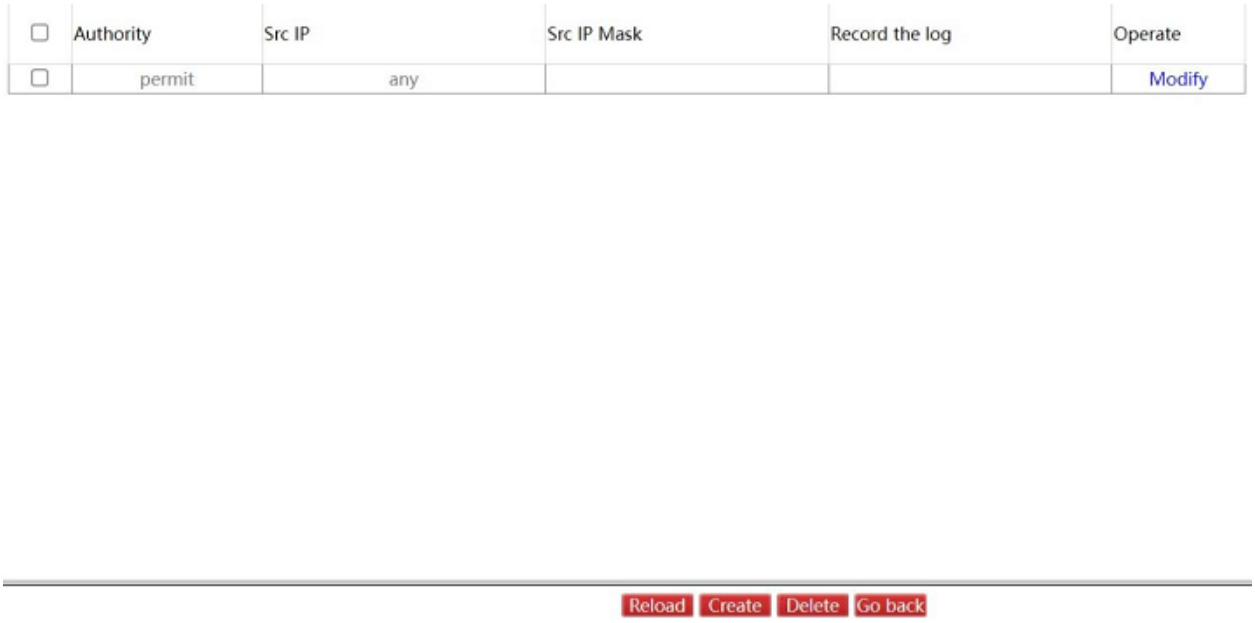


Рисунок 74 – Настройка IP ACL

Нажмите <Modify>, чтобы войти в список контроля доступа и выполнить настройку правил.

Нажмите <Go back>, чтобы вернуться на предыдущую страницу.

Нажмите <Create>, чтобы создать новый список.

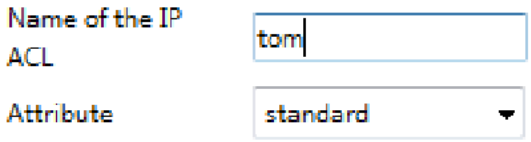


Рисунок 75 – Создание нового IP ACL

Для удаления выбранного списка нажмите <Delete> на нижней панели.

6.3.2 Правила MAC

Нажмите [Network Security] → [Access Control List] → [MAC Rules] на панели навигации, чтобы перейти на страницу настройки.

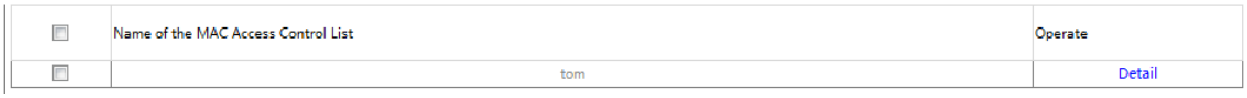


Рисунок 76 – MAC ACL

Нажмите <Create>, чтобы создать новый список. Для удаления выбранного списка нажмите <Delete>.

Рисунок 77 – Создание нового MAC ACL

6.3.3 Распределение списков

Нажмите [Network Security] → [Access Control List] → [Assignment] на панели навигации, чтобы назначить соответствующие ACL для входящего и исходящего трафика.

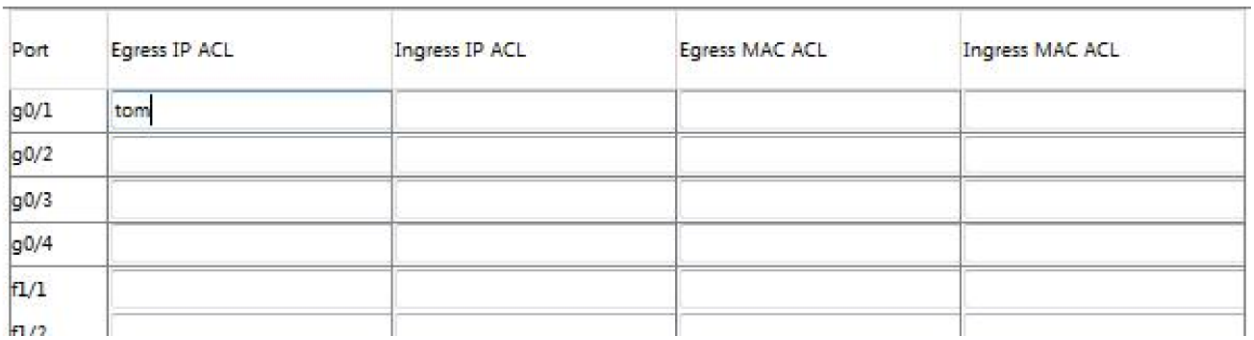


Рисунок 78 – Распределение ACL

6.4 Фильтрация

Нажмите [Network Security] → [Filter Function] на панели навигации, чтобы перейти на страницу глобальной настройки функции фильтрации.

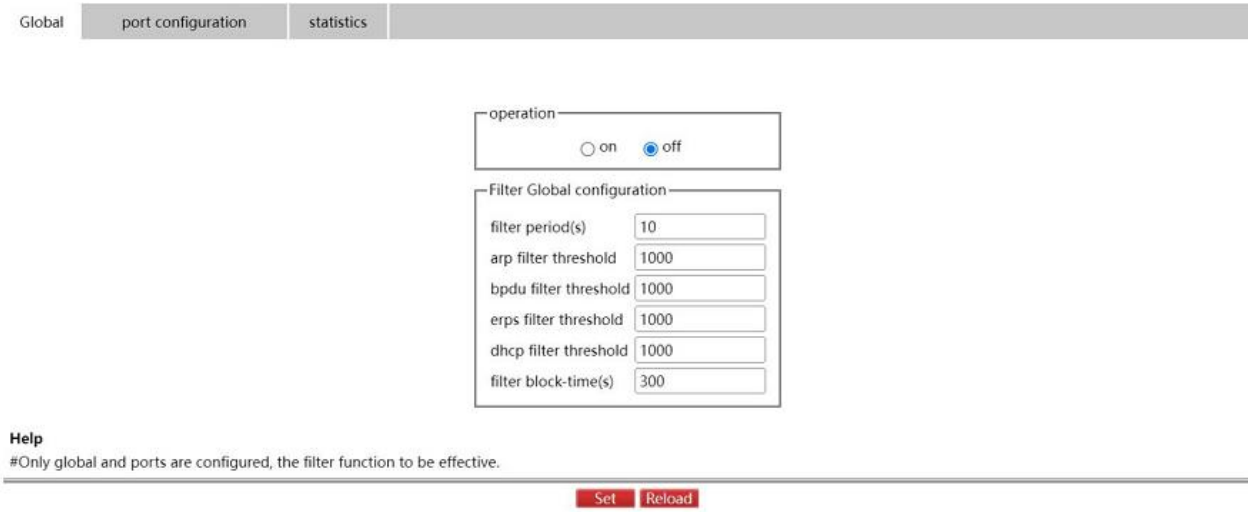


Рисунок 79 – Глобальная настройка фильтрации

После завершения глобальной настройки функции нажмите <Set> на нижней панели управления. Чтобы обновить конфигурацию нажмите <Reload>.

Нажмите [Port Configuration] справа от [Global] и войдите на страницу настройки фильтрации на портах:

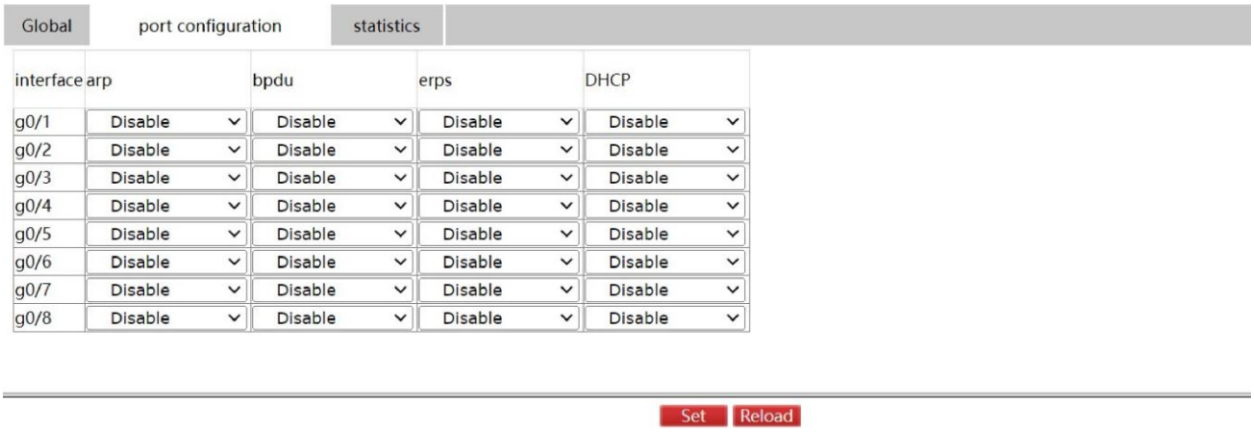


Рисунок 80 – Настройки фильтрации на портах

Для завершения настроек нажмите <Set> на нижней панели управления. Чтобы обновить конфигурацию нажмите <Reload>.

Нажмите [Statistics] справа от [Port Configuration] и войдите на страницу статистики блокировки и учета фильтров:

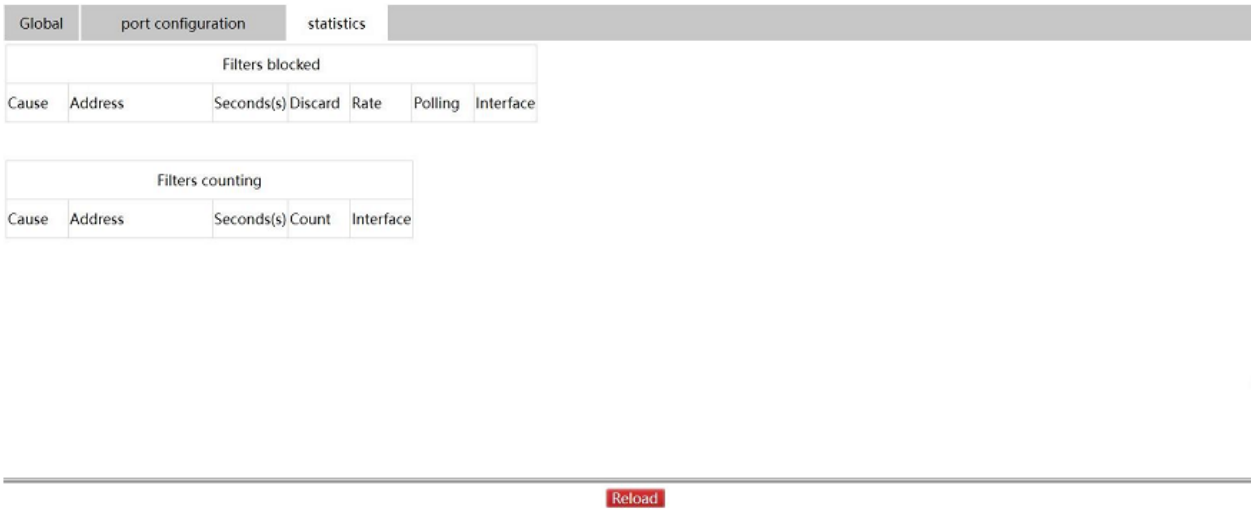


Рисунок 81 – Статистика фильтрации

Чтобы обновить статистическую информацию нажмите <Reload>.

7. Коммутация

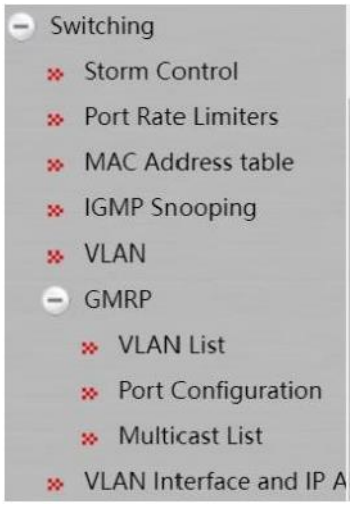


Рисунок 82 – Настройки коммутации на панели навигации

7.1 Контроль штормов

Нажмите [Switching] → [Storm Control] на панели навигации, чтобы перейти на страницу настройки управления широковещательными, многоадресными и одноадресными штормами.

7.1.1 Контроль широковещательных штормов

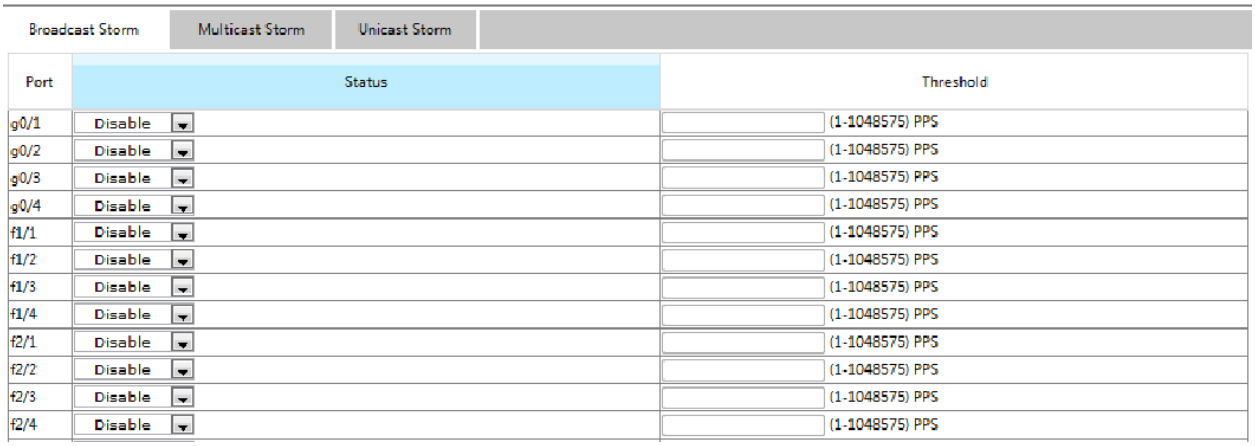


Рисунок 83 – Контроль широковещательных штормов

В раскрывающихся списках в столбце «Status» вы можете выбрать, включать ли управление широковещательным штормом на порту. В столбце «Threshold» можно ввести ограничение количества принимаемых за секунду широковещательных пакетов. Допустимый пороговый диапазон для каждого порта указан справа от поля ввода.

7.1.2 Контроль многоадресных штормов

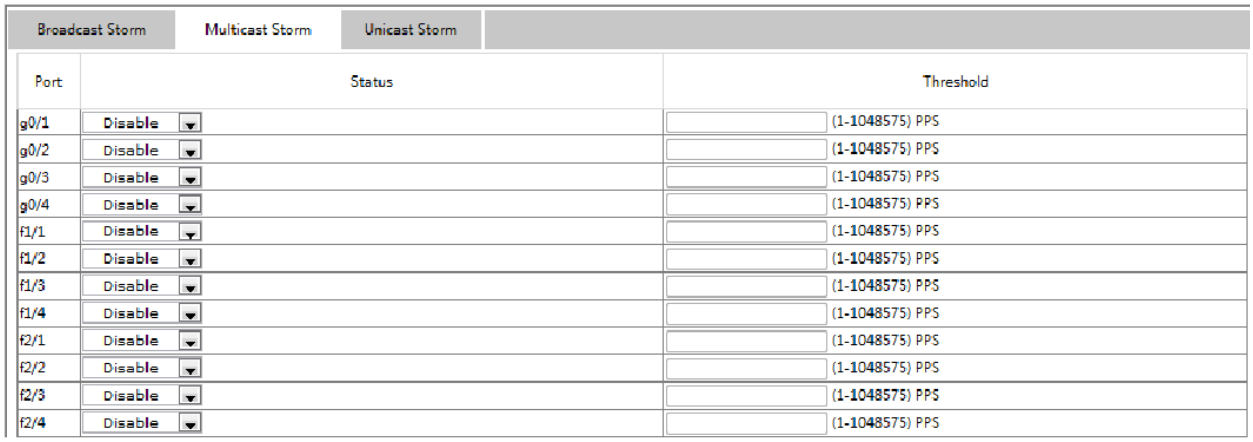


Рисунок 84 – Контроль многоадресных штормов

В раскрывающихся списках в столбце «Status» вы можете выбрать, включать ли управление многоадресным штормом на порту. В столбце «Threshold» можно ввести ограничение количества принимаемых за секунду многоадресных пакетов. Допустимый пороговый диапазон для каждого порта указан справа от поля ввода.

7.1.3 Контроль одноадресных штормов

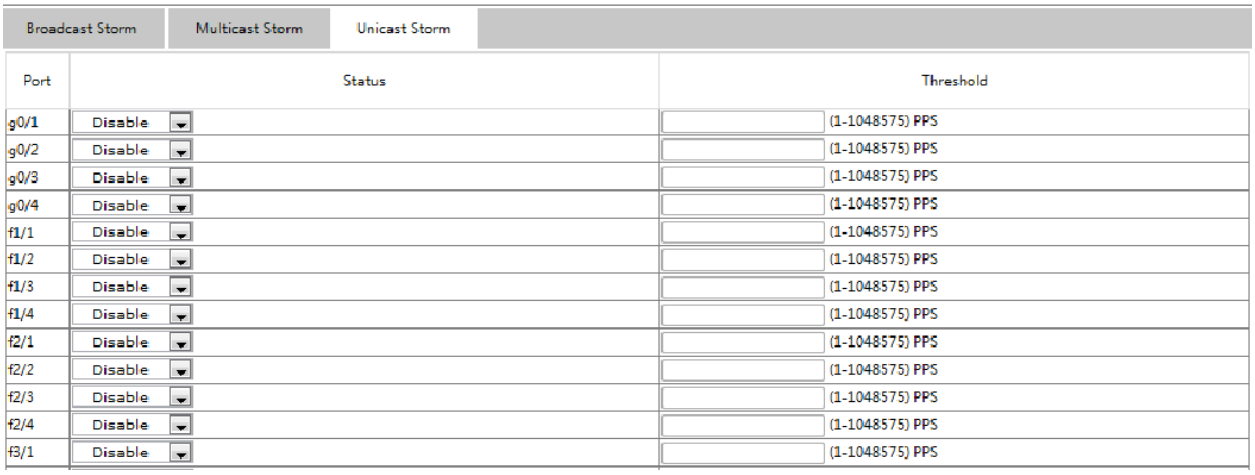


Рисунок 85 – Контроль одноадресных штормов

В раскрывающихся списках в столбце «Status» вы можете выбрать, включать ли управление одноадресным штормом на порту. В столбце «Threshold» можно ввести ограничение количества принимаемых за секунду неизвестных одноадресных пакетов. Допустимый пороговый диапазон для каждого порта указан справа от поля ввода.

7.2 Ограничение скорости портов

Нажмите [Switching] → [Port Rate Limits] на панели навигации, чтобы перейти на страницу настройки.

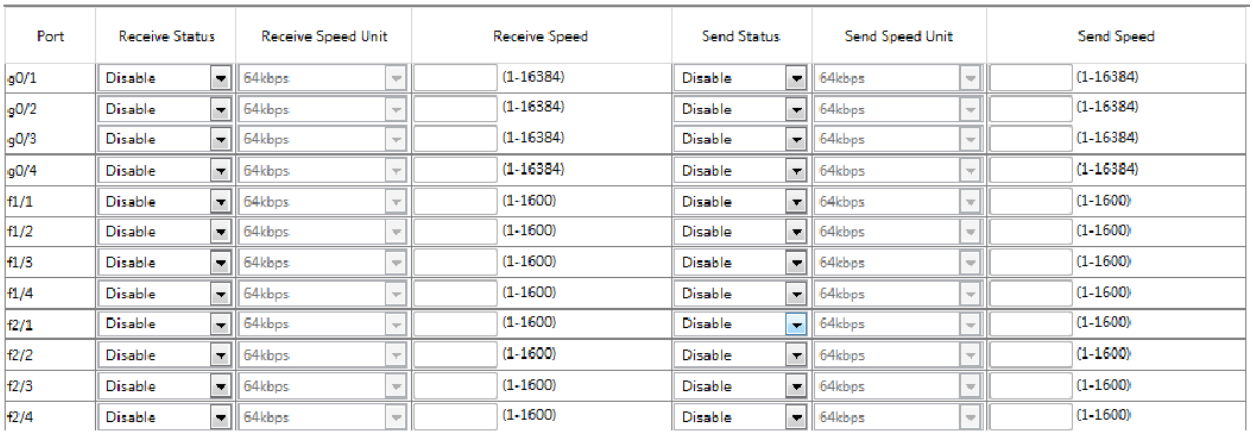


Рисунок 86 – Ограничение скорости портов

На этой странице можно установить ограничение скорости приема и передачи на портах. По умолчанию скорость всех портов не ограничена. Скорость можно настроить в соответствии с соотношением принимаемых и передаваемых данных или единицей измерения, определенной коммутатором.

7.3 Фильтрация MAC-адресов

Нажмите [Switching] → [MAC Address Table] на панели навигации, чтобы открыть статическую таблицу MAC-адресов.

Рисунок 87 – Таблица MAC-адресов

На странице отображаются порядковый номер, статический MAC-адрес, и идентификатор VLAN. Нажмите <Create> или <Modify>, чтобы внести в таблицу новый статический MAC-адрес или отредактировать существующую запись.

Рисунок 88 – Настройка таблицы MAC-адресов

Нажмите [Aging Configuration] справа от [Static MAC Address Table] и перейдите на страницу настройки времени устаревания MAC-адресов:

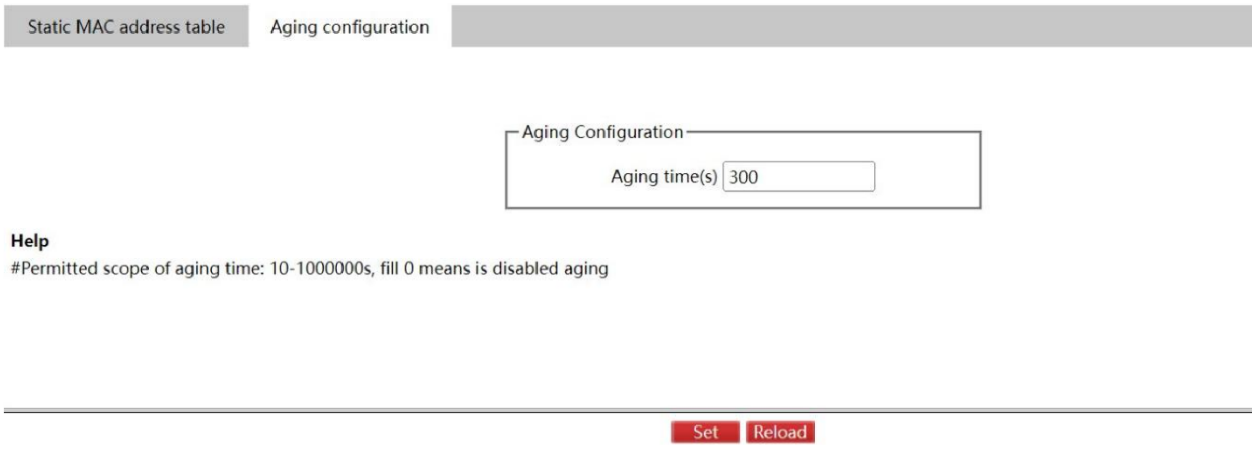


Рисунок 89 – Настройка времени устаревания

7.4 IGMP Snooping

7.4.1 Настройка IGMP Snooping

Нажмите [Switching] → [IGMP Snooping] на панели навигации, чтобы перейти на страницу настройки.

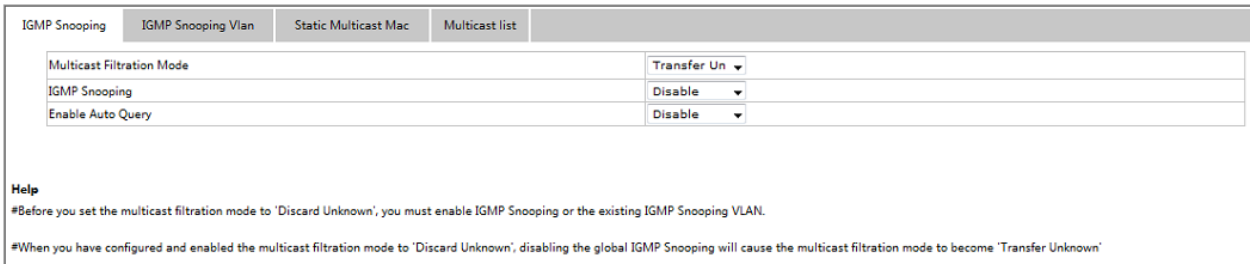


Рисунок 90 – Настройка IGMP Snooping

На этой странице можно настроить метод обработки неизвестной многоадресной рассылки, включение IGMP-Snooping и использование устройства в качестве запросчика IGMP.

7.4.2 Настройка VLAN

Нажмите [IGMP Snooping VLAN], чтобы перейти к списку VLAN, для которых настроен IGMP Snooping.

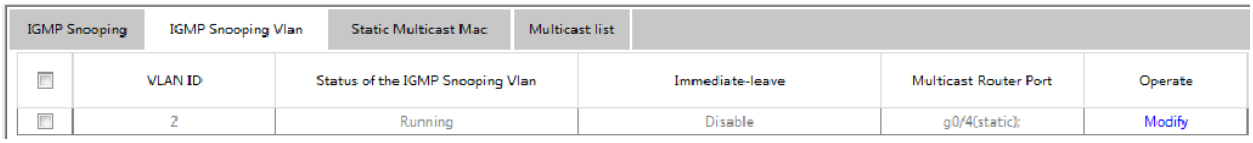


Рисунок 91 – Список IGMP Snooping VLAN

Нажав <Modify>, можно изменить порты-участники, рабочее состояние и настройки немедленного выхода VLAN из группы. Нажмите <Create>, чтобы выполнить настройку VLAN с отслеживанием IGMP. Через веб-интерфейс в каждой VLAN с IGMP Snooping можно настроить до 8 физических портов. Для удаления выбранной VLAN с отслеживанием IGMP нажмите <Delete>.

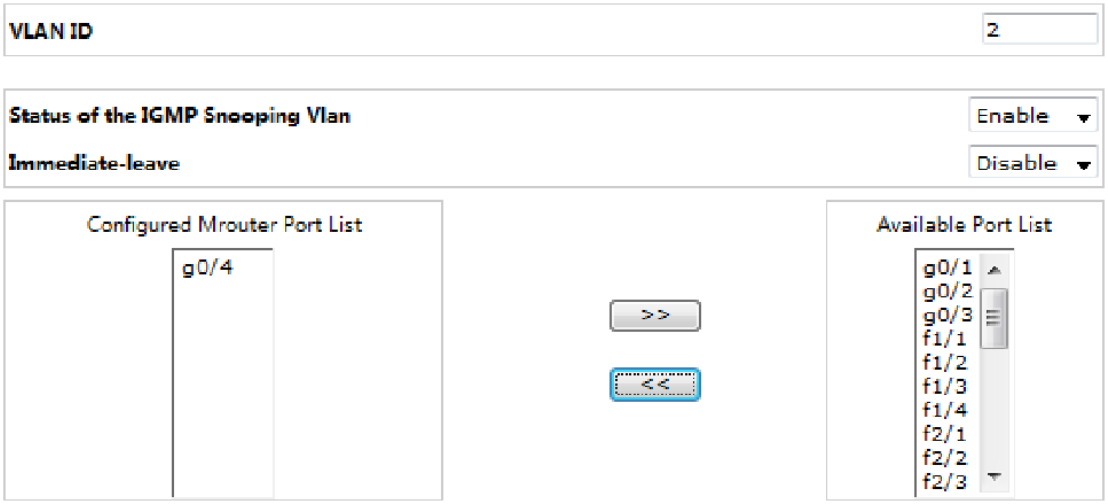


Рисунок 92 – Настройка IGMP Snooping VLAN

Когда создается IGMP Snooping VLAN, ее VLAN ID можно изменить. При редактировании существующей VLAN идентификатор не может быть изменен.

Вы можете нажать «>>» и «<<», чтобы удалить или добавить порт маршрутизации.

7.4.3 Настройка статического MAC-адреса многоадресной рассылки

Нажмите [Static Multicast Mac], чтобы перейти на страницу настройки статического MAC-адреса многоадресной рассылки.

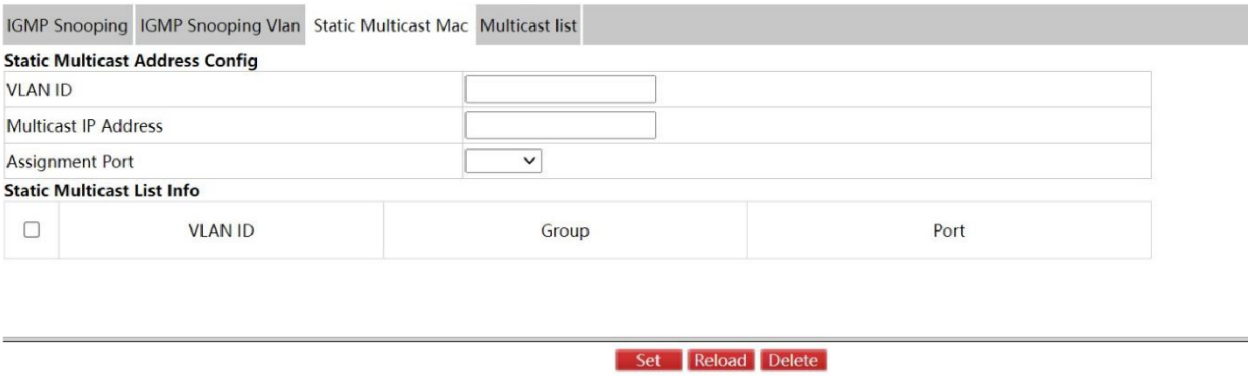


Рисунок 93 – Настройка статического MAC-адреса многоадресной рассылки

На этой странице показаны существующие на данный момент статические мультикастовые группы и их группы портов. Нажмите <Reload>, чтобы обновить содержимое списка.

7.4.4 Список участников многоадресной рассылки

Нажмите [Multicast list], чтобы перейти к списку участников многоадресной рассылки.

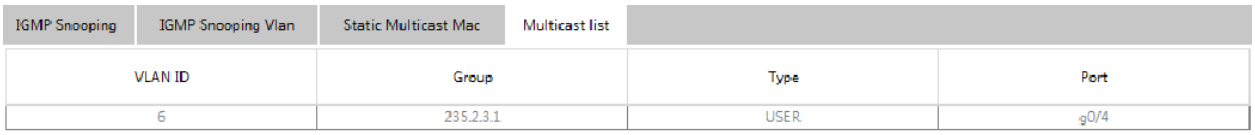


Рисунок 94 – Список участников многоадресной рассылки

На этой странице показаны группы многоадресной рассылки в текущей сети и порты, за которыми находится каждый член группы, учитываемый при помощи IGMP-Snooping. Нажмите <Reload>, чтобы обновить содержимое списка.

По умолчанию список многоадресной рассылки может отображать до 15 элементов VLAN. Вы можете изменить количество элементов многоадресной рассылки при помощи команды **«ip http web igmp-groups»**, войдя на устройство через консольный порт или Telnet.

7.5 VLAN

7.5.1 Настройка VLAN

Нажмите [Switching] → [VLAN] на панели навигации, чтобы перейти на страницу настройки VLAN.

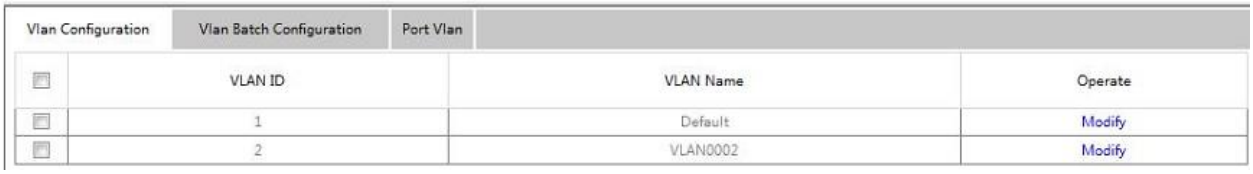


Рисунок 95 – Список VLAN

Нажмите <Modify> в правом столбце выбранной записи, чтобы изменить имя VLAN и функцию порта этой VLAN. Установите флажок перед элементом и нажмите <Delete> на нижней панели управления, чтобы удалить выбранную VLAN.

По умолчанию максимальное количество отображаемых элементов списка VLAN составляет 100. Для изменения количества отображаемых веб-интерфейсом VLAN, войдите в систему через консольный порт или Telnet и в режиме глобальной конфигурации запустите команду **«ip http web max-vlan»**.

Нажмите <Create> или <Modify>, чтобы открыть окно настройки VLAN.

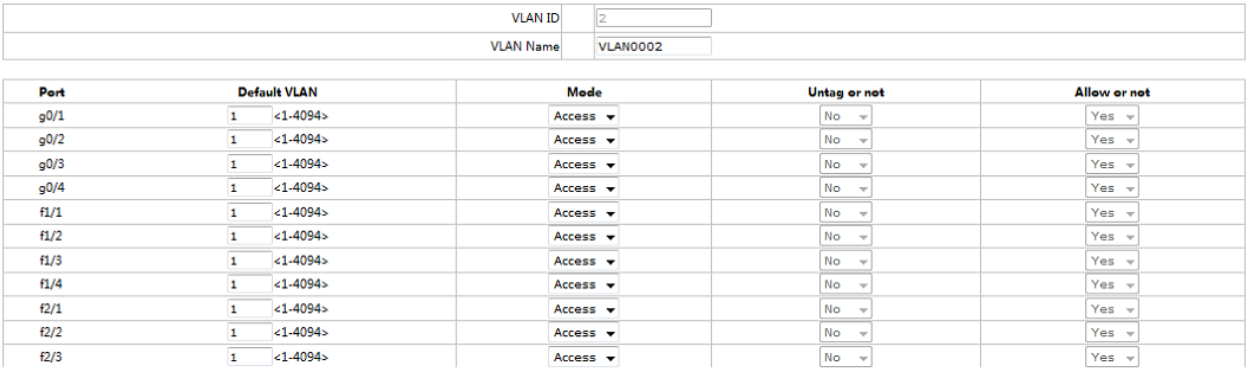


Рисунок 96 – Настройка VLAN

Если вы хотите создать новую VLAN, введите для нее идентификатор и имя; имя VLAN может быть нулевым.

Также вы можете установить для каждого порта коммутатора следующие параметры: VLAN по умолчанию, режим VLAN (транк или доступ), разрешение входа пакетов текущей VLAN и выполнение снятия тега с пакетов текущей VLAN при передаче их через выбранный порт.

Когда транковый порт выступает в роли выходного порта, он по умолчанию снимает теги с пакетов Default VLAN.

7.5.2 Настройка группы VLAN

Для одновременной настройки нескольких VLAN выберете [VLAN Batch Configuration] на странице настройки.

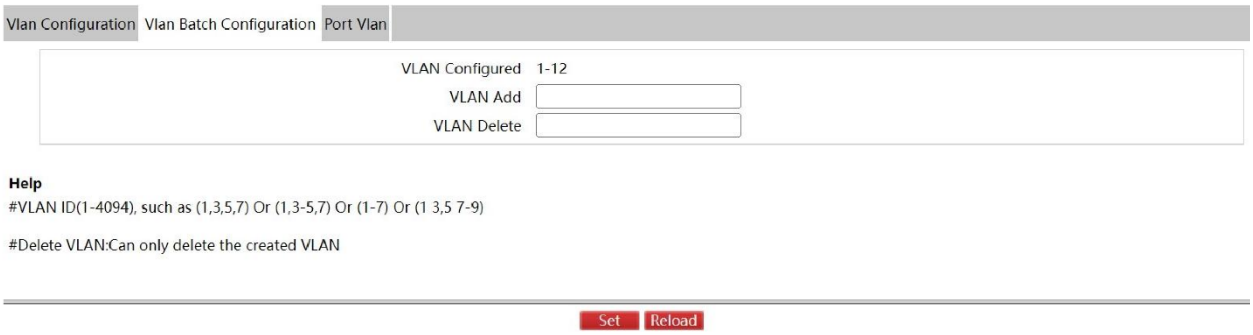
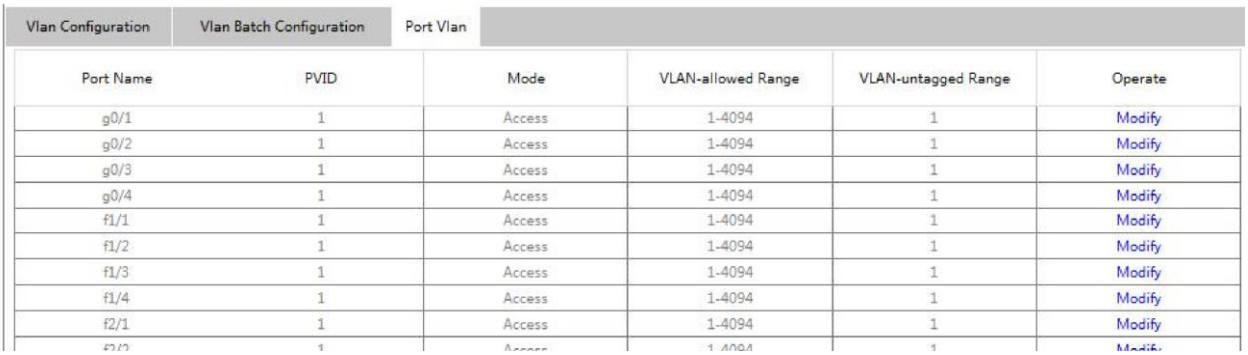


Рисунок 97 – Настройка группы VLAN

Прежде чем VLAN будет удалена, ее следует сначала добавить.

7.5.3 Настройка VLAN на портах

Для просмотра и изменения конфигурации VLAN на портах выберете [Port VLAN] на странице настройки.



Port Name	PVID	Mode	VLAN-allowed Range	VLAN-untagged Range	Operate
g0/1	1	Access	1-4094	1	Modify
g0/2	1	Access	1-4094	1	Modify
g0/3	1	Access	1-4094	1	Modify
g0/4	1	Access	1-4094	1	Modify
f1/1	1	Access	1-4094	1	Modify
f1/2	1	Access	1-4094	1	Modify
f1/3	1	Access	1-4094	1	Modify
f1/4	1	Access	1-4094	1	Modify
f2/1	1	Access	1-4094	1	Modify

Рисунок 98 – Конфигурация VLAN на портах

На этой странице показаны PVID всех портов, режимы, разрешенный диапазон VLAN и диапазон VLAN без тегов. Нажмите <Modify>, чтобы изменить конфигурацию функции VLAN для конкретного порта, включая разрешенные VLAN и VLAN без тегов.

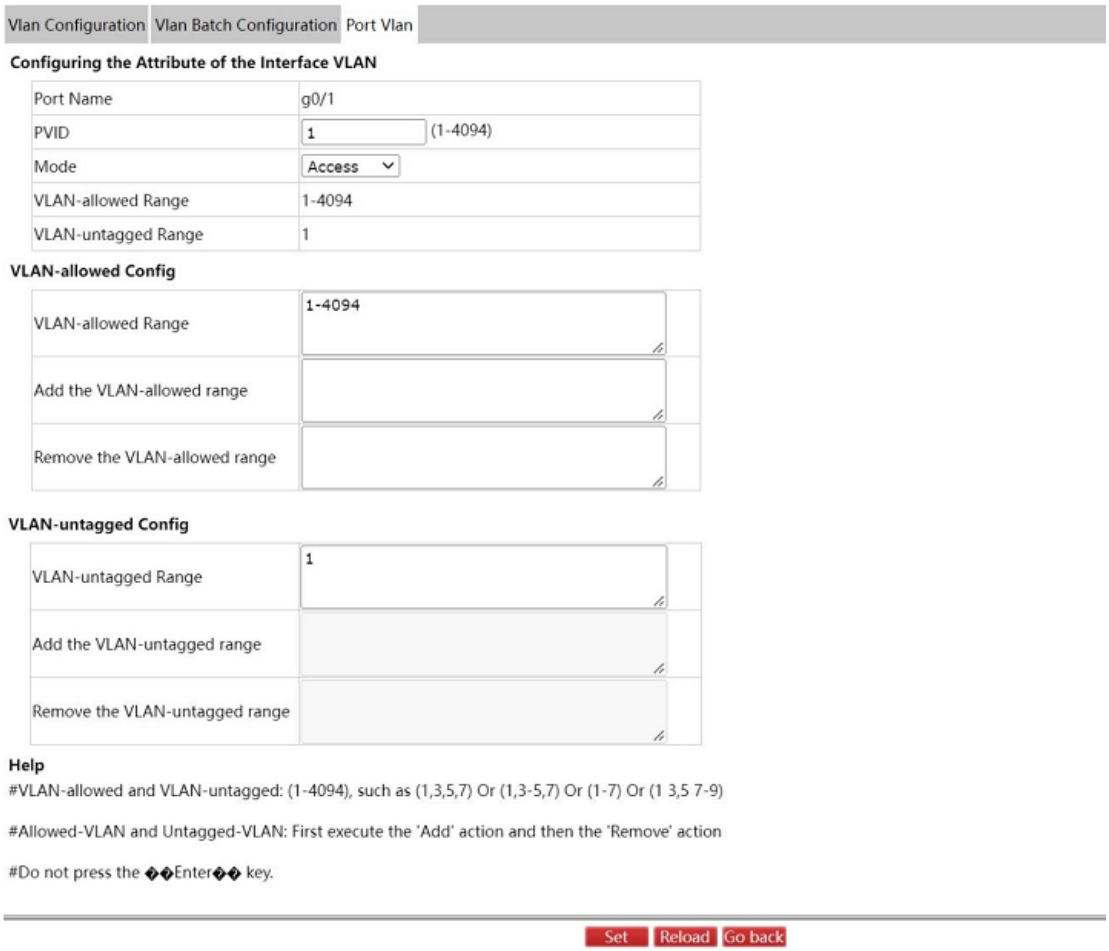


Рисунок 99 – Окно настройки

Разрешенные VLAN и VLAN без тегов следует сначала добавить, прежде чем удалять. Не нажимайте клавишу Enter.

7.6 GMRP

7.6.1 Список VLAN

Нажмите [Switching] → [GMRP] → [VLAN List] на панели навигации, чтобы перейти на страницу настройки.

Рисунок 100 – Список VLAN

На этой странице показан список идентификаторов VLAN GMRP. Нажмите <Reload> на нижней панели управления, чтобы обновить список.

Для создания и настройки новой GMRP-VLAN нажмите <Create> на нижней панели управления.

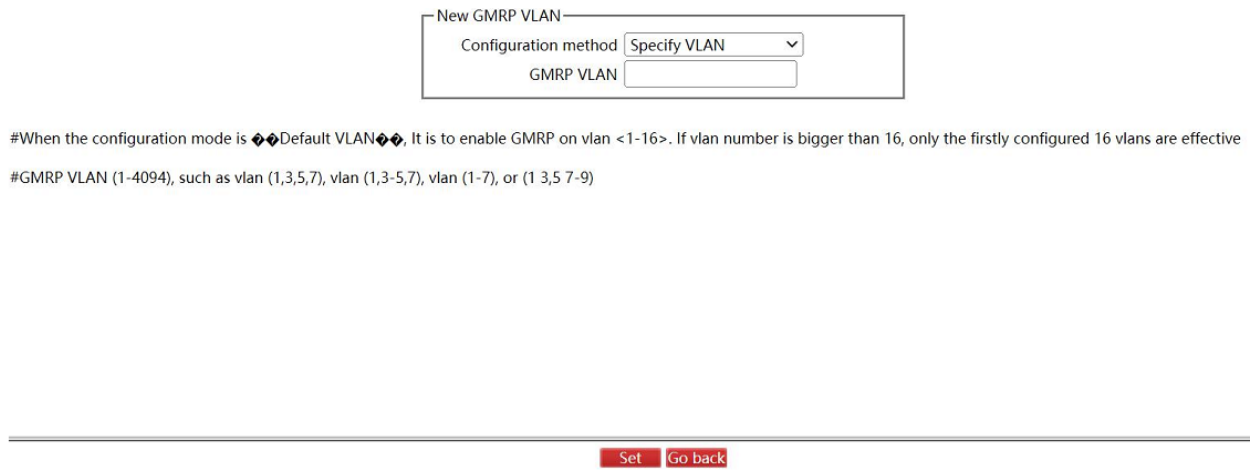


Рисунок 101 – Настройка GMRP для VLAN

7.6.2 Настройка портов

Нажмите [Switching] → [GMRP] → [Port Configuration] на панели навигации, чтобы перейти на страницу настройки.

Port Name	GMRP Status	GMRP Status	GMRP Frames Received	GMRP Frames Transmitted	GMRP Frames Discarded	GMRP Last Pdu Origin
g0/1	Enable	Enabled	0	0	0	0000.0000.0000
g0/2	Enable	Enabled	0	0	0	0000.0000.0000
g0/3	Enable	Enabled	0	0	0	0000.0000.0000
g0/4	Enable	Enabled	0	0	0	0000.0000.0000
g0/5	Enable	Enabled	0	0	0	0000.0000.0000
g0/6	Enable	Enabled	0	0	0	0000.0000.0000
g0/7	Enable	Enabled	0	0	0	0000.0000.0000
g0/8	Enable	Enabled	0	0	0	0000.0000.0000

Help
#Before enabling GMRP on port, please config GMRP VLAN first.

Set Reload

Рисунок 102 – Настройка GMRP на портах

Для завершения настройки нажмите <Set> на нижней панели управления.

7.6.3 Список многоадресной рассылки

Нажмите [Switching] → [GMRP] → [Multicast List] на панели навигации, чтобы перейти на страницу настройки.

Index	VLAN ID	Multicast MAC Address	Port

Reload

Рисунок 103 – Список участников многоадресной рассылки

На этой странице можно посмотреть информацию об участниках многоадресной рассылки, такую как VLAN ID, MAC-адрес и номер порта. Для обновления информации нажмите <Reload>.

8. Маршрутизация

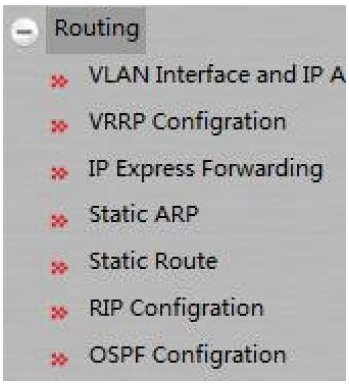


Рисунок 104 – Настройки маршрутизации на панели навигации

8.1 Настройка интерфейса VLAN и IP-адреса

Нажмите [Routing] → [VLAN Interface and IP Address] на панели навигации, чтобы перейти на страницу настройки.

	Name of the VLAN Interface	IP Attribute	IP Address	Directed-Broadcast	Operate
	1	Manual Config	192.168.2.1/24;	off	Modify
	2	Manual Config	182.168.0.2/24;	off	Modify

Рисунок 105 – Настройка интерфейса VLAN и IP-адреса

Нажмите <Modify>, чтобы ввести соответствующие изменения в параметры интерфейса VLAN.

Нажмите <Create>, чтобы создать новый интерфейс VLAN.

Нажмите <Delete>, чтобы удалить выбранный интерфейс VLAN.

Вы можете изменить имя VLAN, нажав кнопку <Create> на нижней панели. Имя VLAN невозможно изменить при нажатии <Modify>, можно только внести изменения в элементы настройки, связанные с VLAN.

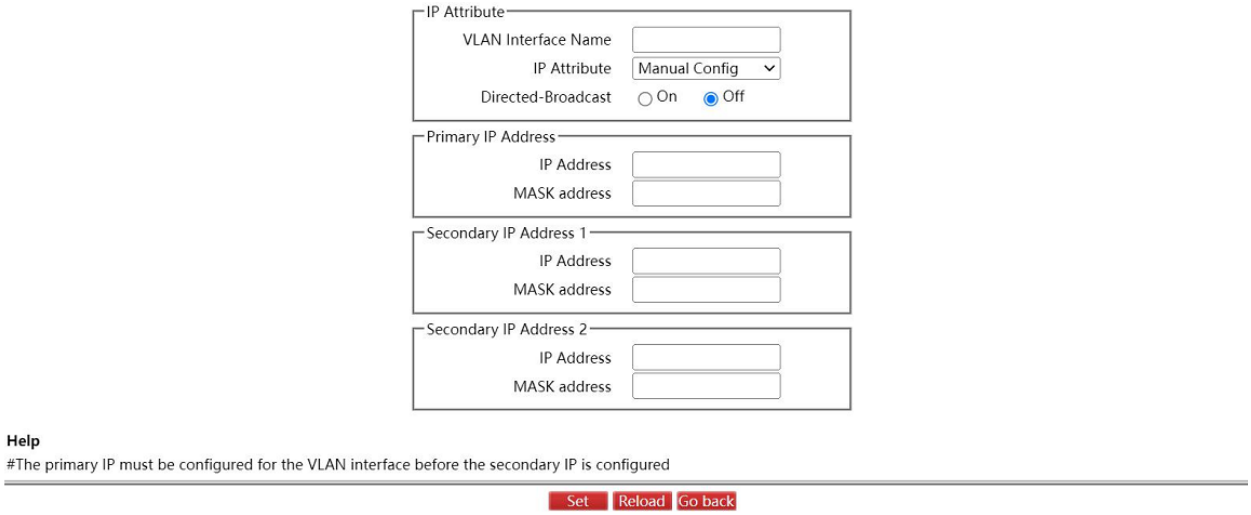


Рисунок 106 – Окно настройки

Прежде чем приступать к настройке вторичного IP-адреса VLAN, необходимо завершить настройку основного IP-адреса.

8.2 Настройка VRRP

Нажмите [Routing] → [VRRP Configuration] на панели навигации, чтобы перейти на страницу настройки.

Рисунок 107 – Список виртуальных маршрутизаторов

Нажмите <Reload> на нижней панели управления для обновления информации в списке VRRP.

Нажмите <Delete> на нижней панели управления, чтобы удалить выбранную конфигурацию VRRP.

Нажмите <Create>, чтобы открыть новую страницу настройки нового виртуального маршрутизатора:

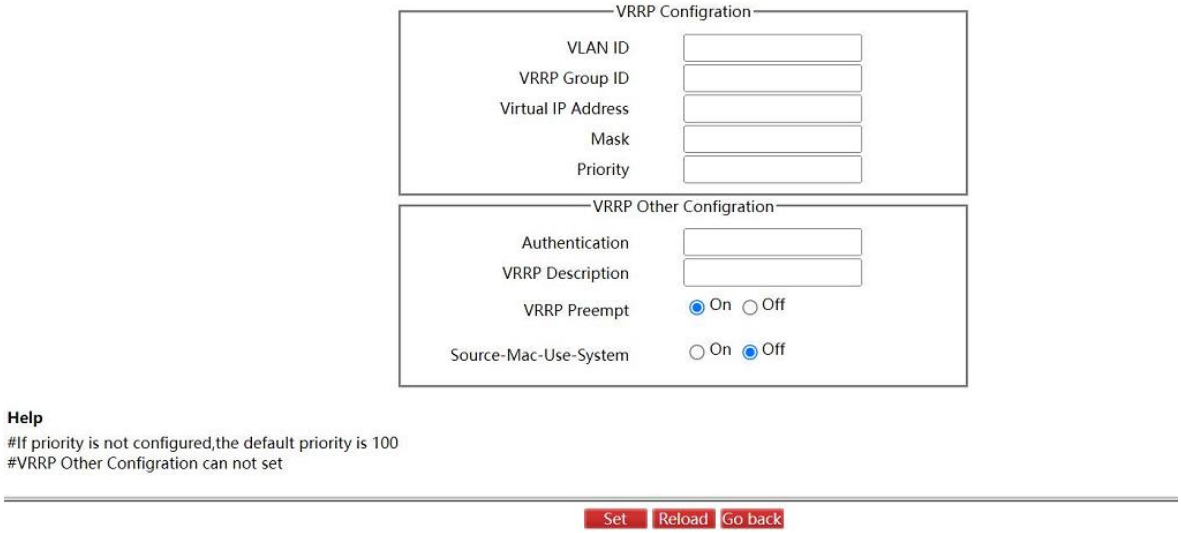


Рисунок 108 – Создание новой конфигурации VRRP

Для завершения настройки нажмите <Set> на нижней панели управления. Для возвращения к списку VRRP нажмите <Go back>

8.3 Высокоскоростная IP-пересылка

Нажмите [Routing] → [IP Express Forwarding] на панели навигации, чтобы перейти на страницу включения функции IP Express Forwarding.

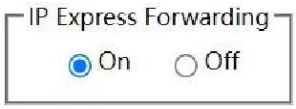


Рисунок 109 – Включение функции IP Express Forwarding

Для завершения настройки нажмите <Set> на нижней панели управления. Для обновления информации о статусе работы функции нажмите <Reload>.

8.4 Статическая настройка ARP

Нажмите [Routing] → [Static ARP] на панели навигации, чтобы перейти на страницу настройки.

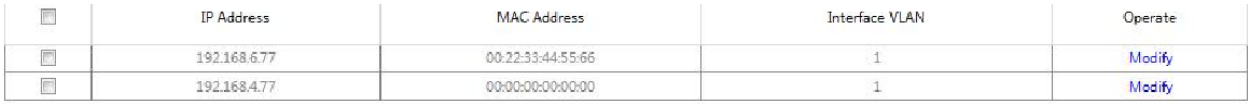


Рисунок 110 – Таблица ARP

Для редактирования существующей записи ARP нажмите <Modify>.

Для удаления выбранной записи нажмите <Delete>.

Для создания новой записи нажмите <Create>:

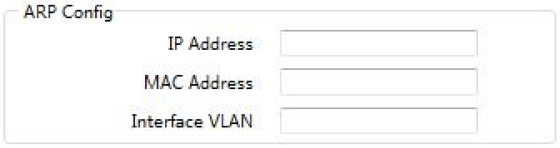


Рисунок 111 – Настройка новой записи ARP

8.5 Настройка статического маршрута

Нажмите [Routing] → [Static Route] на панели навигации, чтобы перейти на страницу настройки.

Рисунок 112 – Статический маршрут

Для редактирования выбранного маршрута нажмите <Modify> справа от записи.

Для обновления информации о маршрутах нажмите <Reload> на нижней панели.

Для удаления выбранной записи нажмите <Delete>.

Для создания нового статического маршрута нажмите <Create>:

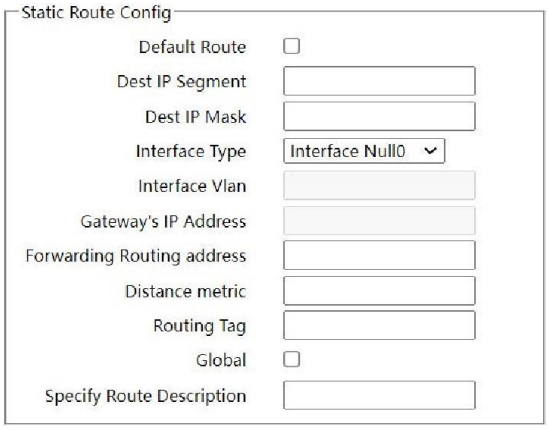


Рисунок 113 – Настройка нового статического маршрута

Только коммутаторы 3-го уровня имеют страницу настройки статического маршрута.

8.6 RIP

8.6.1 Настройка процесса

Нажмите [Routing] → [RIP Configuration] на панели навигации, чтобы перейти на страницу настройки.

Рисунок 114 – Процессы RIP

Прежде чем настраивать запись RIP, необходимо сначала создать процесс RIP.

Для обновления информации о процессах нажмите <Reload> на нижней панели.

Для удаления выбранной записи нажмите <Delete>.

Нажмите <Create>, чтобы создать новый процесс RIP:

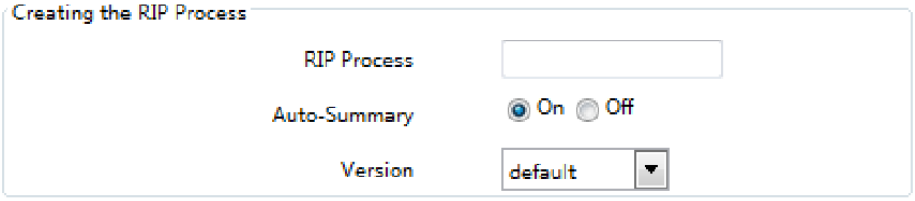


Рисунок 115 – Создание нового процесса RIP

8.6.2 Настройка записей

Для просмотра и изменения записей RIP выберете [RIP Router Entries] на странице настройки RIP.

Рисунок 116 – Выбор процесса RIP

Введите созданный идентификатор процесса RIP. Нажмите <Set>, чтобы перейти на страницу записей выбранного процесса RIP.

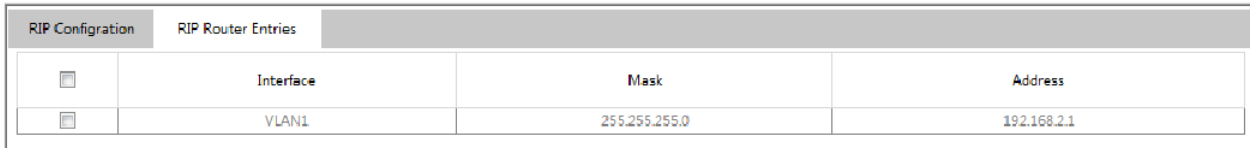


Рисунок 117 – Записи RIP

Нажмите <Create>, чтобы создать новую запись для выбранного процесса RIP.

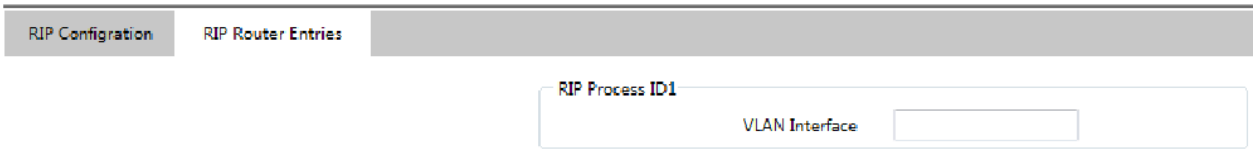


Рисунок 118 – Создание новой записи

8.7 OSPF

8.7.1 Настройка процесса

Нажмите [Routing] → [OSPF Configuration] на панели навигации и выберите вкладку [OSPF Process], чтобы перейти на страницу настройки.

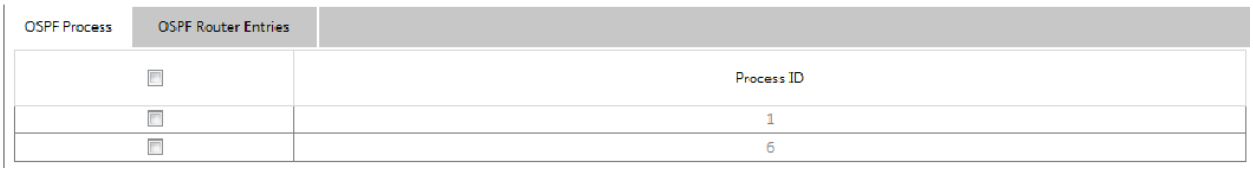


Рисунок 119 – Процессы OSPF

Процесс OSPF должен быть создан до момента начала настройки записей, в противном случае редактирование невозможно.

Для создание нового процесса нажмите <Create>.

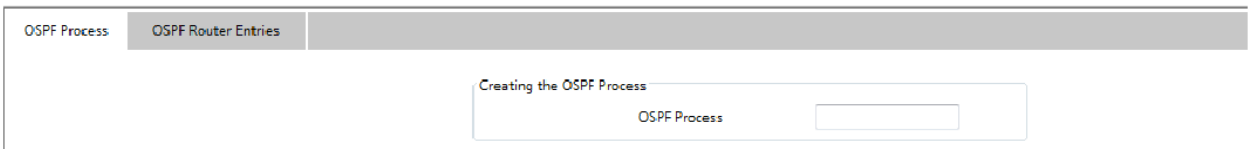


Рисунок 120 – Создание нового процесса OSPF

8.7.2 Настройка записей

Для просмотра и изменения записей OSPF выберете [OSPF Router Entries] на странице настройки OSPF.

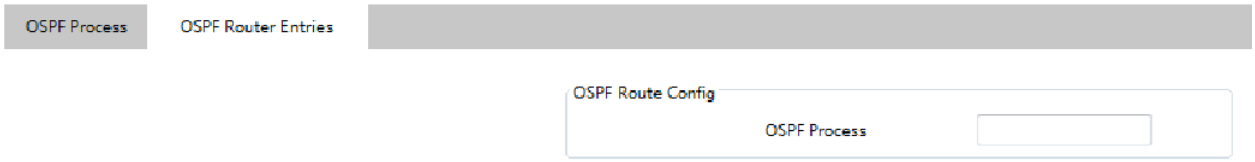


Рисунок 121 – Выбор процесса OSPF

Введите созданный идентификатор процесса OSPF. Нажмите <Set>, чтобы перейти на страницу записей выбранного процесса OSPF.

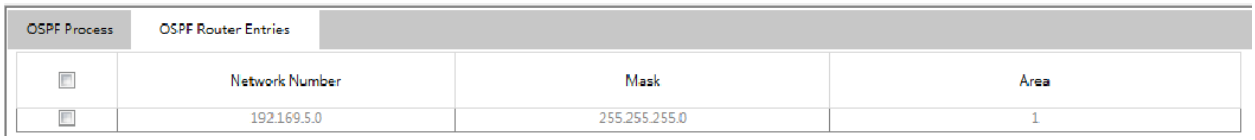


Рисунок 122 – Записи OSPF

Нажмите <Create>, чтобы создать новую запись для выбранного процесса OSPF.

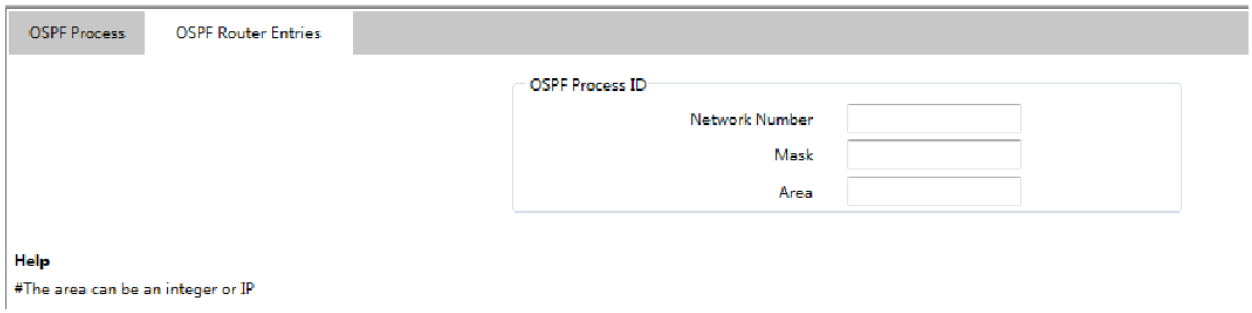


Рисунок 123 – Создание новой записи OSPF

Поле «Area» может принимать формат целого числа или IP-адреса.

9. Приоритеты QoS

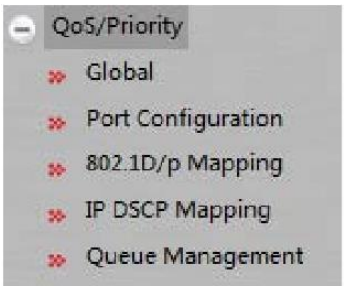


Рисунок 124 – Настройки QoS на панели навигации

9.1 Глобальная настройка

Нажмите [QoS/Priority] → [Global] на панели навигации, чтобы перейти на страницу настройки.

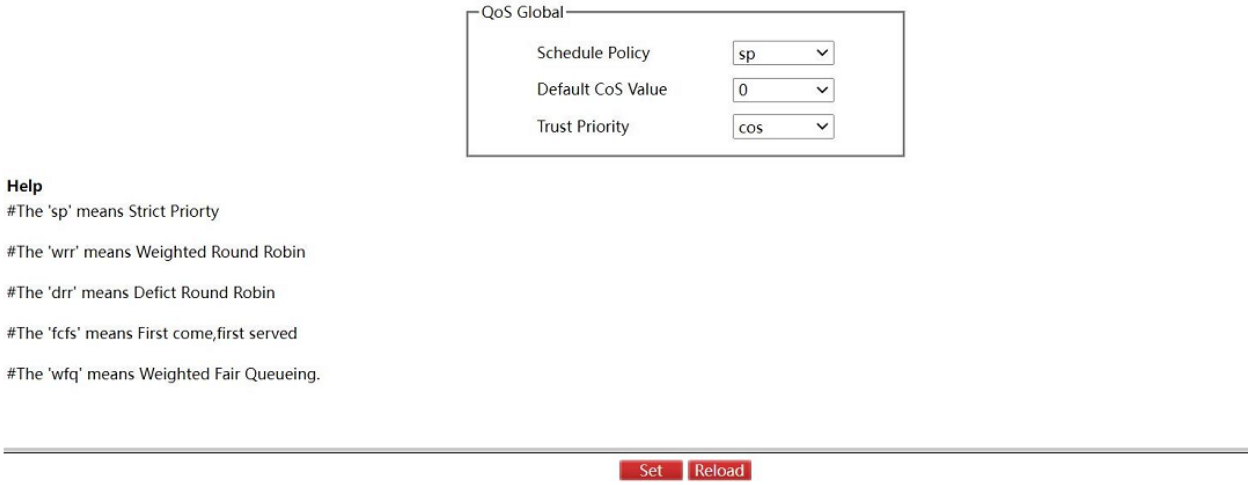


Рисунок 125 – Глобальная настройка QoS

На странице глобальной настройки QoS можно настроить политику расписания, значение CoS по умолчанию и приоритет доверия.

9.2 Настройка на портах

Нажмите [QoS/Priority] → [Port Configuration] на панели навигации, чтобы перейти на страницу настройки.

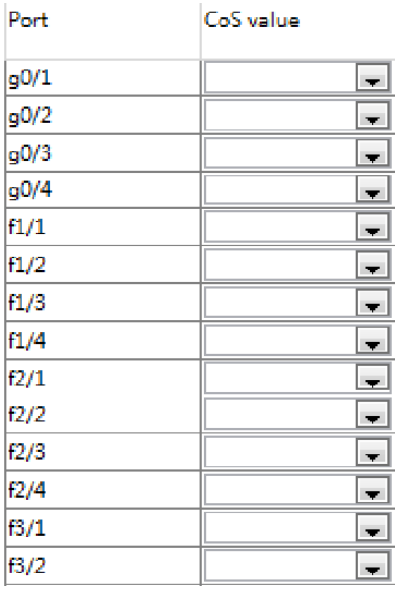


Рисунок 126 – Значение CoS на интерфейсах

Вы можете установить значение CoS для каждого порта, а затем нажать <Set>, чтобы сохранить изменения.

9.3 Настройка сопоставления 802.1D/p

Нажмите [QoS/Priority] → [802.1D/p Mapping] на панели навигации, чтобы перейти на страницу настройки.

CoS Value	Queue
0	Queue 1
1	Queue 1
2	Queue 2
3	Queue 4
4	Queue 5
5	Queue 6
6	Queue 7
7	Queue 8

Рисунок 127 – Сопоставление 802.1D/p

Для сохранения настроек сопоставления нажмите <Set>.

9.4 Настройка сопоставления DSCP

Нажмите [QoS/Priority] → [IP DSCP Mapping] на панели навигации, чтобы перейти на страницу настройки.

DSCP	Mapping DSCP Value	Mapping Priority	Mapping Congestion Bits
0		0	
1		0	
2		0	
3		0	
4		0	
5		0	
6		0	
7		0	
8		0	
9		0	
10		0	
11		0	
12		0	
13		0	
14		0	

Рисунок 128 – Сопоставление DSCP

На этой странице перечислены 64 значения DSCP. Вы можете установить значение сопоставления для каждого DSCP. Нажмите <Clear>, чтобы очистить все настройки сопоставления DSCP.

Количество параметров в таблице может различаться в зависимости от модели устройства.

9.5 Управление очередями

Нажмите [QoS/Priority] → [Queue Management] на панели навигации, чтобы перейти на страницу настройки.

Queue ID	Bandwidth Weight
1	1 (1-15)
2	1 (1-15)
3	1 (0-15)
4	1 (0-15)

Рисунок 129 – Настройка полосы пропускания для очереди

Для сохранения настроек нажмите <Set>.

Если для одного идентификатора очереди (Queue ID) установлено значение веса пропускной способности ноль, то значение веса для тех очередей, которые находятся за этим идентификатором, может быть только нулевое.

---

10. Резервирование

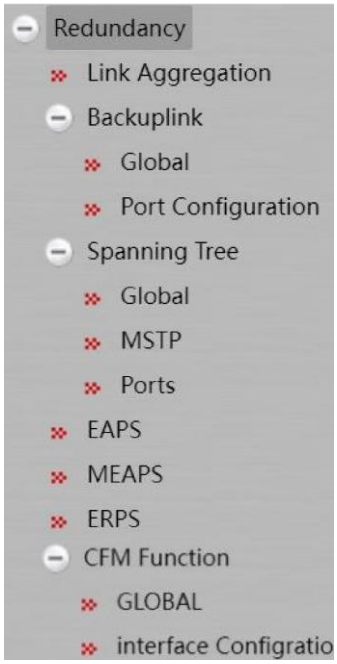


Рисунок 130 – Настройки резервирования на панели навигации

10.1 Агрегация каналов

10.1.1 Настройка агрегации портов

Нажмите [Redundancy] → [Link Aggregation] на панели навигации и выберите раздел <Port Channel>, чтобы перейти на страницу настройки.

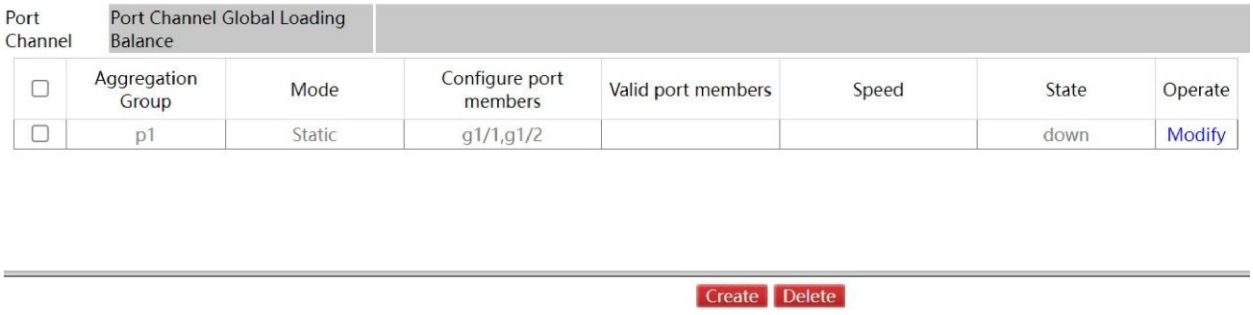


Рисунок 131 – Группы агрегации портов

Нажмите <Modify>, чтобы изменить порты-участники и режим агрегации виртуального порта.

Нажмите <Create>, чтобы создать новую группу агрегации. Через веб-интерфейс можно настроить до 32 групп агрегации. В каждой группе может участвовать до 8 физических портов.

Нажмите <Delete>, чтобы удалить выбранную группу агрегации.

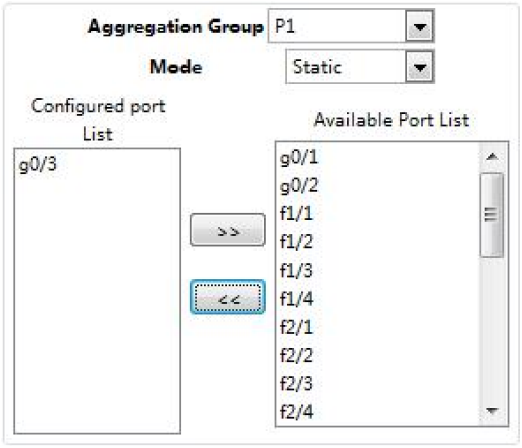


Рисунок 132 – Настройка группы агрегации

Группу агрегации можно выбрать только при ее создании, а не при изменении.

Когда в группе агрегации есть порт-участник, для неё можно выбрать такие режимы агрегации как статический, активный LACP или пассивный LACP.

Вы можете добавить или удалить порт-участник группы с помощью кнопок «>>» или «<<».

10.1.2 Настройка балансировки нагрузки агрегированных каналов

Балансировку нагрузки можно настроить в режиме глобальной конфигурации. Коммутатор поддерживает настройку балансировки нагрузки на основе группы агрегации.

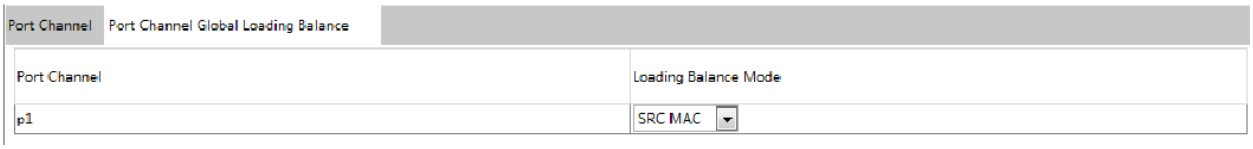


Рисунок 133 – Настройка балансировки нагрузки

Для разных групп агрегации можно установить различные режимы.

10.2 Настройка протокола резервирования канала

10.2.1 Глобальная настройка

Нажмите [Redundancy] → [Backuplink] → [Global] на панели навигации, чтобы перейти на страницу настройки.

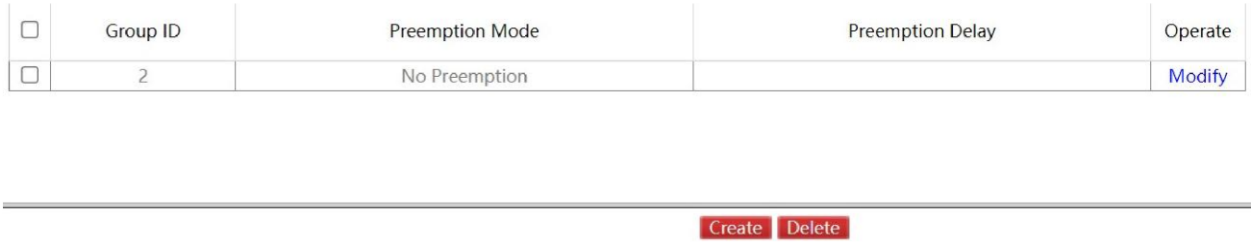


Рисунок 134 – Группы резервирования

На странице указана текущая настроенная группа резервирования канала, включая режим вытеснения и задержку вытеснения. Нажмите <Modify> справа от записи и настройте режим вытеснения и задержку вытеснения для группы. Нажмите <Create>, чтобы создать новую группу.

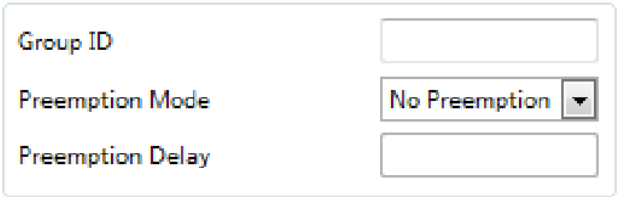


Рисунок 135 – Настройка группы резервирования

- Системой поддерживаются до 8 групп BackupLink, каждая из которых представляет собой определенный набор настроек для резервирования канала.
- Настройка «Preemption Mode» группы резервирования канала определяет политику выбора первичного порта и порта резервирования при передаче пакетов. Режим определяет, в каких случаях и какой порт будет использоваться для передачи данных в ситуации, когда основной порт недоступен или восстанавливается.

10.2.2 Настройка портов BackupLink

Нажмите [Redundancy] → [Backuplink] → [Port Configuration] на панели навигации, чтобы перейти на страницу настройки.

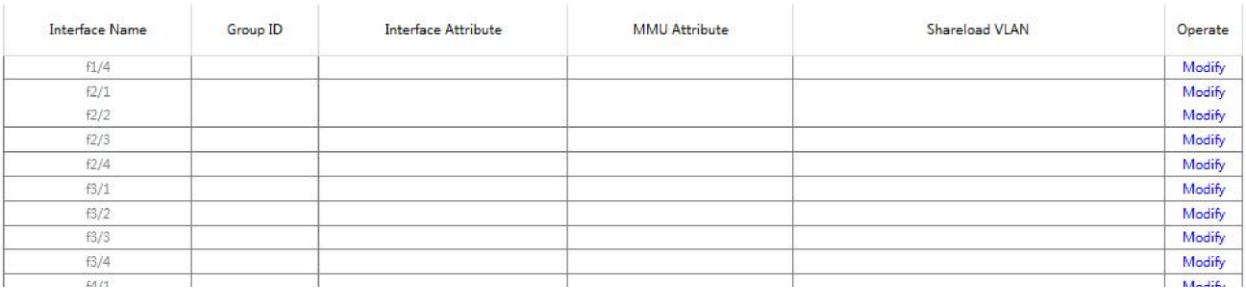


Рисунок 136 – Список портов резервирования канала

На странице указаны порты, участвующие в резервировании каналов, с атрибутами интерфейса и MMU, а также указанием VLAN для управления и разделения трафика между разными устройствами или сегментами сети. Отправка сообщений MMU позволяет их получателю быстро обновлять таблицу MAC-адресов.

Нажмите <Modify> справа от записи, чтобы настроить параметры порта-участника группы BackupLink.

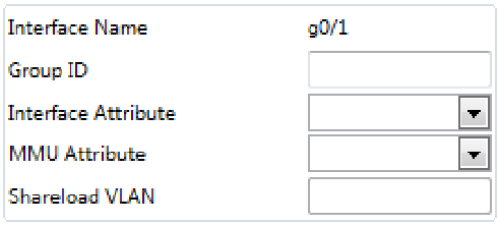


Рисунок 137 – Настройка порта-участника группы BackupLink

После настройки группы в ней нельзя изменить ни основной, ни резервный порт.

10.3 Связующее дерево

10.3.1 Глобальная настройка

Нажмите [Redundancy] → [Spanning Tree] → [Global] на панели навигации, чтобы перейти на страницу настройки.

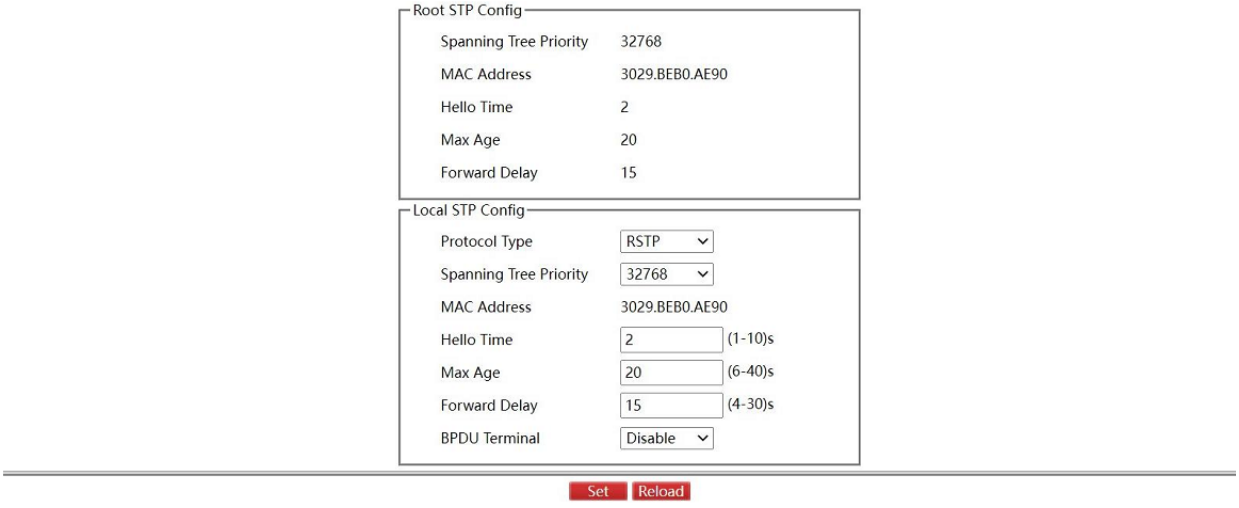


Рисунок 138 – Глобальная настройка STP

На странице можно настроить локальный протокол STP, включая тип протокола, приоритет связующего дерева и т. д. Нажмите <Set>, чтобы сохранить конфигурацию.

10.3.2 MSTP

10.3.2.1 Глобальная настройка

Нажмите [Redundancy] → [Spanning Tree] → [MSTP] на панели навигации, чтобы перейти на страницу настройки.

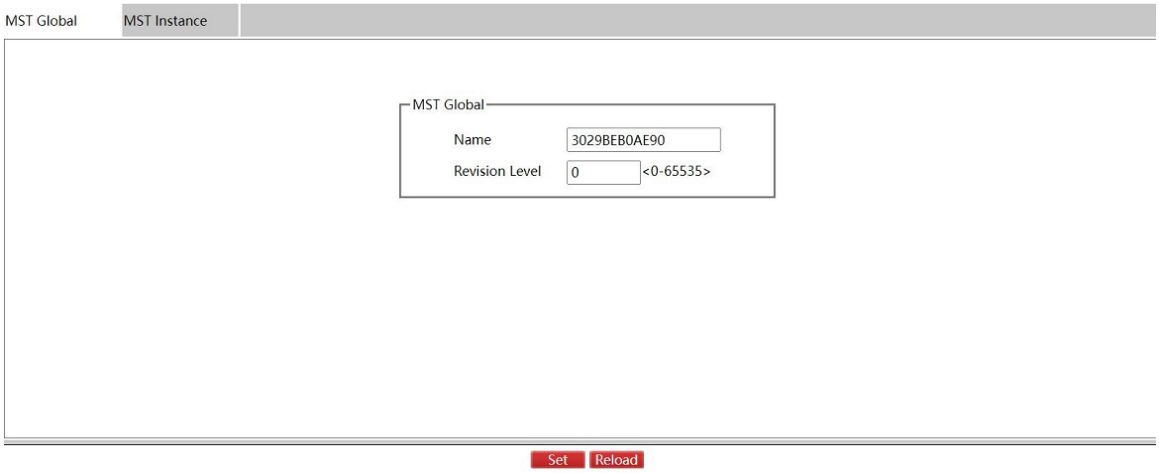


Рисунок 139 – Глобальная настройка MSTP

На этой странице можно установить номер редакции конфигурации MSTP. Для завершения настройки нажмите <Set>.

10.3.2.2 Настройка экземпляра MST

На верхней панели окна настройки MSTP выберите [MST Instance].

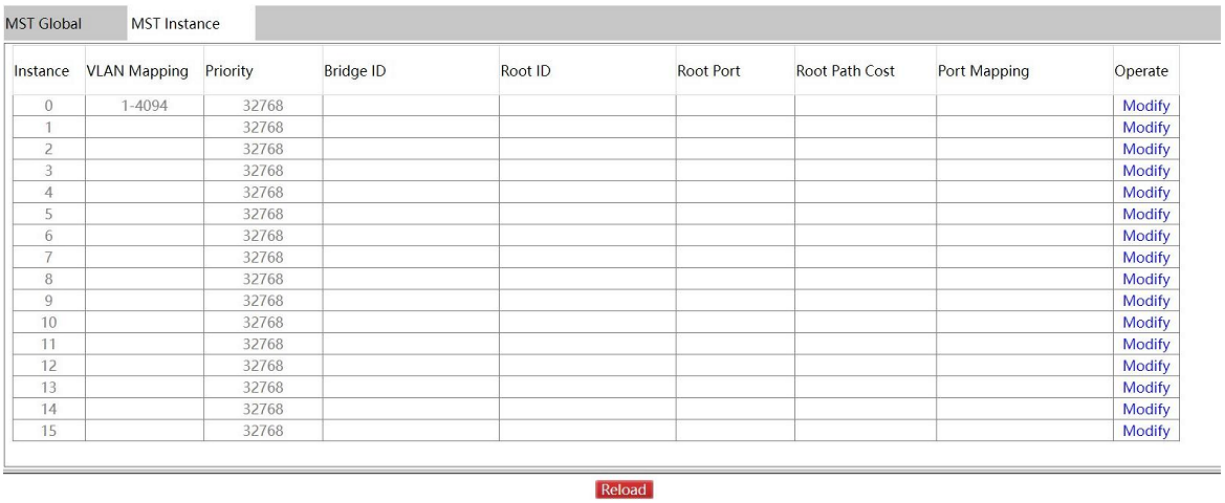


Рисунок 140 – Список экземпляров MST

На странице перечислены параметры, связанные с экземпляром, такие как сопоставление VLAN, приоритет, ID моста, ID корня, корневой порт, стоимость пути до корневого моста, сопоставление портов.

Для обновления информации об экземплярах MST нажмите <Reload> на нижней панели.

Для настройки экземпляра MST нажмите <Modify> справа от записи.

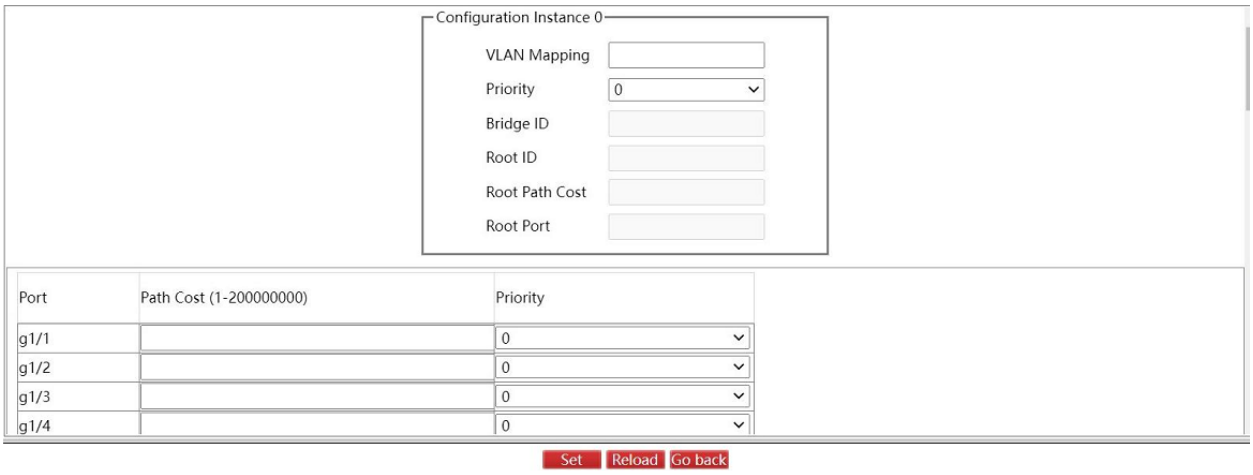


Рисунок 141 – Настройка экземпляра MST

На этой странице можно настроить стоимость пути и приоритеты. Для завершения настройки нажмите <Set>.

10.3.3 Порты связующего дерева

10.3.3.1 Настройка портов

Нажмите [Redundancy] → [Spanning Tree] → [Ports] на панели навигации и выберите раздел [Port Configuration], чтобы перейти на страницу настройки.

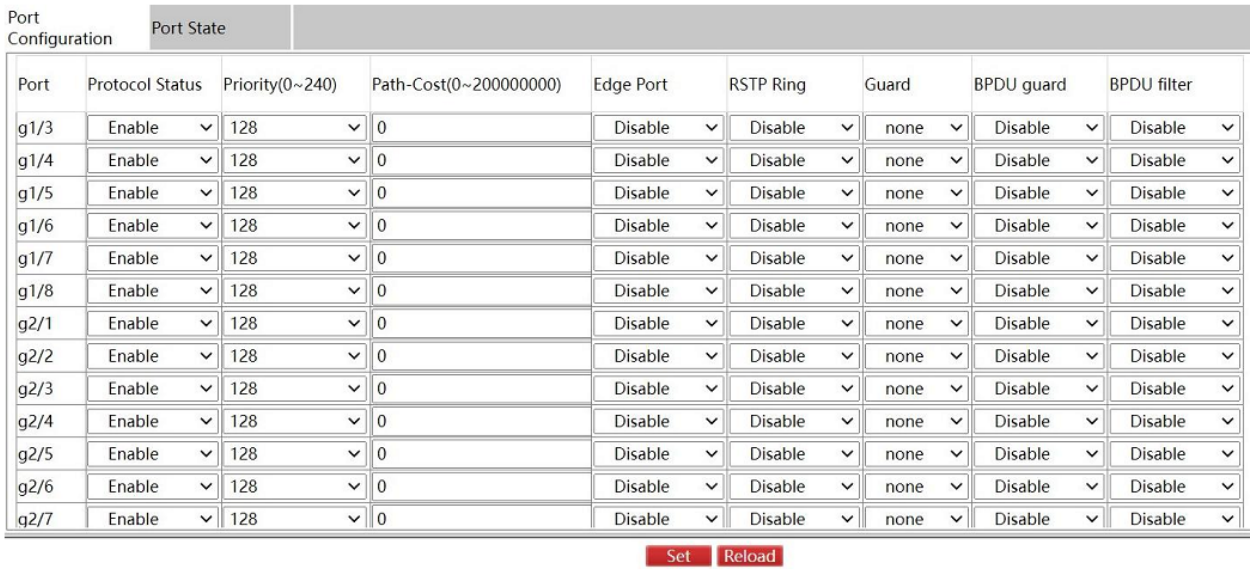


Рисунок 142 – Конфигурация портов

На этой странице отображается состояние протокола, приоритет, стоимость пути, возможность работы в качестве граничного порта, конфигурация BPDU guard и фильтрации BPDU, а также другие параметры, которые можно настроить. После настройки нажмите <Set> на нижней панели управления, чтобы сохранить конфигурацию.

10.3.3.2 Состояние портов

Для просмотра текущего состояния портов связующего дерева нажмите [Port State].

Рисунок 143 – Состояние портов связующего дерева

На этой странице указана информация о портах и статус использования связующего дерева. Для обновления информации нажмите <Reload>.

10.4 EAPS

EAPS (Ethernet Automatic Protection Switching) – протокол канального уровня для создания и поддержки кольцевой топологии сети Ethernet. Нажмите [Redundancy] → [EAPS] на панели навигации, чтобы перейти на страницу настройки.

Рисунок 144 – Список колец EAPS

На странице отображаются настроенные в данный момент кольца EAPS, включая идентификатор кольца, тип узла, описание и состояние кольца, управляющую VLAN, время приветствия, время сбоя, время предварительной пересылки и первичный/вторичный порт на кольце.

Нажмите <Modify> справа от записи, чтобы настроить временные параметры, а также первичный и вторичный порт EAPS.

Нажмите <Create> на нижней панели, чтобы создать новое кольцо EAPS.

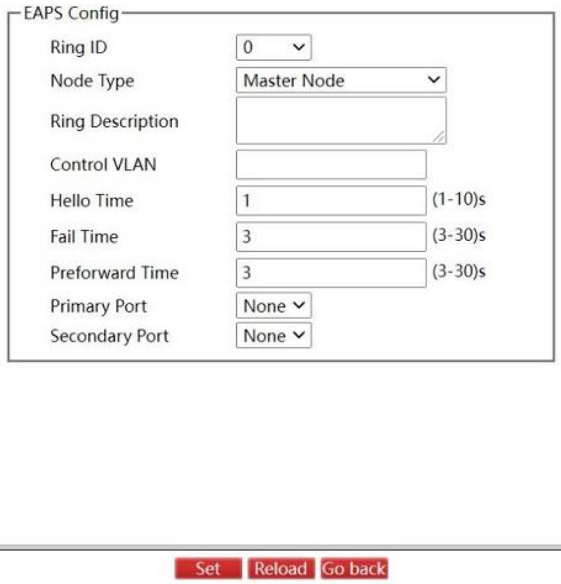


Рисунок 145 – Настройка кольца EAPS

В раскрывающемся списке справа от основного и вторичного порта можно выбрать один из кольцевых портов или оставить значение «None».

- Система поддерживает до 32 колец EAPS.
- После настройки кольца EAPS его идентификатор, тип узла и управляющую VLAN нельзя изменить. Если эти параметры необходимо настроить, удалите выбранное кольцо и создайте новое.

10.5 MEAPS

MEAPS (Multi-Ring Ethernet Automatic Protection Switching) – протокол канального уровня для создания и поддержки кольцевой топологии сети, состоящей из нескольких колец. Нажмите [Redundancy] → [MEAPS] на панели навигации, чтобы перейти на страницу настройки.

Domain ID	Ring ID	Ring Type	Node Type	Control Vlan	Hello Time	Failed Time	Pre Forward Time	Port	Type	Port	Type	Operate
1	2	Major Ring	Master Node	2	3	3	4	None	Primary-Port	None	Secondary-Port	Modify

Рисунок 146 – Список колец MEAPS

На странице отображаются настроенные в данный момент кольца MEAPS, включая идентификатор домена, идентификатор кольца, тип кольца, управляющую VLAN, время приветствия, время сбоя, время предварительной пересылки и первичный/вторичный порт на кольце.

Нажмите <Create>, чтобы создать кольцевую сеть MEAPS.

Нажмите <Modify> справа от записи, чтобы настроить временные параметры, а также первичный и вторичный порт кольцевой сети MEAPS.

- Поддерживается до четырех доменов MEAPS (0–3).
- Поддерживается до восьми колец в одном домене (0–7).
- После настройки кольца MEAPS его идентификатор домена, идентификатор кольца, тип кольца, тип узла и управляющую VLAN нельзя изменить. Если эти параметры необходимо настроить, удалите выбранное кольцо и создайте новое.

Нажмите <Create> на нижней панели или <Modify> справа от записи в списке колец и войдите на страницу настройки MEAPS.

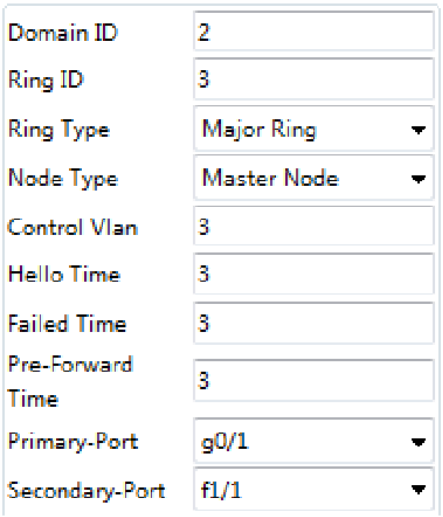


Рисунок 147 – Настройка MEAPS

Для основного кольца можно настраивать только главный и транзитный узел.

Для вторичного кольца можно настраивать первичный, транзитный и граничный узлы.

Первичный и транзитный узлы принадлежат только одному кольцу, а граничный и вспомогательный граничный могут существовать во многих кольцах одновременно.

В текстовых полях «Primary-Port» и «Secondary-Port» выберите порт в качестве кольцевого порта соответственно или выберите «None».

После настройки MEAPS его идентификатор, идентификатор кольца, тип кольца, тип узла и управляющую VLAN нельзя изменить.

10.6 ERPS

Нажмите [Redundancy] → [ERPS] на панели навигации, чтобы перейти на страницу настройки.

Рисунок 148 – Список колец ERPS

На странице отображается настроенные в данный момент кольца ERPS, включая идентификатор кольца, управляющую VLAN, версию протокола, состояние кольца, способ обнаружения сбоя сигнала в ERPS, время ожидания для восстановления кольца, время задержки активации узла ERPS, временной интервал между отправками сообщений о состоянии, первичный и вторичный порт.

- Данная система поддерживает только конфигурацию ERPS с одним кольцом.
- Поддерживается до восьми узлов в кольце ERPS.
- После настройки сети ERPS ее номер, идентификатор кольца, и управляющую VLAN нельзя изменить. Если эти параметры необходимо настроить, удалите выбранную сеть и создайте новую.

Нажмите <Modify> справа от записи, чтобы настроить временные параметры, а также первичный и вторичный порт.

Нажмите <Create>, чтобы создать новое кольцо ERPS.

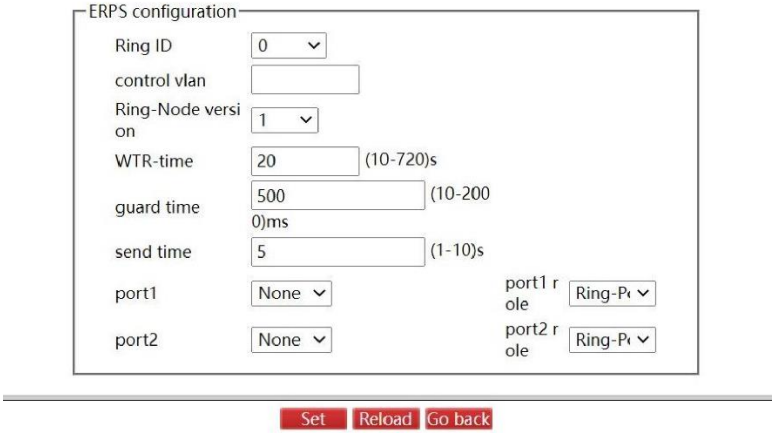


Рисунок 149 – Настройка ERPS

Идентификатор кольца ERPS может принимать значения от 1 до 7.

После настройки портов 1 и 2 необходимо настроить соответствующую роль порта.

В текстовых полях «port1» и «port2» выберите порт в качестве кольцевого порта соответственно или выберите «None».

10.7 Функция CFM

10.7.1 Глобальная настройка

Нажмите [Redundancy] → [CFM Function] → [GLOBAL] на панели навигации, чтобы перейти на страницу настройки.

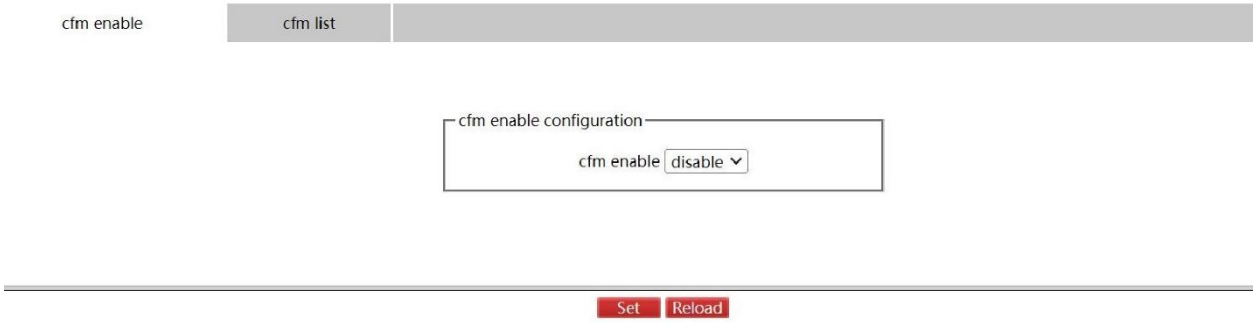


Рисунок 150 – Глобальная настройка CFM

Для завершения настройки нажмите <Set> на нижней панели.

Перейдите в раздел [cfm list]:

Рисунок 151 – Параметры CFM

Для изменения глобальных настроек CFM нажмите <Create> на нижней панели:

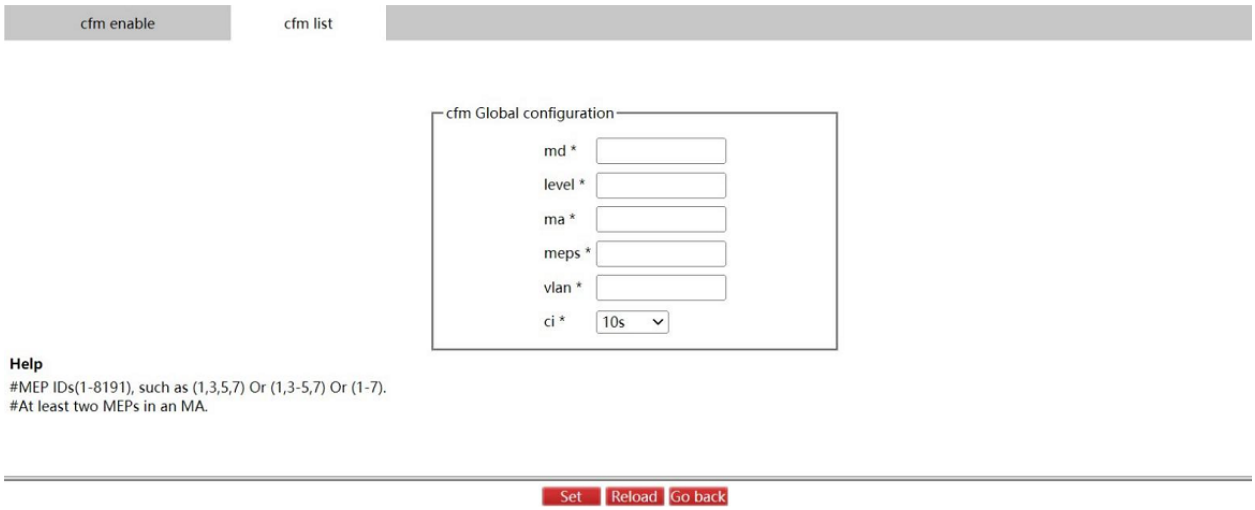


Рисунок 152 – Настройка параметров CFM

После настройки нажмите <Set> на нижней панели, чтобы конфигурация вступила в силу.

Для возвращения на страницу [cfm list] нажмите <Go back>.

10.7.2 Настройка на интерфейсах

Нажмите [Redundancy] → [CFM Function] → [interface configuration] на панели навигации, чтобы перейти на страницу настройки.

Рисунок 153 – Список CFM-портов

Для завершения настройки нажмите <Set> на нижней панели управления.

Чтобы обновить информацию о портах CFM нажмите <Reload>.

Нажмите <Delete> на нижней панели управления, чтобы удалить выбранную конфигурацию порта CFM. Для настройки CFM на порту нажмите <Create>:

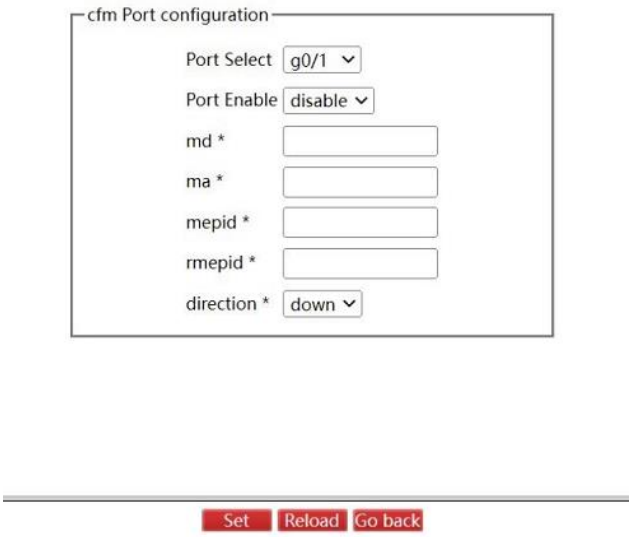


Рисунок 154 – Настройка CFM на интерфейсе

Для завершения настройки нажмите <Set> на нижней панели управления.

Для возвращения к списку CFM-портов нажмите <Go back>.

11. Диагностика

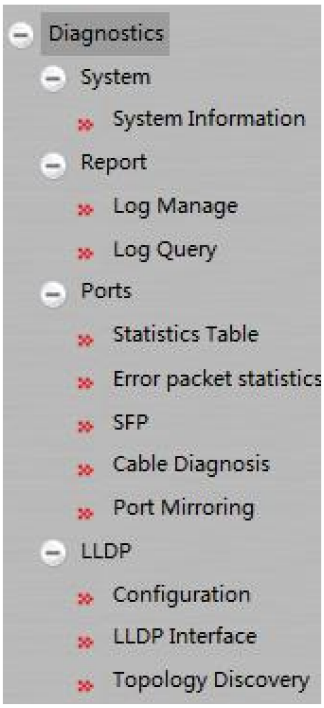


Рисунок 155 – Настройки диагностики на панели навигации

11.1 Система

11.1.1 Системная информация

Нажмите [Diagnostics] → [System] → [System Information] на панели навигации для просмотра информации об устройстве.

System Information

Name	Switch
Device Type	Switch
Serial No.	20043303473
MAC Address	3029.BE01.7E15
IP Address	192.168.2.1
CPU Usage	19%
Memory Usage	57%
Power Supply 1	Abnormal
Power Supply 2	Normal
Uptime	0 Day ,2:7:29
Current Time	1970-1-1 2:7:28
Temperature(℃)	39

Рисунок 156 – Информация о системе

State of Redundancy Protocols

Portocol	State	Information
STP	Running	RSTP

Рисунок 157 – Состояние протокола резервирования

Port Configuration

Port	Enable	State	Speed	Duplex	Flow Control
g0/1	enabled	up	auto	auto	Off
g0/2	enabled	down	auto	auto	Off
g0/3	enabled	down	auto	auto	Off
g0/4	enabled	down	auto	auto	Off
g0/5	enabled	down	auto	full	Off
g0/6	enabled	down	auto	full	Off
g0/7	enabled	down	auto	full	Off
g0/8	enabled	down	auto	full	Off

Рисунок 158 – Конфигурация портов

Port Statistics

Port	Send Bytes	Send Packets	Receive Bytes	Receive Packets	Discard	Discard Rate
g0/1	8221706	22385	2146013	17801	0	0%
g0/2	0	0	0	0	0	0%
g0/3	0	0	0	0	0	0%
g0/4	0	0	0	0	0	0%
g0/5	0	0	0	0	0	0%
g0/6	0	0	0	0	0	0%
g0/7	0	0	0	0	0	0%
g0/8	0	0	0	0	0	0%

Рисунок 159 – Статистика портов

Used Management Ports

Portocol :	SNMP	HTTP	HTTPS
Port:	161	80	443

Display More Diagnostic Information

Reload

Рисунок 160 – Используемые порты управления

На странице указана информация о системе, состояние протоколов резервирования, конфигурация и статистика портов, используемые порты управления. Нажмите <Display more Diagnostic Information>, чтобы просмотреть дополнительную информацию, такую как загрузка ЦП, информация о задачах и т. д.

Tasks:

```
CPU utilization for one second: 21; one minute: 20; five minutes: 20
    P - Pending      D - Delay     R - Ready     S - Suspend   E - Estimated
NAME    ENTRY  TID       PRI    PC       Stk Ptr   SP lmt    ERR.NO ST    CPU    invoked
-------------------------------------------------------------------------------
tExc 812065e4 81f38a78 000 8122f0fc 81f4eba0 81f4ccb8 000000 P    0.00          0
tJob 812076a8 8218f310 000 8122f0fc 8218f1a8 8218d3d0 000000 P    0.00          5
IDLE 80708204 821945e0 255 80708218 82194438 821925e0 000000 R   83.65    3966610
```

Рисунок 161 – Дополнительная информация

11.2 Отчетность

11.2.1 Настройка журналирования

Нажмите [Diagnostics] → [Report] → [Log Manage] на панели навигации, чтобы перейти на страницу управления журналом.

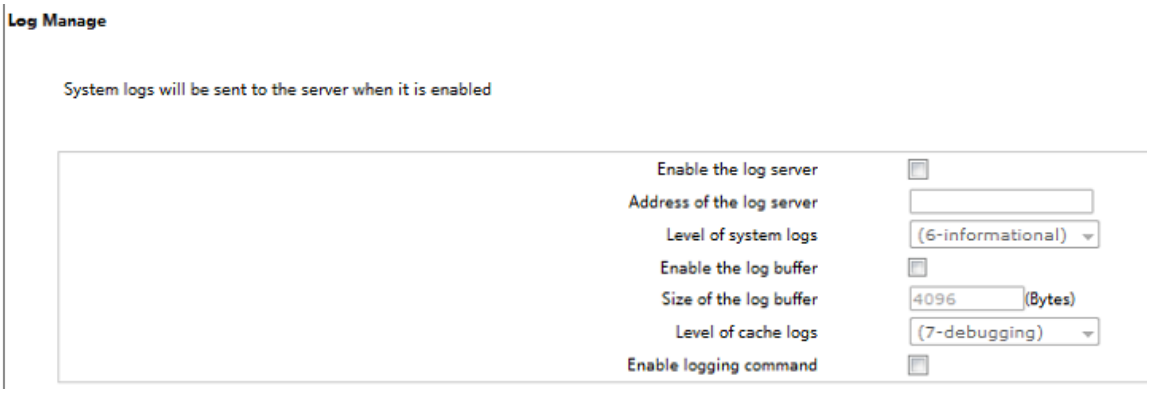


Рисунок 162 – Настройка журналирования

Если выбран параметр «Enable the log server», устройство будет передавать информацию журнала на назначенный сервер. В этом случае необходимо ввести адрес сервера в текстовом поле «Address of log server» и выбрать уровень журналирования в раскрывающемся списке «Level of cache logs» (7 – самый низкий уровень).

Если была выбрана буферизация логов, устройство будет записывать информацию журнала в память. Войдя на устройство через консольный порт или Telnet, вы можете запустить команду **show log**, чтобы просмотреть логи, сохраненные на устройстве. Информация журнала, сохраненная в памяти, будет потеряна при перезапуске устройства. Введите размер буферной области в текстовое поле «Size of the log buffer» и выберите уровень сохраняемых логов в раскрывающемся списке.

11.2.2 Запрос журнала

Нажмите [Diagnostics] → [Report] → [Log Query] на панели навигации, чтобы перейти на страницу настройки запроса.

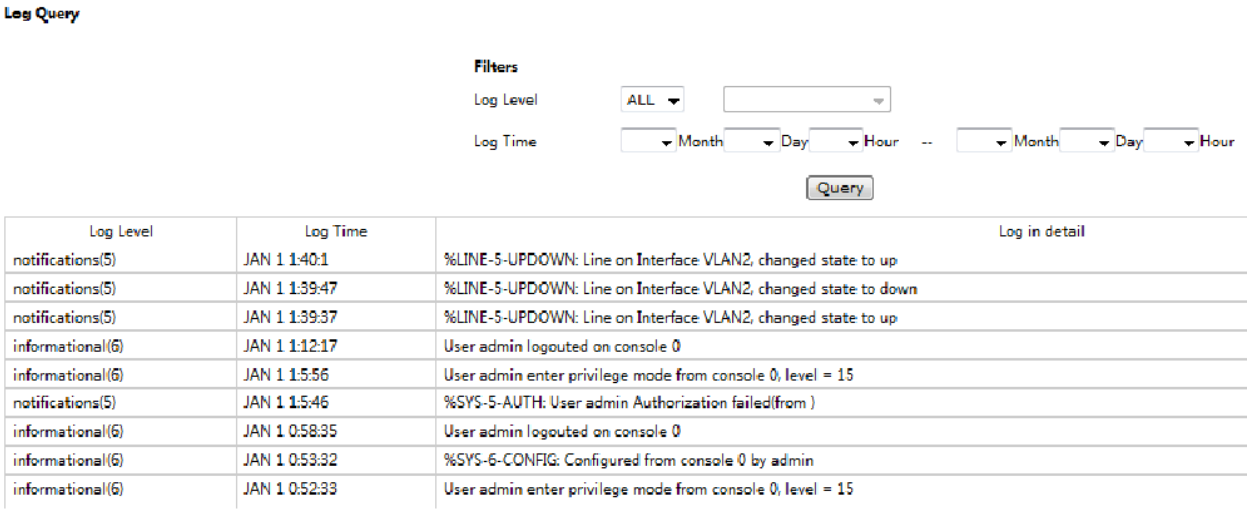


Рисунок 163 – Запрос системного журнала

Для получения интересующей информации укажите в запросе уровень журнала и временной период отображаемых событий. Если не указать временные рамки, коммутатор покажет все сохраненные логи.

11.3 Порты

11.3.1 Таблица статистики

Нажмите [Diagnostics] → [Ports] → [Statistics Table] на панели навигации, чтобы перейти на страницу статистики портов.

Port	Receive Packets	Receive Bytes	Received Unicast Packets	Received Multicast Packets	Received Broadcast Packets	Transmitted Packets	Transmitted Bytes	Transmitted Unicast Packets	Transmitted Multicast Packets	Transmitted Broadcast Packets	Discard	Discard Rate
g0/1	0	0	0	0	0	0	0	0	0	0	0	0%
g0/2	0	0	0	0	0	0	0	0	0	0	0	0%
g0/3	0	0	0	0	0	0	0	0	0	0	0	0%
g0/4	0	0	0	0	0	0	0	0	0	0	0	0%
f1/1	0	0	0	0	0	0	0	0	0	0	0	0%
f1/2	0	0	0	0	0	0	0	0	0	0	0	0%
f1/3	0	0	0	0	0	0	0	0	0	0	0	0%
f1/4	0	0	0	0	0	0	0	0	0	0	0	0%
f2/1	0	0	0	0	0	0	0	0	0	0	0	0%
f2/2	0	0	0	0	0	0	0	0	0	0	0	0%
f2/3	0	0	0	0	0	0	0	0	0	0	0	0%
f2/4	0	0	0	0	0	0	0	0	0	0	0	0%
f3/1	0	0	0	0	0	0	0	0	0	0	0	0%
f3/2	0	0	0	0	0	0	0	0	0	0	0	0%
f3/3	0	0	0	0	0	0	0	0	0	0	0	0%
f3/4	0	0	0	0	0	0	0	0	0	0	0	0%
f4/1	6	384	0	6	0	5862	1432525	0	5818	44	0	0%
f4/2	0	0	0	0	0	0	0	0	0	0	0	0%
f4/3	0	0	0	0	0	0	0	0	0	0	0	0%

Рисунок 164 – Статистика портов

На странице указана информация о порте, включая полученные и отправленные байты и пакеты, тип трафика и т. д.

11.3.2 Статистика ошибочных пакетов

Нажмите [Diagnostics] → [Ports] → [Error Packet Statistics] на панели навигации, чтобы перейти на страницу статистики ошибок.

Port	Received Discard	Received Error Packets	FCS Packets	Jabber Packets	Received Oversize Packets	Received undersize Packets	Transmitted Discard	Transmitted Error Packets	Transmitted Oversize Packets
g1/1	0	0	0	0	0	0	0	0	0
g1/2	0	0	0	0	0	0	0	0	0
g1/3	0	0	0	0	0	0	0	0	0
g1/4	0	0	0	0	0	0	0	0	0
g1/5	0	0	0	0	0	0	0	0	0
g1/6	111	0	0	0	0	0	0	0	0
g1/7	0	0	0	0	0	0	0	0	0
g1/8	0	0	0	0	0	0	0	0	0
g2/1	0	0	0	0	0	0	0	0	0
g2/2	0	0	0	0	0	0	0	0	0
g2/3	0	0	0	0	0	0	0	0	0
g2/4	0	0	0	0	0	0	0	0	0
g2/5	0	0	0	0	0	0	0	0	0
g2/6	118	0	0	0	0	0	45	0	0
g2/7	0	0	0	0	0	0	0	0	0
g2/8	0	0	0	0	0	0	0	0	0
g3/1	0	0	0	0	0	0	0	0	0
g3/2	0	0	0	0	0	0	0	0	0
g3/3	0	0	0	0	0	0	0	0	0

Reload Clear

Рисунок 165 – Статистика ошибок

На этой странице показаны данные связи, включая отброшенные входящие и исходящие пакеты, полученные и переданные пакеты с ошибками, пакеты FCS, пакеты Jabber, полученные и переданные пакеты увеличенного и недостаточного размера и т. д.

Нажмите <Clear> на нижней панели управления, чтобы очистить всю статистическую информацию об ошибках.

11.3.3 Информация SFP

Нажмите [Diagnostics] → [Ports] → [SFP] на панели навигации, чтобы перейти на страницу информации о состоянии SFP-модулей.

Port	TX Power (dBM)	RX Power (dBM)	Temperature (°C)	Supply Voltage (V)	Bias (mA)

Рисунок 166 – Состояние SFP-модулей

Информацию о состоянии SFP-модуля можно прочитать только когда включена функция DDM.

11.3.4 Диагностика кабеля

Нажмите [Diagnostics] → [Ports] → [Cable Diagnosis] на панели навигации, чтобы перейти на страницу настройки.

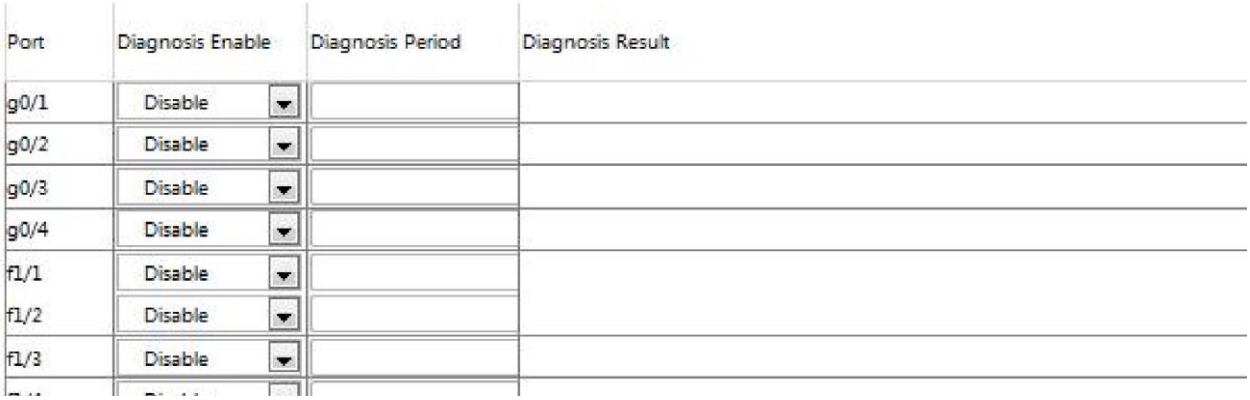


Рисунок 167 – Настройка диагностики кабеля

На этой странице можно включить или отключить функцию, а также настроить период диагностики.

Нажмите <Set>, чтобы просмотреть результаты диагностики.

11.3.5 Зеркалирование портов

Нажмите [Diagnostics] → [Ports] → [Port Mirroring] на панели навигации, чтобы перейти на страницу настройки.

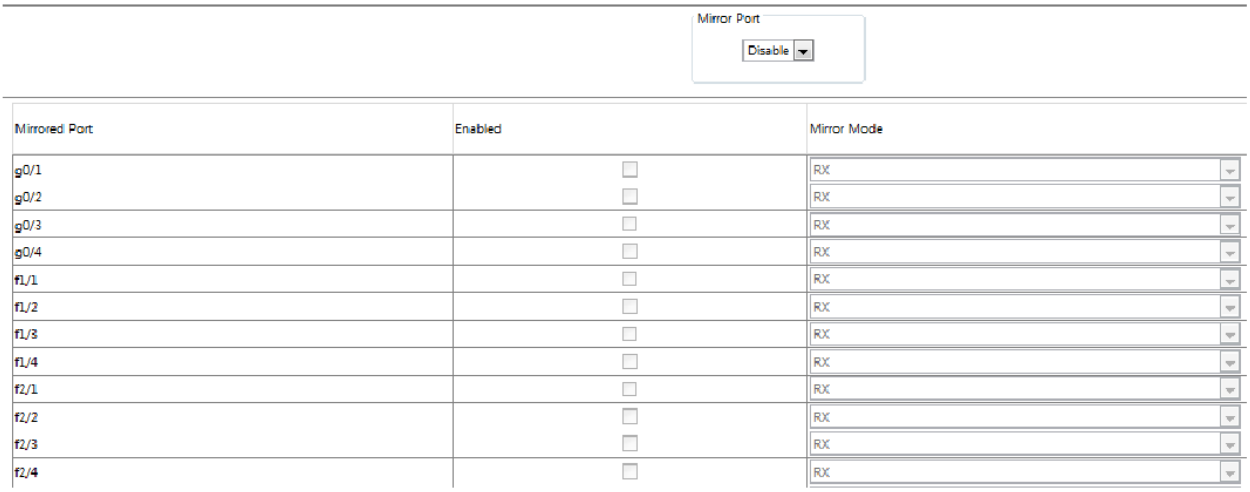


Рисунок 168 – Настройка зеркалирования

В раскрывающемся списке поля «Mirror Port» выберите порт, который будет портом назначения зеркалирования. Установите флажок и выберите порт источника зеркалирования:

- RX – полученные пакеты будут зеркально отражены на порт назначения;
- TX – переданные пакеты будут зеркально отражены на порт назначения;
- RX&TX – будут зеркалироваться и полученные, и переданные пакеты.

11.4 LLDP

11.4.1 Базовая настройка

Нажмите [Diagnostics] → [LLDP] → [Configuration] на панели навигации, чтобы перейти на страницу настройки.

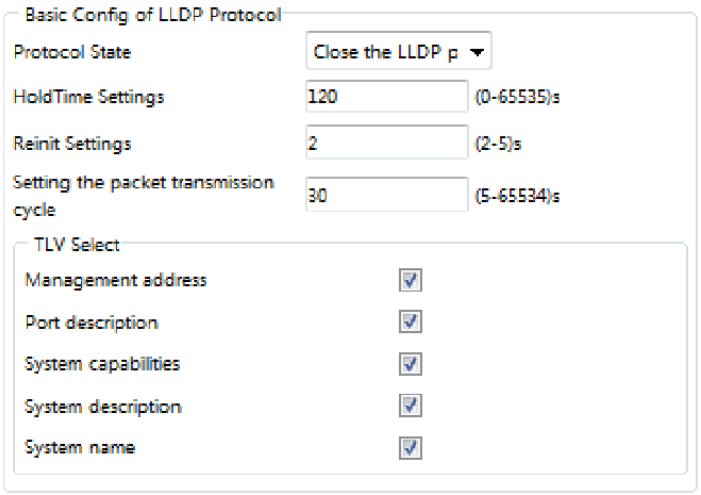


Рисунок 169 – Базовая настройка LLDP

На этой странице можно включить или отключить протокол LLDP. Если функция отключена, настроить LLDP на порту невозможно.

«HoldTime» относится к значению TTL для передачи сообщения LLDP. Значение по умолчанию – 120 с.

«Reinit» относится к задержке передачи LLDP. Значение по умолчанию – 2 с.

11.4.2 Настройка на портах

Нажмите [Diagnostics] → [LLDP] → [LLDP Interface] на панели навигации, чтобы перейти на страницу настройки.

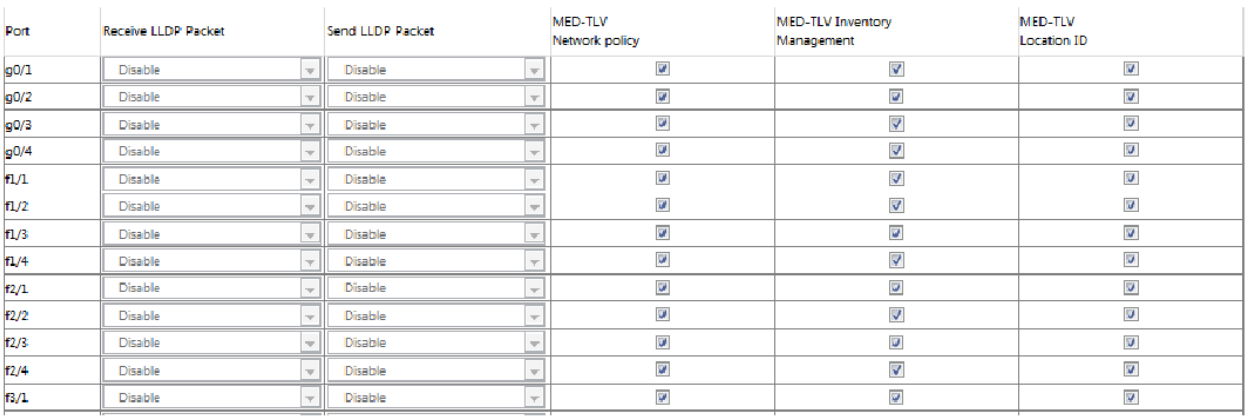


Рисунок 170 – Настройка LLDP на портах

На этой странице можно включить и настроить передачу пакетов LLDP на каждом порту. По умолчанию прием и передача LLDP на портах отключены, но вся информация MED-TLV разрешена.

11.4.3 Обнаружение топологии

Для просмотра информации LLDP нажмите [Diagnostics] → [LLDP] → [Topology Discovery].

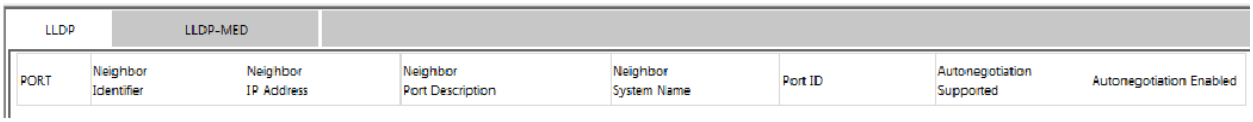


Рисунок 171 – Список обнаруженных устройств

На этой странице перечислены устройства, обнаруженные коммутатором.

12. Расширенные настройки

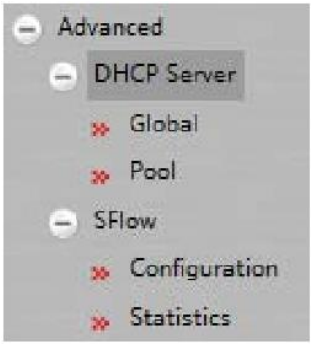


Рисунок 172 – Дополнительные настройки на панели навигации

12.1 DHCP-сервер

12.1.1 Глобальная настройка

Нажмите [Advanced] → [DHCP Server] → [Global] на панели навигации, чтобы перейти на страницу настройки.

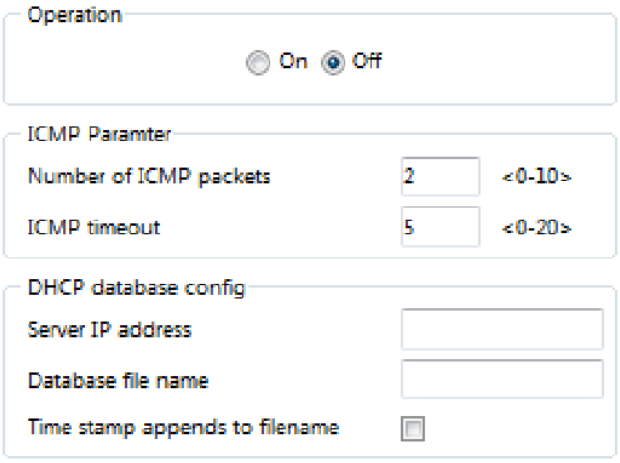


Рисунок 173 – Глобальная настройка DHCP-сервера

На этой странице можно включить или отключить функцию DHCP-сервера. Значение по умолчанию для количества пакетов ICMP – 2, значение тайм-аута ICMP по умолчанию – 5 секунд. Также можно настроить параметры базы данных DHCP, такие как IP-адрес сервера, имя файла базы данных и добавление отметки времени к имени файла.

12.1.2 Настройка пула адресов

Нажмите [Advanced] → [DHCP Server] → [Pool] на панели навигации, чтобы перейти на страницу настройки.

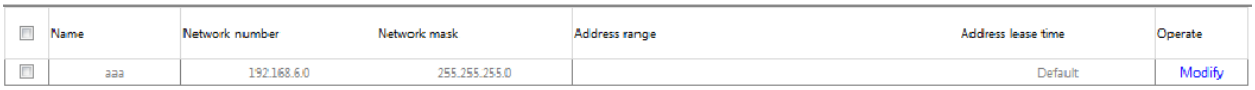


Рисунок 174 – Список настроенных адресных диапазонов

Для создания нового пула нажмите <Create>:

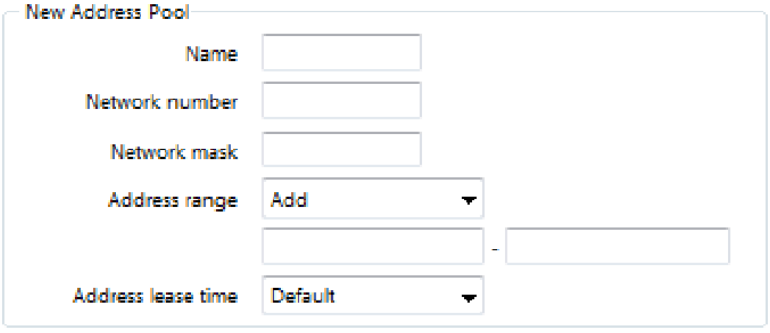


Рисунок 175 – Создание пула адресов

Для изменения параметров существующего пула нажмите <Modify> справа от записи.

12.2 SFlow

12.2.1 Глобальная настройка

Нажмите [Advanced] → [SFlow] → [Configuration] на панели навигации и выберите раздел [Global], чтобы перейти на страницу настройки.

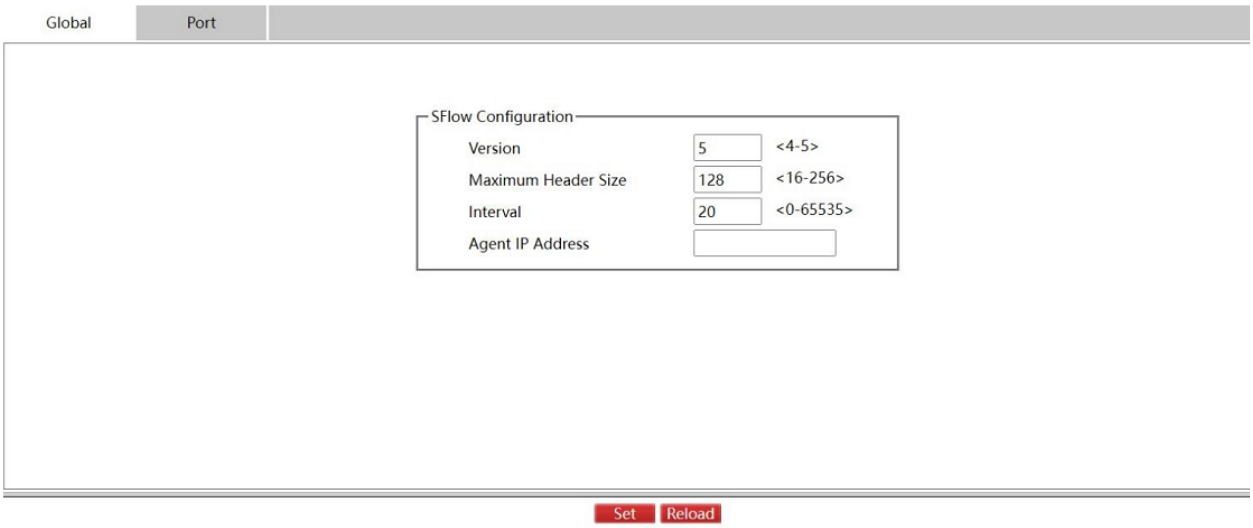


Рисунок 176 – Глобальная настройка SFlow

На этой странице можно настроить IP-адрес агента, версию SFlow и максимальный размер заголовка. Значение по умолчанию – 20 (максимальное значение – 128).

Выберите раздел [Port], чтобы перейти на страницу настройки SFlow на портах.

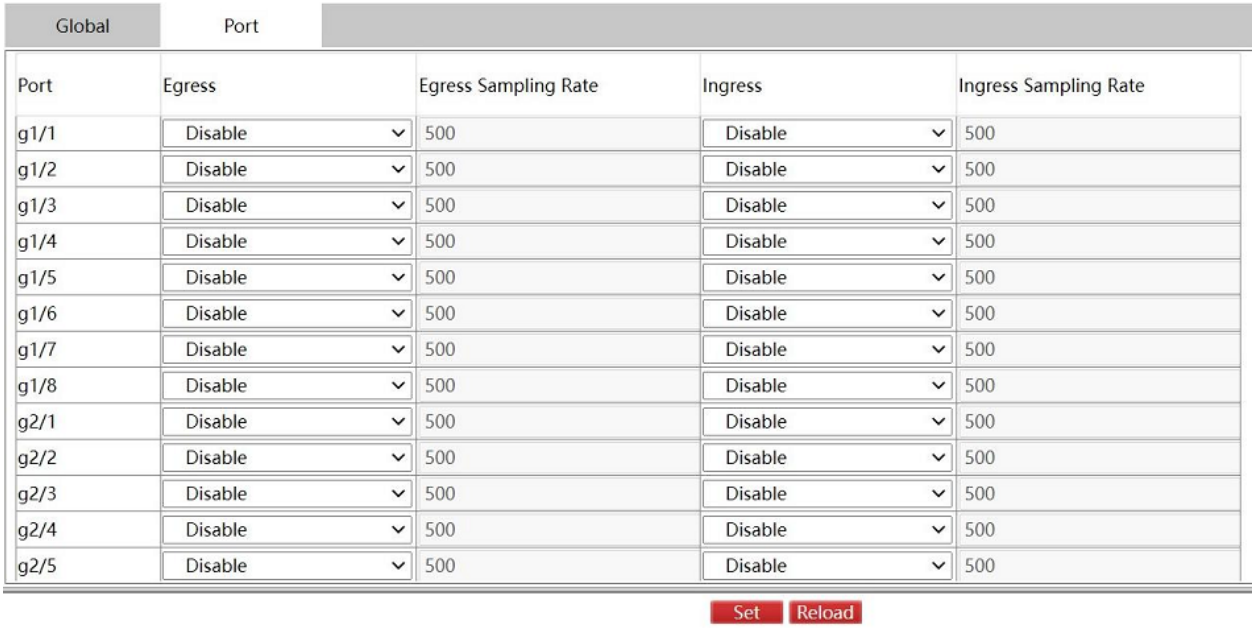


Рисунок 177 – Настройка SFlow на портах

На странице указаны порты со статусом включения/выключения SFlow. Значение по умолчанию для частоты выборки исходящего/входящего трафика равно 500. Это значение можно изменить, когда функция SFlow на порту включена.

12.2.2 Статистика SFlow

Нажмите [Advanced] → [SFlow] → [Statistics] на панели навигации и выберите раздел [Poller], чтобы перейти на страницу с информацией опросчика SFlow.

Рисунок 178 – Статистика поллера

Нажмите [Advanced] → [SFlow] → [Statistics] на панели навигации и выберите раздел [Sampler], чтобы перейти на страницу с информацией о выборках SFlow.

Рисунок 179 – Статистика сэмплера

Расшифровка аббревиатур

ACL	Access Control List	Список управления доступом
ARP	Address Resolution Protocol	Протокол определения MAC-адреса другого узла по известному IP-адресу
BPDU	Bridge Protocol Data Unit	Блок данных протокола управления сетевыми мостами
CFM	Connectivity Fault Management	Протокол обнаружения и устранения проблем сетевой связи
CLI	Command Line Interface	Интерфейс командной строки
CoS	Class of Service	Класс сервиса
DDM	Digital Diagnostics Monitoring	Функция цифрового контроля параметров производительности SFP-трансивера
DHCP	Dynamic Host Configuration Protocol	Протокол динамической настройки узла
DOS	Denial of Service	Отказ в обслуживании (тип сетевой атаки)
DSCP	Differentiated Services Code Point	Точка кода дифференцированных услуг. Использует 6-битное поле 8-битного IP-заголовка DS
EAPS	Ethernet Automatic Protection Switching	Протокол канального уровня для построения и защиты кольцевой топологии Ethernet
ERPS	Ethernet Ring Protection Switching	Кольцевой протокол, использующийся для исключения образования петель в топологии
FCS	Frame Check Sequence	Часть кадра, содержащая контрольную сумму (CRC), используемую для проверки целостности данных внутри кадра
GARP	Generic Attribute Registration Protocol	Протокол регистрации основных атрибутов
GMRP	GARP Multicast Registration Protocol	Протокол GARP для регистрации многоадресных групп
HTTP	Hyper Text Transfer Protocol	Протокол передачи гипертекста
HTTPS	Hypertext Transfer Protocol Secure	Безопасный протокол передачи гипертекста
ICMP	Internet Control Message Protocol	Протокол межсетевых управляющих сообщений
IGMP	Internet Group Management Protocol	Протокол управления группами Интернета (протокол управления многоадресной передачей данных в сетях, основанных на протоколе IP)
IGMP Snooping	Internet Group Management Protocol Snooping	Протокол отслеживания сетевого трафика IGMP
IP	Internet Protocol	Интернет-протокол
LLDP	Link Layer Discovery Protocol	Протокол обнаружения канального уровня

MEAPS	Multi-Ring Ethernet Automatic Protection Switching	Протокол канального уровня для создания и поддержки кольцевой топологии сети, состоящей из нескольких колец
MED	Media Endpoint Discovery	Протокол, используемый для обнаружения и передачи информации о мультимедийных конечных точках в сети
MMU	Multicast MAC Address Update	Многоадресное сообщение об обновлении MAC-адреса
MST	Multiple Spanning Tree	Множественное связующее дерево
MSTP	Multiple Spanning Tree Protocol	Протокол множественного связующего дерева
NAS	Network Access Server	Сервер сетевого доступа
NTP	Network Time Protocol	Сетевой протокол синхронизации времени
OSPF	Open Shortest Path First	Протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала и передающий информацию по наилучшему пути
PTP	Precision Time Protocol	Протокол точного времени
PVID	Port VLAN Identifier	Идентификатор VLAN по умолчанию для порта
QoS	Quality of Service	Качество обслуживания (технология предоставления различным классам трафика различных приоритетов в обслуживании)
RADIUS	Remote Authentication Dial-In User Service	Служба удалённой аутентификации пользователей
RIP	Routing Information Protocol	Протокол дистанционно-векторной маршрутизации
SFlow	Sampled Flow	Протокол, используемый для мониторинга выборочного трафика в сети
SFP	Small Form-factor Pluggable	Промышленный стандарт модульных компактных приемопередатчиков (трансиверов), используемых для передачи и приема данных в телекоммуникациях
SNMP	Simple Network Management Protocol	Простой протокол сетевого управления (интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP)
SSL	Secure Sockets Layer	Уровень защищённых сокетов; криптографический протокол, который отвечает за безопасную передачу данных на сеансовом уровне
STP	Spanning Tree Protocol	Протокол связующего дерева
TCP	Transmission Control Protocol	Протокол управления передачей
TFTP	Trivial File Transfer Protocol	Простой протокол передачи файлов

TLV	Type Length Value	Структура данных, используемая в протоколе LLDP для передачи информации о сетевых устройствах
TTL	Time to Live	предельный период времени или число итераций (переходов), которые пакет данных может осуществить (прожить) до своего исчезновения
UDP	User Datagram Protocol	Протокол пользовательских дейтаграмм
VLAN	Virtual Local Area Network	Виртуальная локальная сеть
VRRP	Virtual Router Redundancy Protocol	Протокол резервирования виртуальных маршрутизаторов