Промышленный управляемый коммутатор STEZ33xxG

Руководство пользователя

Оглавление

Введение

Данное руководство описывает способы доступа и настройки коммутаторов серии STEZ 33xxG. Дано описание настройки коммутаторов через Web интерфейс.

Структура руководства

Руководство разделено на следующие главы：

Основные главы	**Описание**
1. Общие данные	➢ Описание ➢ Функции управления
2. Доступ к коммутатору	➢ Типы доступа ➢ Доступ через консольный порт ➢ Доступ через Telnet ➢ Доступ через Web интерфейс
3. Пользователи	➢ Управление пользователями ➢ Типы авторизации
4. Система	➢ Основная информация ➢ Управление конфигурацией ➢ Управление часами ➢ Обновление программного обеспечения (HTTP, FTP, TFTP） ➢ Выбор активного программного обеспечения ➢ Перезагрузка ➢ Данные о коммутаторе
5. Сервисные функции	➢ Конфигурация SSL ➢ SNMP v1/v2c/v3 ➢ Конфигурация SSH ➢ Конфигурация TACACS+ ➢ Конфигурация RADIUS ➢ DNS

	➢ RMON
6. Настройка тревог	
7. Функции управления	➢ Конфигурация портов ➢ VLAN ➢ IP конфигурация ➢ Агрегация портов ➢ Резервирование ➢ Конфигурация ARP ➢ Конфигурация ACL ➢ Конфигурация MAC адресов ➢ Конфигурация PoE ➢ IGMP snooping ➢ Конфигурация DHCP ➢ Конфигурация IEEE802.1X ➢ GMRP ➢ Статическая маршрутизация ➢ Конфигурация QoS
8. Определение петель	➢ Конфигурация определения петель
9. Функции диагностики	➢ Лог ➢ Зеркалирование портов ➢ Конфигурация LLDP ➢ Трассировка маршрутов ➢ Ping ➢ Конфигурация фильтра IP Source Guard ➢ Диагностика оптических модулей DDM

Принятые обозначения и форматирование

1. Обозначения в тексте руководства

Формат	**Описание**
< >	Текст в < > обозначает название кнопки в интерфейсе. Например, кнопка <Apply>.
[ ]	Текст в [ ] обозначает название окна или меню. Например, кликните пункт меню [File].
{ }	Текст в { } обозначает список связанных параметров. Например, {IP address, MAC address} обозначает, что IP адрес и MAC адрес связаны между собой и могут быть настроены и отображены совместно.
→	Многоуровневые меню разделены с помощью знака →. Например, Start → All Programs → Accessories.
/	Выбор одного варианта из нескольких с помощью знака /. Например, Сложение/Вычитание обозначает сложение или вычитание.
~	Обозначает диапазон. Например, 1~255 обозначает диапазон от 1 до 255.

2. Обозначения командной строки CLI

Формат	**Описание**
Жирный	Команды и ключевые слова. Например, **show version**.
Курсив	Список параметров. Например, для команды **show vlan** *vlan id* необходимо указать значение параметра *vlan id.*

3. Используемые символы

Символ	Назначение
 **Предупреждение:**	Вопросы, требующие внимания во время настройки.
 **Примечание:**	Дополнительная информация.
 **Внимание:**	Вопросы, требующие особого внимания. Неверные действия могут привести к потере данных или повреждению устройства.

Документация

Документация на коммутатор STEZ 33xxG включает в себя：

Наименование документа	Содержание документа
Руководство по монтажу коммутаторов серии STEZ 33xx	Описывает технические характеристики коммутаторов, размеры, способы монтажа.
Руководство пользователя коммутаторов серии STEZ 33xxG	Описывает функции управления коммутаторов, возможности конфигурирования через Web интерфейс.

1 Информация об устройстве

1.1 Обзор

Коммутаторы серии STEZ33xxG включают в себя серию управляемых промышленных Ethernet-коммутаторов. Коммутаторы STEZ33xx представляют собой коммутаторы уровня 2, поддерживают установку до 4-х модулей SFP 100/1000Мбит/с с функцией цифровой диагностики и могут иметь до 8-ми медных портов 10/100/1000 Мбит/с. Коммутаторы серии STEZ33xx имеют конфигурацию до 8 PoE портов IEEE 802.3af/at, до 30 Вт на порт.

Коммутаторы поддерживает семейства протоколов резервирования STRP/DHP, MSTP/RSTP/STP и ST-Ring, поддерживает методы управления CLI, Telnet и Web, а также программное обеспечение для управления сетью на основе SNMPv1/v2c/v3. Продукты серии STEZ 33xxG способны стабильно и надежно работать в промышленных условиях в диапазоне температур от -40 до +75 ^{0}C.

1.2 Программные функции

Коммутаторы STEZ 33xxG содержат множество функций управления, что позволяет использовать данную серию коммутаторов для самых различных приложений.

- Протоколы резервирования: STRP, RSTP/STP, MSTP, ST-Ring;
- Протоколы для работы с Multicast: IGMP Snooping, GMRP;
- Протоколы для работы с атрибутами: VLAN, GVRP, QoS, ARP;
- Управление пропускной способностью: статическая агрегация портов, LACP, ограничение скорости порта, функция подавления широковещательных штормов;
- Безопасность: управление пользователями, управление доступом, SSH, SSL, TACACS+, RADIUS, IEEE802.1X, ACL, IP Source Guard и изоляция портов;
- Протоколы синхронизации времени: SNTP, NTP;
- Управление устройством: обновление программного обеспечения, загрузка/выгрузка конфигурационных файлов, ведение лог файлов с возможностью

их выгрузки;

- Возможности диагностики: зеркалирование портов, LLDP;
- Аварийные сообщения: ошибка питания, ошибка порта, ошибка резервирования, конфликт адресов IP/MAC;
- Управление коммутатором: управление через CLI, Telnet, Web интерфейс, поддержка DHCP, управление и контроль на основе SNMPv1/v2c/v3;
- И многие другие.

2 Доступ к коммутатору

Для доступа к коммутатору можно использовать один из указанных способов подключения:

- Доступ через консольный порт RS-232;
- Доступ по протоколу Telnet/SSH;
- Web интерфейс;
- Доступ через приложение для управления сетью с поддержкой SNMPv1/v2c/v3.

2.1 Уровни доступа через терминал

Управление коммутатором возможно с помощью интерфейса командной строки CLI (command line interface). Для этого необходимо подключиться к консольному порту коммутатора или использовать подключение по протоколу Telnet/SSH. Доступны различные уровни доступа для управления коммутатором.

Таблица 1. Уровни доступа.

Вид командной строки	**Уровень доступа**	**Функции**	**Команда для смены уровня**
SWITCH #	Привелегированный режим	Просмотр ранее введенных команд; Просмотр ответных сообщений на команду ping; Загрузка/выгрузка конфигурационных файлов; Восстановление конфигурации по умолчанию; Перезагрузка коммутатора; Сохранение текущей конфигурации; Отображение текущей конфигурации; Обновление программного обеспечения.	Введите **configure terminal** для перехода в Конфигурационный режим; Введите **exit** для выхода.
SWITCH (config) #	Конфигурационный режим	Доступны все функции.	Введите **exit** или **end** для перехода в Привилегированный режим.

При использовании CLI, символ «?» используется для получения справки. В справочных данных используются следующие форматы. <1,255> обозначает диапазон чисел; <xx:xx:xx:xx:xx:xx> обозначает MAC адрес; <word31> обозначает диапазон значений 1~31. Клавиши ↑ и ↓ могут использоваться для просмотра недавно введенных команд.

2.2 Доступ к коммутатору с помощью консольного порта

Консольный порт имеет разъем RJ45. Доступ к коммутатору с помощью консольного порта можно получить с помощью представленного далее способа.

- DB9-RJ45 консольный кабель

В качестве примера приведен пример подключения с помощью приложения PuTTY.

1. Подключите разъем DB9 к Com порту персонального компьютера (ПК), подключите разъем RJ45 к консольному порту коммутатора. Используйте кабель DB9-RJ45;

2. Запустите приложение PuTTY или аналогичное приложение для эмуляции терминала; см. рис. 1.

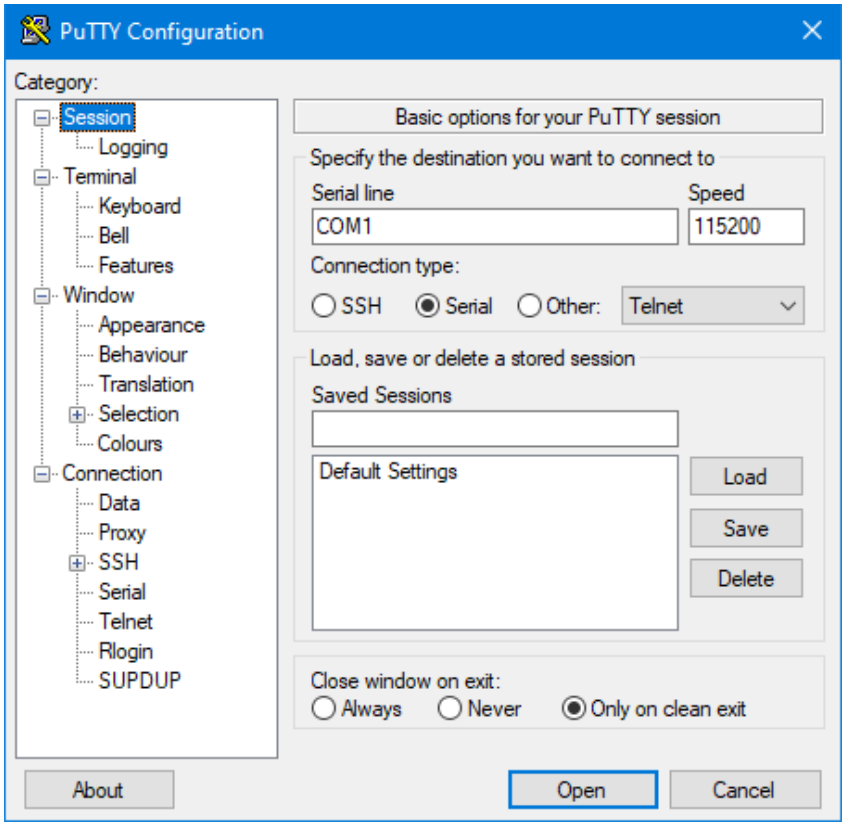


Рис. 1. Выбор типа подключения

3. Перейдите в категорию Serial и задайте параметры порта;

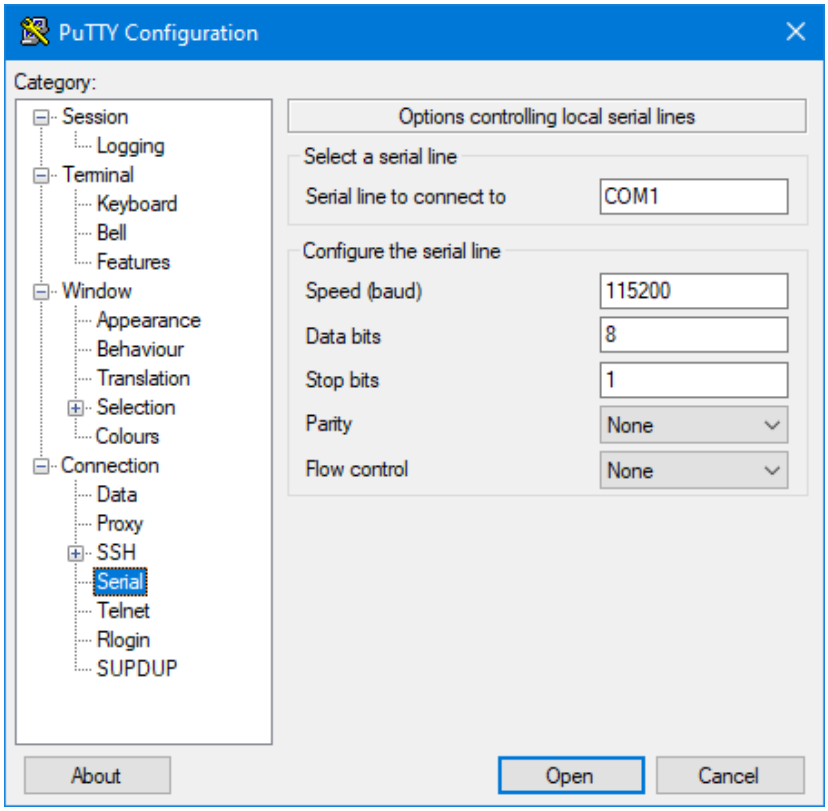


Рис. 2. Настройка параметров COM порта в приложении PuTTY

4. Нажмите <Open> для доступа к CLI интерфейсу;

Для проверки номера используемого Com порта зайдите в диспетчер устройств ПК.

5. Параметры подключения порта: 115200 бит/с, количество бит данных - 8, проверка на четность - Нет, количество стоповых бит - 1, управление потоком - Нет;

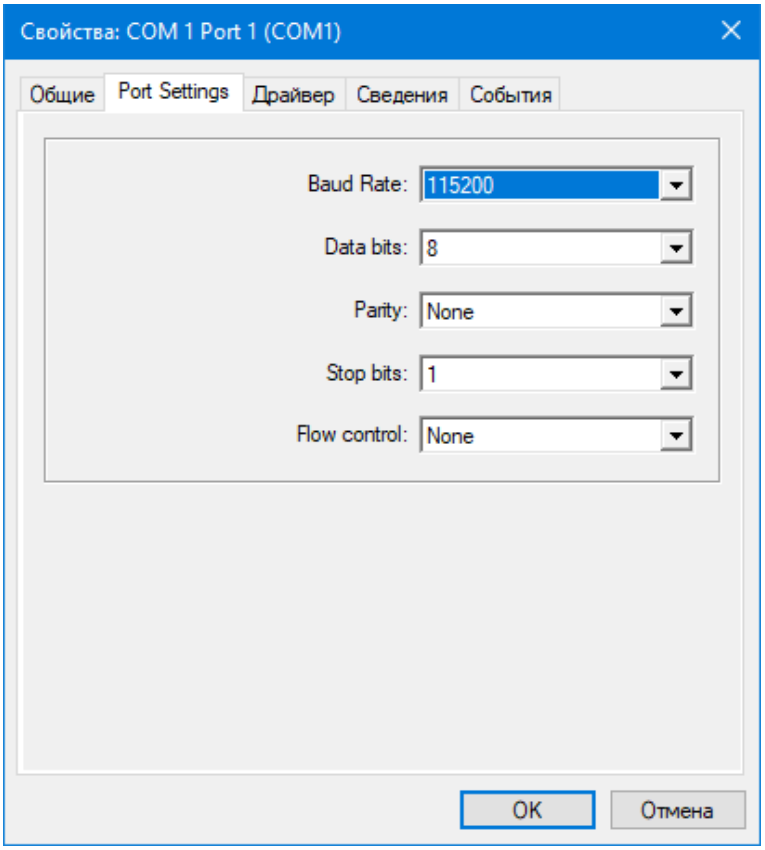


Рис. 3. Конфигурация Com порта

6. В приложении терминала введите имя пользователя «admin», пароль «STEZ». Будет произведен доступ к коммутатору в привилегированном режиме.

2.3 Доступ к коммутатору через Telnet

Для использования подключения через Telnet требуется подключение ПК и коммутатора RJ45-RJ45, корректные сетевые настройки ПК.

1. Настройте подключение по через Telnet. В качестве примера приведен пример настройки в приложении PuTTY для Windows. Укажите IP адрес коммутатора.

IP адрес в приведенном примере 192.168.0.2;

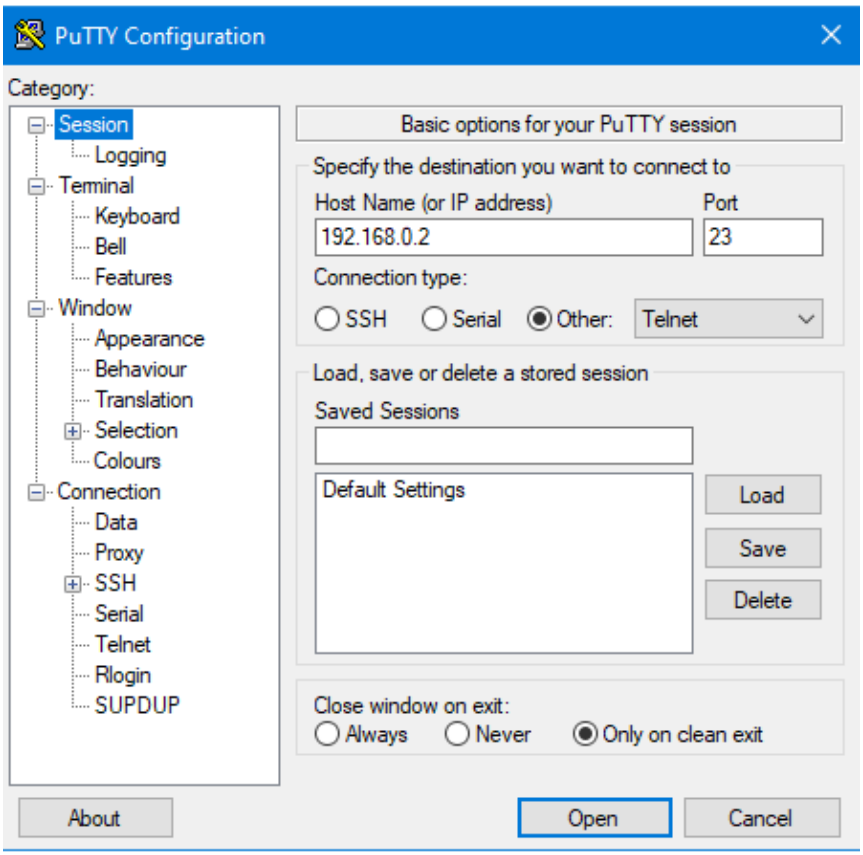


Рис. 4. Настройка доступа через Telnet

Если вы не знаете IP-адрес текущего коммутатора, обратитесь к главе «7.3 Конфигурация IP», чтобы получить IP-адрес.

2. Введите имя пользователя по умолчанию «admin» и пароль «STEZ» в интерфейсе Telnet.

Рис. 5. Интерфейс Telnet

2.4 Доступ к коммутатору через Web интерфейс

Для использования подключения через Web интерфейс требуется подключение ПК и коммутатора RJ45-RJ45, корректные сетевые настройки ПК.

Рекомендуется использовать браузер версии IE8.0 или выше.

1. Введите «IP-адрес» в адресную строку браузера. IP-адрес коммутатора по умолчанию 192.168.0.1 (указан на маркировочной наклейке на коммутаторе). В появившемся диалоговом окне входа в систему введите имя пользователя по умолчанию «admin» и пароль «STEZ».

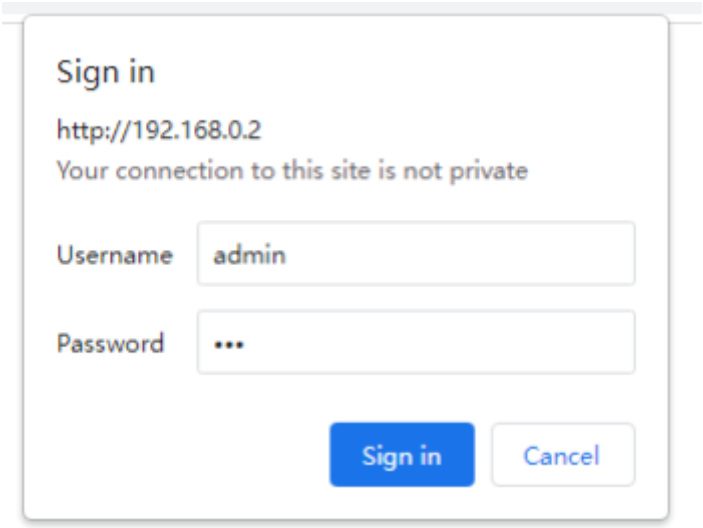


Рис. 6. Подключение через Web интерфейс

Войдите в основной интерфейс. Интерфейс выполнен на английском языке.

Если вы не знаете IP-адрес текущего коммутатора, обратитесь к главе «7.3 Конфигурация IP», чтобы получить IP-адрес.

2. После успешного ввода логина и пароля произойдет переход на Web страницу коммутатора.

3 Пользователи

3.1 Управление пользователями

3.1.1 Введение

Чтобы устранить риски безопасности, вызванные несанкционированным доступом пользователей к коммутатору, коммутатор предоставляет иерархическую функцию управления пользователями, основанную на различных идентификаторах пользователей, различные разрешения формулируются для удовлетворения разнообразных потребностей контроля прав пользователей.

3.1.2 Web конфигурация

1. Создайте нового пользователя, как показано на рисунке далее.

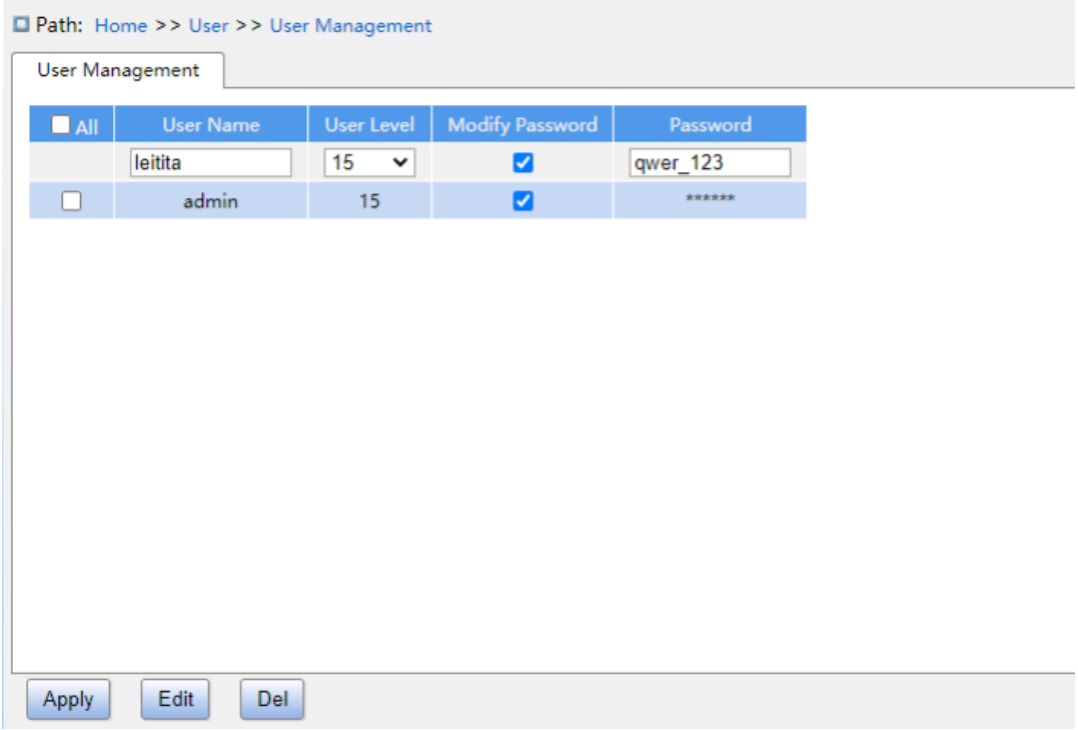


Рис. 7. Создание нового пользователя

Добавьте нового пользователя в поле «User Name», назначьте уровень доступа и пароль. Максимально до 20 пользователей может быть создано. Нажмите <Apply>.

User Name

Диапазон: 1~31 символ

Функция: создание имени пользователя.

User Level

Диапазон: 0~15

Функция: Настройка уровня доступа пользователя.

Password

Диапазон: 0~31 символ

Функция: установка и изменение пароля пользователя

2. Редактирование свойств пользователей показано на рисунке далее.

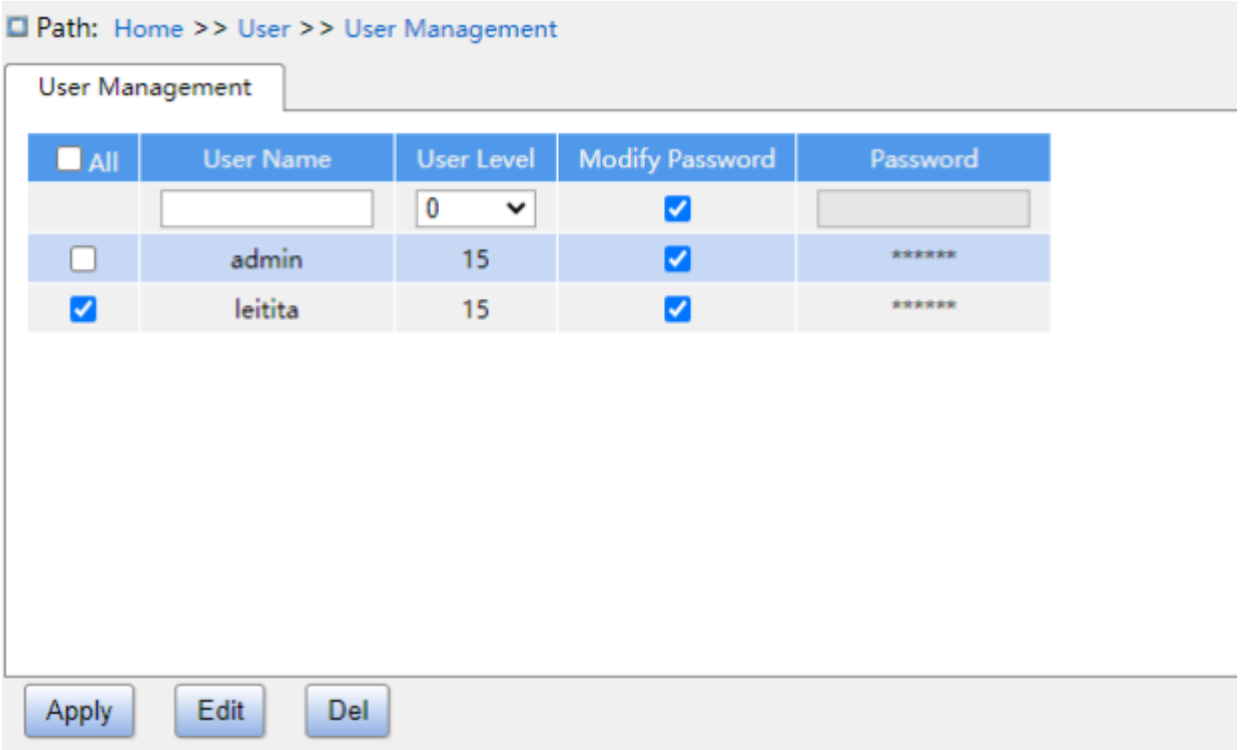


Рис. 8. Редактирование свойств пользователя

Выберите пользователя свойства, которого нужно изменить. Нажмите <Edit> для изменения пароля и уровня доступа.

Нажмите <Del> для удаления отмеченного пользователя.

- Пользователь по умолчанию admin не может быть удален

3. Редактирование уровней доступа для групп пользователей показано на рисунке далее.

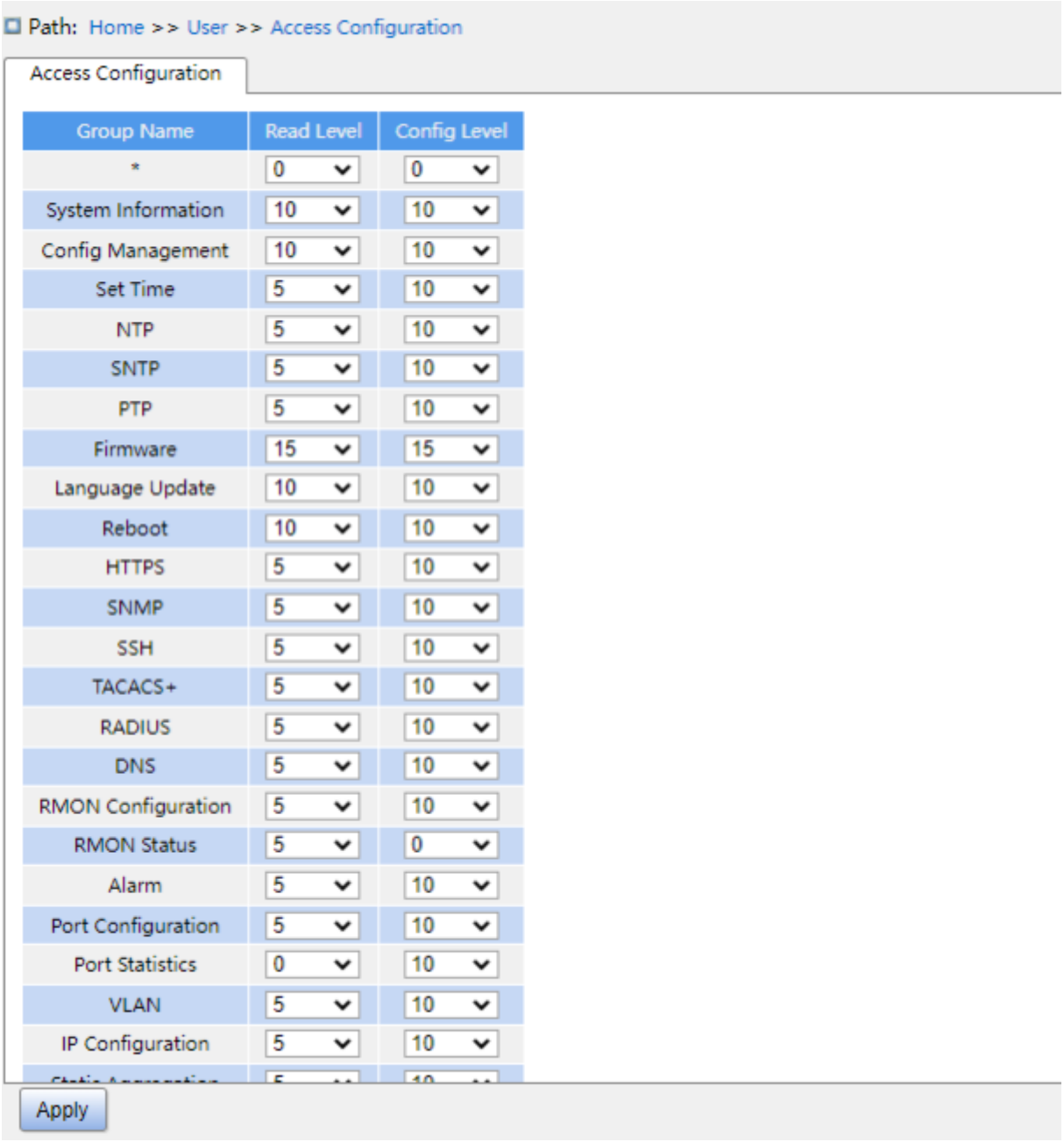


Рис. 9. Редактирование групп пользователей

Group Name

Диапазон: Функциональная группа

Функция: Выберите группу пользователей для настройки уровня доступа

Read Level

Диапазон: 0-15

Конфигурация по умолчанию: 5

Функция: Настройка уровней доступа на чтение данных. Различные уровни отображают различную информацию для пользователя.

Config Level

Диапазон: 0-15

Конфигурация по умолчанию: 10

Функция: Настройка уровня доступа на изменение конфигурации. Различные уровни позволяют производить различные настройки конфигурации.

Если уровень пользователя больше или равен уровня группы, то пользователь может получить доступ на чтение или изменение конфигурации для данной группы.

3.2 Типы аутентификации

Настройте метод аутентификации и последовательность аутентификации, используемые для доступа к методу входа в систему коммутатора, как показано на рисунке далее.

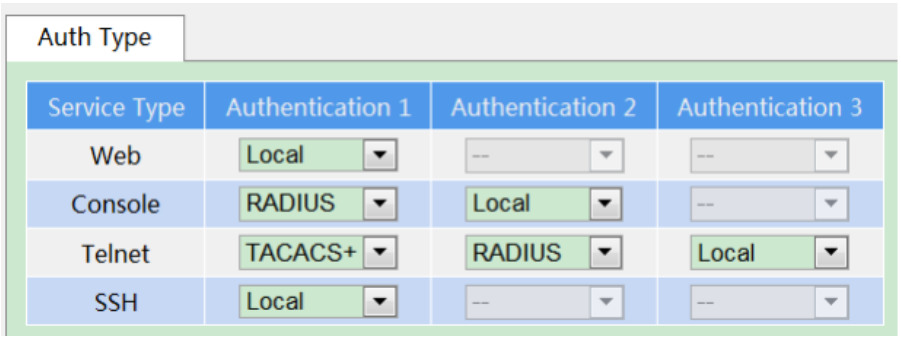


Рис. 10. Конфигурация аутентификации при входе в систему

Service Type

Диапазон: Web/console/telnet/ssh

Функция: выбор режима доступа к коммутатору

Authentication1/ Authentication2/ Authentication3

Диапазон: --/Local/RADIUS/TACACS+

Конфигурация по умолчанию: Local

Функция: Методы аутентификации выполняются слева направо. Выберите последовательность аутентификации. Первым выполняется метод Authentication1. Если аутентификация происходит с ошибкой, то выполняется метод Authentication2. Если оба метода 1 и 2 выполняются с ошибкой, то происходит переход к Authentication3.

Описание: -- обозначает, что аутентификация отключена и подключение (логин) не возможен; Local обозначает использование логина и пароля для локального подключения к коммутатору; TACACS+ обозначает использование логина и пароля на сервере TACACS для аутентификации; RADIUS обозначает использование логина и пароля на сервере RADIUS для аутентификации.

Если в качестве методов аутентификации Authentication1 и Authentication2 выбраны TACACS+/RADIUS серверы, то для метода аутентификации Authentication3 рекомендуется выбрать метод Local. На случай если серверы будут недоступны.

4 Система

4.1 Основная информация

Системная информация содержит следующие данные:

Обозначение	Описание
Device Type	Тип устройства
Device Name	Имя устройства
MAC Address	Мас адрес
Hardware Version	Аппаратная версия
Logic Version	Версия логики
Software Version	Версия программного обеспечения
Code Date	Дата программного обеспечения
CPU Used	Нагрузка на процессор
Memory Used	Количество использованной памяти
System Date	Дата и время коммутатора
System Uptime	Время в работе
Contact and Location	Контактные данные

4.2 Управление конфигурацией

1. Сохранение текущей конфигурации возможно через меню Save Configuration, как показано на следующем рисунке.

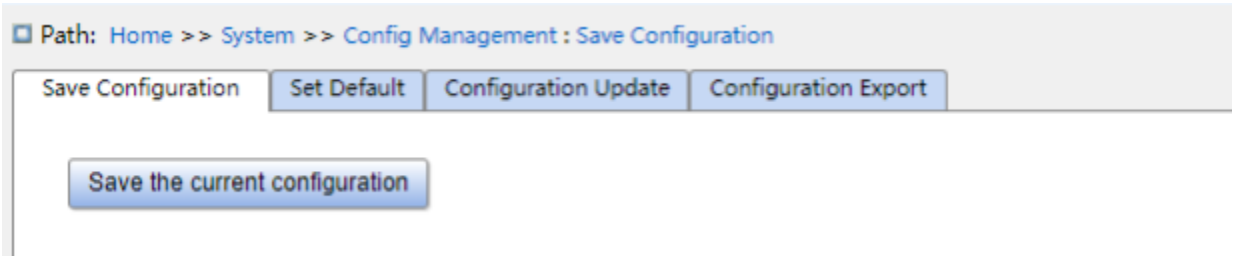


Рис. 11. Сохранение текущей конфигурации

2. Восстановление заводских настроек производится через меню Set Default.

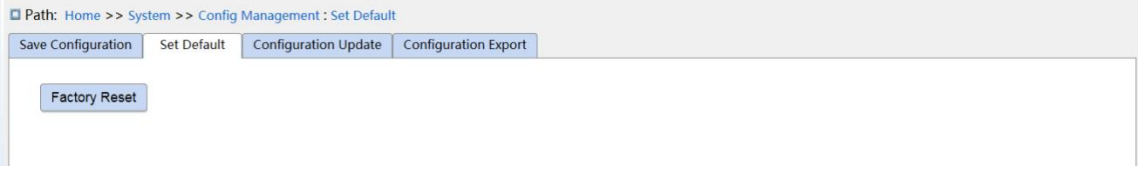


Рис. 12. Восстановление заводских настроек

3. Сохранение конфигурации (локально или на сервер) производится через меню Configuration Export.

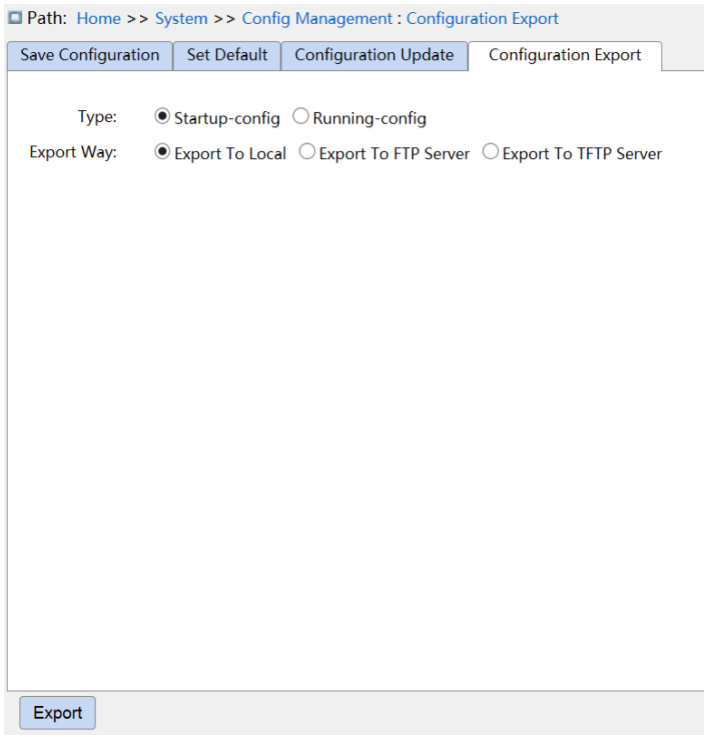


Рис. 13. Сохранение файла конфигурации по HTTP

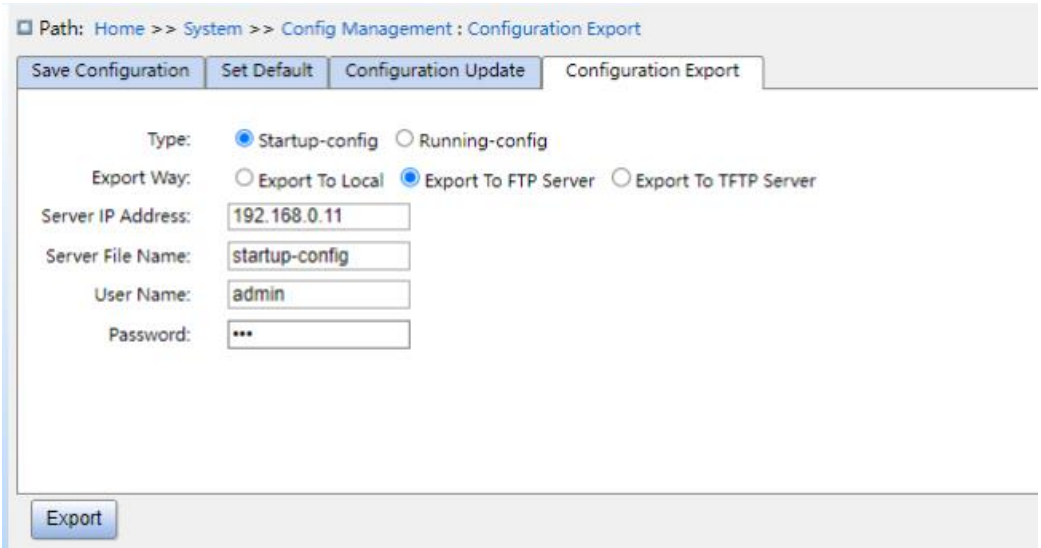


Рис. 14. Сохранение файла конфигурации на FTP сервер

Server IP address

Формат: A.B.C.D

Описание: Укажите IP адрес FTP сервера.

Server file name

Диапазон: 1~63 символа

Описание: Укажите имя файла для сохранения на FTP сервере.

{User Name, Password}

Диапазон: {1~63 символа,1~63 символа}

Описание: введите имя пользователя и пароль, созданные на FTP сервере.

- Для подключения к FTP серверу необходимо указать IP адрес FTP сервера, имя пользователя на FTP сервере и пароль.
- FTP сервер должен быть доступен при загрузке/сохранении файла.

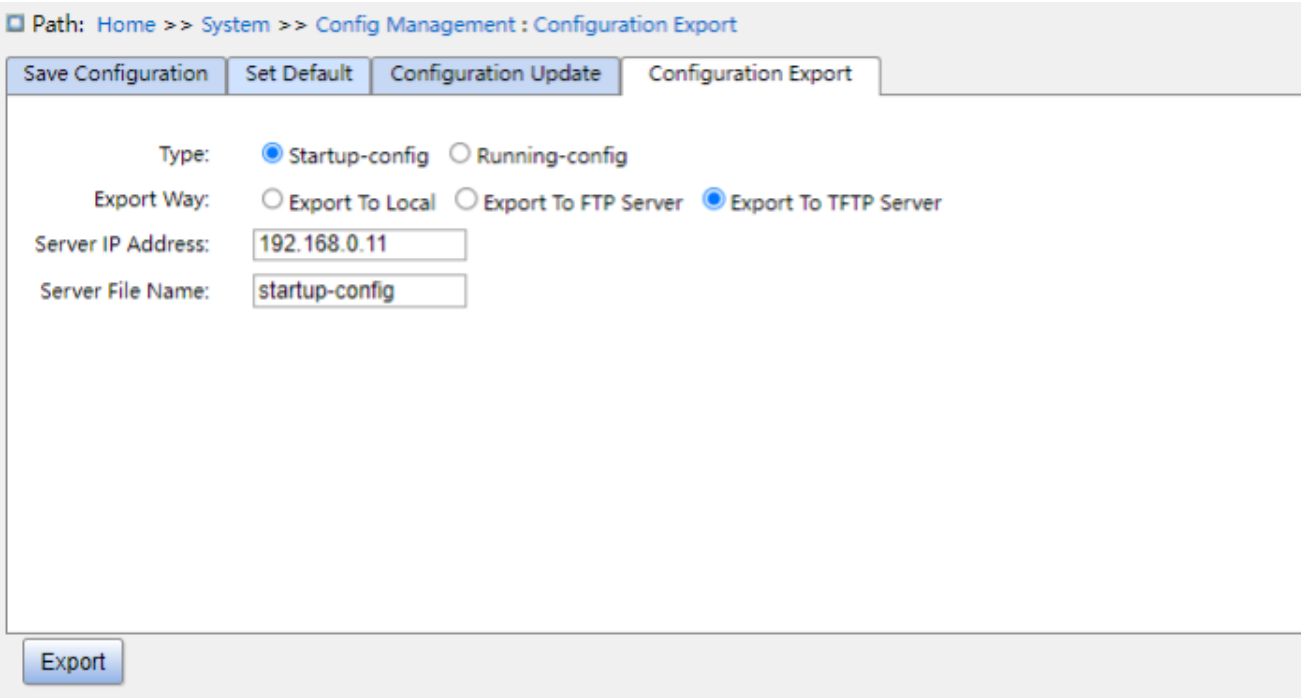


Рис. 15. Сохранение файла конфигурации на TFTP сервер

Сохранение файла конфигурации производится локально или на сервер.

Running-config - сохранение текущей конфигурации коммутатора.

Startup-config - сохранение конфигурации загруженной при запуске коммутатора.

Выберите тип файла и нажмите <Export> для сохранения файла локально или на сервер.

4. Загрузка файла конфигурации в коммутатор производится локально или с сервера. Загрузка файла Startup-config показана далее.

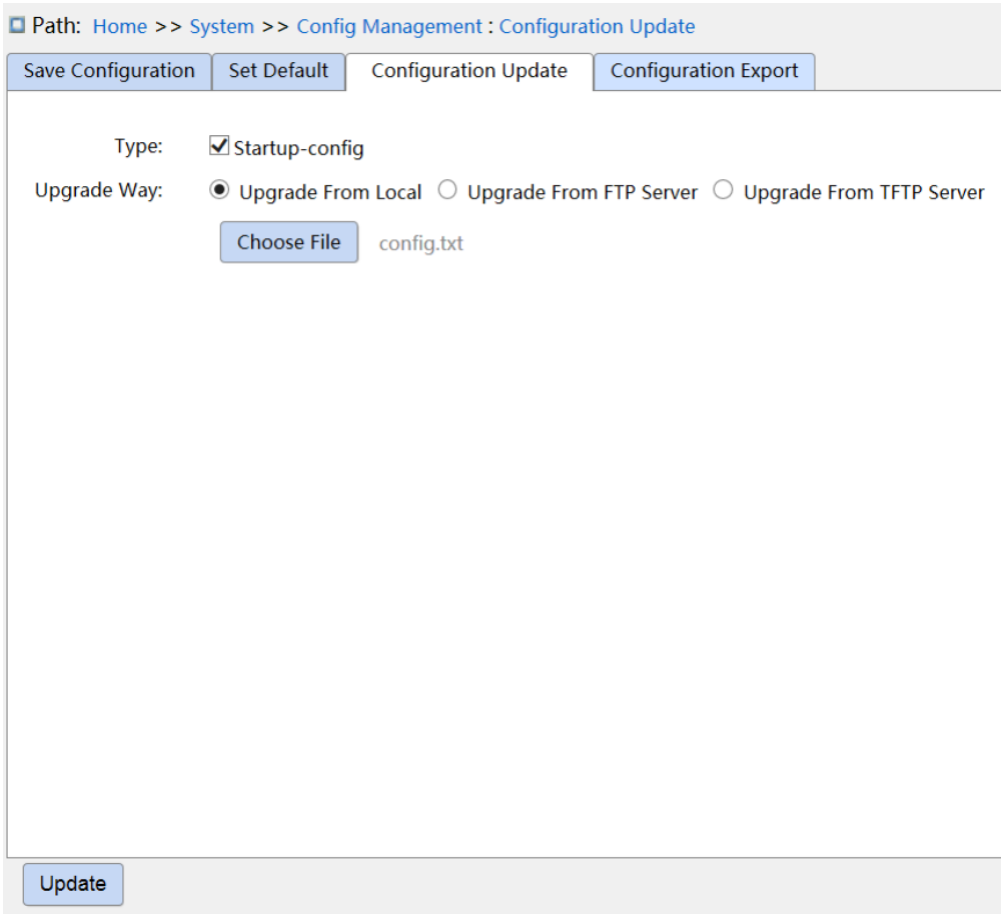


Рис. 16. Загрузка файла конфигурации в коммутатор по HTTP

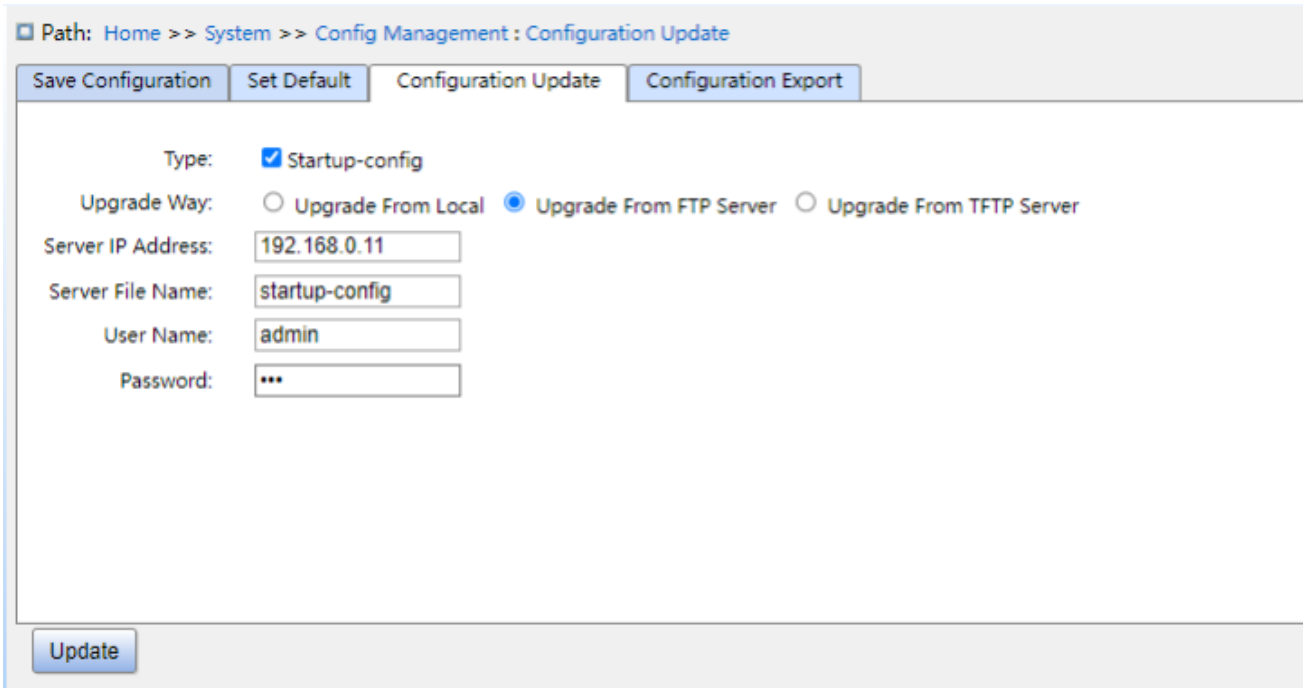


Рис. 17. Загрузка файла конфигурации в коммутатор по FTP

Server IP address

Формат: A.B.C.D

Описание: Укажите IP адрес FTP сервера.

Server file name

Диапазон: 1~63 символа

Описание: Укажите имя файла конфигурации на FTP сервере.

{User Name, Password}

Диапазон: {1~63 символа,1~63 символа}

Описание: введите имя пользователя и пароль, созданные на FTP сервере.

- Для подключения к FTP серверу необходимо указать IP адрес FTP сервера, имя пользователя на FTP сервере и пароль.
- FTP сервер должен быть доступен при загрузке/сохранении файла.

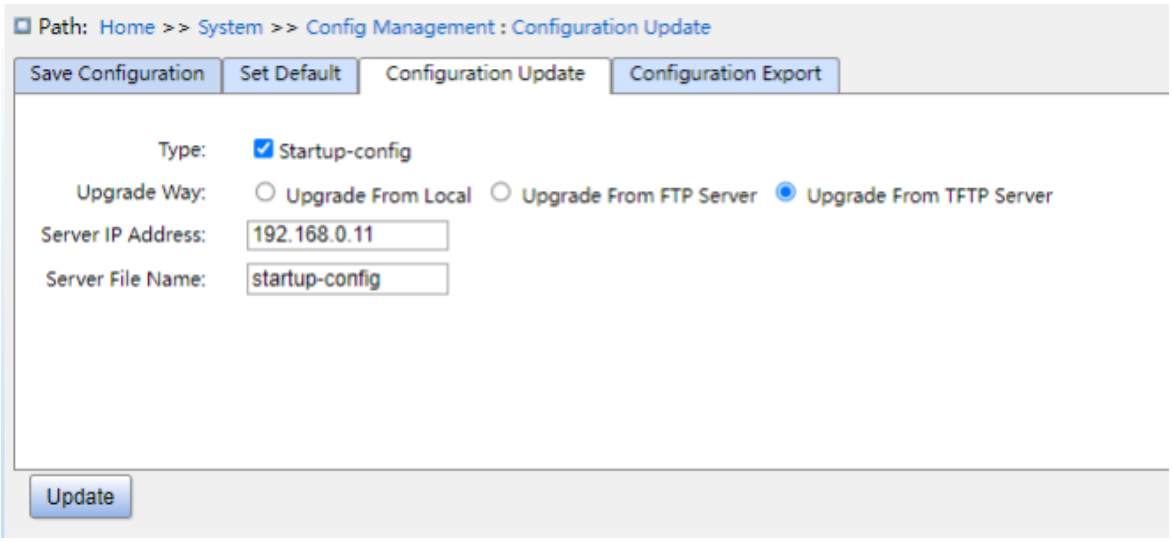


Рис. 18. Загрузка файла конфигурации в коммутатор по TFTP

Загрузка файла конфигурации на коммутатор производится локально или с сервера. При загрузке файла происходит перезапись **Startup-config** файла коммутатора.

Нажмите <Update> для загрузки файла локально или с указанного сервера.

4.3 Управление часами

1. Настройка функции DST (переход на летнее время) показана далее.

Функция DST может быть отключена (Disable), быть повторяющейся (Recurring) и неповторяющейся (Non-Recurring).

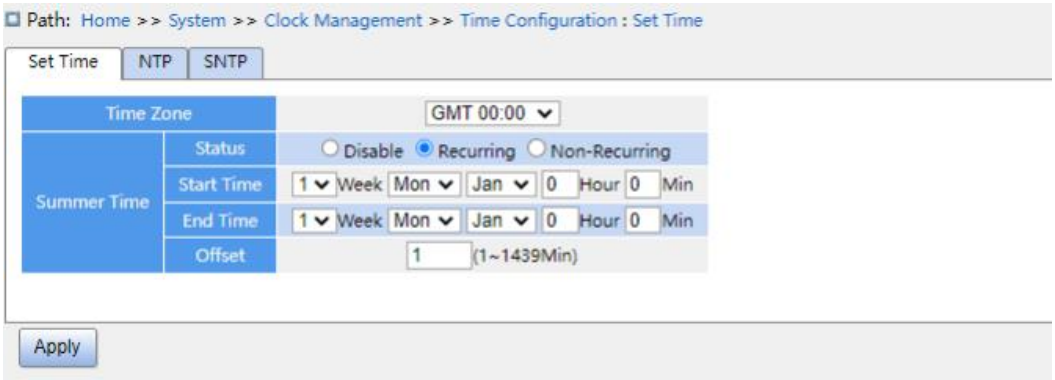


Рис. 19. Конфигурация функции DST

Time zone

Функция: установка часового пояса

DST status

Возможности конфигурации: disable/recurring/non-recurring

Конфигурация по умолчанию: disable (рекомендованная установка для России)

Функция: В случае активации функции DST, выберите повторяющийся (recurring) или неповторяющийся переход (non-recurring) на летнее время.

Start time/End Time

Функция: после включения функции DST задайте временной диапазон для работы функции. Для неповторяющегося перехода (non-recurring) на летнее время задайте год, месяц, день, час и минуту для начала (Start Time) и окончания (End Time) работы функции DST. Для повторяющегося перехода (recurring) на летнее время задайте месяц, неделю, день недели, час и минуту для начала (Start Time) и окончания (End Time) работы функции DST.

Offset

Диапазон: 1~1439 мин.

Конфигурация по умолчанию: 1 мин.

Функция: Устанавливает положительное смещение для DST на заданное время в минутах.

- Время Start Time и End Time должны отличаться.
- Время Start Time - время без учета DCT, время End Time - время с учетом DCT.

2. Конфигурация NTP

NTP(Network Time Protocol) используется для синхронизации времени между удаленным сервером и клиентом. NTP позволяет синхронизировать время между всеми устройствами в сети. Примечание: Это устройство поддерживает работу только в качестве NTP-клиента и не может использоваться в качестве сервера NTP.

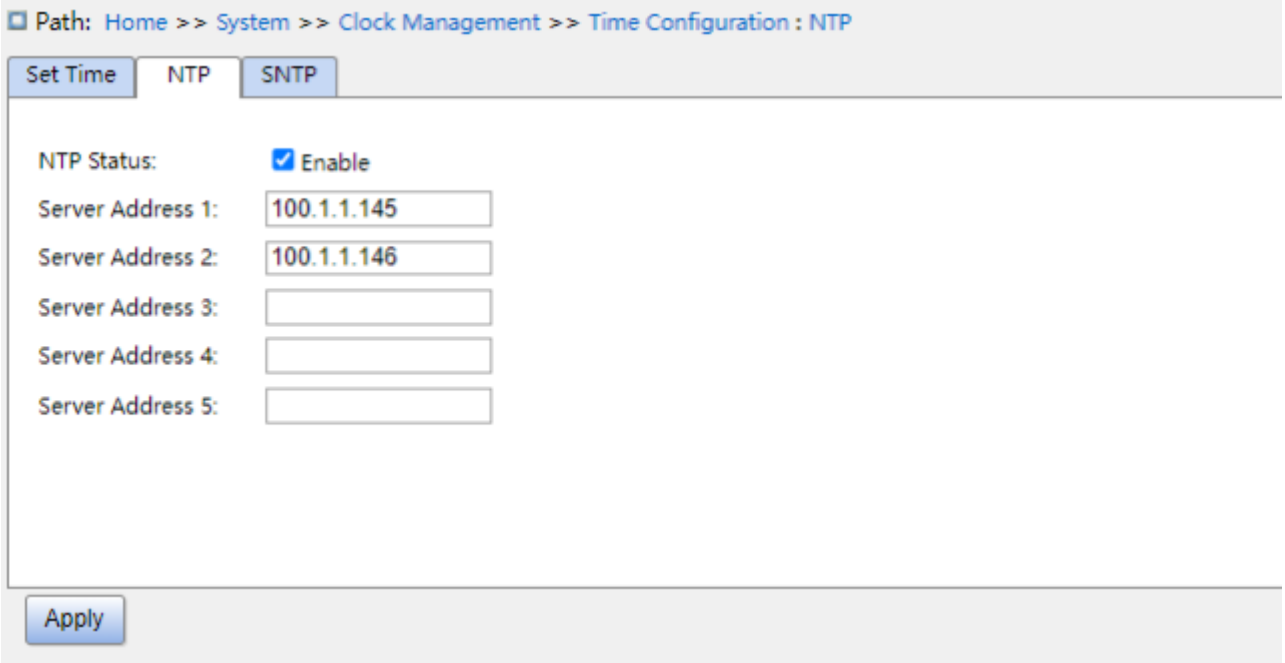


Рис. 20. Конфигурация NTP

NTP status

Возможности конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: включение глобальной службы NTP

- Протоколы NTP и SNTP являются взаимоисключающими. Поскольку NTP и SNTP используют один и тот же номер порта UDP, оба не могут быть включены одновременно.
- Когда служба NTP не включена, службу NTP можно настроить и сохранить. То есть независимо от того, включена служба NTP или нет, это не влияет на конфигурацию службы NTP.

Server address 1/ server address 2/ server address 3/ server address 4/ server address 5

Формат: A.B.C.D

Функция: Настройте IP-адрес NTP-сервера, и клиент будет устанавливать время в соответствии с сообщениями NTP-сервера.

3. Конфигурация SNTP

SNTP (Simple Network Time Protocol) протокол устанавливает время с помощью запросов и ответов между сервером и клиентом. Коммутатор действует как клиент для установки времени на основе сообщений сервера.

- При активации функции SNTP на коммутаторе SNTP сервер должен быть доступен.
- В протоколе SMTP передается время с часовым поясом GMT 0.

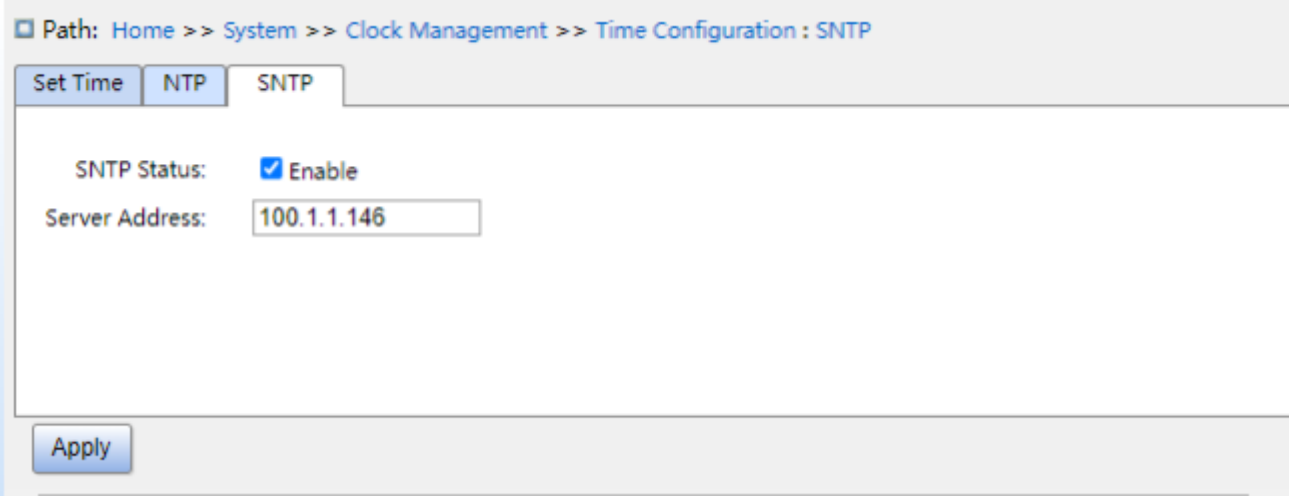


Рис. 21. Конфигурация SNTP

SNTP status

Возможности конфигурации: enable/disable

Конфигурация по умолчанию: disable

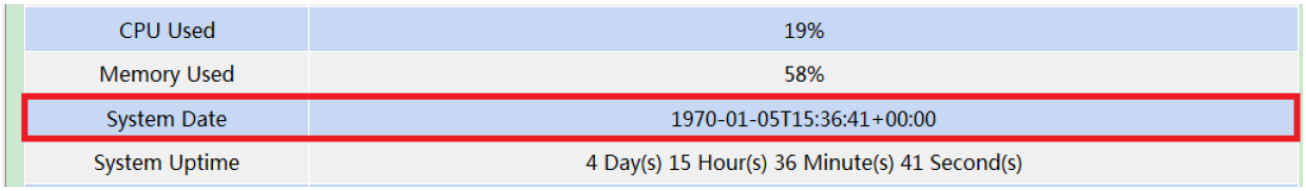
Функция: включение работы по протоколу SNTP

Server address

Формат: A.B.C.D

Функция: Настройте IP-адрес SNTP-сервера, и клиент будет устанавливать время в соответствии с сообщениями SNTP-сервера.

4. Для проверки синхронизировано ли время коммутатора с сервером времени перейдите в [System] → [Basic information].



CPU Used	19%
Memory Used	58%
System Date	1970-01-05T15:36:41+00:00
System Uptime	4 Day(s) 15 Hour(s) 36 Minute(s) 41 Second(s)

Рис. 22. Информация о текущем времени коммутатора

Время коммутатора отображается с учетом времени сервера, часового пояса и конфигурации DST.

4.4 Обновление программного обеспечения

Обновление программного обеспечения (ПО) для данной серии коммутаторов состоит из двух частей. Обновление ПО загрузчика (Bootloader) и обновление основного ПО (Application). В первую очередь необходимо производить обновление Bootloader. После этого необходимо производить обновление Application. Если версия Bootloader не меняется, то возможно производить только обновление Application. Обновление ПО возможно производить локально через Web интерфейс, или загружать с FTP/TFTP сервера.

4.4.1 Локальное обновление

1. Локальное обновление показано на рисунке далее.

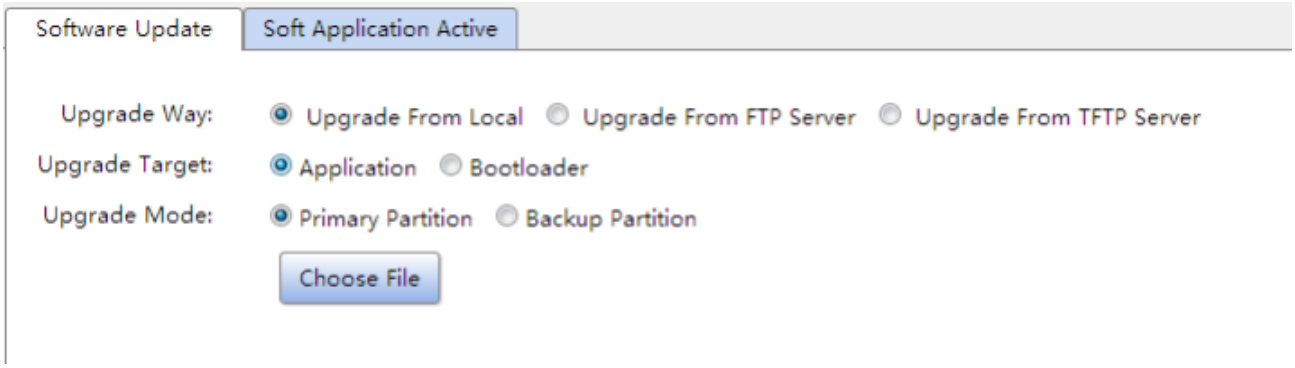


Рис. 23. Локальное обновление ПО

Upgrade way

Варианты конфигурации: Upgrade From Local / Upgrade From FTP Server / Upgrade From TFTP

Функция: выбор источника обновления

Upgrade target

Варианты конфигурации: Application / Bootloader

Функция: выбор типа обновления. Обновление загрузчика или обновление основного ПО.

Upgrade mode

Варианты конфигурации: primary partition/backup partition

Описание: можно загрузить две версии программного обеспечения, эти две версии могут быть одинаковыми или различными.

2. После успешного обновления активируйте версию программного обеспечения и перезагрузите устройство, затем проверьте, соответствует ли версия программного обеспечения обновленной версии в системной информации.

- После успешного обновления ПО необходимо активировать версию ПО и перезагрузить устройство, прежде чем версия ПО вступит в силу;
- Не перезапускайте коммутатор после сбоя обновления, чтобы избежать потери текущей версии файла ПО. Иначе устройство не сможет нормально запуститься.

4.4.2 Обновление по FTP

Установите FTP-сервер. Далее в качестве примера используется ПО WFTPD для настройки FTP-сервера и обновления ПО коммутатора.

1. Нажмите [Security] → [Users/Rights]. Откроется диалоговое окно "Users/Rights Security Dialog". Нажмите <New User>, чтобы создать нового пользователя FTP, как показано на рисунке далее. Задайте имя пользователя и пароль.

Например, имя пользователя "admin" и пароль "STEZ". Нажмите <OK>.

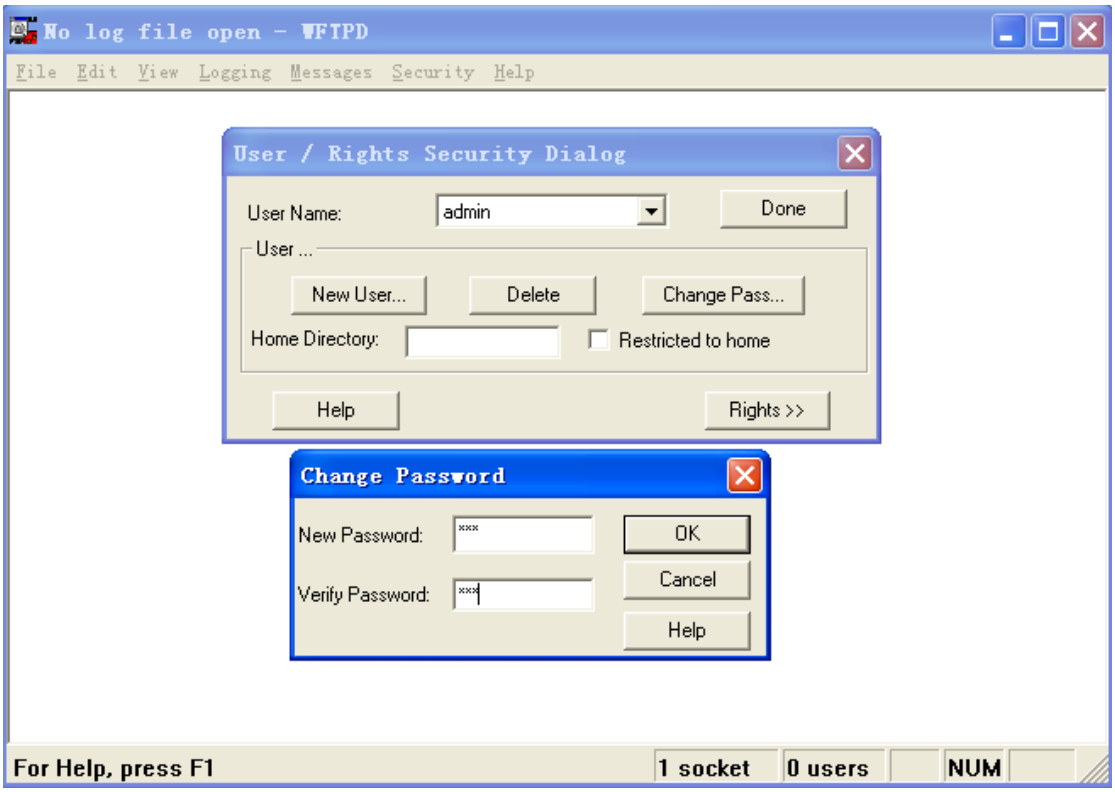


Рис. 24. Пример создания пользователя в ПО WFTPD

2. Введите путь к файлу обновления в "Home Directory", как показано на рисунке далее. Нажмите <Done>.

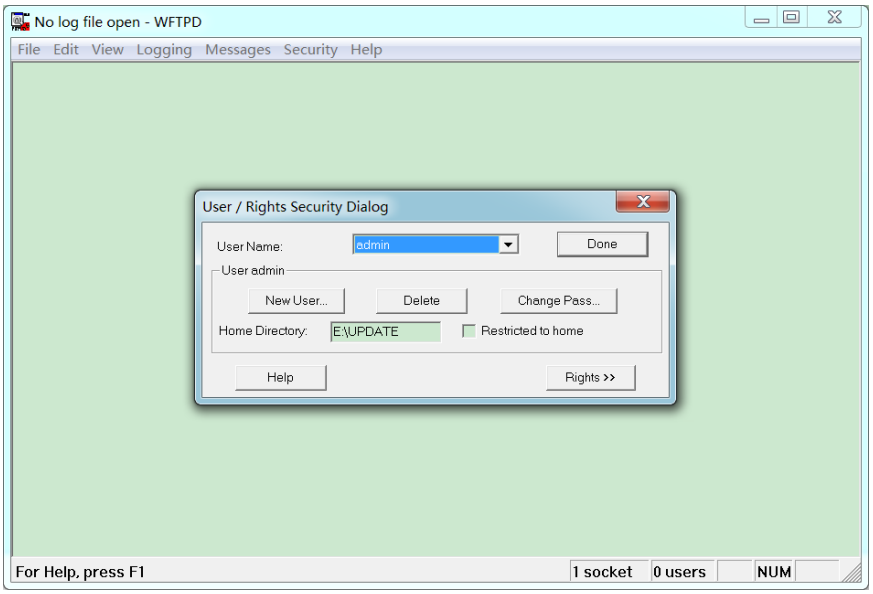


Рис. 25. Путь к файлу обновления

3. Нажмите [System] → [Software Update] в дереве навигации чтобы перейти на страницу обновления программного обеспечения, как показано на рисунке далее. Введите IP-адрес FTP-сервера, имя пользователя FTP, пароль и имя файла на сервере. Нажмите <Update>.

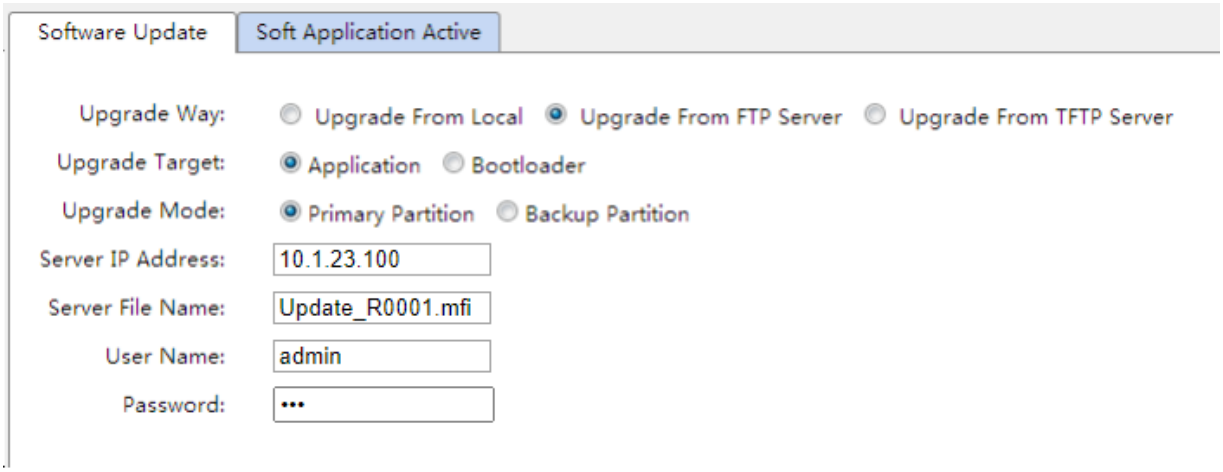


Рис. 26. Обновление ПО по FTP

Upgrade Way

Варианты конфигурации: Upgrade From Local / Upgrade From FTP Server / Upgrade From TFTP Server

Описание: Выберите источник обновления ПО

UpgradeTarget

Варианты конфигурации: Appication/Bootloader

Функция: выберите вид обновления. Приложение или загрузчик.

Upgrade Mode

Варианты конфигурации: Primary Partition/Backup Partition

Описание: в коммутатор можно загрузить две версии встроенного ПО. Версии могут быть одинаковыми или разными.

- Имя файла должно содержать расширение. В противном случае обновление может завершиться с ошибкой.

4. Убедитесь в нормальном обмене данными между FTP-сервером и коммутатором, как показано далее.

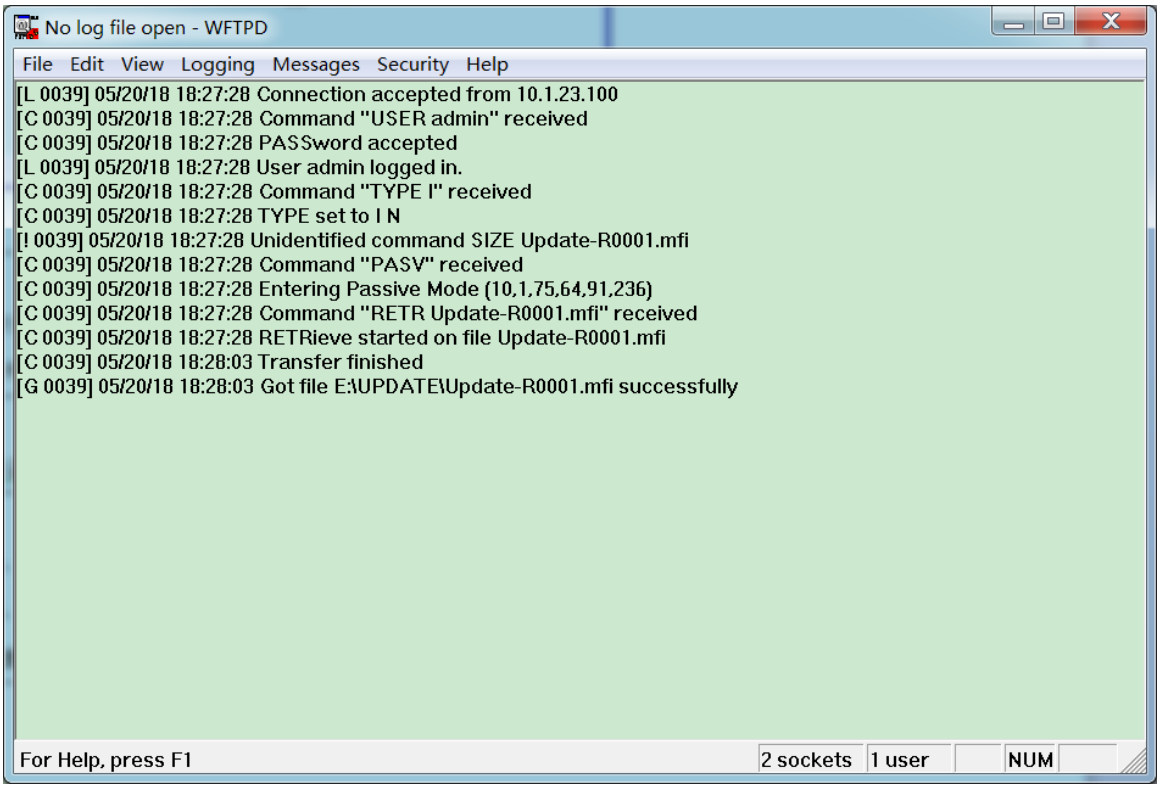


Рис. 27. Связь между FTP-сервером и коммутатором

Чтобы отобразить информацию журнала обновлений, как показано на рисунке выше, нужно нажать [Logging] → [Log Options] в WFTPD и выбрать Enable Logging.

5. Дождитесь завершения обновления, как показано на рисунке

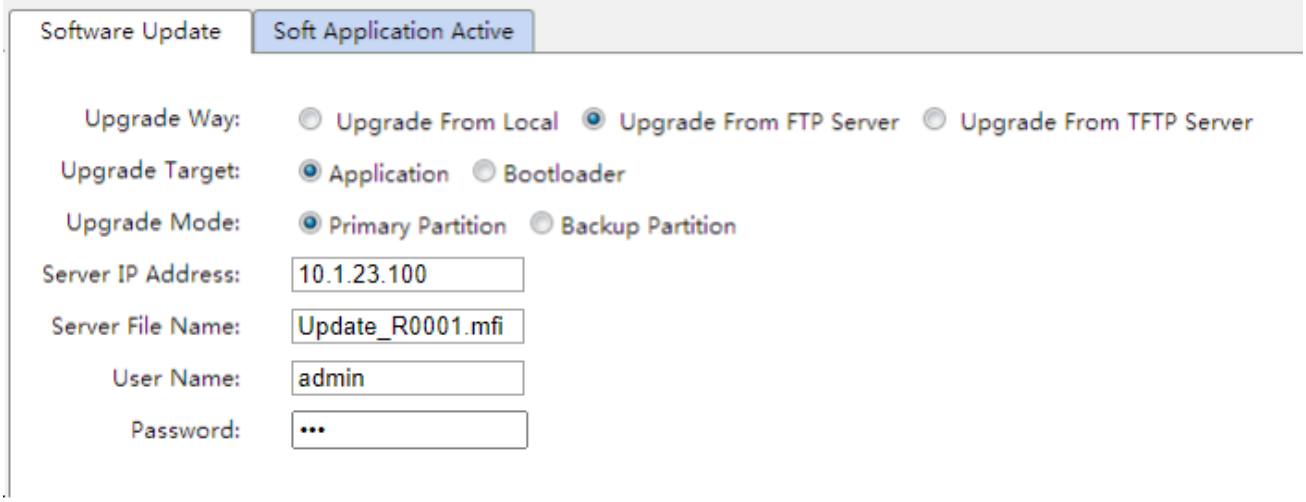


Рис. 28. Обновление коммутатора по FTP

6. Когда обновление будет завершено, перезагрузите устройство и откройте страницу Switch Basic Information для проверки того, что обновление выполнено успешно и активна новая версия.

- В процессе обновления ПО не прерывайте соединение с FTP-сервером.
- Когда обновление завершится, перезагрузите устройство, чтобы активировать новую версию.
- Не перезапускайте коммутатор после сбоя обновления, чтобы избежать потери текущей версии файла ПО. Иначе устройство не сможет нормально запуститься.

4.4.3 Обновление по TFTP

Установите TFTP-сервер. Далее используется ПО TFTP в качестве примера для настройки конфигурации TFTP-сервера.

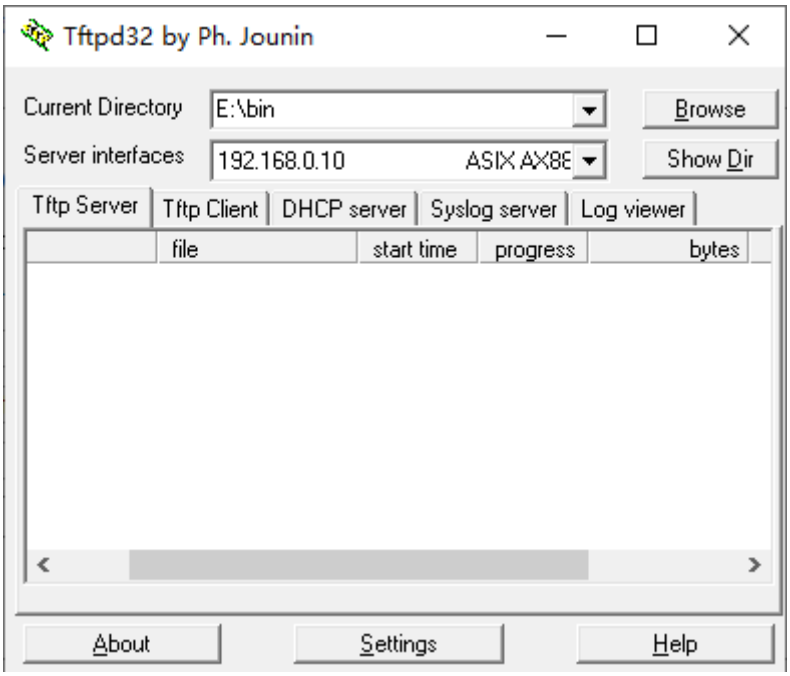


Рис. 29. Настройка TFPT сервера

1. В "Current Directory" выберите путь к расположению файла. Введите IP-адрес сервера в "Server interface".

2. Нажмите [System] → [Software Update] в дереве навигации, чтобы перейти на страницу обновления ПО, как показано далее. Введите IP-адрес TFTP-сервера и имя

файла на сервере. Нажмите <Update> и дождитесь завершения обновления.

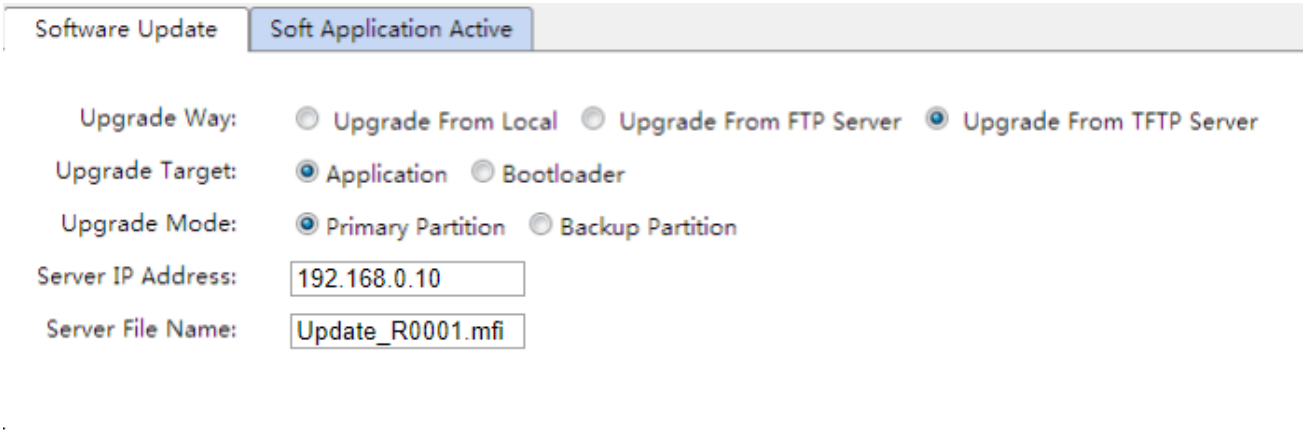


Рис. 30. Обновление ПО коммутатора по TFTP

3. Убедитесь в нормальном обмене данными между TFTP-сервером и коммутатором, как показано далее.

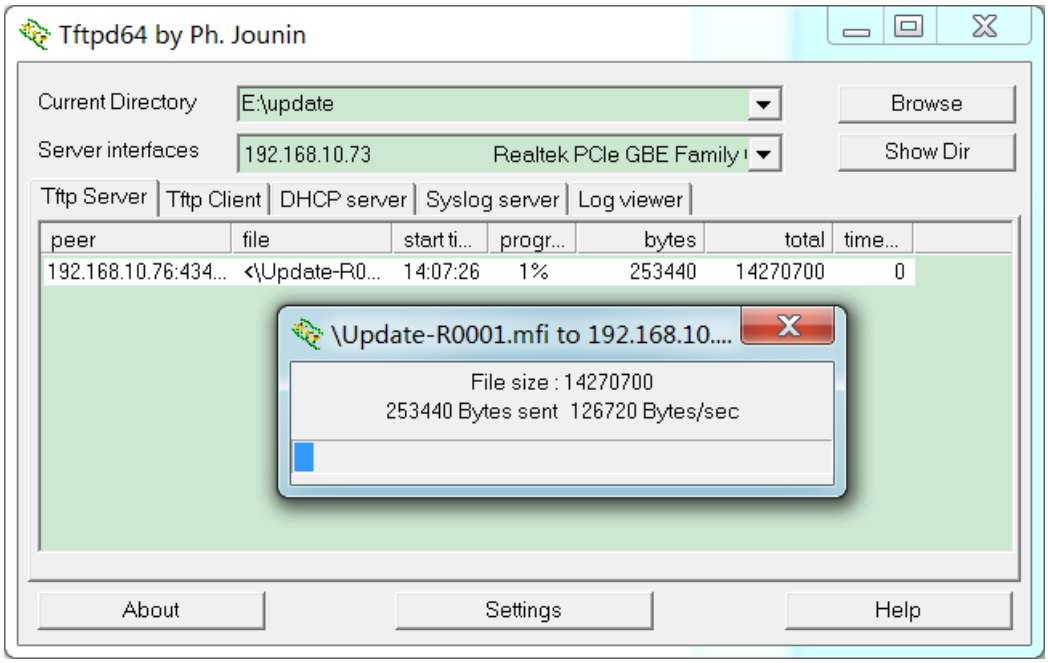


Рис. 31. Загрузка ПО коммутатора по TFTP

4. Дождитесь завершения обновления.

5. Когда обновление будет завершено, перезагрузите устройство и откройте страницу Switch Basic Information для проверки того, что обновление выполнено успешно и активна новая версия.

- В процессе обновления ПО не прерывайте соединение с FTP-сервером.
- Когда обновление завершится, перезагрузите устройство, чтобы активировать новую версию.
- Не перезапускайте коммутатор после сбоя обновления, чтобы избежать потери текущей версии файла ПО. Иначе устройство не сможет нормально запуститься.

В случае если на коммутаторе загружено несколько версий ПО. Активируйте встроенное ПО коммутатора, как показано на рисунке далее.

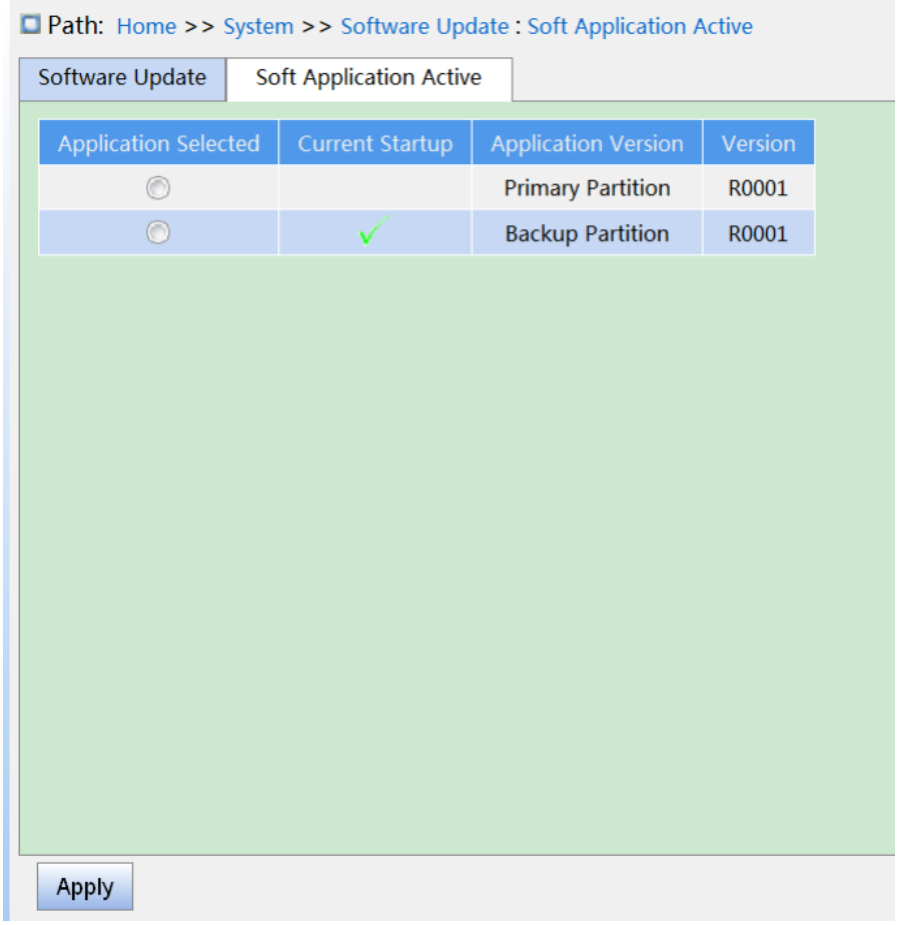


Рис. 32. Выбор активной версии ПО коммутатора

4.5 Перезагрузка коммутатора

Перезагрузите устройство, как показано далее.

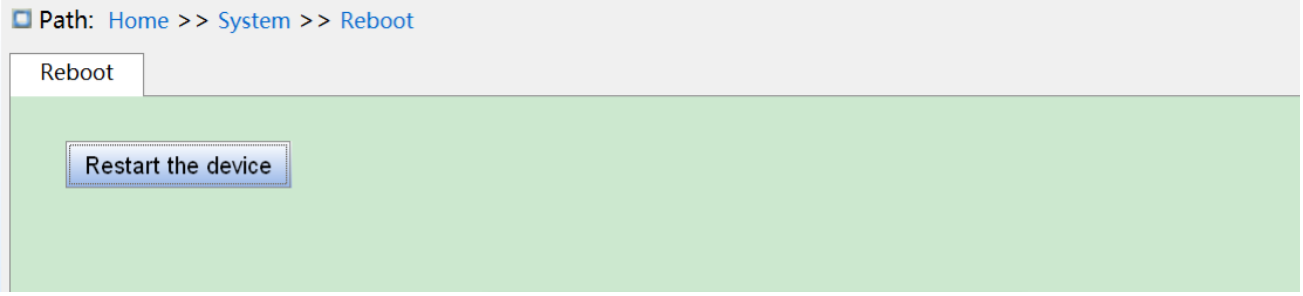


Рис. 33. Перезагрузка коммутатора

Перед перезапуском коммутатора проверьте, сохранена ли текущая конфигурация. Если нет, то конфигурация коммутатора будет восстановлена до последней сохраненной конфигурации после перезагрузки.

5 Сервисные функции коммутатора

5.1 Конфигурация SSL

5.1.1 Введение

SSL (Secure Socket Layer) - это протокол безопасности, который обеспечивает безопасную связь для протокола прикладного уровня на основе TCP, такого как HTTPS. SSL шифрует сетевое соединение на транспортном уровне и использует алгоритм симметричного шифрования для обеспечения безопасности данных, а также использует код аутентификации с секретным ключом для обеспечения надежности информации. Этот протокол широко используется в веб-браузерах, при получении и отправке электронной почты, общении в режиме реального времени и так далее, предоставляя протокол шифрования для обеспечения безопасности передачи данных в сети.

5.1.2 Web конфигурация

1. Включите HTTPS, как показано далее.

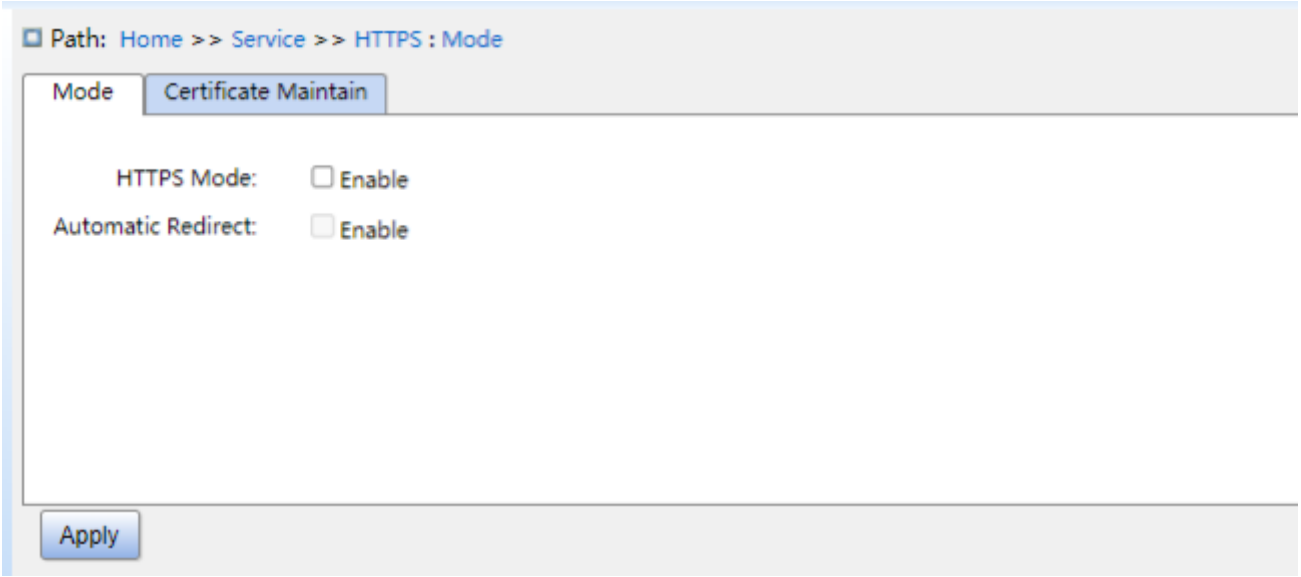


Рис. 34. Включение HTTPS в коммутаторе

HTTPS Mode

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включите или отключите HTTPS. После включения вы сможете использовать только безопасную ссылку https://IP-адрес для входа на веб-страницу коммутатора.

Automatic redirection

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Если этот параметр отключен, использование http://ip-адреса для входа на веб-страницу коммутатора не приведет к автоматическому переключению на защищенную ссылку, что делает невозможным доступ к веб-странице коммутатора. Параметр Automatic redirection можно настроить только при включенном HTTPS Mode.

2. Управление сертификатами показано далее на рисунке.

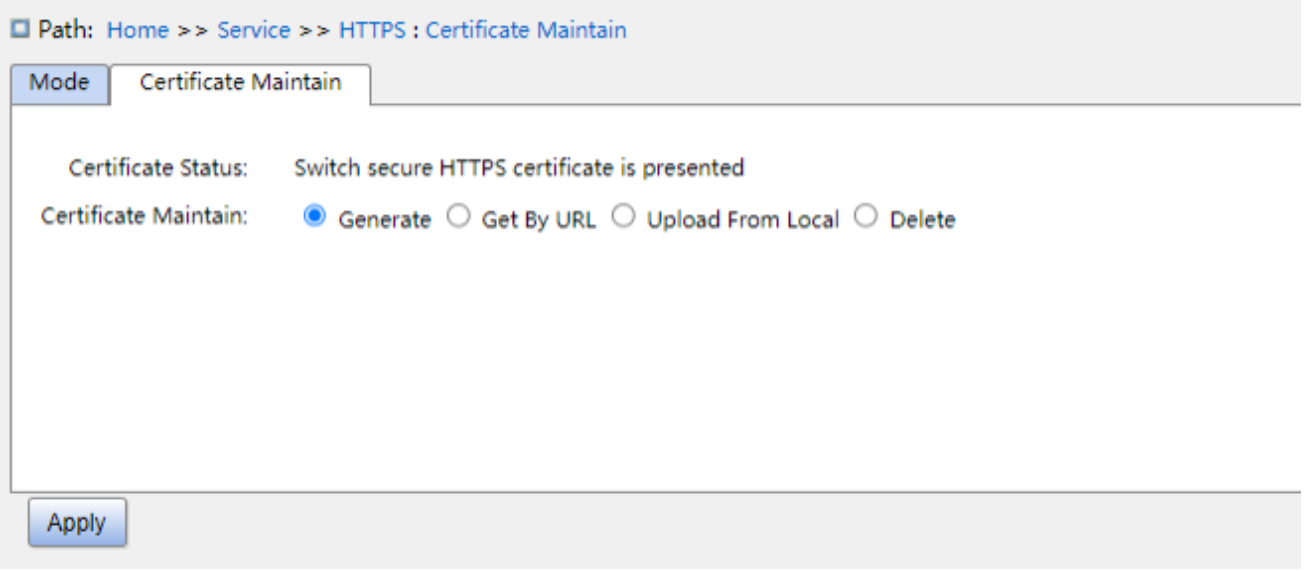


Рис. 35. Сгенерировать сертификат

Certificate Maintain

Варианты конфигурации: Generate/Get by URL/Upload From Local/Delete

Функция: Выберите способ загрузки или создания сертификата

Generate

Функция: Генерирование сертификата на коммутаторе.

Get By URL

Функция: Задайте путь до сертификата.

Например, https://10.10.10.10:80/new_image_path/new_image.dat

Upload from Local

Функция: Выберите файл сертификата HTTPS на локальном диске.

5.2 SNMP v1/SNMP v2c

5.2.1 Введение

Протокол Simple Network Management Protocol (SNMP) - это платформа, использующая TCP/IP для управления сетевыми устройствами. С помощью функции SNMP администратор может запрашивать информацию об устройстве, изменять настройки параметров, отслеживать состояние устройства и обнаруживать сетевые сбои.

5.2.2 Реализация

SNMP использует два режима работы: станция управления и агент. Таким образом, SNMP включает в себя два типа: Network Management Station (NMS) и агент (agent).

NMS - это станция, на которой запущен клиент программного обеспечения для управления сетью с поддержкой SNMP. Это ядро для сетевого управления сетью с помощью SNMP.

Агент - это процесс в управляемых сетевых устройствах. Он получает и обрабатывает пакеты запросов от NMS. Когда возникает сигнал тревоги, агент сообщает об этом в NMS.

NMS является менеджером сети SNMP, в то время как агент является

управляемым устройством сети SNMP. NMS и агенты обмениваются пакетами управления через SNMP.

SNMP включает в себя следующие основные операции:

Get-Request

Get-Response

Get-Next-Request

Set-Request

Trap

NMS отправляет Get-Request, Get-Next-Request и Set-Request агентам для запроса, настройки переменных и управления ими. После получения этих запросов агенты отвечают пакетами Get-Response. Когда возникает сигнал тревоги, агент сообщает об этом NMS с помощью Trap пакета.

5.2.3 Принцип работы

Коммутаторы данной серии поддерживают SNMP v2c. SNMP v2c совместим с SNMPv1.

SNMPv1 использует имя сообщества (SNMP community) для аутентификации. Имя сообщества действует как пароль, ограничивая доступ NMS к агентам. Если имя сообщества, передаваемое SNMP-пакетом, не подтверждается коммутатором, запрос завершается неудачей и возвращается сообщение об ошибке.

SNMP v2c также использует имя сообщества для аутентификации. Он совместим с SNMPv1 и расширяет функции SNMP v1.

Для обеспечения связи между NMS и агентом, версии SNMP должны совпадать. На агенте можно настроить разные версии SNMP для связи с NMS.

5.2.4 Принцип работы MIB

Любое управляемое устройство называется управляемым объектом. Management Information Base (MIB) представляет собой набор управляемых объектов. Он определяет иерархические отношения между управляемыми объектами и рядом

атрибутов объектов, таких как имя объекта, права доступа и типы данных. Каждый агент имеет свою собственную библиотеку MIB. NMS может выполнять операции чтения/записи объектов в MIB на основе разрешений. Взаимосвязь между NMS, агентом и MIB показана на рисунке далее.

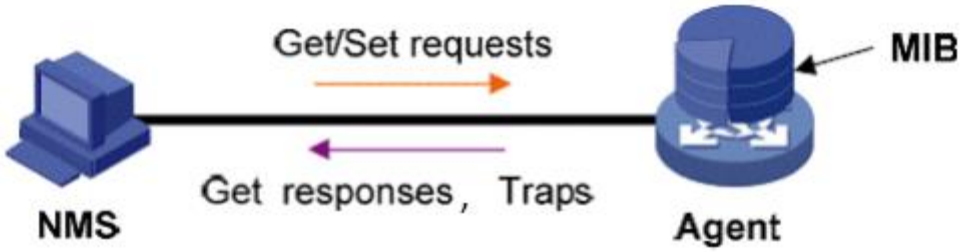


Рис. 36. Взаимодействие между NMS, агентом и MIB

MIB определяет древовидную структуру. Узлы дерева (nodes) представляют собой управляемые объекты. Каждый узел содержит уникальный OID (Object Identifier, идентификатор объекта). OID указывает положение узла в древовидной структуре MIB, как показано на рисунке далее. Как показано на рисунке OID управляемого объекта A (Object A) равен 1.2.1.1.

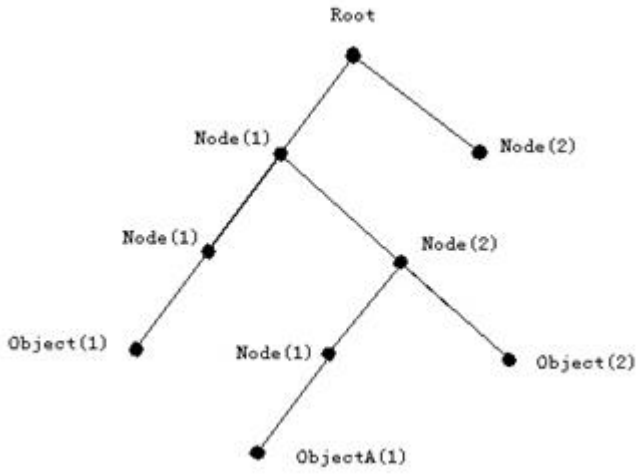


Рис. 37. Древовидная структура MIB

5.2.5 Web конфигурация SNMP

1. Включите протокол SNMP, как показано на рисунке далее

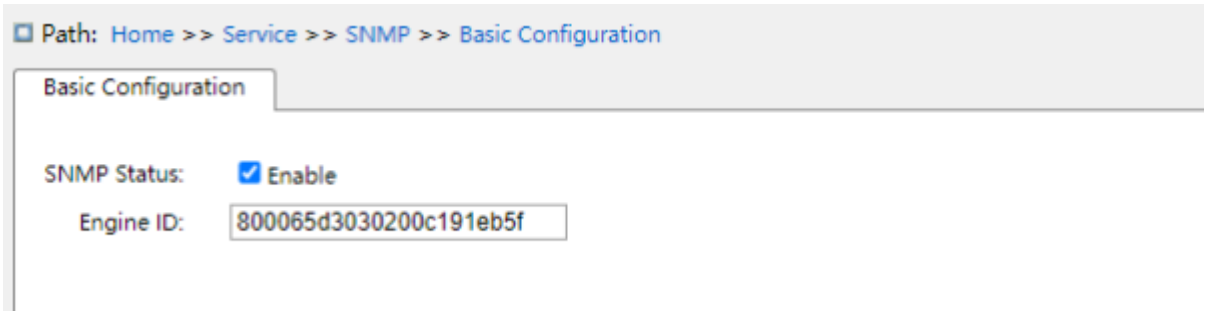


Рис. 38. Включение протокола SNMP

SNMP status

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Enable

Функция: Включение протокола SNMP на коммутаторе

Engine ID

Диапазон: Четное шестнадцатеричное число, не может быть все 0 или все F. Диапазон значений четного числа составляет 10~64.

Функция: Идентификатор Engine ID для SNMP v3, при изменении engine ID пользователь, соответствующий engine ID устройства в таблице пользователей, будет удален.

2. Настройте имя сообщества, как показано на рисунке далее.

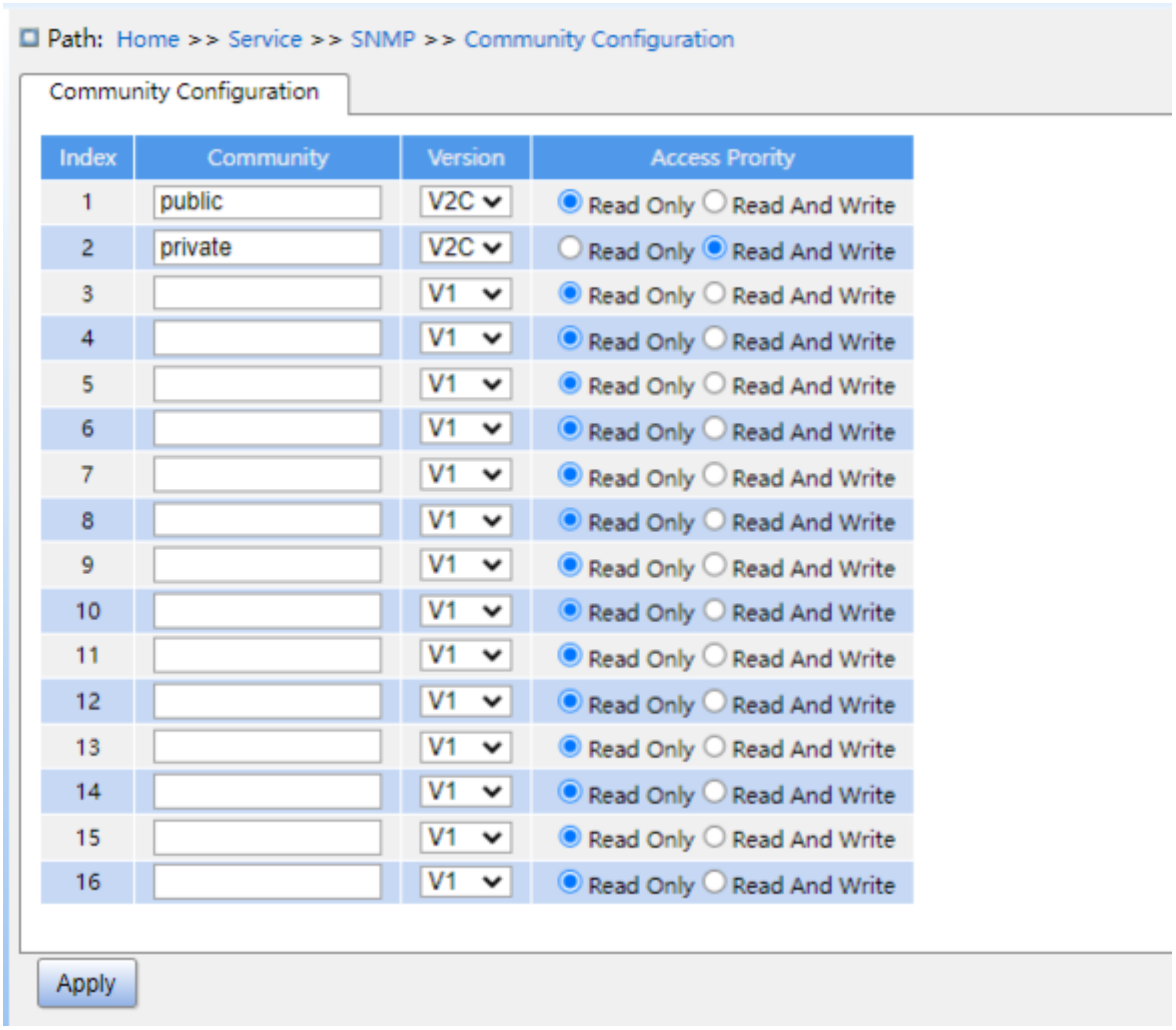


Рис. 39. Настройка имени сообщества SNMP

Community

Диапазон: 1~32 символа

Функция: Настройка имени сообщества для коммутатора

Описание: Доступ к информации в библиотеке MIB коммутатора возможен только в том случае, если имя сообщества в SNMP-сообщении соответствует имени сообщества в коммутаторе.

Описание: можно настроить до 16 имен сообщества

Access Priority

Варианты конфигурации: Read Only/Read And Write

Конфигурация по умолчанию: Read Only

Функция: настройка приоритета доступа к библиотеке MIB

Описание: Разрешение Read Only позволяет только читать информацию из библиотеки MIB; разрешение Read And Write позволяет читать и записывать информацию библиотеки MIB.

3. Настройте передачу trap сообщений, как показано на рисунке далее.

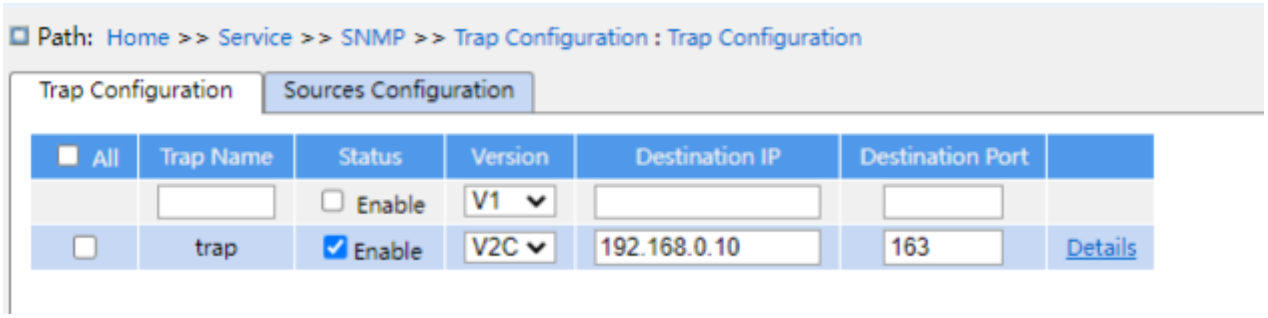


Рис. 40. Настройка trap сообщений

Trap name

Диапазон: 1~32 символа

Функция: Задайте имя для trap

Status

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включите или отключите trap сообщения. Коммутатор отправляет соответствующее сообщение trap сообщение на сервер, если включено

Version

Варианты конфигурации: V1/ V2C/ V3

Конфигурация по умолчанию: V1

Функция: Настройте номер версии для trap сообщений, отправляемых коммутатором на сервер.

Destination IP

Формат: A.B.C.D

Функция: Настройте адрес сервера для отправки trap сообщений.

Destination Port

Диапазон: 1~65535

Конфигурация по умолчанию: 162

Функция: Настройте номер порта для отправки trap сообщений

4. Нажмите на Details чтобы просмотреть детали конфигурации trap сообщений, как показано на рисунке далее.

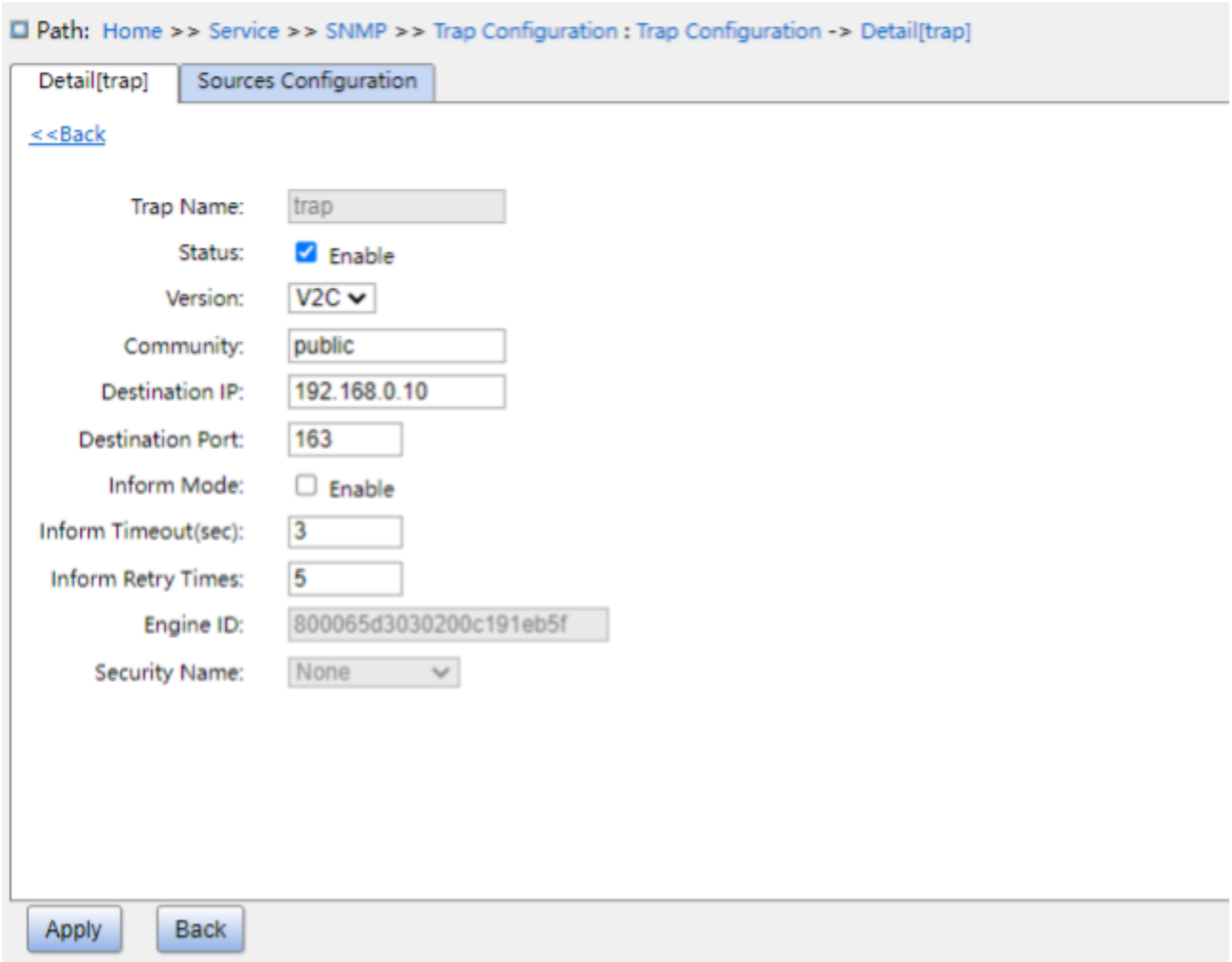


Рис. 41. Дополнительная настройка trap

Community

Диапазон: 0~255 символов

Конфигурация по умолчанию: public

Функция: Настройте имя сообщества, которое будет указано в отправляемом trap сообщении.

Inform Mode

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: После получения trap сообщения сервер отправляет коммутатору ответное сообщение.

Inform Timeout

Диапазон: 0~2147 сек.

Конфигурация по умолчанию: 3 сек.

Функция: Настройте тайм-аут отправки trap сообщения; после того, как коммутатор отправит trap сообщение, если в течение этого времени от сервера не будет ответа, то коммутатор повторно отправит trap сообщение.

Inform retry Times

Диапазон: 0~255

Конфигурация по умолчанию: 5

Функция: Настройте количество раз для срабатывания Inform Timeout. Если суммарное количество раз отправки превышает заданное значение, а сервер не отвечает, значит, возникает ошибка отправки trap сообщения.

5. Настройте события для отправки Trap сообщений, как показано на рисунке далее.

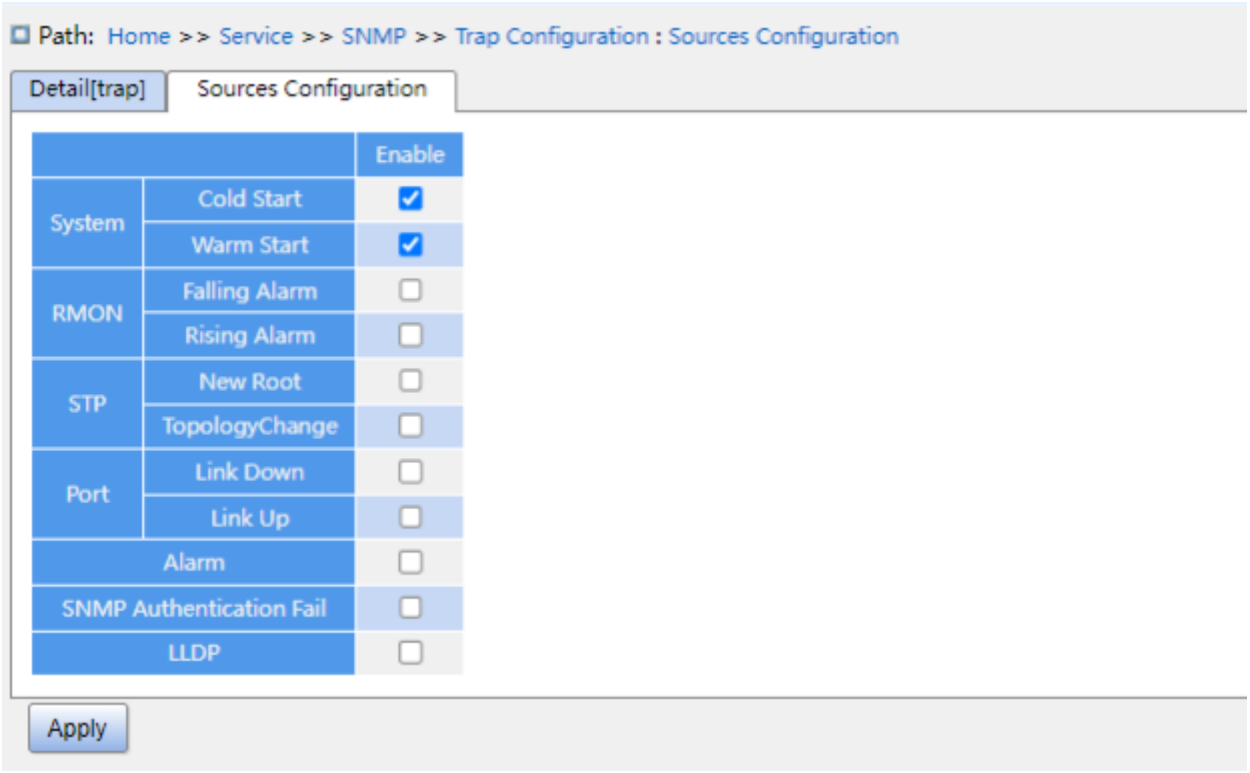


Рис. 42. Настройка событий для trap сообщений

System warm start/cold start

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Отправка trap сообщения в случае warm start / cold start коммутатора

RMON falling alarm/rising alarm

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Отправка trap сообщения в случае, когда RMON генерирует включение / выключение сигнала тревоги коммутатора.

STP new root/ topology change

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Отправка trap сообщения в случае, когда состояние STP (Spanning Tree Protocol) изменилось.

Port link up/down

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Отправка trap сообщения при включении / отключении порта или при изменении статуса порта коммутатора.

Alarm

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Отправка trap сообщения при наличии информации о тревоге.

SNMP authentication fail

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Отправка trap сообщения при сбое аутентификации SNMP.

LLDP

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Отправка LLDP trap сообщения при изменении статуса соседнего устройства.

5.2.6 Пример конфигурации SNMP

Станция управления SNMP и коммутатор подключены через Ethernet. IP-адрес станции управления - 192.168.0.23, IP-адрес коммутатора - 192.168.0.2. NMS получает данные и управляет агентом через SNMP v2c, считывает и записывает информацию об узле MIB агента. Агент отправляет Trap-сообщения в NMS, чтобы сообщить о ситуации, когда состояние агента изменяется, как показано на рисунке далее.

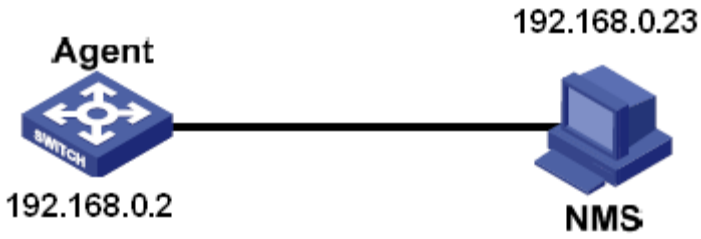


Рис. 43. Пример конфигурации SNMP v2c

Конфигурация агента:

1. Включите SNMP v2c; настройте права доступа Read only (Только для чтения) для сообщества «public»; настройте права доступа Read and write (Чтение и запись) для сообщества "private", как показано на рис. 38, 39;

2. Настройте режим передачи trap сообщений, как показано на рис. 40;

3. Создайте trap с именем 111, включите режим передачи trap сообщений; установите версию trap SNMP v2c, IP-адрес назначения 192.168.0.23. Выберите систему, интерфейс, аутентификацию, переключите все события для генерации trap сообщений и примените настройки по умолчанию для других параметров, как показано на рис. 42.

Для отслеживания и управления SNMP агентом, запустите соответствующее программное обеспечение управления на NMS.

5.3 SNMPv3

5.3.1 Введение

SNMP v3 предоставляет механизм аутентификации на основе User-Based Security Model (USM). Вы можете настроить функции аутентификации и шифрования. Аутентификация используется для проверки подлинности отправителя пакета, предотвращая несанкционированный доступ пользователей. Шифрование используется для шифрования пакетов, передаваемых между NMS и агентом, во избежание перехвата. Функции аутентификации и шифрования позволяют повысить

безопасность связи между SNMP NMS и SNMP-агентом.

Чтобы обеспечить связь между NMS и агентом, их версии SNMP должны совпадать. На агенте можно настроить разные версии SNMP, чтобы он мог использовать разные версии для связи с разными NMS.

5.3.2 Реализация

SNMP v3 предоставляет четыре таблицы конфигурации. Каждая таблица может содержать 16 записей. Эти таблицы определяют, могут ли конкретные пользователи получать доступ к информации MIB.

Возможно создать несколько пользователей в таблице пользователей, и каждый пользователь будет использовать разные политики для реализации таких функций безопасности, как аутентификация и шифрование пользователей.

Таблица для групп представляет собой совокупность нескольких пользователей. Разрешения доступа предназначены для группы пользователей. Разрешения доступа группы применяются ко всем пользователям в группе.

Таблица представлений относится к информации представления MIB, чтобы указать информацию MIB, к которой пользователи могут получить доступ. Представление MIB может содержать все узлы определенного поддерева MIB (т. е. разрешен доступ ко всем узлам поддерева MIB) или может не содержать все узлы определенного поддерева MIB (т. е. доступ ко всем узлам поддерева MIB запрещен).

Таблица доступа осуществляет доступ к информации узла MIB, сопоставляя имя группы, режим безопасности и уровень безопасности.

5.3.3 Web конфигурация SNMP v3

1. Включите SNMP, как показано далее.

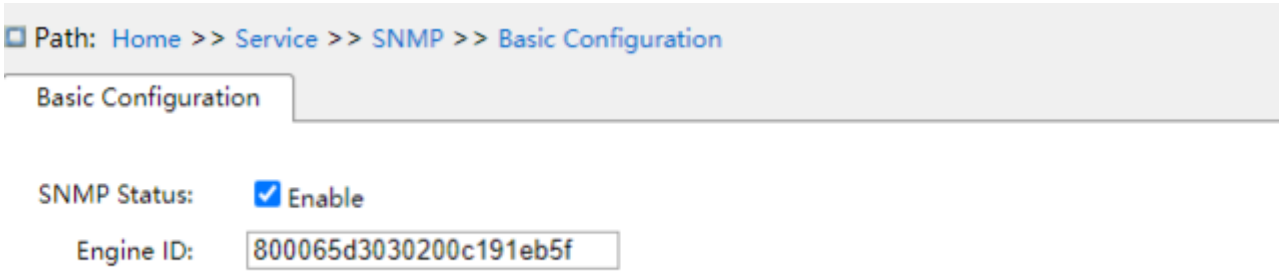


Рис. 44. Включение SNMP

SNMP Status

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Enable

Функция: Включение протокола SNMP на коммутаторе

Engine ID

Диапазон: Четное шестнадцатеричное число, не может быть все 0 или все F. Диапазон значений четного числа составляет 10~64.

Функция: Идентификатор Engine ID для SNMP v3, при изменении engine ID пользователь, соответствующий engine ID устройства в таблице пользователей, будет удален.

2. Настройте передачу trap сообщений, как показано на рисунке далее.

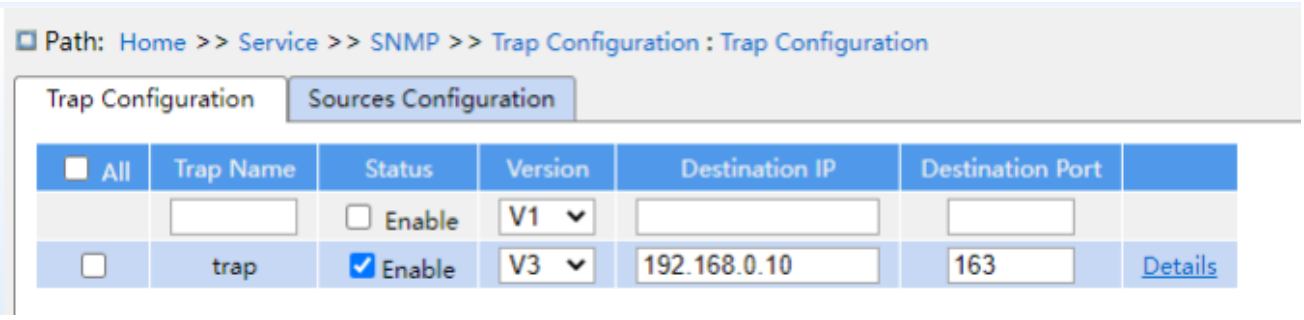


Рис. 45. Настройка trap сообщений

Trap name

Диапазон: 1~32 символа

Функция: Задайте имя для trap

Status

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включите или отключите trap сообщения. Коммутатор отправляет соответствующее сообщение trap сообщение на сервер, если включено

Version

Варианты конфигурации: V1/ V2C/ V3

Конфигурация по умолчанию: V1

Функция: Настройте номер версии для trap сообщений, отправляемых коммутатором на сервер.

Destination IP

Формат: A.B.C.D

Функция: Настройте адрес сервера для отправки trap сообщений.

Destination Port

Диапазон: 1~65535

Конфигурация по умолчанию: 162

Функция: Настройте номер порта для отправки trap сообщений

3. Нажмите на Details чтобы просмотреть детали конфигурации trap сообщений, как показано на рисунке далее.

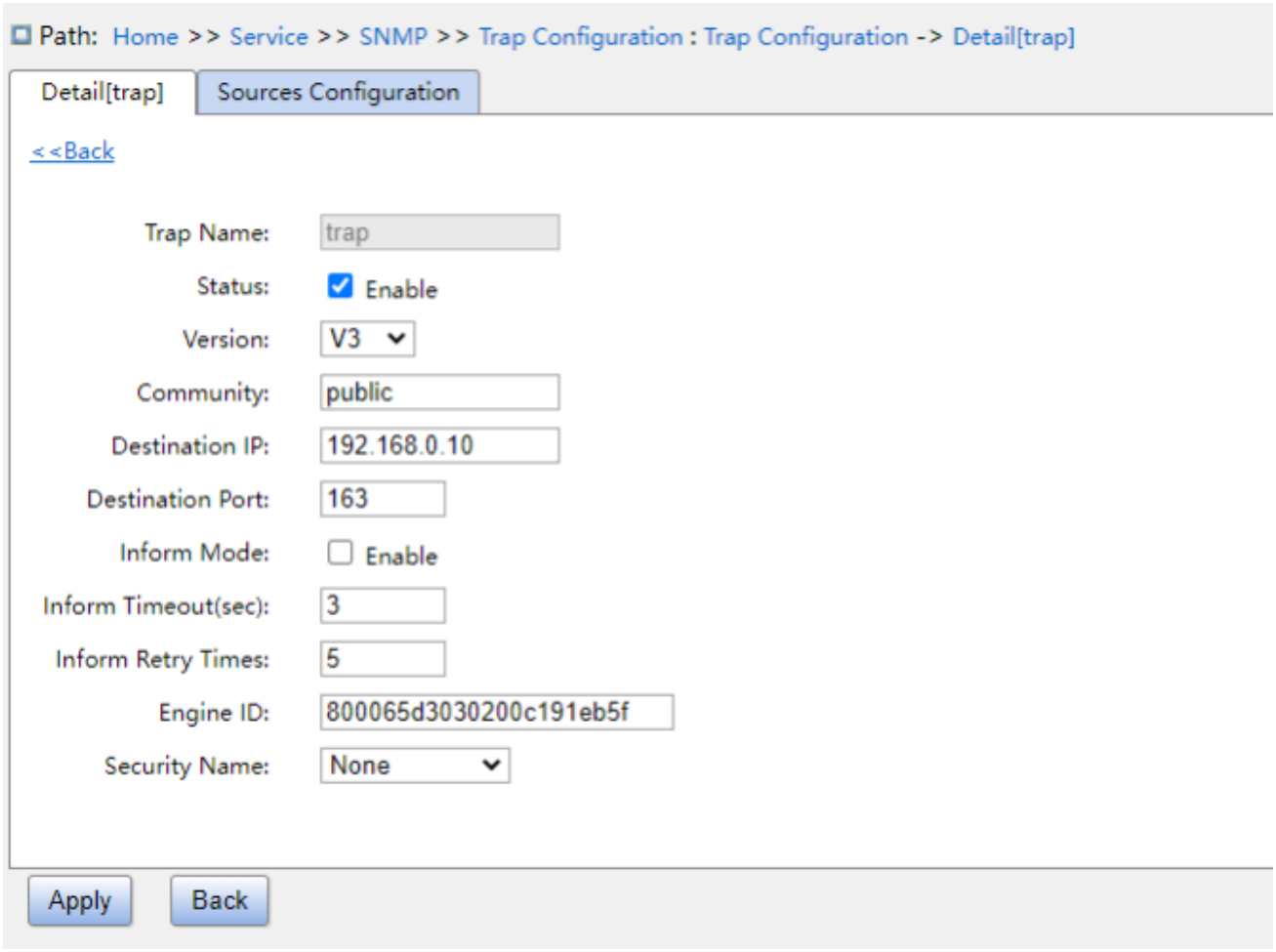


Рис. 46. Дополнительная настройка trap сообщений

Community

Диапазон: 0~255 символов

Конфигурация по умолчанию: public

Функция: Настройте имя сообщества, которое будет указано в отправляемом trap сообщении.

Inform Mode

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: После получения trap сообщения сервер отправляет коммутатору ответное сообщение.

Inform Timeout

Диапазон: 0~2147 сек.

Конфигурация по умолчанию: 3 сек.

Функция: Настройте тайм-аут отправки trap сообщения; после того, как коммутатор отправит trap сообщение, если в течение этого времени от сервера не будет ответа, то коммутатор повторно отправит trap сообщение.

Inform retry Times

Диапазон: 0~255

Конфигурация по умолчанию: 5

Функция: Настройте количество раз для срабатывания Inform Timeout. Если суммарное количество раз отправки превышает заданное значение, а сервер не отвечает, значит, возникает ошибка отправки trap сообщения.

Engine ID

Диапазон: Четное шестнадцатеричное число, не может быть все 0 или все F. Диапазон значений четного числа составляет 10~64.

Функция: Настройте значение идентификатора engine ID, которое содержится в trap-сообщении SNMP v3.

4. Настройте события для отправки Trap сообщений, как показано на рисунке далее.

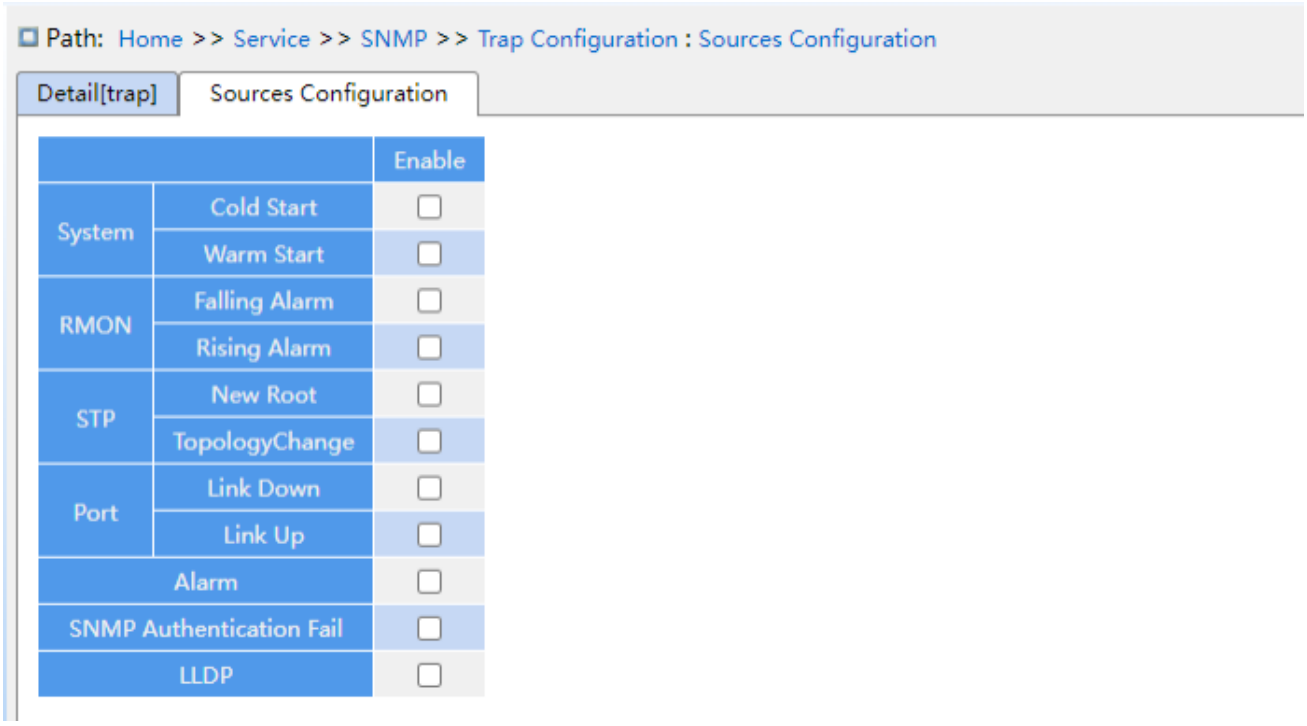


Рис. 47. Настройка событий для trap сообщений

System warm start/cold start

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Отправка trap сообщения в случае warm start / cold start коммутатора

RMON falling alarm/rising alarm

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Отправка trap сообщения в случае, когда RMON генерирует включение / выключение сигнала тревоги коммутатора.

STP new root/ topology change

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Отправка trap сообщения в случае, когда состояние STP (Spanning Tree Protocol) изменилось.

Port link up/down

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Отправка trap сообщения при включении / отключении порта или при изменении статуса порта коммутатора.

Alarm

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Отправка trap сообщения при наличии информации о тревоге.

SNMP authentication fail

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Отправка trap сообщения при сбое аутентификации SNMP.

LLDP

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Отправка LLDP trap сообщения при изменении статуса соседнего устройства.

5. Настройте таблицу имен пользователей, как показано далее.

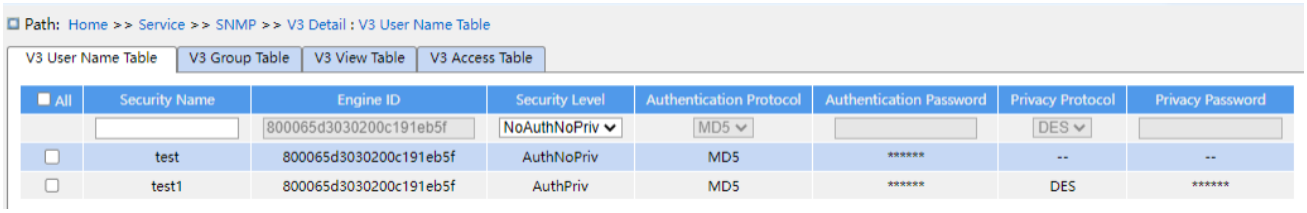


Рис. 48. Настройка таблицы пользователей для протокола SNMP v3

Security Name

Диапазон: 1~32 символа

Функция: Создание имени пользователя.

Engine ID

Диапазон: Четное шестнадцатеричное число, не может быть все 0 или все F. Диапазон значений четного числа составляет 10~64.

Функция: Настройте значение идентификатора engine ID, которое содержится в trap-сообщении SNMP v3.

Security Level

Варианты конфигурации: NoAuthNoPriv/AuthNoPriv/AuthPriv

Конфигурация по умолчанию: NoAuthNoPriv

Функция: Настройка уровня безопасности для выбранного пользователя.

Описание: NoAuthNoPriv не требует ни аутентификации, ни шифрования; AuthNoPriv требует аутентификации, но не шифрования; AuthPriv требует и аутентификации и шифрования.

Authentication Protocol

Варианты конфигурации: MD5/SHA

Конфигурация по умолчанию: MD5

Функция: Выберите протокол аутентификации. При выборе authnopriv/authpriv в уровне безопасности (Security Level), вам необходимо настроить протокол аутентификации и пароль.

Authentication Password

Диапазон: 8~32 символов（SHA протокол）8~40 символов（MD5 протокол）

Функция: Создание пароля аутентификации.

Privacy Protocol

Варианты конфигурации: DES/AES

Конфигурация по умолчанию: DES

Функция: Выберите протокол шифрования. Протокол шифрования и пароль необходимо настроить при выборе AuthPriv на уровне безопасности.

Privacy Password

Диапазон: 8~32 символов

Функция: Задайте пароль для протокола шифрования.

Можно настроить до 16 пользователей.

6 . Настройте таблицу для групп, как показано на рисунке далее.

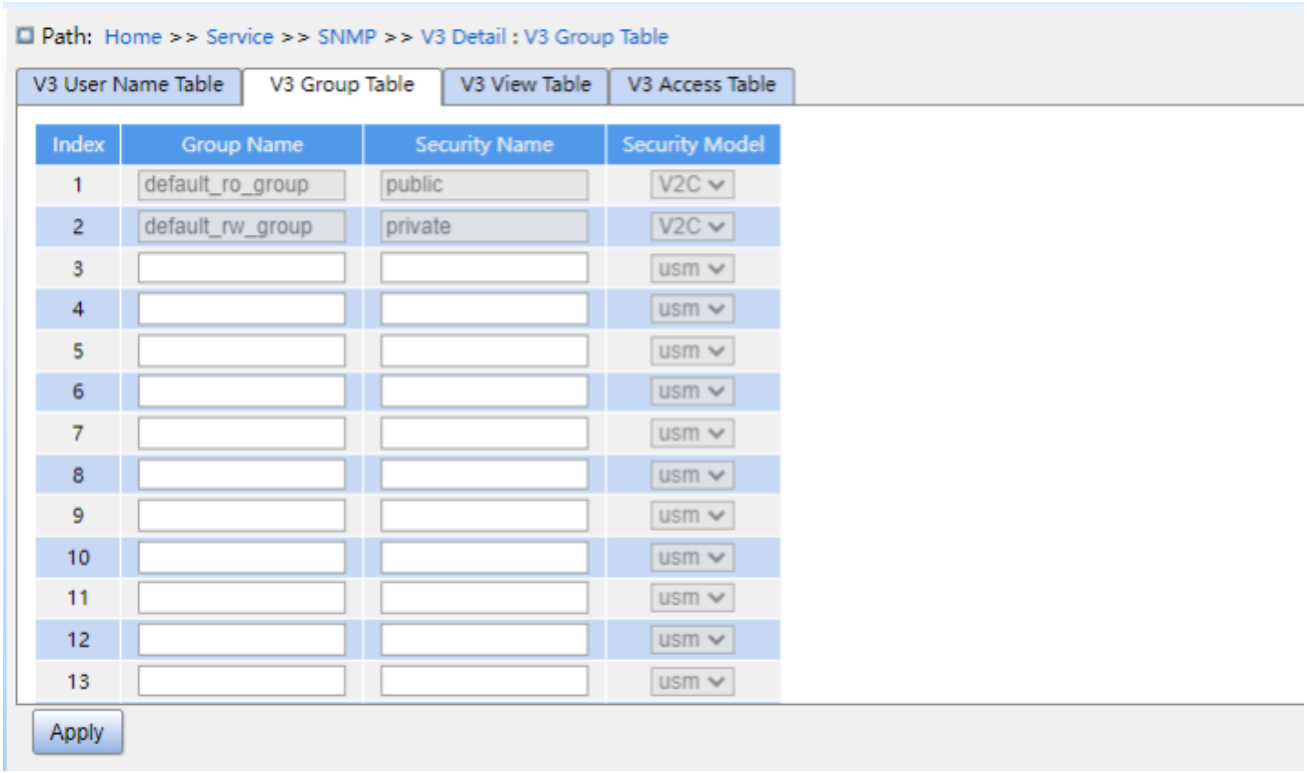


Рис. 49. Настройка таблицы групп пользователей SNMP v3

Group name

Диапазон: 1~32 символа

Функция: Настройте имя группы пользователей. Пользователи с одинаковым именем группы принадлежат к одной группе пользователей.

Security model

Диапазон: v1, v2, usm

Конфигурация по умолчанию: usm

Функция: Выберите режим безопасности текущей группы (то есть номер версии SNMP). SNMPv3 использует технологию usm (user-based security model). В настоящее время эта опция обязательна для режима SNMP v3.

Security name

Диапазон: Созданное имя пользователя, 1~32 символа

Функция: Настройте Security name. Security name должно совпадать с конфигурацией имени пользователя в таблице пользователей для протокола SNMP v3. Для v1 и v2 Security name должно совпадать именем Community для протокола SNMP.

Можно настроить до 32 групповых таблиц.

7. Настройте таблицу представлений, как показано на рисунке далее.

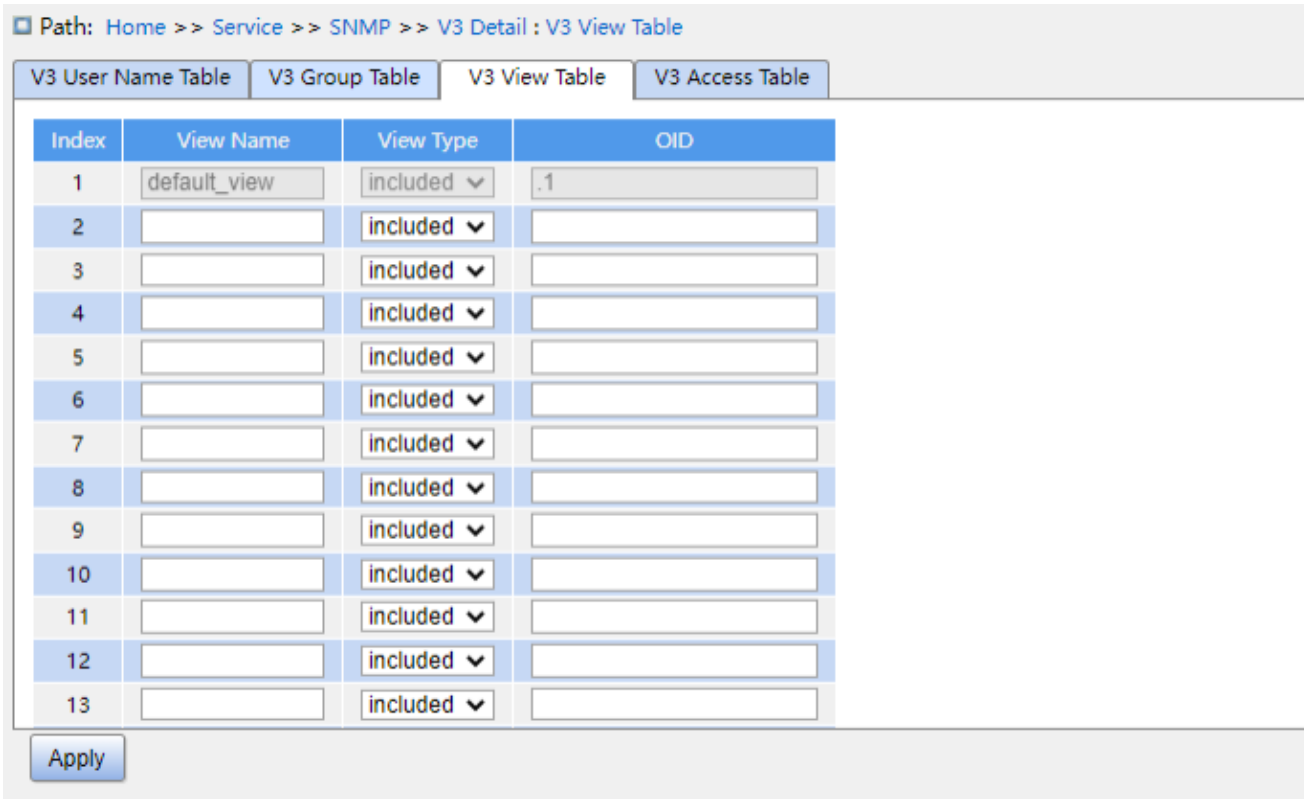


Рис. 50. Настройка таблицы представлений для SNMP v3

View Name

Диапазон: 1~32 символа

Функция: Задайте имя для представления.

View Type

Варианты конфигурации: included/excluded

Функция: Включено (included) указывает, что текущее представление включает все узлы поддерева MIB, исключено (excluded) указывает, что текущее представление не включает ни одного узла поддерева MIB.

OID subnode

Функция: Настройте поддерево MIB, OID Subnode задается относительно корневого узла.

Можно настроить до 16 таблиц представления.

По умолчанию таблица представлений default_view существует в коммутаторе и содержит все узлы 1-го поддерева (subnode .1).

8. Настройте таблицу доступа, как показано далее.

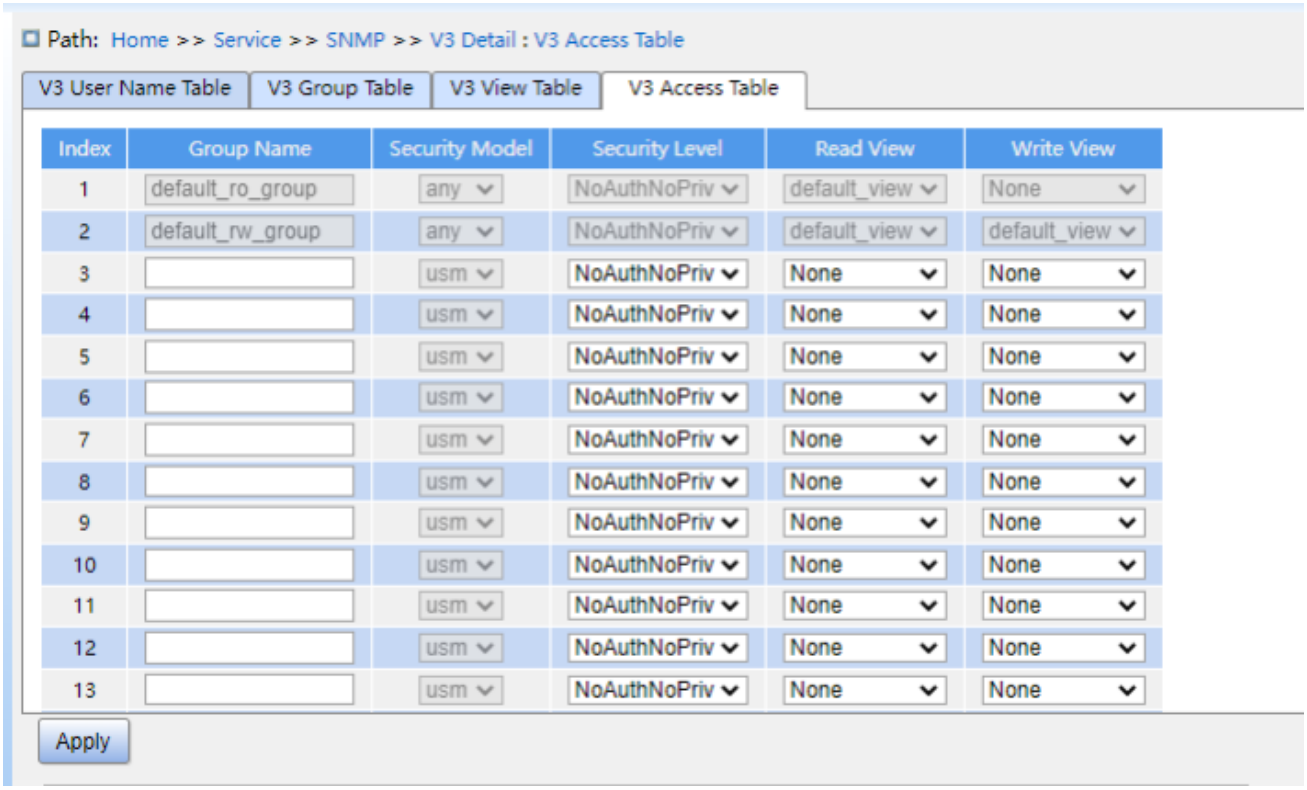


Рис. 51. Настройка таблицы доступа для SNMP v3

Group Name

Диапазон: Созданное имя группы, 1~32 символа

Описание: Все пользователи в группе имеют одинаковые права доступа

Security Model

Конфигурация по умолчанию: any/v1/v2/usm

Функция: Выберите Security Model для текущей группы (то есть номер версии SNMP), SNMPv3 использует технологию USM. Any означает использование любой модели безопасности. Имя группы, конфигурация модели безопасности должны соответствовать имени группы и модели безопасности в таблице V3 Group Table.

Security Level

Варианты конфигурации: NoAuthNoPriv/AuthNoPriv/AuthPriv

Функция: Настройте уровень безопасности текущей группы

Описание: NoAuthNoPriv не требует ни аутентификации, ни шифрования; AuthNoPriv требует аутентификации, но не шифрования; AuthPriv требует и аутентификации и шифрования. Когда требуется шифрование, протокол аутентификации/шифрования, пароль аутентификации/шифрования на стороне NMS должны соответствовать конфигурации пользовательской таблицы, тогда к информации об узле коммутатора можно успешно получить доступ.

Уровень безопасности NoAuthNoPriv AuthNoPriv AuthPriv имеют приоритет по возрастанию. Т.е. низкий уровень безопасности позволяет получить к нему доступ с высоким уровнем безопасности. Если для группы настроен уровень безопасности AuthNoPriv, пользователи с уровнем безопасности AuthNoPriv и AuthPriv в этой группе могут успешно получить доступ к коммутатору, если оба протокола аутентификации / шифрования и пароль аутентификации / шифрования указаны правильно. Но пользователи с уровнем безопасности NoAuth/ NoPriv не смогут получить доступ к коммутатору, т.к. имеют более низкий приоритет.

Read View

Варианты конфигурации: default_view/None/Созданное имя представления

Функция: Выберите имя представления доступное только для чтения

Write View

Варианты конфигурации: default_view/None/ Созданное имя представления

Функция: Выберите имя представления доступное для чтения и записи

Можно настроить до 16 таблиц доступа (исключая 2 записи по умолчанию).

Таблицы доступа на коммутаторе по умолчанию: {default_ro_group, any, NoAuth,NoPriv, default_view, None}, {default_rw_group, any, NoAuth,NoPriv, default_view, default_view}

5.3.4 Пример конфигурации SNMP v3

Станция управления SNMP подключена к коммутатору через Ethernet, IP-адрес станции управления - 192.168.0.23, а IP-адрес коммутатора - 192.168.0.2. Пользователь 1111 и пользователь 2222 зарегистрированы в агенте SNMP v3. Уровень безопасности установлен AuthNoPriv, который позволяет выполнять операции только для чтения со всей информацией узла в агенте.

При возникновении аварийного сигнала агент отправляет сообщения trap v3 в NMS, как показано на рисунке далее.

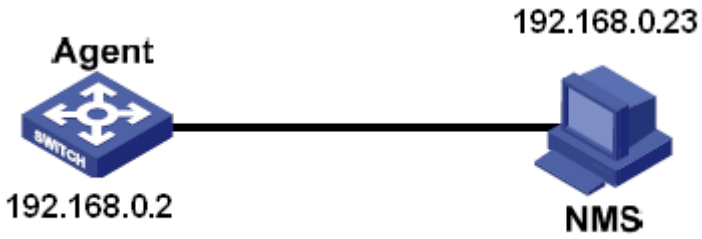


Рис. 52. Пример конфигурации SNMP v3

Конфигурация агента (Agent):

1. Активировать протокол SNMP v3 как показано на рис. 44

2. Сконфигурировать таблицу пользователей SNMP v3

Имя пользователя: 1111, уровень безопасности: Auth, Priv, протокол аутентификации: MD5, пароль аутентификации: aaaaaaaa, протокол шифрования: DES, пароль шифрования: xxxxxxxxx;

Имя пользователя: 2222, Уровень безопасности: Auth, Priv, Протокол аутентификации: SHA, Пароль аутентификации: bbbbbbbb, Протокол шифрования: AES, Пароль шифрования: yyyyyyyy; см. рис. 48

3. Создайте группу в режиме безопасности usm, включая пользователей 1111 и 2222; см. рис. 49

4. Настройка таблицы доступа SNMP v3

Имя группы: group, режим безопасности: usm, уровень безопасности: Auth, NoPriv, имя представления чтения: default_view, имя представления записи: None; см. рис. 51

5. Включить режим trap; см. рис. 45

6. Создайте запись trap 222, включите режим trap, выберите для trap версию SNMP v3, адрес назначения - 192.168.0.23, выберите систему, интерфейс, аутентификацию и обмен всеми событиями для события trap, а для остальных параметров используйте конфигурацию по умолчанию.

Если вы хотите отслеживать состояние устройства-агента и управлять им, вам необходимо запустить соответствующее программное обеспечение управления на стороне NMS.

5.4 Конфигурация SSH

5.4.1 Введение

SSH (Secure Shell) — это сетевой протокол для безопасного удаленного входа в систему. SSH шифрует передаваемые данные для предотвращения утечки информации. При использовании SSH пользователи могут использовать только командную строку для конфигурирования коммутаторов.

Данная серия коммутаторов поддерживает функцию сервера SSH, позволяя нескольким пользователям SSH одновременно подключаться для входа в систему на удаленных устройствах через SSH.

5.4.2 Реализация

Чтобы добиться безопасного SSH-соединения, сервер и клиент должны пройти пять этапов.

Этап согласования номера версии. В настоящее время SSH включает две версии SSH1 и SSH2. Обе стороны определяют, какую версию использовать, путем согласования версии.

Этап согласования ключа и алгоритма. SSH поддерживает несколько алгоритмов шифрования, и обе стороны согласовывают окончательный алгоритм, который будет

использоваться на основе поддерживаемых алгоритмов.

Фаза аутентификации. Клиент SSH инициирует запрос аутентификации на сервер, и сервер аутентифицирует клиента.

Фаза запроса сеанса. После прохождения аутентификации клиент отправляет запрос сеанса на сервер.

Фаза сеанса. После прохождения запроса сеанса сервер и клиент обмениваются информацией.

5.4.3 Web конфигурация SSH

1. Включите протокол SSH, как показано на рисунке далее.

Рис. 53. Включение SSH протокола

SSH Status

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Enable

Функция: Включить / Отключить протокол SSH. При включении коммутатор действует как SSH-сервер.

5.4.4 Пример конфигурации SSH

ПК (Host) действует как SSH-клиент для установления локального соединения с коммутатором (Switch), как показано на рисунке далее.

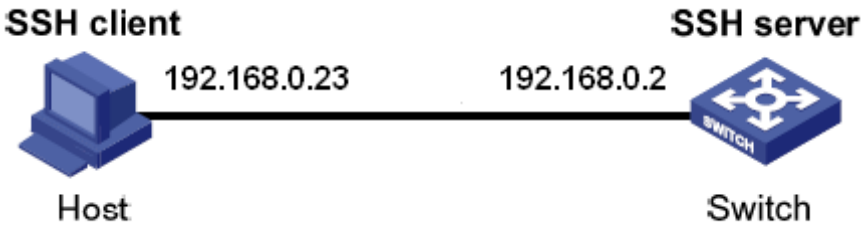


Рис. 54. Пример конфигурации SSH

1. Включите протокол SSH, как показано на рис. 53.

2. Откройте программу PuTTY.exe, как показано на рис. 55, введите IP-адрес SSH-сервера в поле Host Name (or IP address): 192.168.0.2.

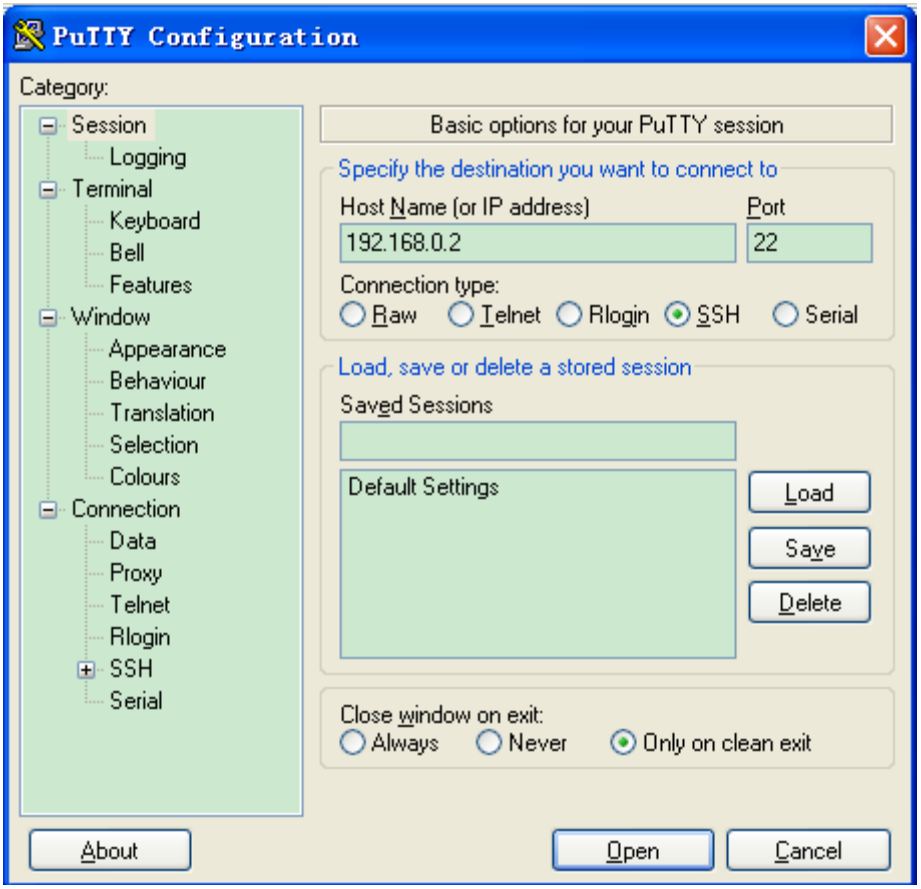


Рис. 55. Конфигурация SSH-клиента

3. Нажмите кнопку <Open>. Когда появится предупреждающее сообщение, нажмите кнопку <Yes (Y)>.

4. Введите имя пользователя: admin и пароль «STEZ» для входа в интерфейс конфигурации коммутатора, как показано на рисунке далее.

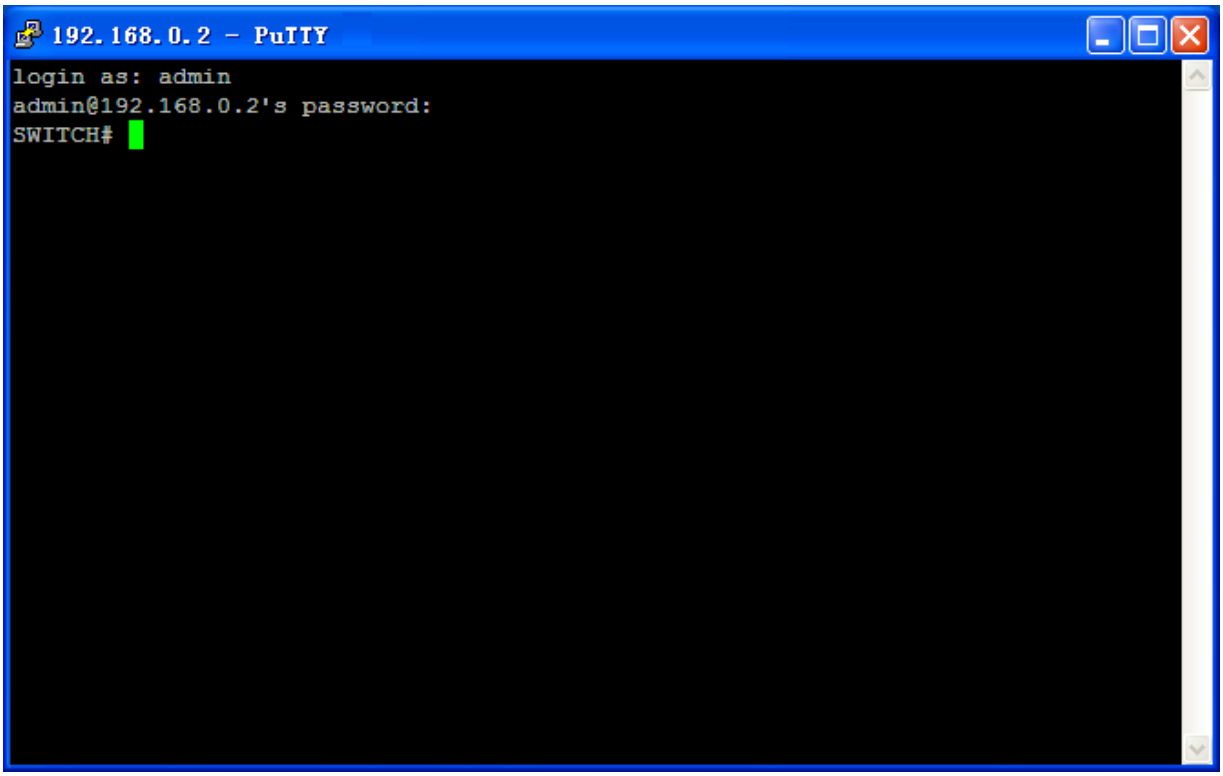


Рис. 56. Интерфейс входа в систему с аутентификацией по паролю SSH

5.5 Конфигурация TACACS+

5.5.1 Введение

Terminal Access Controller Access Control System (TACACS+) — это приложение на основе TCP, которое использует режим клиент/сервер для реализации связи между сервером доступа к сети Network Access Server (NAS) и сервером TACACS+. Клиент работает на NAS, а управление информацией о пользователях осуществляется централизованно на сервере. NAS — это сервер для пользователей, но клиент для сервера TACACS+. Структурная схема представлена на рисунке далее.

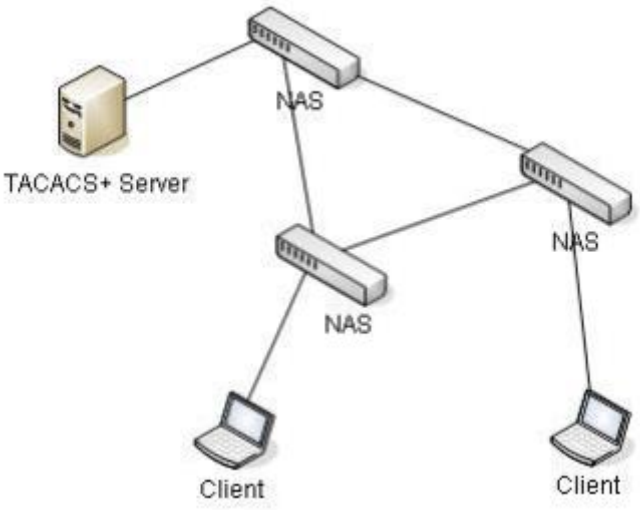


Рис. 57. Структурная схема TACACS+

Протокол аутентифицирует, авторизует и устанавливает права пользователям терминала, которым необходимо войти в систему для выполнения операций. Коммутатор выступает в качестве клиента TACACS+ и отправляет имя пользователя и пароль на сервер TACACS+ для аутентификации. Сервер получает запросы TCP-соединения от пользователей, отвечает на запросы аутентификации и проверяет легитимность пользователей. Если пользователь проходит аутентификацию, он может войти в устройство для выполнения операций.

5.5.2 Web конфигурация TACACS+

1. Настройте сервер TACACS+, как показано далее.

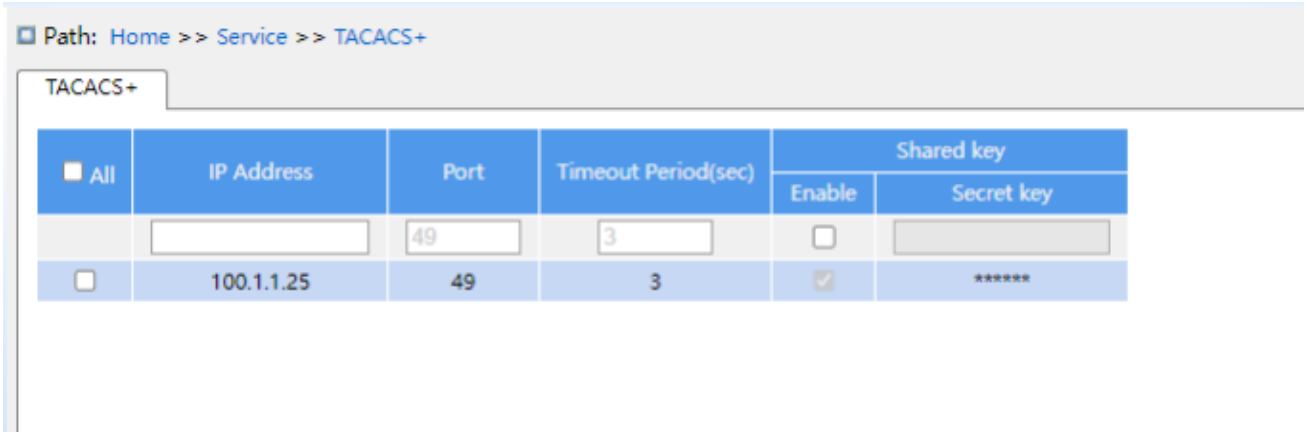


Рис. 58. Конфигурация сервера TACACS+

IP Address

Функция: Настройте IP-адрес или имя хоста сервера TACACS+. Можно настроить максимум 5 серверов TACACS+.

Port

Диапазон: 1~65535

Конфигурация по умолчанию: 49

Функция: Настройте номер порта аутентификации TCP сервера TACACS+.

Timeout Period (sec)

Диапазон: 1~1000 сек.

Конфигурация по умолчанию: 3

Функция: Настройте тайм-аут ответа сервера TACACS+. После того, как устройство отправит сообщение запроса TACACS+, оно не получит ответ от сервера TACACS+ в течение этого периода времени, аутентификация не будет выполнена, и устройство считает, что сервер недоступен.

Share Key

Диапазон: 0~63 символов

Функция: Настройте общий ключ (Share Key) на устройстве и на сервере TACACS+. Необходимо убедиться, что общий ключ, настроенный на устройстве, совпадает с ключом на сервере TACACS+.

5.5.3 Пример конфигурации TACACS+

Сервер TACACS+ может аутентифицировать и авторизовать пользователей с помощью коммутатора. IP-адрес сервера — 192.168.0.23, а общий ключ, используемый при обмене пакетами между коммутатором и сервером, — aaa. Способ подключения показан на рис. далее.

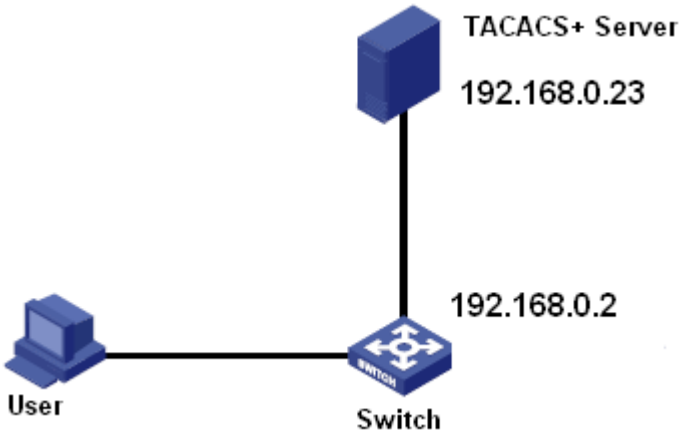


Рис. 59. Пример аутентификации TACACS+

1. Конфигурация сервера TACACS+, IP-адрес 192.168.0.23, общий ключ — aaa, см. рис. 58.
2. При входе в коммутатор через Web интерфейс используется тип аутентификации Local. При входе через Telnet используется тип аутентификации TACACS+. См. рис. 10.
3. Настройте имя пользователя и пароль «bbb», общий ключ «aaa» на сервере TACACS+.
4. При входе в коммутатор через Web введите имя пользователя admin и пароль STEZ для успешного доступа к коммутатору посредством локальной аутентификации.
5. При входе в коммутатор через Telnet введите имя пользователя и пароль bbb, чтобы успешно получить доступ к коммутатору через аутентификацию TACACS+.

5.6 Конфигурация RADIUS

5.6.1 Введение

RADIUS (Remote Authentication Dial-In User Service) — это протокол распределенного обмена информацией. Он определяет формат кадра RADIUS на основе UDP и механизм передачи информации, защищая сети от несанкционированного доступа. RADIUS обычно используется в сетях, требующих высокой безопасности и удаленного доступа пользователей.

RADIUS использует режим клиент / сервер для обеспечения связи между NAS (Network Access Server) и сервером RADIUS. Клиент RADIUS работает на NAS. Сервер RADIUS обеспечивает централизованное управление пользовательской информацией. NAS является сервером для пользователей, но клиентом для сервера RADIUS. Пример структуры сети показан на рисунке далее.

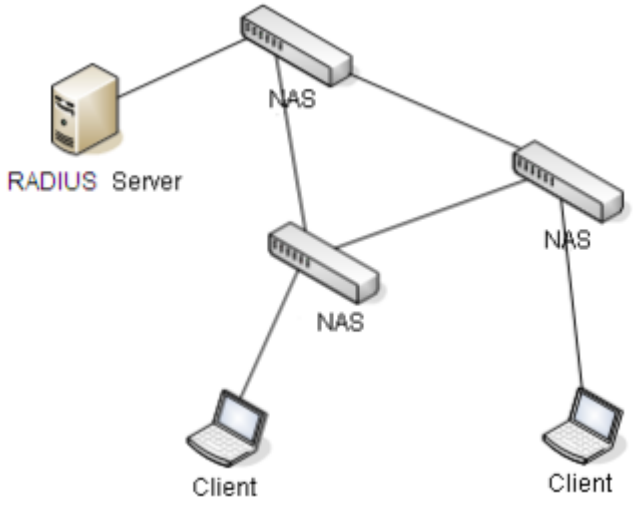


Рис. 60. Структурная схема RADIUS

Протокол аутентифицирует пользователей терминала, которым необходимо войти в систему для работы. Выступая в качестве клиента RADIUS, устройство отправляет информацию о пользователе на сервер RADIUS для аутентификации и разрешает или запрещает пользователям вход в устройство в соответствии с результатами аутентификации.

5.6.2 Web конфигурация RADIUS

1. Настройте сервер RADIUS, как показано на рисунке далее.

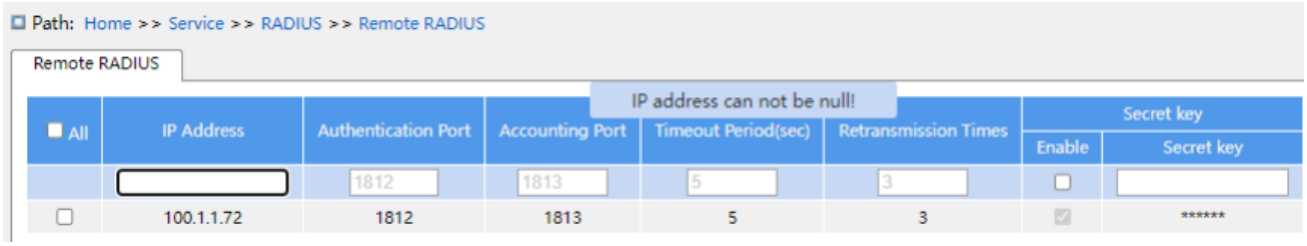


Рис. 61. Конфигурация RADIUS-сервера

IP Address

Функция: Настройте IP-адрес или имя хоста сервера RADIUS. Можно настроить максимум 5 серверов RADIUS.

Authentication Port

Диапазон: 0~65535

Конфигурация по умолчанию: 1812

Функция: Настройте номер порта аутентификации UDP на сервере RADIUS.

Accounting Port

Диапазон: 0~65535

Конфигурация по умолчанию: 1813

Функция: Установите UDP-порт RADIUS-сервера для учета. Поскольку RADIUS использует разные UDP-порты для приема и отправки сообщений аутентификации и учета, для аутентификации и учета должны быть настроены разные номера портов.

Timeout Period (sec)

Диапазон: 1~1000 сек.

Конфигурация по умолчанию: 5 сек.

Функция: Установите время ожидания ответа от сервера RADIUS. После отправки пакета запроса RADIUS устройство повторно передаст пакет запроса RADIUS, если по истечении указанного времени оно по-прежнему не получит ответа от сервера RADIUS.

Retransmission Times

Диапазон: 1~1000

Конфигурация по умолчанию: 3

Функция: Установите максимальное количество попыток повторной передачи для пакетов запросов RADIUS. Если устройство не получает ответных пакетов от сервера RADIUS после максимального количества попыток повторной передачи (Retransmission Times), аутентификация завершается неудачей, и устройство будет считать сервер RADIUS недействительным.

Secret Key

Диапазон: 0~63 символов

Функция: Настройте секретный ключ (Secret Key) на устройстве и на сервере RADIUS. Необходимо убедиться, что секретный ключ, настроенный на устройстве совпадает с ключом на сервере RADIUS.

Приоритет “Timeout Period”, “Retransmission Times” и “Secret Key” в конфигурации сервера RADIUS выше, чем в глобальной конфигурации.

2. Настройте глобальную конфигурацию RADIUS, как показано далее

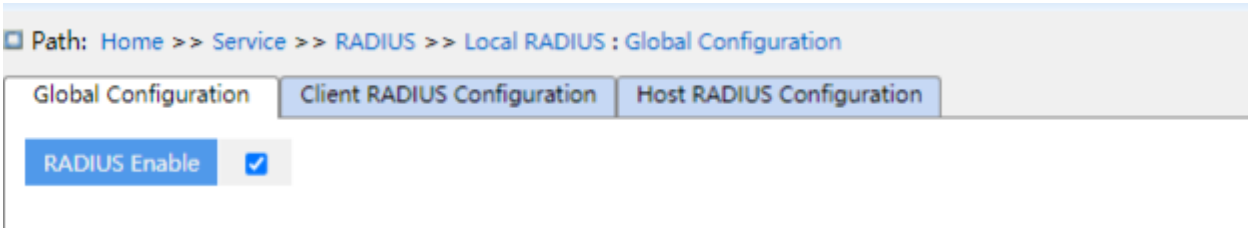


Рис. 62. Глобальная конфигурация RADIUS

RADIUS Enable

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включить ли локальный RADIUS для использования другими устройствами в качестве серверов RADIUS.

1. Конфигурация RADIUS-клиента, как показано на рисунке далее.

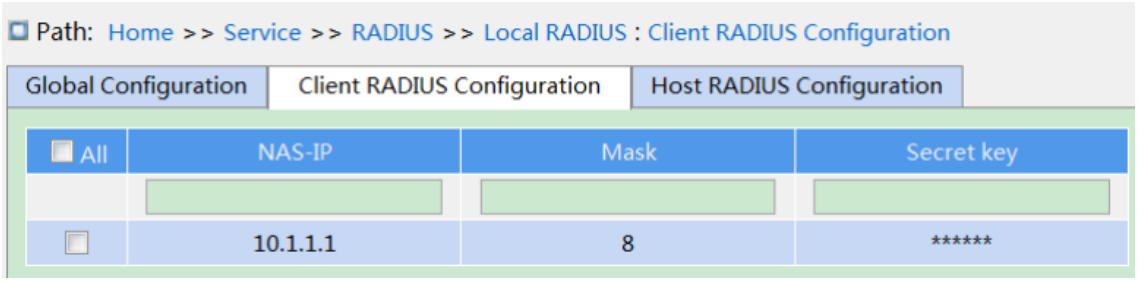


Рис. 63. Конфигурация клиента RADIUS

NAS-IP

Функция: Настройка IP-адреса или сегмента IP-адреса для RADIUS-клиента

Mask

Диапазон: 1-32

Функция: Настройте сегмент сети с адресом клиента RADIUS. Для IP-адресов в одном сегменте сети необходимо настроить только один сегмент сети.

Secret key

Диапазон: 1~63 символов

Функция: Настройте секретный ключ (Secret Key) на устройстве и клиенте. Необходимо убедиться, что секретный ключ, настроенный на устройстве совпадает с ключом на клиенте.

2. Настройте конфигурацию пользователя RADIUS, как показано на рисунке далее.

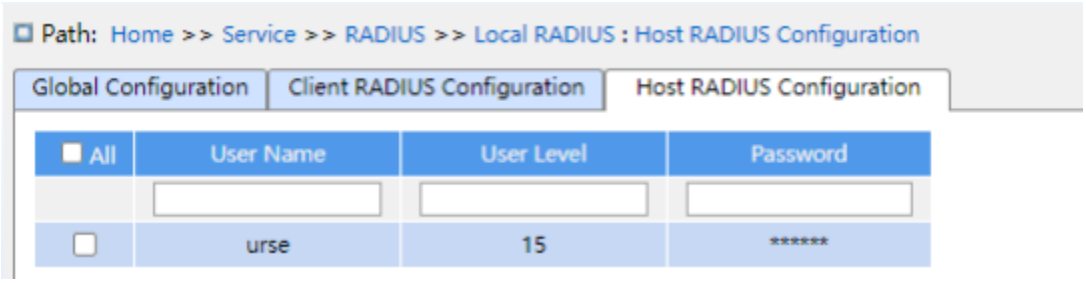


Рис. 64. Конфигурация пользователя RADIUS

User Name

Диапазон: 1~31 символов

Функция: Настройте имя пользователя RADIUS

User Level

Диапазон: 1~15

Функция: Настройте уровень полномочий пользователя. Пользователи с разными уровнями полномочий имеют разные права доступа.

Password

Диапазон: 1~31 символов

Функция: Настройте пароль для входа пользователя

5.6.3 Пример конфигурации RADIUS

Как показано на рисунке далее, IEEE802.1X включен на порте 1 коммутатора. Затем пользователи могут войти в систему на коммутаторе через порт 1 после прохождения аутентификации на сервере RADIUS. IP-адрес сервера - 192.168.0.23. Ключ для обмена пакетами между коммутатором и сервером задан “aaa”.

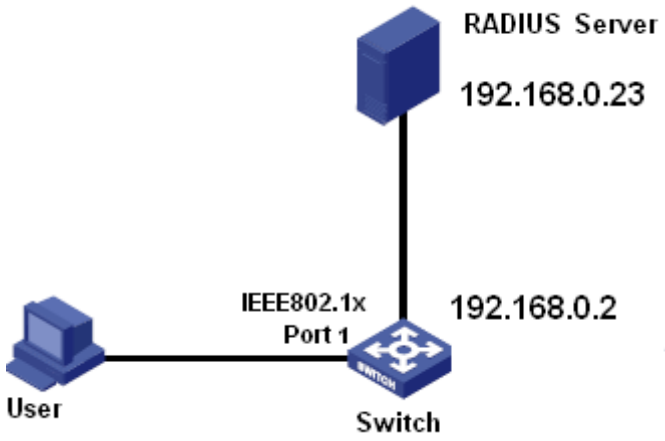


Рис. 65. Пример аутентификации RADIUS

1. Установите IP-адрес сервера аутентификации равным 192.168.0.23, а пароль “aaa”, как показано на рис. 61.

2. Конфигурация функции IEEE802.1X: включите функцию IEEE802.1X глобально, выберите RADIUS в качестве метода аутентификации, настройте статус управления порта 1 на 802.1X на основе порта и оставьте другие конфигурации по умолчанию.

3. Настройте имя пользователя и пароль на сервере RADIUS как “ccc”, а ключ как “aaa”.

4. Установите и запустите клиентское программное обеспечение аутентификации 802.1X на ПК, введите имя пользователя и пароль ccc, и пользователь сможет

получить доступ к коммутатору посредством аутентификации.

5.7 RMON

5.7.1 Введение

Remote Network Monitoring (RMON) протокол, основанный на архитектуре SNMP, позволяет устройствам сетевого управления отслеживать управляемые устройства и управлять ими. Сеть RMON обычно включает в себя станцию управления сетью Network Management Station (NMS) и агентов Agent. NMS управляет агентами, а агенты могут собирать статистику по различным типам трафика на портах.

RMON в основном предоставляет статистику и функции сигнализации. С помощью функции статистики агенты могут периодически собирать статистику по различным типам трафика на портах. Например, количество пакетов, полученных из определенного сегмента сети за определенный период. Функция сигнализации заключается в том, что агенты могут отслеживать значения назначенных переменных MIB. Когда значение достигает порога тревоги (например, количество пакетов достигает заданного значения), агент может автоматически записывать события в журнал тревог RMON или отправлять сообщение об ошибке на устройство управления.

5.7.2 Группы RMON

RMON (RFC 2819) определяет несколько групп RMON. Устройства серии поддерживают группу статистики, группу истории, группу событий и группу аварийных сигналов в общедоступном (public) MIB.

- Группа статистики (Statistics group)

С помощью группы статистики система собирает статистику по всем типам трафика на портах и сохраняет статистику в таблице статистики Ethernet для дальнейшего запроса устройством управления. Статистика включает в себя количество сетевых коллизий, пакетов с ошибками CRC, пакетов меньшего размера или с избыточным объемом, широковещательных и многоадресных пакетов, принятых

байт и принятых пакетов. После успешного создания записи статистики по указанному порту группа статистики подсчитывает количество пакетов на порте, и статистика продолжает непрерывно накапливаться.

- Группа истории (History group)

Группа истории производит выборку всех видов трафика на портах и сохраняет значения выборки в таблице записей истории для дальнейшего запроса устройством управления. Группа истории подсчитывает статистические значения всех видов данных в интервале выборки.

- Группа событий (Event group)

Группа событий используется для определения индексов событий и методов обработки событий. События, определенные в группе событий, используются в элементе конфигурации группы тревог. Событие срабатывает, когда контролируемое устройство удовлетворяет условию тревоги.

События обрабатываются следующими способами:

Log: регистрирует событие и связанную с ним информацию в таблице журнала событий.

Trap: отправляет сообщение о Trap в NMS и информирует NMS о событии.

Log-Trap: регистрирует событие и отправляет сообщение о Trap в NMS.

Нет: указывает на отсутствие действия.

- Группа тревог (Alarm group)

RMON alarm management может отслеживать переменные сигналов тревоги. После определения сигналов тревоги система начинает контролировать сигналы тревоги за определенный период. Тревоги обрабатываются в соответствии с определенными событиями.

Если значение переменной alarm превышает пороговое значение несколько раз в одном и том же направлении, то событие alarm срабатывает только в первый раз. Если сигнал alarm срабатывает в разных направлениях (о превышении и понижении), то

сигналы генерируется для каждого события.

5.7.3 Web конфигурация RMON

1. Настройте группу статистики, как показано на рисунке далее.

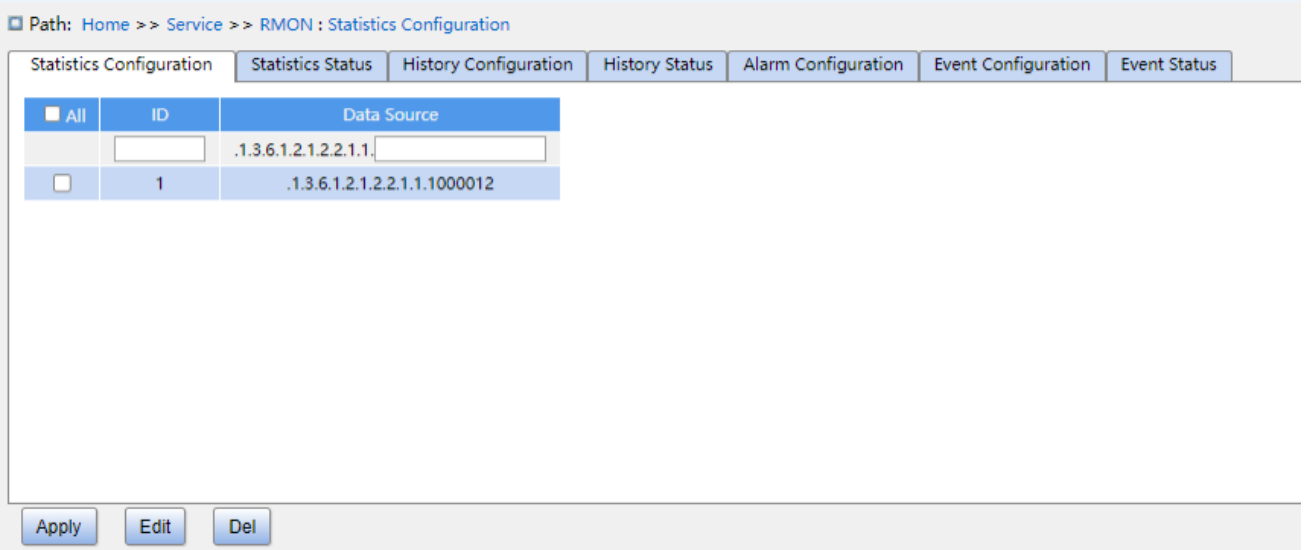


Рис. 66. Настройка группы статистики RMON

ID

Диапазон: 1~65535

Функция: Настройте количество записей статистической информации. Поддерживается максимум 128 статистических записей.

Data Source

Варианты конфигурации: 1000001-1000024 port ID

Функция: Выберите порт для сбора статистики.

2. Проверьте статистику по группе статистики, как показано на рисунке далее.

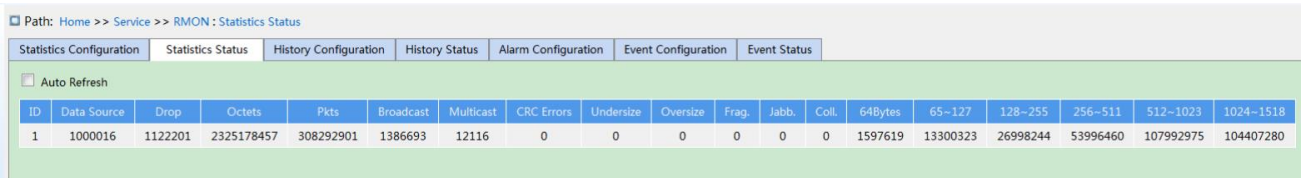


Рис. 67. Обзор группы статистики

Drop: количество пакетов, отброшенных портом.

Octets: количество байт, полученных портом.

Pkts: количество пакетов, полученных портом.

Broadcast: количество широковещательных пакетов, полученных портом.

Multicast: количество многоадресных пакетов, полученных портом.

CRC Errors: количество пакетов с ошибкой CRC длиной от 64 до 9600 байт, полученных портом.

Undersize: количество пакетов размером менее 64 байт, полученных портом.

Oversize: количество пакетов размером более 9600 байт, полученных портом.

Frag.: количество пакетов с ошибкой CRC длиной менее 64 байт, полученных портом.

Jabb.: количество пакетов с ошибкой CRC размером более 9600 байт, полученных портом.

Coll.: количество коллизий, полученных портом в полудуплексном режиме.

64 Bytes: количество пакетов длиной 64 байта, полученных портом.

65~127: количество пакетов длиной от 65 до 127 байт, полученных портом.

128~255: количество пакетов длиной от 128 до 255 байт, полученных портом.

256~511: количество пакетов длиной от 256 до 511 байт, полученных портом.

512~1023: количество пакетов длиной от 512 до 1023 байт, полученных портом.

1024~1588: количество пакетов длиной от 1024 до 1588 байт, полученных портом.

Превышение размера зависит от параметра «Максимальный размер кадра» в конфигурации порта, как показано в разделе 7.1 «Конфигурация порта». В приведенном выше примере превышение размера составляет 9600 байт.

3. Настройте группу истории, как показано далее.

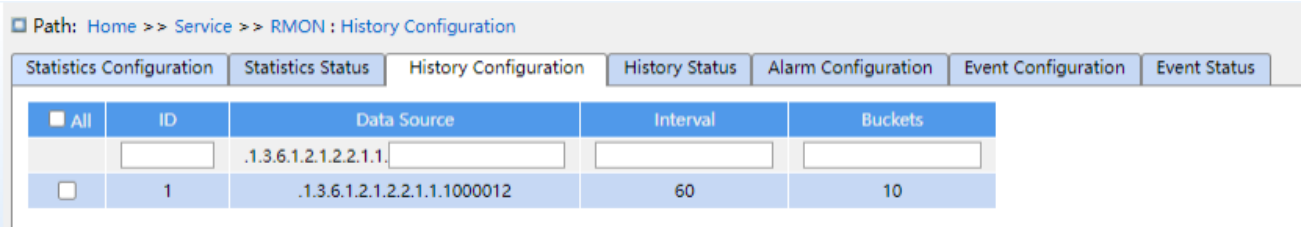


Рис. 68. Настройка группы истории

ID

Диапазон: 1~65535

Функция: Настройте количество элементов таблицы истории. Поддерживается максимум 256 элементов таблицы истории.

Data Source

Варианты конфигурации: 1000001-1000024 portid

Функция: Выберите порт для сбора статистики.

Interval

Диапазон: 1~3600 сек.

Значение по умолчанию: 1800 сек.

Функция: Настройте период выборки для порта

Buckets

Диапазон: 1~65535

Значение по умолчанию: 50

Функция: Настраивает количество последних значений выборки, хранящейся в RMON.

4. Просмотр статуса группы истории показан на рисунке далее.

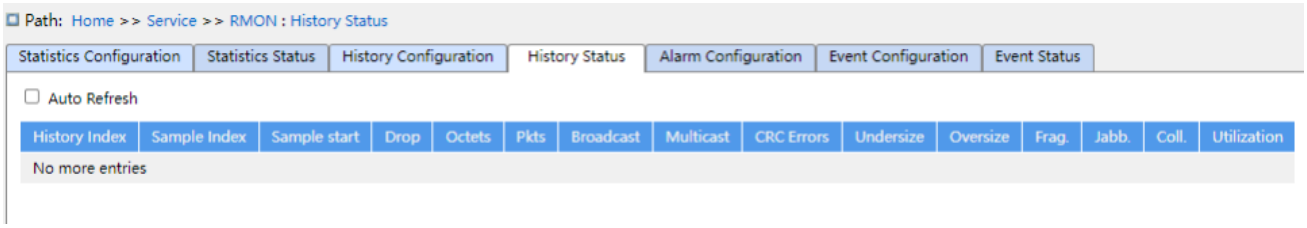


Рис. 69. Обзор статистики группы истории

5. Настройте группу событий, как показано далее

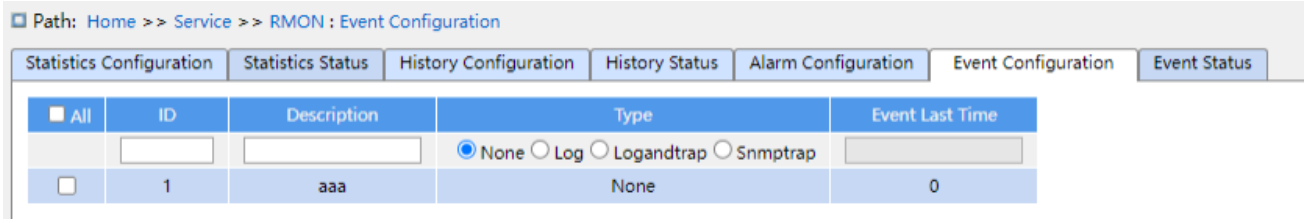


Рис. 70. Настройка группы событий

ID

Диапазон: 1~65535

Функция: Настройте количество элементов таблицы событий. Поддерживается максимум 128 элементов таблицы событий.

Description

Диапазон: 0~127 символов

Функция: Описание события

Type

Варианты конфигурации: none/log/snmptrap/logandtrap

Конфигурация по умолчанию: none

Функция: Настройте тип события, используемого при возникновении сигнала тревоги. То есть способ обработки сигнала тревоги.

Event Last Time

Функция: Отображает значение sysUpTime, которое показывает время последнего возникновения события.

6. Просмотр статуса для группы событий показан на рисунке далее.

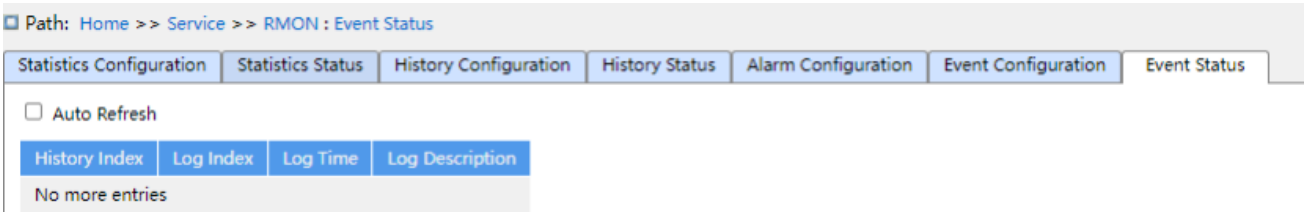


Рис. 71. Обзор статистики группы событий

7. Настройте таблицу тревог, как показано далее.

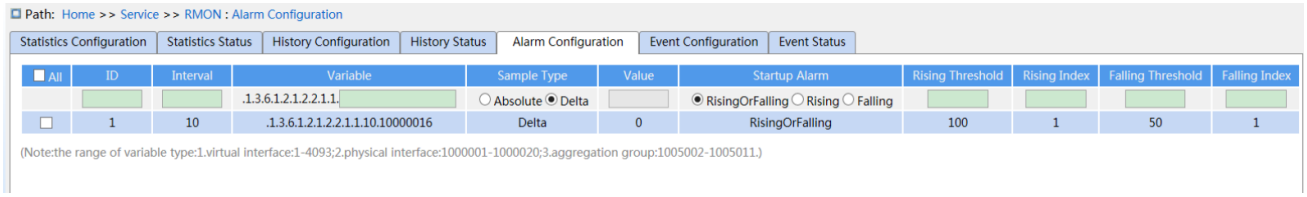


Рис. 72. Настройка группы тревог

ID

Диапазон: 1~65535

Функция: Настройте количество элементов таблицы тревог. Поддерживается

максимум 256 элементов таблицы тревог.

Interval

Диапазон: 1~2147483647 сек.

Значение по умолчанию: 30 сек.

Функция: Настройте период выборки информации.

Variable

Формат: A.10000portid/A.vlanid

Диапазон: A:10~21

Функция: Выберите информацию MIB для порта для ведения мониторинга.

InOctets: A=10, количество байт, полученных портом.

InUcastPkts: A=11 количество одноадресных пакетов, полученных портом.

InNUcastPkts: A=12 количество широковещательных и многоадресных пакетов, полученных портом.

InDiscards: A=13, количество пакетов, отброшенных портом.

InErrors: A=14, количество пакетов ошибок, полученных портом.

InUnknownProtos: A=15, количество неизвестных пакетов, полученных портом.

OutOctets: A=16, количество байт, отправленных портом.

OutUcastPkts: A=17, количество одноадресных пакетов, отправленных портом.

OutNUcastPkts: A=18 количество широковещательных и многоадресных пакетов, отправленных портом.

OutDiscards: A=19, количество отброшенных пакетов, отправленных портом.

OutErrors: A=20, количество пакетов ошибок, отправленных портом.

OutQLen: A=21, длина пакетов в очереди на выходе порта.

Sample Type

Варианты конфигурации: Absolute/Delta

Конфигурация по умолчанию: Delta

Функция: Выбрать метод сравнения значения выборки и порога

Описание: Absolute: напрямую сравнивать каждое значение выборки с порогом;

Delta: в разностном методе текущее значение выборки вычитается из предыдущего значения выборки, и разница сравнивается с порогом.

Startup Alarm

Варианты конфигурации: Rising/Falling/RisingOrFalling

Конфигурация по умолчанию: RisingOrFalling

Функция: Выберите тип сигнала тревоги, включая сигнал тревоги по нарастающему фронту, сигнал по заднему фронту, а также сигнал по нарастающему и заднему фронту.

Rising Threshold

Диапазон: 1~2147483647

Функция: Настройте порог нарастающего фронта. Когда значение выборки превышает порог нарастающего фронта и тип сигнала тревоги RisingAlarm или RisingOrFalling, выдается сигнал тревоги и активируется индекс Rising Threshold.

Rising Index

Диапазон: 1~65535

Функция: Настройте индекс нарастающих событий, то есть, как обрабатывать сигналы тревоги нарастающего фронта.

Falling Threshold

Диапазон: 1~2147483647

Функция: Настройте порог спадающего фронта. Когда значение выборки ниже порога спадающего фронта и тип сигнала тревоги Falling или RisingOrFalling, выдается сигнал тревоги и активируется индекс Falling Threshold.

Falling Index

Диапазон: 1~65535

Функция: Настройте индекс спадающих событий, то есть, как обрабатывать сигналы тревоги спадающего фронта.

6 Аварийная сигнализация

6.1 Введение

Коммутаторы данной серии поддерживают следующие типы сигналов тревоги:

- Сигнал тревоги по питанию: сигнал тревоги генерируется, когда один из входов питания отключается или выходит из строя;
- Конфликт IP/MAC: при конфликте IP/MAC-адресов будет генерироваться сигнал тревоги;
- Сигнализация использования CPU / памяти: сигнал тревоги генерируется, когда использование CPU / памяти коммутатора превышает заданный порог;
- Сигнал тревоги порта: сигнал тревоги генерируется при отключении соединения с портом (Link down);
- Сигнал тревоги о трафике порта: генерируется сигнал тревоги, когда количество входящего/исходящего трафика порта превышает указанный порог;
- Сигнал тревоги об ошибке CRC /потере пакета: генерируется сигнал тревоги, когда количество ошибок CRC /потерь пакетов порта превышает указанный порог;
- Сигнал тревоги для кольцевой топологии: при изменении в кольцевой топологии срабатывает сигнал тревоги;
- DDM сигнал тревоги: будет выдаваться сигнал тревоги, когда мощность передачи оптического модуля SFP опустится ниже порогового значения.

6.2 Web конфигурация сигналов тревоги

1. Базовая конфигурация сигналов тревоги показана на рис. ниже.

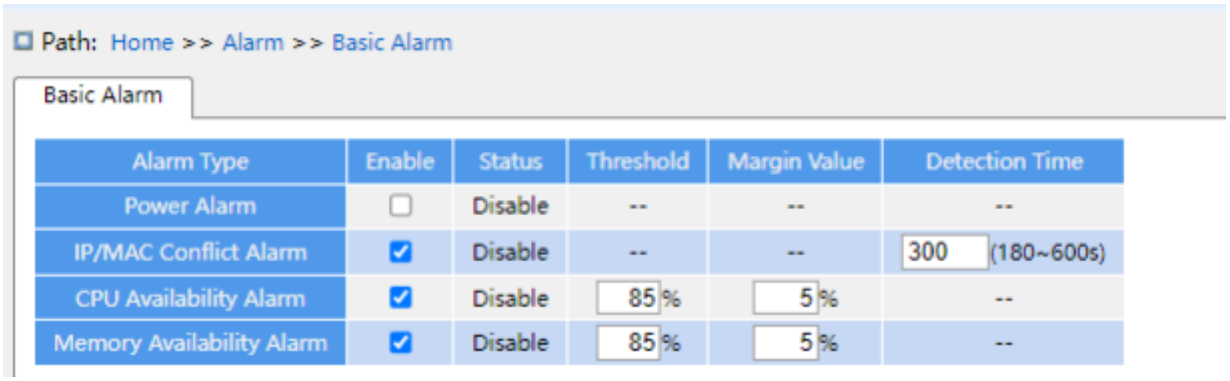


Рис. 73. Основные тревоги

Power Alarm

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включение / отключение сигнализации тревог по питанию.

Status

Варианты отображения: Normal/Alarm

Функция: Просмотр состояния сигнализации по питанию.

Alarm: Для устройств с резервным питанием один из модулей питания вышел из строя или работает ненормально, и срабатывает аварийный сигнал.

Normal: Для одиночных источников питания модуль питания подает питание в обычном режиме; для резервного источника питания два модуля питания подают питание в обычном режиме.

IP, MAC Conflict

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включение/выключение сигнализации о конфликте IP/MAC адресов.

Status

Варианты отображения: Conflict / No Conflict

Описание: Когда возникает конфликт IP/MAC адреса, отображается Conflict; в

противном случае отображается No Conflict.

Check Time

Диапазон: 180~600 сек.

Конфигурация по умолчанию: 300 сек.

Функция: Настройка интервала для обнаружения конфликтов IP/MAC.

CPU/Memory Availability Alarm

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включение/выключение сигнала тревоги о доступности процессора/памяти коммутатора.

Threshold (%)

Диапазон: 50~100

Конфигурация по умолчанию: 85

Функция: Настройте порог загрузки процессора/памяти коммутатора. Когда загрузка процессора/памяти коммутатора превысит это значение, будет выдан сигнал тревоги о том, что загрузка процессора/памяти превышает пороговое значение.

Margin Value (%)

Диапазон: 1~20

Конфигурация по умолчанию: 5

Функция: Установите предельное значение использования процессора/памяти.

Описание: Если загрузка процессора/памяти колеблется в пределах порогового значения, сигналы тревоги могут генерироваться и сбрасываться повторно. Чтобы предотвратить это явление, вы можете указать значение Margin Value (по умолчанию 5%). Сигнал тревоги будет снят только в том случае, если загрузка процессора/памяти будет ниже порогового значения на величину Margin Value или более. Например, порог использования памяти установлен на 60%, а значение Margin Value на 5%. Если использование памяти коммутатора меньше или равно 60%, сигнал тревоги не генерируется. Если использование памяти превысит 60%, будет выдан сигнал тревоги.

Сигнал тревоги будет снят только в том случае, если использование памяти равно или ниже 55%.

2. Настройте сигнал тревоги порта, как показано далее.

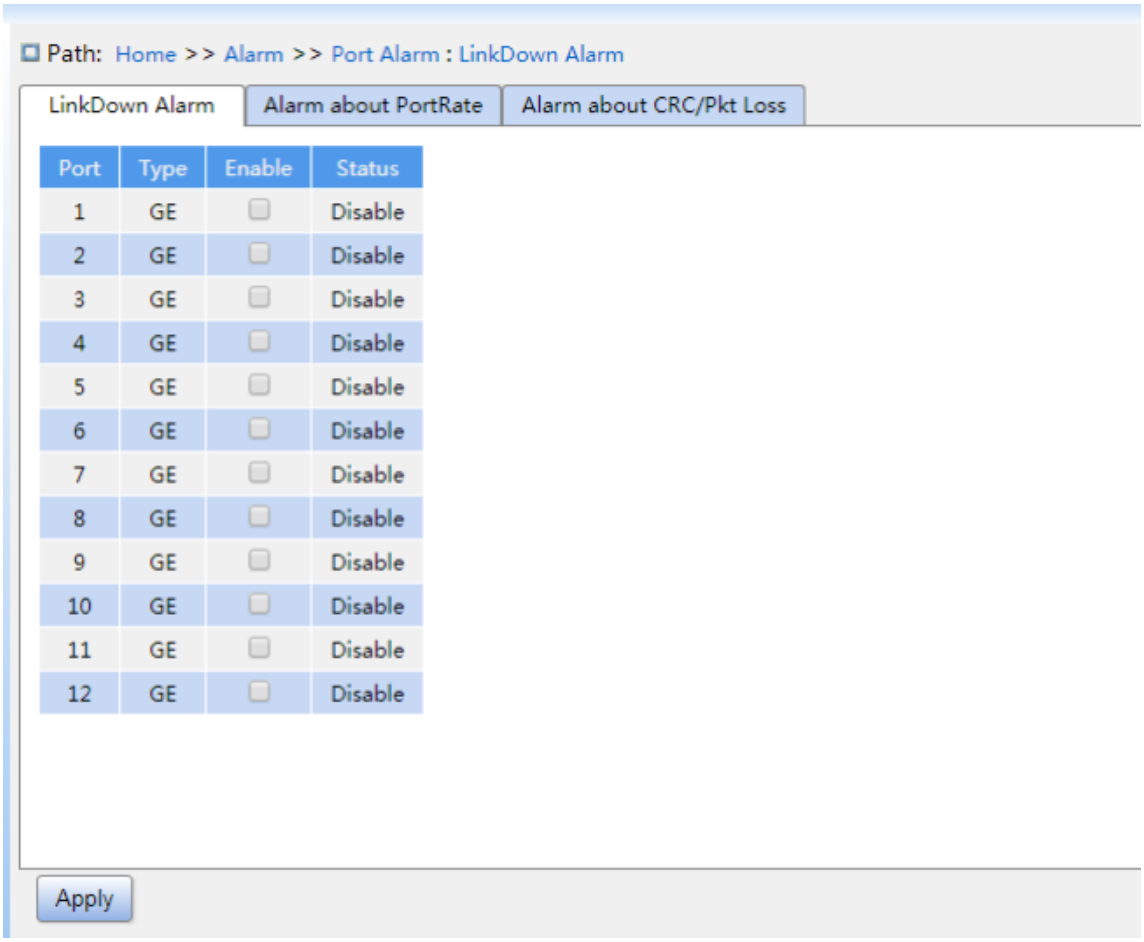


Рис. 74. Сигнал тревоги порта

Port Alarm Configuration

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включение/выключение сигнализации порта.

Status

Варианты отображения: Disable / Link Up/ Link Down

Описание: Link Up означает, что порт находится в состоянии подключения и поддерживает нормальную связь. Link Down означает, что порт отключен или находится в аварийном соединении (сбой связи).

3. Настройте сигнал тревоги о трафике порта, как показано далее.

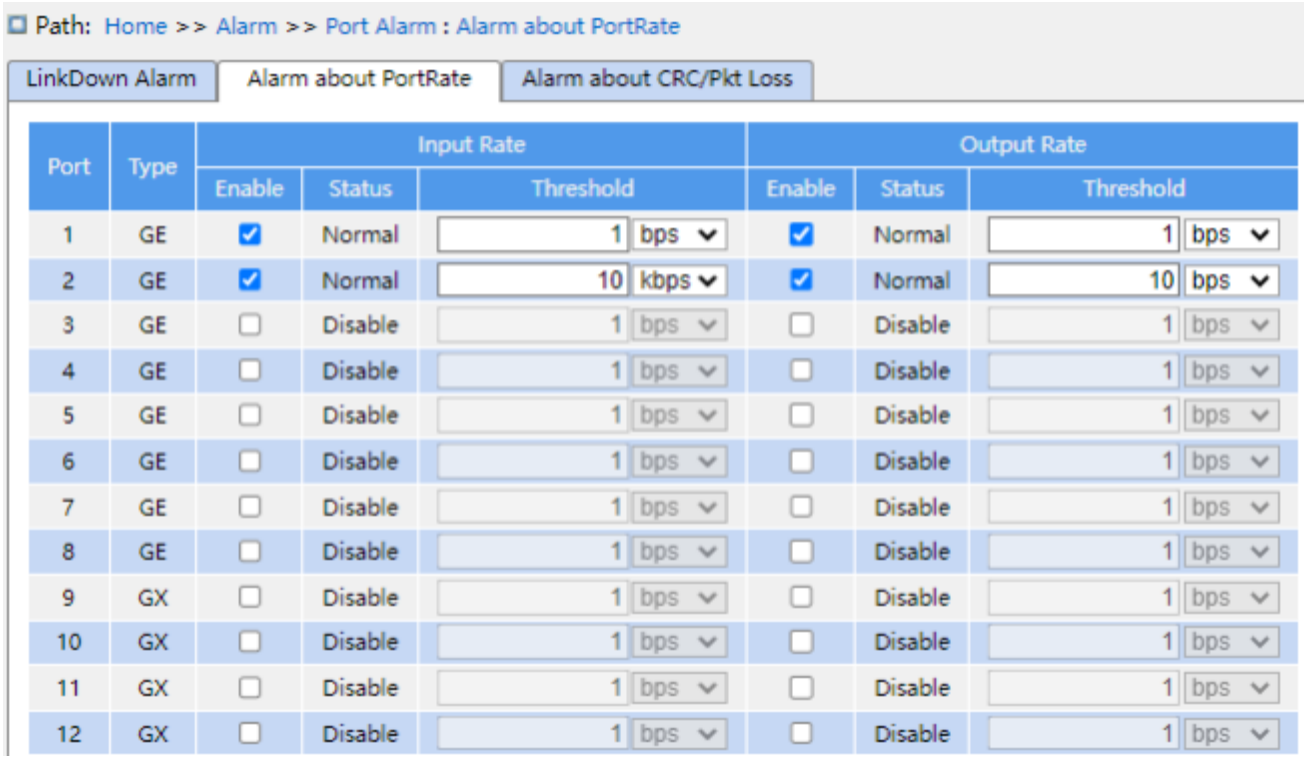


Рис. 75. Настройка сигнала тревоги о трафике порта

Input rate alarm/Output rate alarm

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включение/выключение сигнализации о трафике порта.

Threshold

Диапазон: 1~1000000000bps или 1~1000000kbps

Функция: Настройте порог для трафика порта.

Alarm Status

Варианты отображения: Disable / Alarm/ Normal

Функция: Просмотр состояния трафика порта. Alarm означает, что скорость входящего/исходящего трафика превышает пороговое значение и вызывает Alarm.

4. Настройте сигнал ошибки CRC / потери пакетов, как показано далее.

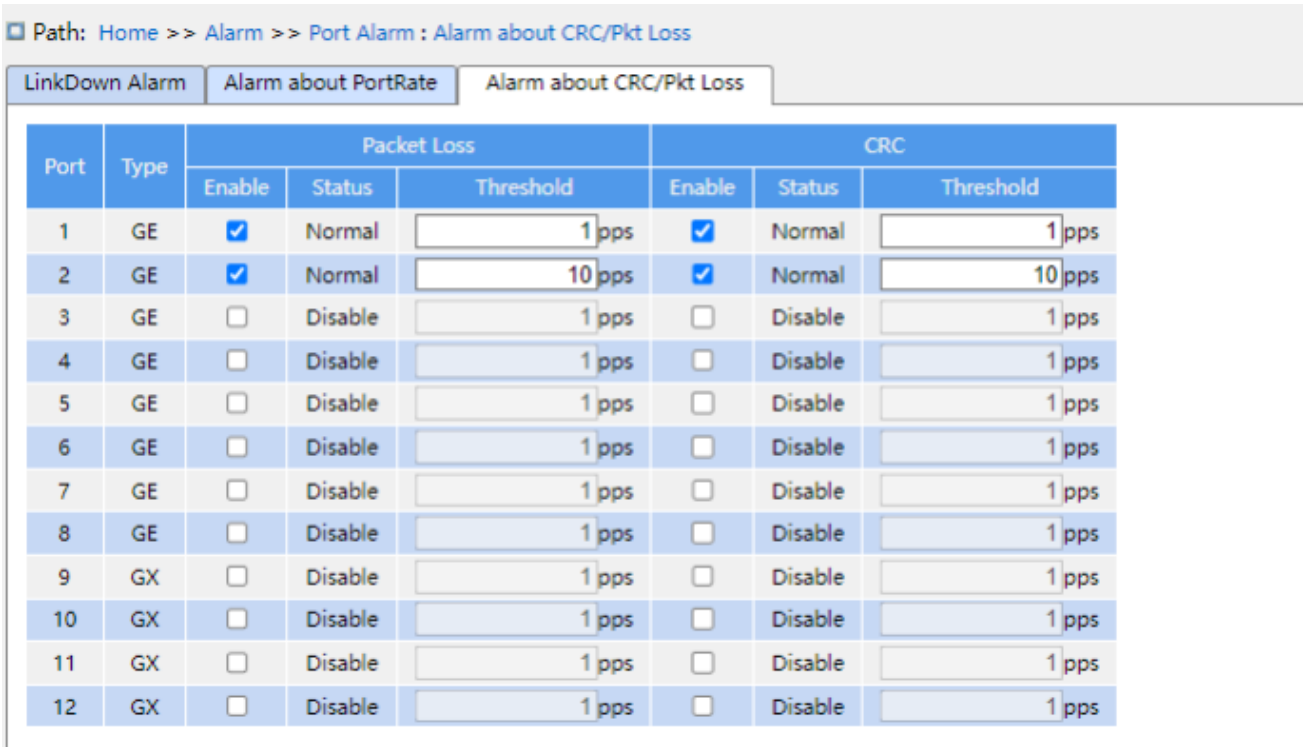


Рис. 76. Настройка сигнала ошибки CRC / потери пакетов

CRC/Pkt Loss Alarm

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включение / выключение сигнала ошибки CRC / потери пакетов.

Threshold

Диапазон: 1~1000000pps

Функция: Задает порог срабатывания для сигнала ошибки CRC / потери пакетов.

Alarm Status

Варианты отображения: Disable / Alarm / Normal

Функция: Просмотр состояния потери CRC/ Pkt порта. Сигнал Alarm означает, что потеря CRC/ Pkt порта превышает пороговое значение и вызывает сигнал Alarm.

5. Настройте сигнал тревоги для кольцевой топологии.

[Home] → [Alarm] → [Alarm about Ring]

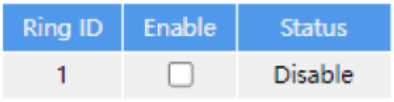


Рис. 77. Сигнал тревоги для кольцевой топологии

Alarm About STRP

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включение/выключение STRP тревоги.

Alarm Status

Варианты отображения: Disable / Alarm/---

Описание: Просмотр статуса STRP. --- означает, что кольцо замкнуто, нет тревоги STRP. Сигнал Alarm означает, что кольцо разомкнуто или находится в ненормальном состоянии, есть тревога STRP.

6. Конфигурация сигнала тревоги оптического модуля SFP.

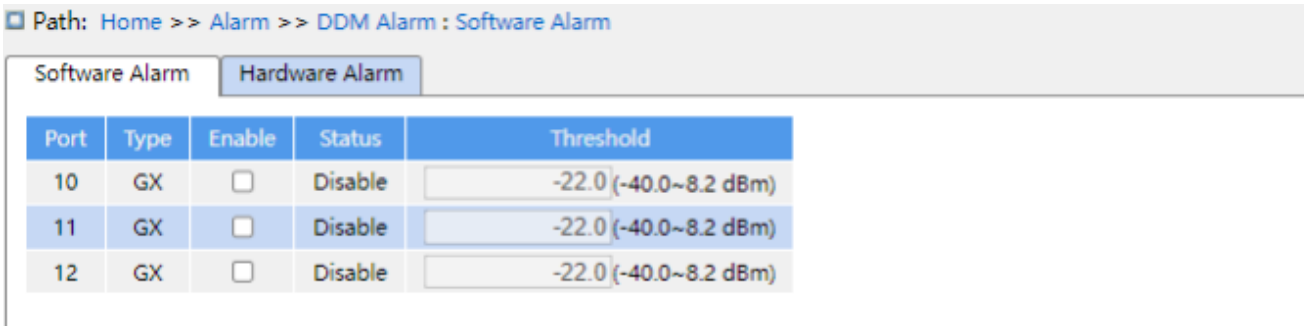


Рис. 78. Конфигурация сигнала тревоги оптического модуля SFP

Alarm

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включить / отключить сигнализацию по входной оптической мощности порта.

Threshold

Диапазон: -40~8,2 dBm

Конфигурация по умолчанию: -22,0 dBm

Функция: Настройка порога тревоги по оптической мощности приема.

Status

Варианты конфигурации: Alarm/Normal

Описание: Когда оптический модуль SFP получает значение оптической мощности ниже порогового значения тревоги, отображается сигнал тревоги (Alarm); когда оптический модуль SFP получает значение оптической мощности не ниже порога тревоги, то сигнал тревоги не активен (Normal).

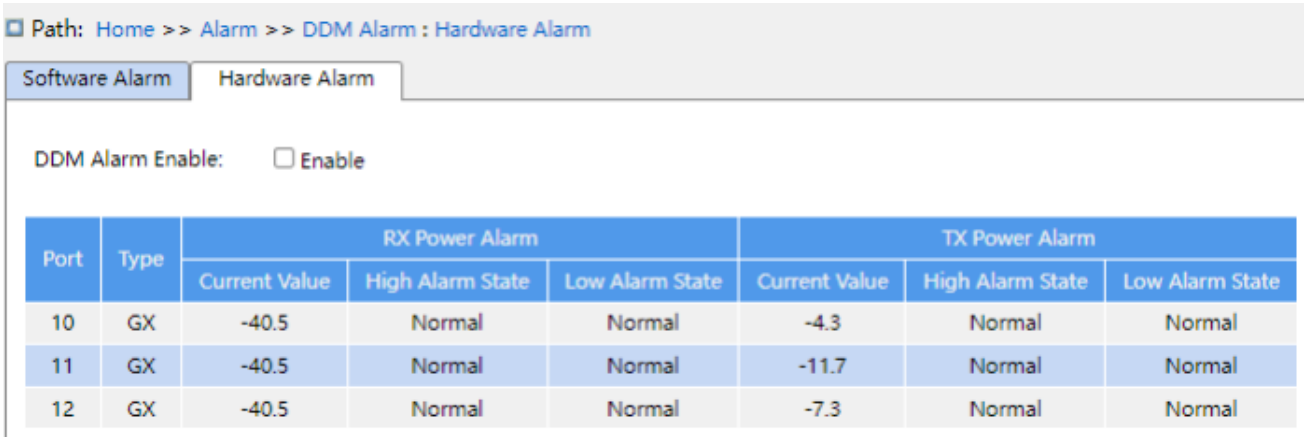
7. Конфигурация аппаратной сигнализации модуля SFP.

Hardware Alarm

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включить / выключить сигнализацию мощности оптического модуля SFP. Когда текущее значение оптической мощности ниже порога нижнего предела, генерируется сигнал тревоги нижнего предела оптической мощности; когда текущее значение оптической мощности превышает верхний предел тревоги, генерируется сигнал тревоги верхнего предела оптической мощности.



Port	Type	RX Power Alarm			TX Power Alarm		
		Current Value	High Alarm State	Low Alarm State	Current Value	High Alarm State	Low Alarm State
10	GX	-40.5	Normal	Normal	-4.3	Normal	Normal
11	GX	-40.5	Normal	Normal	-11.7	Normal	Normal
12	GX	-40.5	Normal	Normal	-7.3	Normal	Normal

Рис. 79. Конфигурация аппаратной сигнализации модуля SFP

Верхний и нижний пороги оптической мощности определяются аппаратно и не могут быть настроены.

7 Функции управления

7.1 Конфигурация портов

1. Настройте состояние порта, скорость порта, управление потоком, другие параметры, как показано далее.

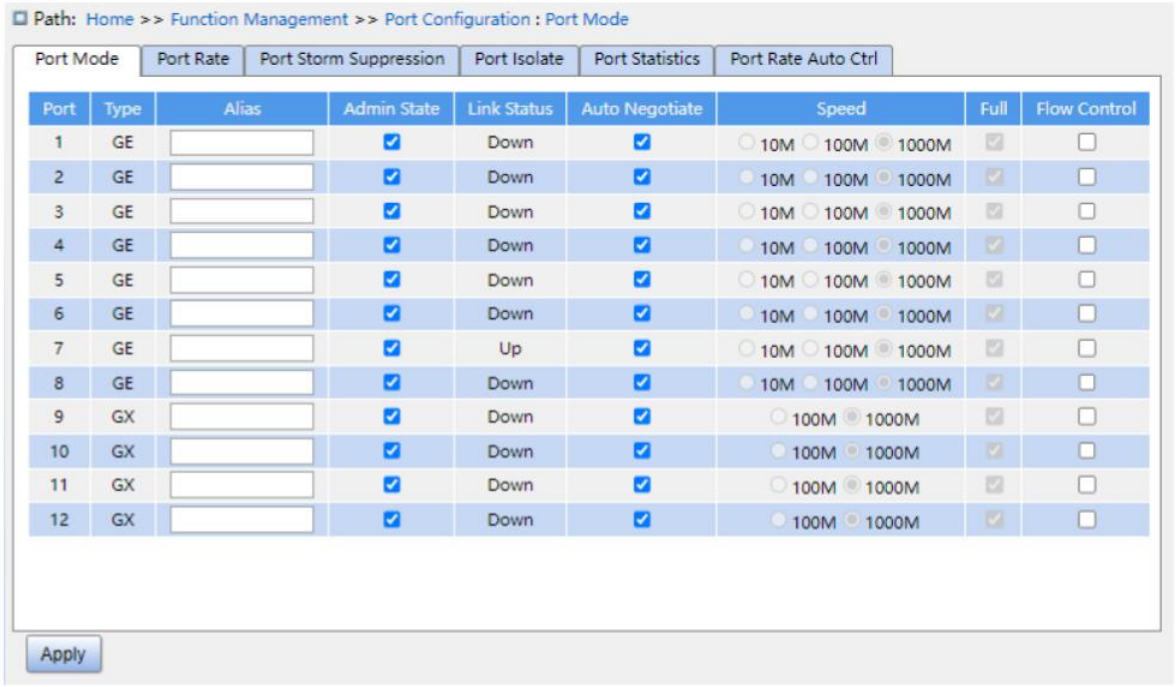


Рис. 80. Конфигурация портов коммутатора

Admin State (Статус управления)

Варианты конфигурации: Enable/ Disable

Конфигурация по умолчанию: Enable

Функция: Разрешена / запрещена передача данных для данного порта.

Описание: Включение / выключения порта для передачи данных. Эта опция напрямую влияет на аппаратное состояние порта и запускает сигнализацию порта.

Link Status (Статус подключения)

Отображает состояние подключения для текущего порта.

Up означает, что порт находится в состоянии LinkUp, соединение установлено.

Down означает, что порт находится в состоянии LinkDown, соединение не установлено.

Auto Negotiate (Автоматическое согласование)

Варианты конфигурации: Enable/ Disable

Конфигурация по умолчанию: Enable

Функция: Настройка скорости порта и дуплексного режима.

Описание: Скорость порта и дуплексный режим могут согласовываться автоматически или принудительно. Скорость порта и дуплексный режим автоматически согласовываются в соответствии с состоянием соединения обоих портов, если настроен режим автоматического согласования. Пользователю рекомендуется настроить скорость и дуплексный режим порта на автоматическое согласование, чтобы избежать проблем с подключением, вызванных несоответствием конфигурации порта. Если пользователь настраивает порт на принудительную скорость/дуплексный режим, убедитесь, что конфигурация скорости соединения/дуплексного режима на обоих концах одинакова.

Гигабитный электрический порт можно настроить на автоматическое согласование, полнодуплексный порт 10M, полудуплексный порт 10M, полный дуплекс 100M, полудуплексный порт 100M, полный дуплексный порт 1000M.

Speed (Скорость порта)

Варианты конфигурации: 10M/100M/1000M

Функция: Настройка скорости автоматического согласования порта.

Описание: При настройке режима порта на автоматическое согласование скорость порта по умолчанию определяется посредством автоматического согласования с противоположным портом. Согласованная скорость может быть любой из диапазона скоростей порта.

Конфигурацию дуплекса и скорости можно настроить только в том случае, если режим автосогласования отключен.

Full (Полный дуплекс)

Варианты конфигурации: Enable / Disable

Функция: Настройка полнодуплексного режима порта в режиме автосогласования.

Описание: Полнодуплексный режим означает, что порт может получать данные во время отправки данных; полудуплексный режим означает, что порт может одновременно только отправлять или получать данные. Если режим порта настроен как автосогласование, дуплексный режим порта определяется автоматическим согласованием с партнером по умолчанию. Согласованный дуплексный режим может быть либо полнодуплексным, либо полудуплексным.

Настраивая возможность дуплекса, порт может согласовывать только определенный дуплексный режим, тем самым управляя согласованием дуплексного режима.

Flow Control (Управление потоком)

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включение / отключение управление потоком.

Описание: Если трафик, полученный портом, превышает максимальное значение, которое может разместить кэш порта, то порт уведомит отправляющую сторону, что необходимо замедлить скорость отправки, чтобы предотвратить потерю пакетов. Для полудуплексного режима и полнодуплексного режима управление потоком реализуется по-разному. В полнодуплексном режиме принимающая сторона уведомляет отправляющую сторону о прекращении отправки сообщений путем отправки специального кадра данных (pause frame). После получения кадра паузы передающая сторона прекратит отправку сообщений в соответствии со временем ожидания в кадре. Полудуплексный режим поддерживает управление потоком противодавления. Принимающая сторона может намеренно создать конфликт или сигнал несущей. После того, как передающая сторона обнаруживает конфликт или сигнал несущей, то задерживает отправку данных.

2. Настройте пропускную способность порта, как показано далее.

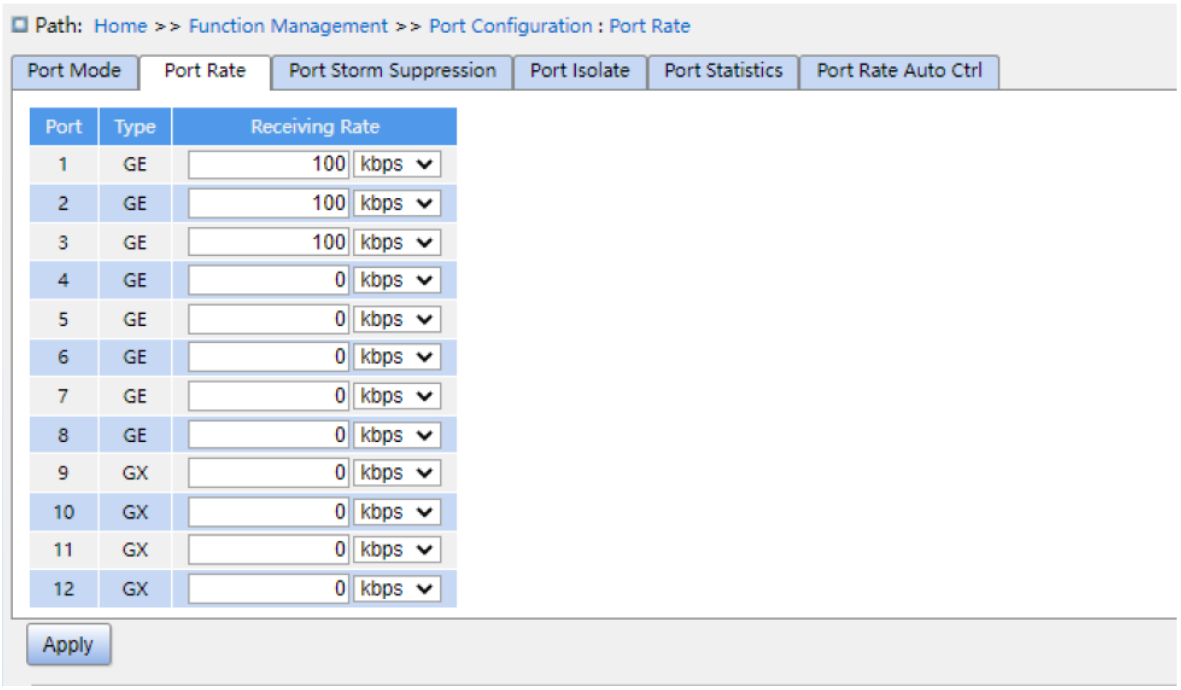


Рис. 81. Настройка скорости порта

Receiving Rate

Диапазон: 0 / 10~13128147kbps / 10~13128147fps /1~13128kfps / 1~13128mbps

Конфигурация по умолчанию: 0 (значение 0 означает отключение ограничения)

Функция: Настройка порога для ограничения скорости порта . Сообщения, превышающие пороговое значение, будут отброшены.

3. Конфигурация подавления шторма в порте (Port Storm Suppression) показана далее.

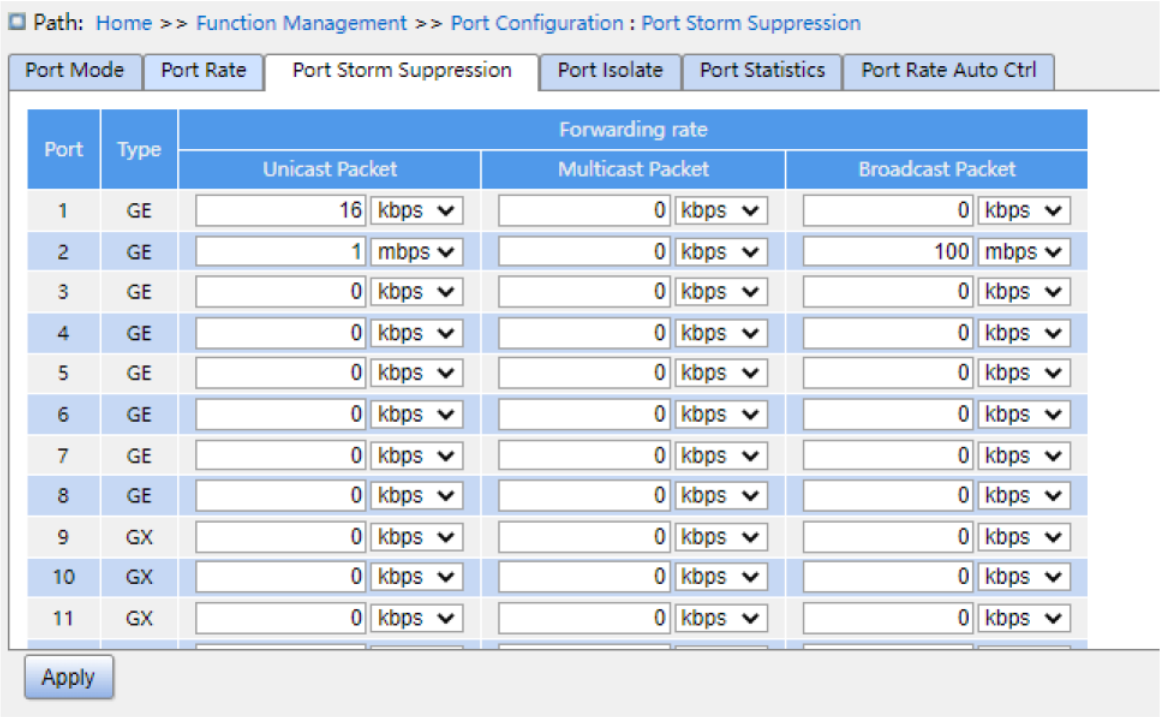


Рис. 82. Настройка Port Storm Suppression

Forwarding Rate

Варианты конфигурации: Unicast Packet/Multicast Packet/Broadcast Packet

Диапазон: 0 / 10~13128147kbps / 10~13128147fps / 1~13128kfps / 1~13128mbps

Конфигурация по умолчанию: 0 (отключить подавление шторма)

Функция: настройте пороговое значение скорости пересылки пакетов. Тип пакетных данных, превышающий пороговое значение, будет отброшен.

4. Конфигурация изоляции порта, как показано далее.

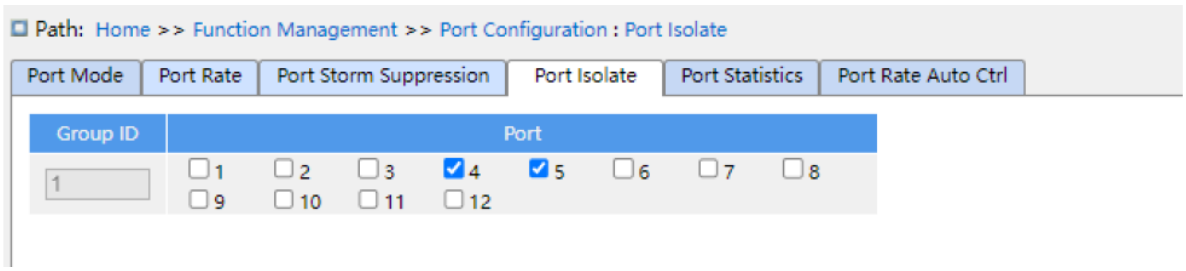


Рис. 83. Настройка изоляции порта

Enable Port Isolate

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включите / отключите изоляцию порта.

Примечание: существует только одна группа изоляции портов.

5. Статистика портов.

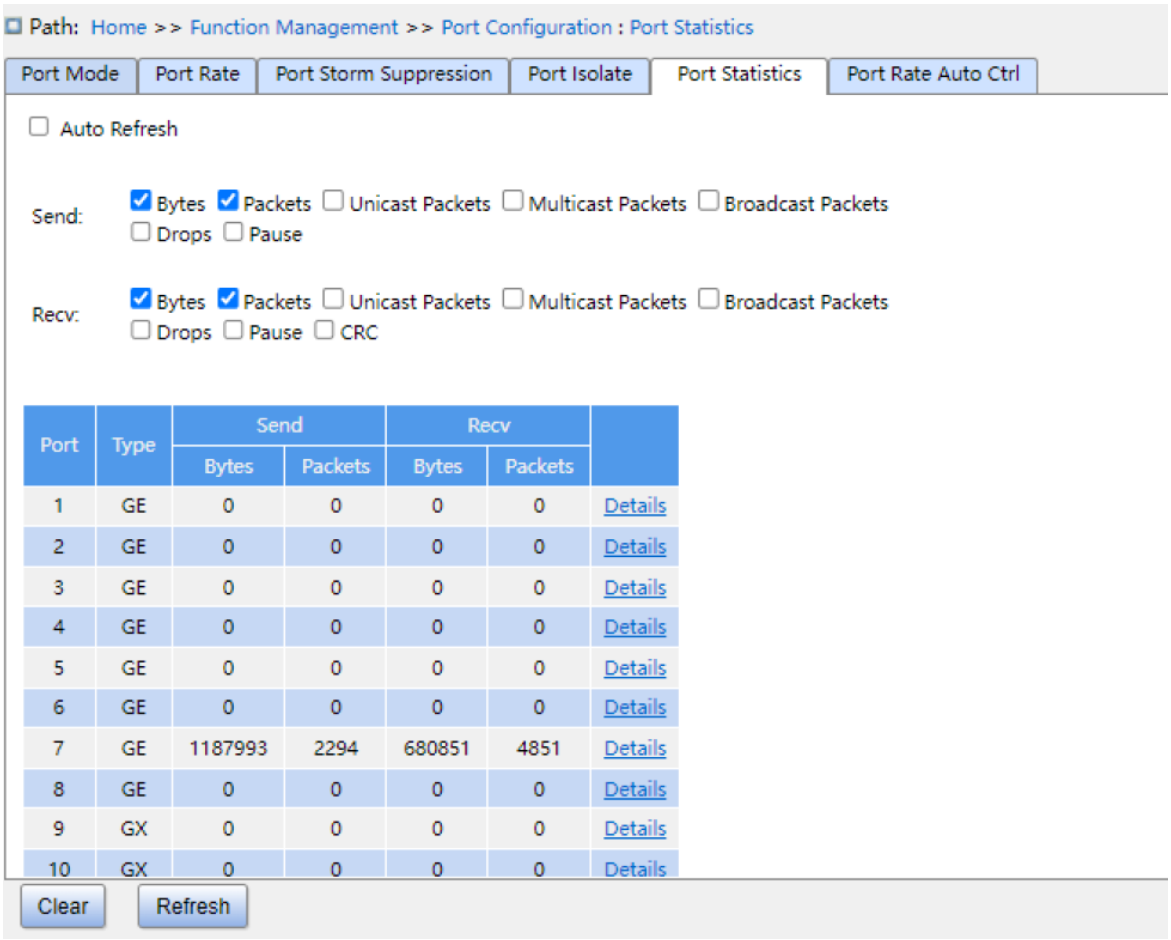


Рис. 84. Статистика портов коммутатора

Bytes

Количество полученных/отправленных байт.

Packets

Количество полученных/отправленных пакетов.

Unicast Packets

Количество полученных/отправленных одноадресных пакетов.

Multicast Packets

Количество полученных/отправленных многоадресных пакетов.

Broadcast Packets

Количество полученных/отправленных широковещательных пакетов.

Drops

Количество сообщений, отброшенных из-за конфликтов при получении/отправке.

Pause

Количество принятых/отправленных Pause кадров.

CRC

Количество полученных/отправленных CRC-сообщений.

Нажмите на ссылку Details на номере порта, чтобы войти в интерфейс статистики подробной информации о порте.

6. Статистика подробной информации о порте.

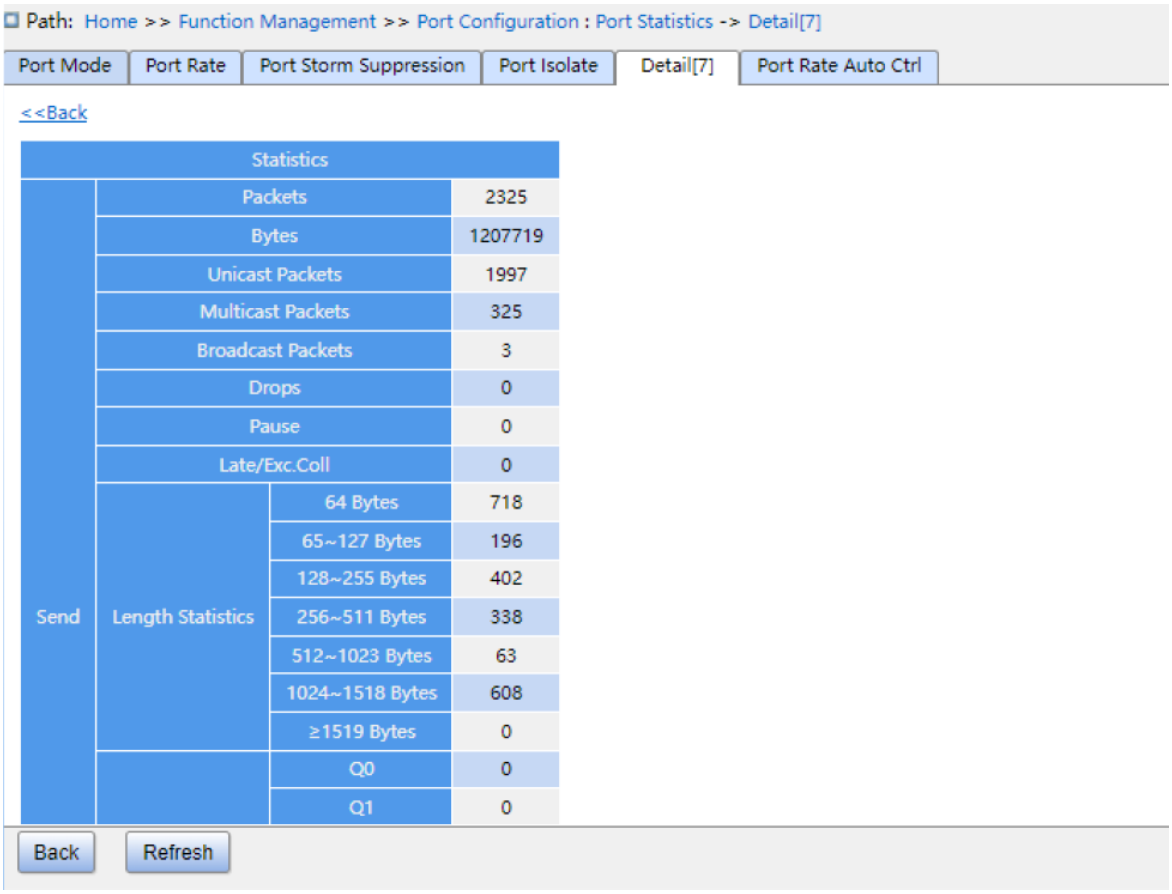


Рис. 85. Статистика подробной информации о порте

7. Включение автоматического ограничения скорости порта, как показано далее.

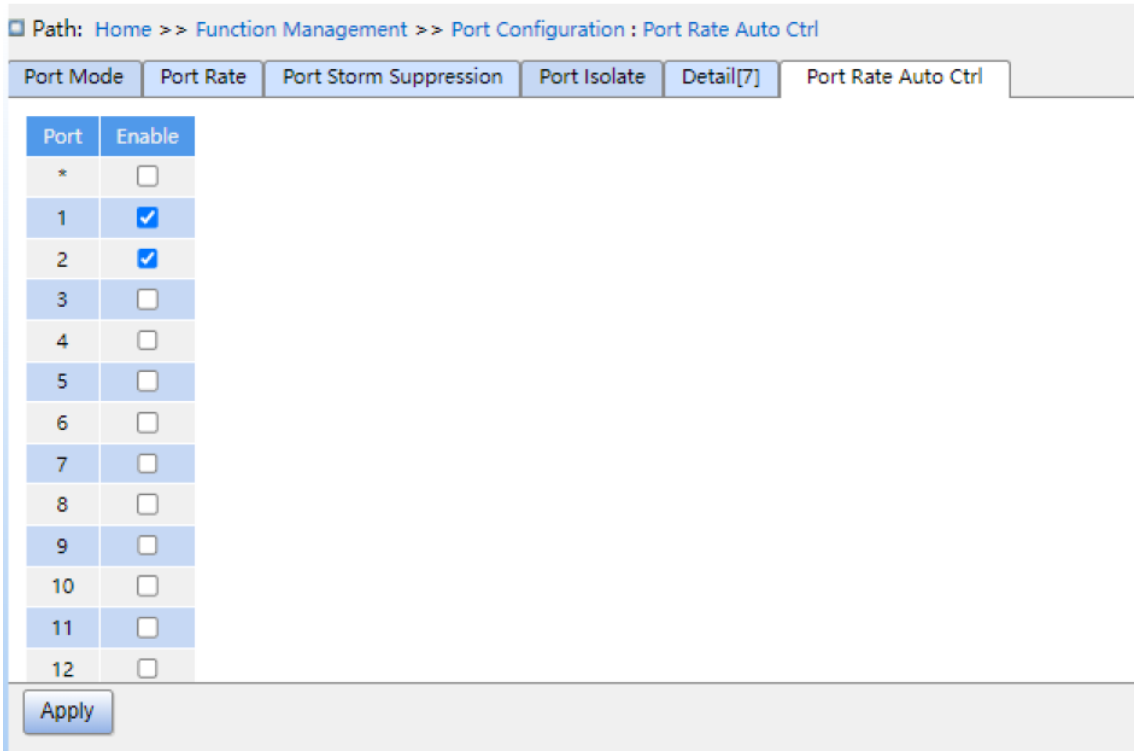


Рис. 86. Автоматическое ограничения скорости порта

Port

Варианты конфигурации: все порты коммутатора.

Enable

Варианты конфигурации: enable/disable

Функция: Включает или отключает функцию автоматического ограничения скорости порта.

7.2 VLAN

7.2.1 Конфигурация VLAN

7.2.1.1 Введение

Одна локальная сеть LAN может быть разделена на несколько логических виртуальных локальных сетей Virtual Local Area Networks (VLAN). Устройство может взаимодействовать только с устройствами в одной и той же VLAN. В результате

широковещательные пакеты ограничиваются VLAN, что оптимизирует безопасность локальной сети.

Раздел VLAN не ограничен физическим местоположением. Каждая VLAN рассматривается как логическая сеть. Если хосту в одной VLAN необходимо отправить пакеты данных хосту в другой VLAN, должен быть задействован маршрутизатор или устройство уровня 3 (L3).

7.2.1.2 Принцип работы

Чтобы сетевые устройства могли различать пакеты из разных VLAN, к пакетам необходимо добавить поля для идентификации VLAN. В настоящее время наиболее часто используемым протоколом для идентификации VLAN является IEEE802.1Q. В таблице 2 показана структура кадра 802.1Q.

Таблица 2. Структура кадра 802.1Q

DA	SA	802.1Q header				Length/type	Data	FCS
		TPID	PRI	CFI	VID			

К традиционному кадру данных Ethernet добавляется 4-байтовый заголовок 802.1Q в качестве тега VLAN.

TPID: 16 бит. Используется для идентификации кадра данных, содержащего тег VLAN. Значение равно 0x8100. Значение TPID, указанное в протоколе 802.1Q, равно 0x8100.

PRI: три бита, идентифицирующие приоритет пакета 802.1p.

CFI: 1 бит, указывает, инкапсулирован ли MAC-адрес в стандартном формате в различных средах передачи. Значение 0 указывает, что MAC-адрес инкапсулирован в стандартный формат, а значение 1 указывает, что MAC-адрес инкапсулирован в нестандартный формат.

VID: 12 бит, обозначающий номер VLAN. Значение находится в диапазоне от 1 до 4093. 0, 4094 и 4095 - зарезервированные значения.

- VLAN 1 является VLAN по умолчанию, VLAN 1 нельзя создать и удалить вручную.
- Зарезервированные сети VLAN зарезервированы для реализации определенных функций системы и не могут быть созданы и удалены вручную.

Пакет, содержащий заголовок 802.1Q, является маркированным пакетом (Tag); пакет без заголовка 802.1Q представляет собой нетегированный пакет (Untag). Все пакеты в коммутаторе содержат тег 802.1Q.

7.2.1.3 Port-based VLAN

VLAN может быть основан на портах (port-based) или MAC-адресах. Коммутаторы этой серии поддерживают разделение VLAN на основе портов (port-based). Члены VLAN могут быть определены на основе портов коммутатора. После добавления порта в указанную VLAN порт может пересылать пакеты с тегом для этой VLAN.

1. Режим порта (Port Mode)

Порты делятся на два типа в зависимости от того, как они обрабатывают теги VLAN при пересылке пакетов.

Access: В режиме доступа порт можно добавить только к одной VLAN. По умолчанию все порты коммутатора являются портами доступа и принадлежат VLAN1. Пакеты, пересылаемые портом доступа, не имеют тегов VLAN. Порты доступа обычно используются для подключения к терминалам, не поддерживающим 802.1Q.

Trunk: В транковом режиме порт можно добавить ко многим VLAN. При отправке пакетов PVID на транковом порте можно указать, будет ли передаваться тег. Он несет этот тег при отправке других пакетов. Транковые порты обычно используются для подключения сетевых передающих устройств.

Hybrid: в гибридном режиме порт можно добавить во многие VLAN. Вы можете установить тип пакетов, которые будут приниматься гибридным портом, а также указать, будет ли передаваться тег, когда гибридный порт отправляет пакеты. Гибридный порт можно использовать для подключения сетевых устройств и пользовательских устройств.

Разница между гибридным портом и транковым портом заключается в следующем: гибридный порт не несет тег при отправке пакетов из нескольких VLAN, а транковый порт не несет тег только при отправке пакетов PVID.

2. PVID

Каждый порт имеет PVID. При получении нетегированного пакета порт добавляет к пакету тег в соответствии с PVID. PVID по умолчанию для всех портов равен 1.

- PVID порта следует выбирать из идентификаторов VLAN, которым разрешено проходить через порт, иначе порт не сможет пересылать пакеты;
- При добавлении тега PVID в пакет Untag значения PRI и CFI порта по умолчанию показаны в конфигурации параметров PCP и DEI (гл. 7.17.3)

В таблице 3 показано, как коммутатор обрабатывает полученные и пересылаемые пакеты в зависимости от режима порта и PVID.

Таблица 3. Различные режимы обработки пакетов

<table>
<tr><th colspan="2">Обработка полученных пакетов</th><th colspan="2">Обработка пакетов для пересылки</th></tr>
<tr><th>Untagged пакеты</th><th>Tagged пакеты</th><th>Режим порта</th><th>Обработка пакетов</th></tr>
<tr><td rowspan="3">Добавить теги PVID в пакеты:
➢ Если PVID находится в списке разрешенных VLAN, то принять пакет.
➢ Если PVID отсутствует в списке разрешенных VLAN, то отбросить пакет.</td><td rowspan="3">➢ Если идентификатор VLAN в пакете находится в списке разрешенных VLAN, то принять пакет.
➢ Если идентификатор VLAN в пакете отсутствует в списке разрешенных VLAN, то отбросить пакет.</td><td>Access</td><td>Переслать пакет после удаления тега.</td></tr>
<tr><td>Trunk</td><td>Пересылаем пакет согласно конфигурации «Egress Tagging»:
➢ Untag Port VLAN: Если идентификатор VLAN в пакете совпадает с PVID и в списке разрешенных VLAN, пересылать пакет после удаления тега. Если идентификатор VLAN в пакете отличается от PVID и в списке разрешенных VLAN, сохранить тег и переправить пакет.
➢ Tag All: если идентификатор VLAN в пакете находится в списке разрешенных VLAN, сохранить тег и переправить пакет.</td></tr>
<tr><td>Hybrid</td><td>Пересылаем пакет согласно конфигурации «Egress Tagging»:
➢ Untag Port VLAN: то же, что и выше.
➢ Tag All: то же, что и выше.
➢ Untag All: если идентификатор VLAN в пакете находится в списке разрешенных VLAN, переслать пакет после удаления тега.</td></tr>
</table>

7.2.1.4 Web конфигурация VLAN

1. Настройка режима соединения портов (Link Mode).

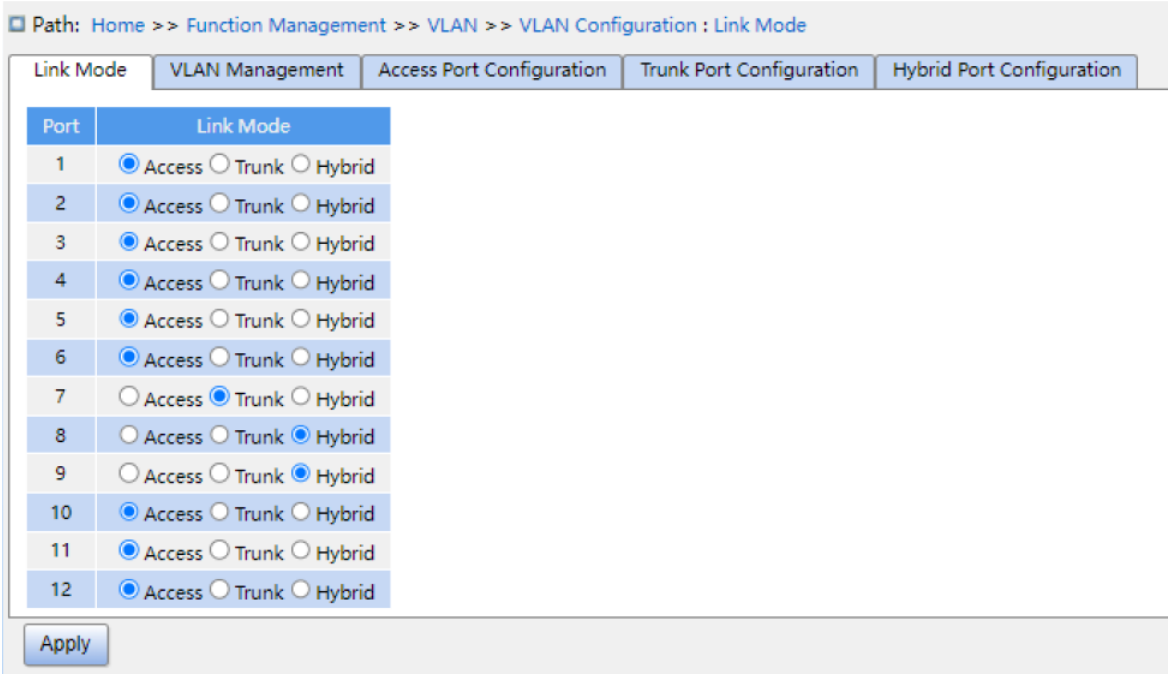


Рис. 87. Настройка Link Mode

Link Mode

Варианты конфигурации: Access, Trunk, Hybrid

Конфигурация по умолчанию: Access

Функция: Выберите режим соединения портов.

2. Управление списком VLAN.

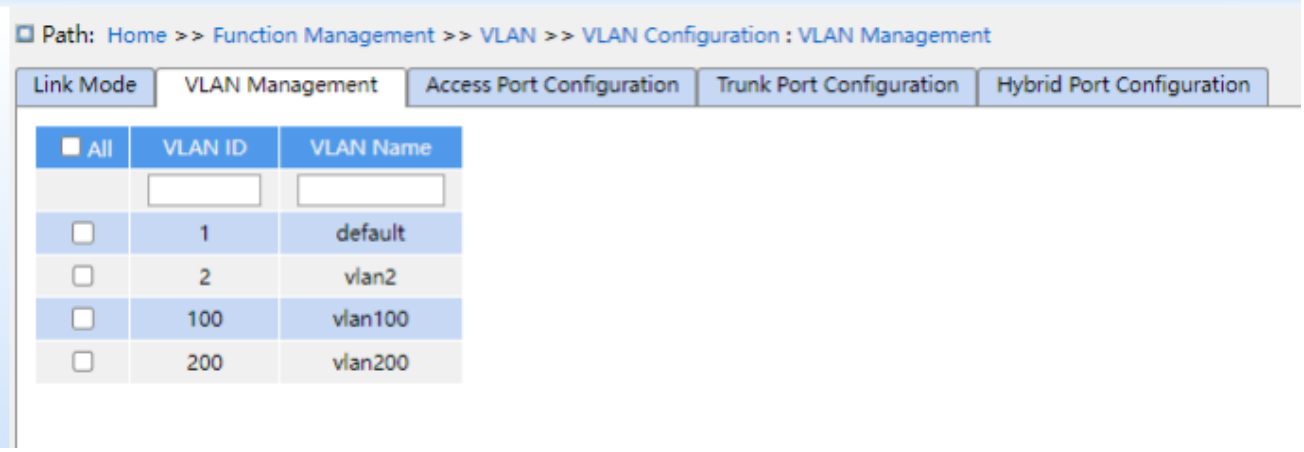


Рис. 88. Настройка VLAN Management

VLAN ID

Диапазон: 1~4093

Конфигурация по умолчанию: 1

Функция: Создание VLAN.

VLAN Name

Диапазон: 1~32 символа, включая заглавные буквы, строчные буквы, цифры и подчеркивания.

Функция: настройка имени VLAN.

3. Настройка Access портов.

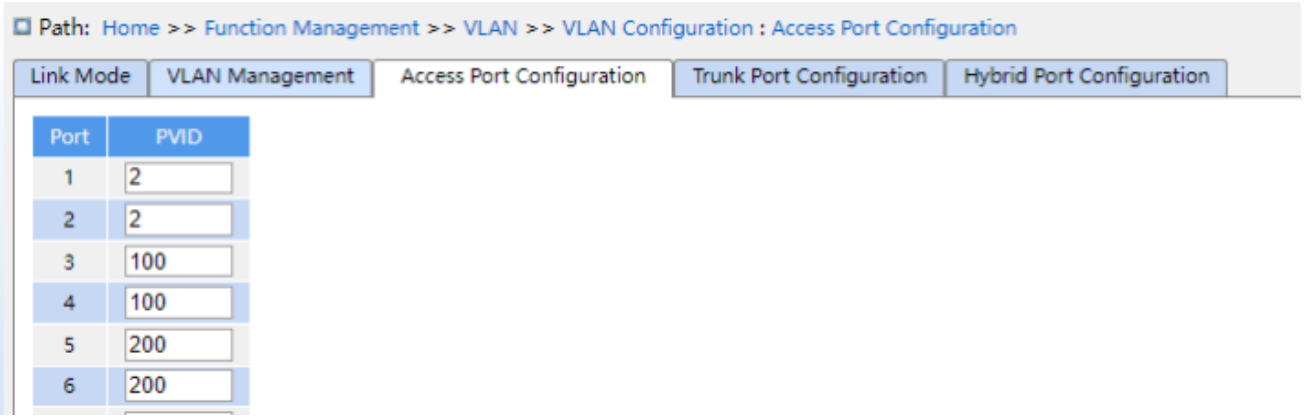


Рис. 89. Настройка Access портов.

PVID

Диапазон: 1~4093

Конфигурация по умолчанию: 1

Функция: Настройка VLAN по умолчанию для Access порта.

VLAN необходимо создать перед настройкой Access порта, Trunk порта, Hybrid порта так далее.

4. Настройка Trunk портов.

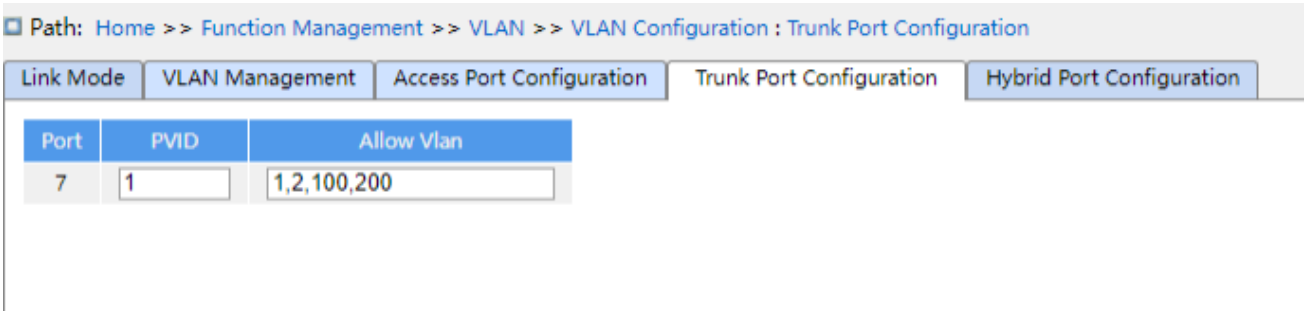


Рис. 90. Настройка Trunk портов.

PVID

Диапазон: 1~4093

Конфигурация по умолчанию: 1

Функция: Настройка VLAN по умолчанию для Trunk порта.

Allowed VLAN

Диапазон: 1~4093, разделенные запятой «,» и дефисом «-» (M-N, M должно быть меньше N). Например: 2, 33, 34-77

Конфигурация по умолчанию: 1

Функция: Настройка разрешенных VLAN для Trunk порта.

5. Настройка Hybrid портов.

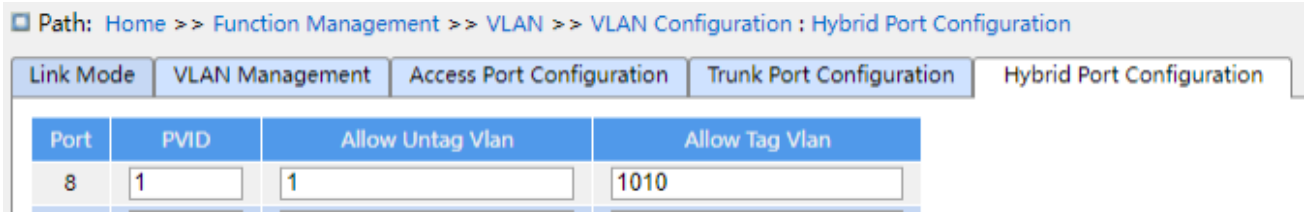


Рис. 91. Настройка Hybrid портов.

PVID

Диапазон: 1~4093

Конфигурация по умолчанию: 1

Функция: Настройка VLAN по умолчанию для Hybrid порта.

Allowed Untag VLAN

Диапазон: 1~4093, разделенные запятой «,» и дефисом «-» (M-N, M должно быть меньше N). Например: 2, 33, 34-77

Конфигурация по умолчанию: 1

Функция: Настройка разрешенных Untag VLAN для Hybrid порта.

Allowed Tag VLAN

Диапазон: 1~4093, разделенные запятой «,» и дефисом «-» (M-N, M должно быть меньше N). Например: 2, 33, 34-77

Конфигурация по умолчанию: None

Функция: Настройка разрешенных Tag VLAN для Hybrid порта.

7.2.1.5 Пример конфигурации VLAN

Как показано на рис. 92, вся локальная сеть разделена на 3 VLAN: VLAN2, VLAN100 и VLAN200. Требуется, чтобы устройства в одной VLAN могли взаимодействовать друг с другом, но разные VLAN были изолированы. Терминальные компьютеры не могут различать помеченные пакеты, поэтому порты, соединяющие коммутатор A и коммутатор B с ПК, настроены на Access порт. Пакеты VLAN2, VLAN100 и VLAN200 должны передаваться между коммутатором A и коммутатором B, поэтому порты, соединяющие коммутатор A и коммутатор B, должны быть установлены как trunk порты, позволяющие проходить пакетам VLAN 2, VLAN 100 и VLAN 200. В Таблице 4 показана конфигурация VLAN для коммутаторов A и B.

Таблица 4. Конфигурация VLAN

VLAN	**Конфигурация**
VLAN2	Настройте порт 1 и порт 2 коммутатора A и B как Access порты, а порт 7 как Trunk порт.
VLAN100	Настройте порт 3 и порт 4 коммутатора A и B как Access порты, а порт 7 как Trunk порт.
VLAN200	Настройте порт 5 и порт 6 коммутатора A и B как Access порты, а порт 7 как Trunk порт.

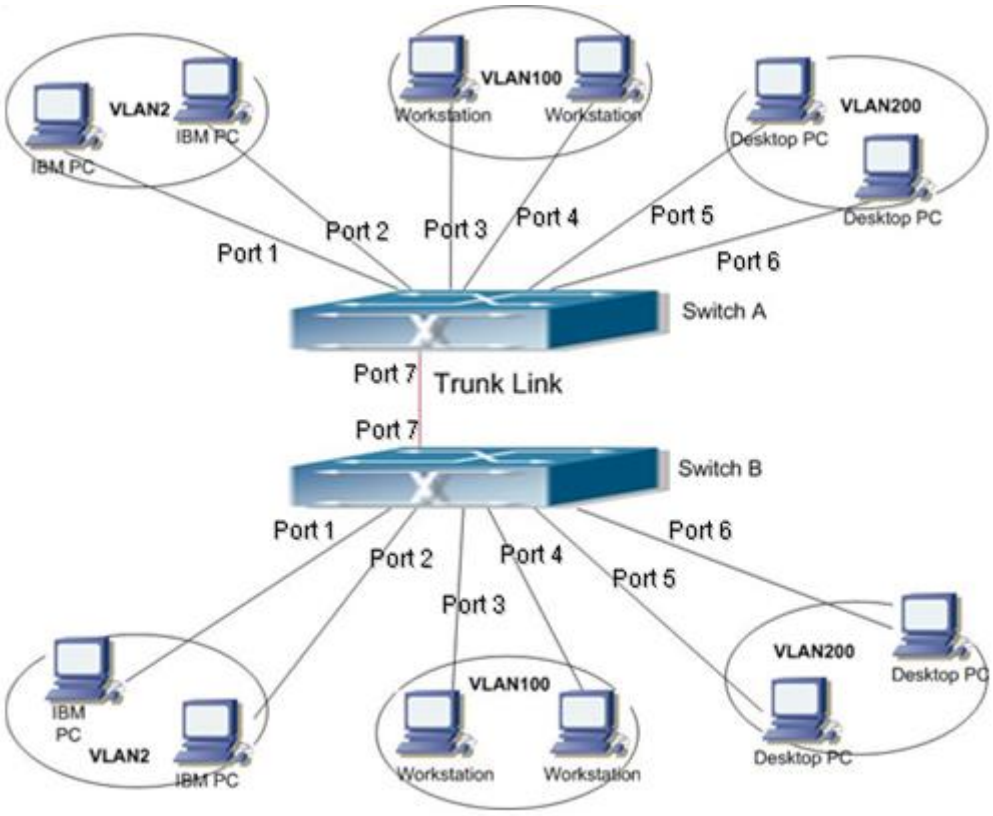


Рис. 92. Пример применения VLAN

Конфигурация коммутатора A и коммутатора B:

1. Настройте разрешенные доступы VLAN на 1,2,100,200, как показано на рис. 88.

2. Настройте порты 1, 2 как Access порты, задайте VLAN как 2. Настройте порты 3, 4 как Access порты, задайте VLAN как 100. Настройте порты 5 , 6 как Access порты, задайте VLAN как 200. Настройте порт 7 как Trunk порт, задайте VLAN как 1, разрешенные VLAN — 1,2,100,200, как показано на рис. 89, 90.

3. Оставьте все остальные параметры по умолчанию.

7.2.2 GVRP

7.2.2.1 Принцип работы GARP

Generic Attribute Registration Protocol (GARP) используется для распространения, регистрации и отмены атрибутов (VLAN, адреса многоадресной рассылки) между коммутаторами в одной сети.

При использовании GARP информация о конфигурации GARP будет распространяться на всю сеть. Участник (подписчик) GARP инструктирует других участников GARP зарегистрировать или отменить свою собственную конфигурационную информацию посредством сообщения о присоединении/выходе (join/leave) соответственно. Участник также регистрирует или отменяет информацию о конфигурации других участников на основе сообщений о присоединении/выходе.

GARP включает три типа сообщений: Join, Leave и LeaveAll.

Когда устройство GARP хочет зарегистрировать свою собственную информацию на других коммутаторах, устройство отправляет сообщение о присоединении. Сообщения о присоединении делятся на два типа: JoinEmpty и JoinIn. Сообщение JoinIn отправляется для объявления зарегистрированного атрибута, а сообщение JoinEmpty отправляется для объявления атрибута, который еще не зарегистрирован.

Когда устройство GARP хочет отменить свою собственную информацию на других коммутаторах, устройство отправляет сообщение Leave.

После запуска приложения GARP на коммутаторе оно запускает таймер LeaveAll. По истечении времени таймера приложение отправляет сообщение LeaveAll.

Объект приложения указывает порт с поддержкой GARP (GARP-enabled port).

Таймеры GARP включают Hold timer, Join timer, Leave timer, LeaveAll timer.

Hold Timer: когда коммутатор с поддержкой GARP получает сообщение о регистрации, он запускает таймер удержания (Hold Timer), а не немедленно отправляет сообщение о присоединении. Когда таймер удержания истечет, он поместит всю

регистрационную информацию, полученную за это время, в одно сообщение о присоединении и отправит его, уменьшив тем самым количество отправляемых сообщений.

Join Timer: чтобы гарантировать, что сообщение о присоединении может быть надежно передано другим коммутаторам, коммутатор с поддержкой GARP будет ожидать временной интервал таймера присоединения (Join Timer) после отправки первого сообщения о присоединении. Если коммутатор не получит сообщение о присоединении в течение этого времени, он снова отправит сообщение о присоединении, в противном случае он не отправит второе сообщение.

Leave Timer: когда коммутатору с поддержкой GARP необходимо, чтобы другие коммутаторы аннулировали информацию его атрибута, он отправляет сообщение Leave. Другие коммутаторы с поддержкой GARP, получившие это сообщение, активируют (Leave Timer). Если коммутаторы не получат сообщение о присоединении (Join message) до истечения времени таймера, они аннулируют эту информацию атрибута.

LeaveAll Timer: когда коммутатор включает GARP, он одновременно запускает таймер LeaveAll. По истечении времени таймера коммутатор отправит сообщение LeaveAll другим коммутаторам с поддержкой GARP и позволит им повторно зарегистрировать всю информацию об их атрибутах, а затем перезапустит таймер LeaveAll, чтобы начать новый цикл.

7.2.3 Принцип работы GVRP

GVRP (GARP VLAN Registration Protocol) — это приложение GARP, основанное на механизме GARP для поддержания информации о регистрации VLAN на устройстве и распространения этой информации на другие устройства.

Устройство с поддержкой GVRP может получать информацию о регистрации VLAN от других устройств и динамически обновлять информацию о регистрации VLAN на устройстве, обеспечивая согласованность информации VLAN на всех устройствах в

одной и той же локальной сети. Информация о регистрации VLAN, распространяемая GVRP, содержит не только информацию о локальной статической регистрации, настроенную вручную, но также информацию о динамической регистрации от других устройств.

Порты GVRP и порты агрегации являются взаимоисключающими, то есть порт с включенной функцией GVRP не следует добавлять в группу агрегации; порт, добавленный в группу агрегации, не должен иметь включенную функцию GVRP.

7.2.3.1 Web конфигурация GVRP

1. Включите протокол GVRP на коммутаторе и настройте таймеры.

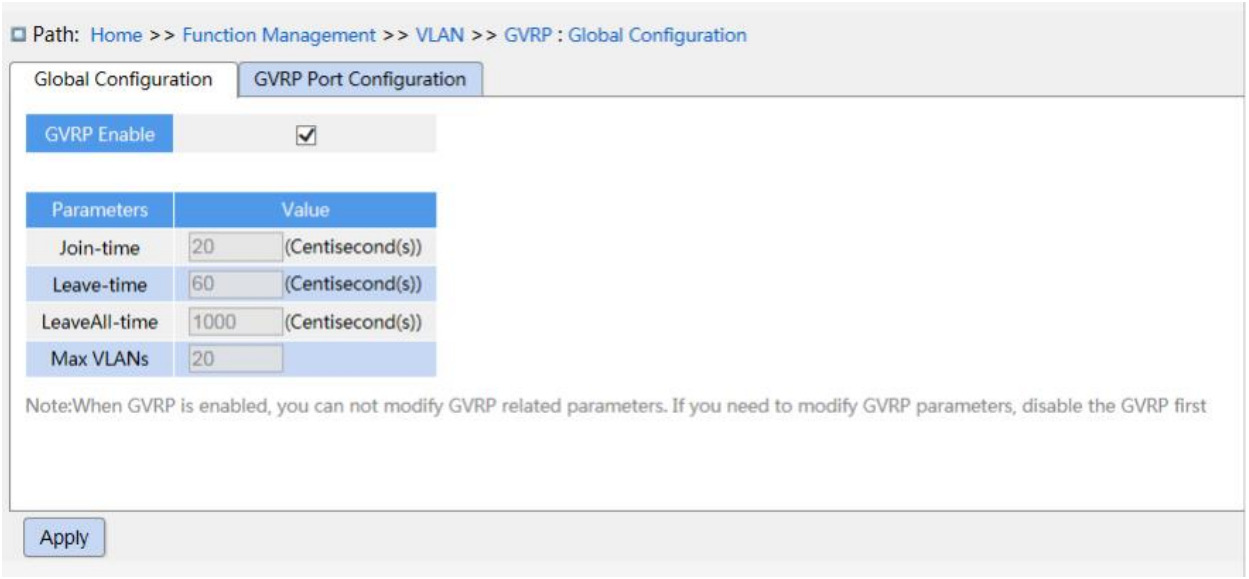


Рис. 93. Глобальная конфигурация GVRP

GVRP enable

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включение / отключение GVRP протокола.

Join timer

Диапазон: 1~20 (centisecond)

Конфигурация по умолчанию: 20 (centisecond)

Функция: Настройка значения для таймера Join timer.

Centisecond (сантисекунда) = 0,01 сек.

Leave timer

Диапазон: 60~300 (centisecond)

Конфигурация по умолчанию: 60 (centisecond)

Функция: Настройка значения для таймера Leave timer.

LeaveAll timer

Диапазон: 1000~5000 (centisecond)

Конфигурация по умолчанию: 1000 (centisecond)

Функция: Настройка значения для таймера LeaveAll timer.

Описание: если время таймера LeaveAll для разных устройств истекает одновременно, одновременно отправляется несколько сообщений LeaveAll, что увеличивает нагрузку на сеть. Чтобы избежать одновременного истечения таймера LeaveAll на разных устройствах, значение фактического LeaveAll таймера - это случайное значение, которое больше значения LeaveAll таймера в 1,5 раза.

Max VLANs

Диапазон: 1~4093

Конфигурация по умолчанию: 20

Функция: Настройте максимальное количество виртуальных сетей VLAN, динамически регистрируемых портом GVRP.

При настройке таймеров GVRP и максимальных параметров VLAN вам необходимо сначала отключить функцию GVRP.

2. Конфигурация GVRP для портов коммутатора.

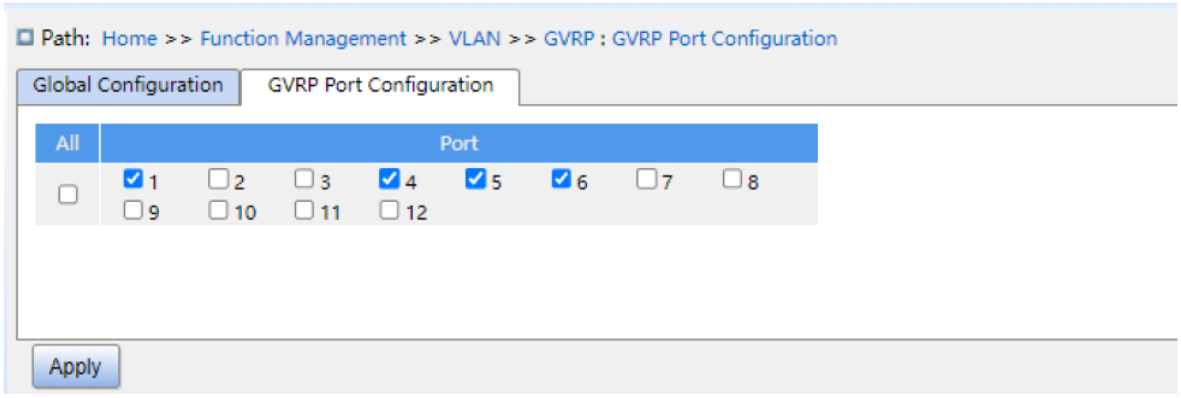


Рис. 94. Конфигурация GVRP для портов

Port

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включение / отключение GVRP для выбранного порта.

- Порт GVRP должен быть настроен как Trunk порт;
- Порт GVRP заполняет атрибуты VLAN других портов GVRP в состоянии Up (подключено).

7.2.3.2 Пример конфигурации GVRP

Как показано на рисунке далее, GVRP необходимо включить на устройствах, чтобы информация VLAN динамически регистрировалась и обновлялась между устройством A и устройством B.

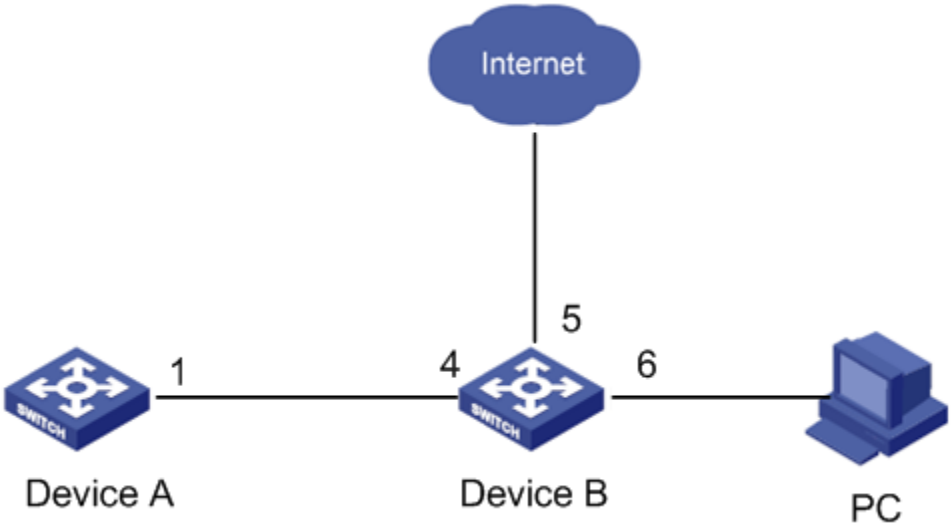


Рис. 95. Пример конфигурации GVRP

Конфигурация устройства A:

1. Настройте порт 1 как trunk порт, разрешите VLAN 1.

2. Включите глобальный GVRP, как показано на рис. 93.

3. Включите GVRP на порте 1, как показано на рис. 94.

Конфигурация устройства B:

1. Настройте порт 4 как trunk порт, разрешите VLAN 1; настройте порт 5 как access port, разрешите VLAN 5; настройте порт 6 как trunk порт, разрешите VLAN 1, 6.

2. Включите глобальный GVRP, как показано на рис. 93.

3. Включите GVRP на портах 4, 5, 6, как показано на рис. 94. Порт 1 коммутатора A может регистрировать ту же информацию VLAN, что и порты 5 и 6 коммутатора B.

7.2.3.3 Отображение состояния VLAN

Отображение состояния VLAN в коммутаторе.

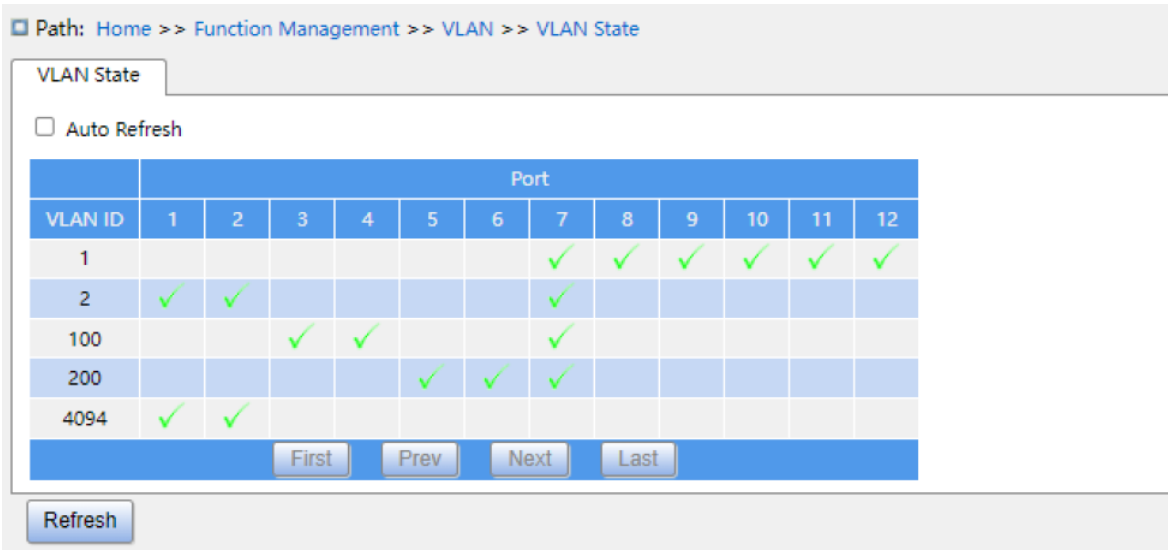


Рис. 96. Состояние VLAN для портов коммутатора

7.3 Конфигурация IP

7.3.1 Конфигурация IP адреса

1. Просмотр IP-адреса коммутатора через консольный порт.

Войдите в CLI коммутатора через консольный порт. Чтобы просмотреть IP-адрес коммутатора запустите команду **show interface vlan 1** в режиме привилегированного пользователя, как показано на рис. далее.

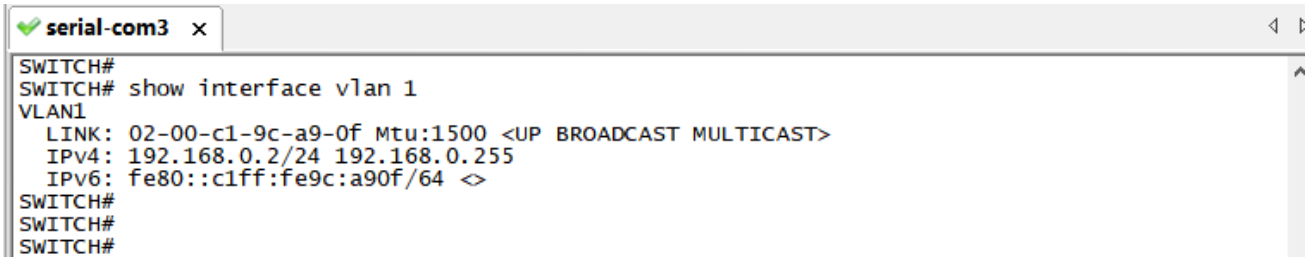


Рис. 97. Отображение IP адреса

2. Создание IP интерфейса.

Хосты в разных VLAN не могут взаимодействовать друг с другом. Их коммуникационные пакеты должны пересылаться маршрутизатором или коммутатором уровня 3 через IP-интерфейс. Коммутаторы этой серии поддерживают IP-интерфейсы, которые представляют собой виртуальные интерфейсы уровня 3 (L3), используемые для связи между VLAN. Вы можете создать один IP-интерфейс для каждой VLAN. Интерфейс используется для пересылки пакетов уровня 3 (L3) портов в VLAN.

3. Настройка основного IP-адреса.

Основной IP-адрес коммутатора можно получить как вручную, так и автоматически, как показано далее.

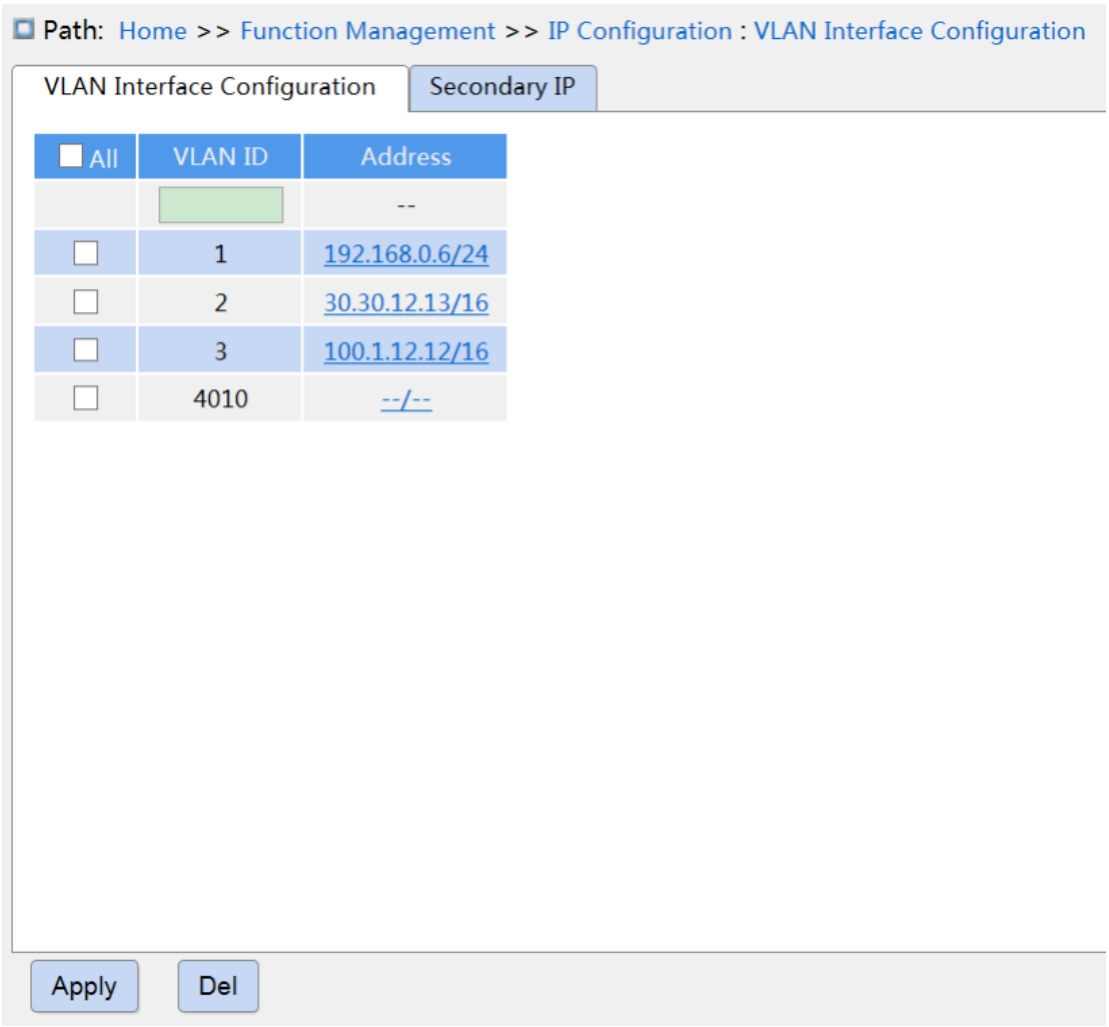


Рис. 98. Конфигурация интерфейса VLAN

VLAN ID

Функция: Настройте свойство VLAN для IP-интерфейса. Только порт-участник VLAN сможет получить доступ к текущему IP-интерфейсу.

Address

Функция: IP-адрес и маска, полученные интерфейсом по VLAN.

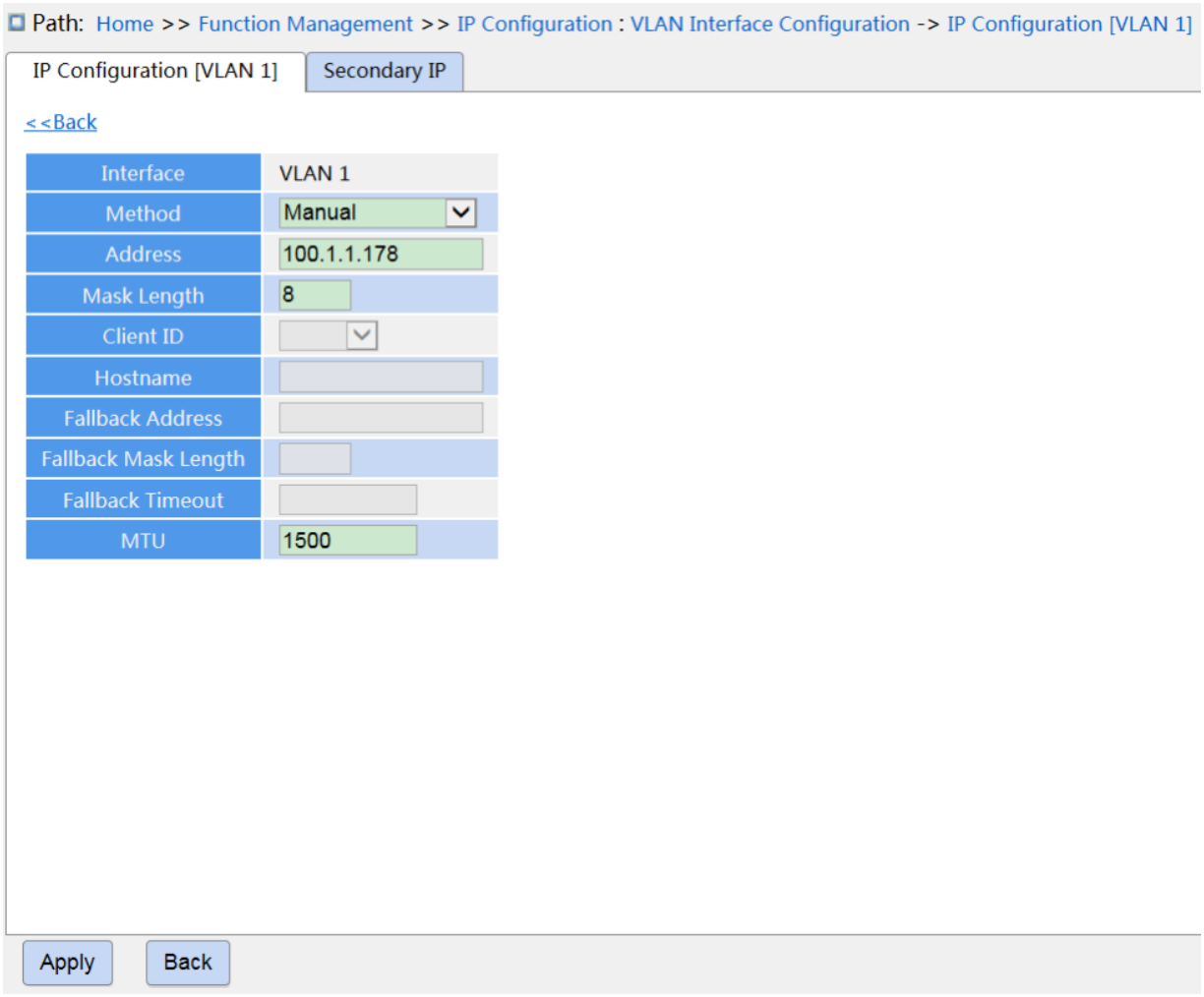


Рис. 99. Настройка IP адреса

Method

Варианты конфигурации: None/DHCP/ Manual

Конфигурация по умолчанию: None

Функция: Manual (вручную), вам необходимо вручную настроить IP-адрес и маску подсети. DHCP, коммутатор автоматически получает IP-адрес через протокол DHCP в качестве клиента DHCP. В этом случае должен быть DHCP-сервер, который будет назначать IP-адрес и маску подсети клиенту в сети.

Address

Формат: A.B.C.D

Функция: IP-адрес интерфейса Vlan.

Mask Length

Функция: Маска подсети — это 32-битное число, состоящее из последовательности «1» и последовательности «0». «1» соответствует полю номера сети и полю номера подсети, а «0» соответствует полю номера хоста. Mask Length — это число единиц в маске.

Client ID

Варианты конфигурации: Hex/ASCII/Port

Функция: Когда указанный IP-интерфейс отправляет запрос DHCP, он передает информацию о заполнении поля option61. Hex заполняет поле option61 в виде 01+mac-адрес; ASCII заполняет поле option61 в виде 00+строка; Port заполняет поле option61 соответствующим интерфейсом mac.

Hostname

Диапазон: 0~63 символов

Функция: Настройка имени хоста для интерфейса VLAN.

Fallback Address

Формат: A.B.C.D

Функция: После того, как интерфейс Vlan получает IP-адрес через протокол DHCP и истекает время ожидания, адрес устанавливается в качестве резервного IP-адреса.

Fallback Mask Length

Функция: Маска подсети - это 32-битное число, состоящее из последовательности «1» и последовательности «0». «1» соответствует полю номера сети и полю номера подсети, а «0» соответствует полю номера хоста. Mask Length - это число единиц в маске.

Fallback Timeout

Диапазон: 0~4294967295 сек.

Функция: Если значение не равно 0, коммутатор пытается получить IP-адрес через протокол DHCP. По истечении времени ожидания IP-адрес, настроенный вручную, вступит в силу. Если значение равно 0, коммутатор будет повторять попытки,

пока не получит IP-адрес через протокол DHCP. В этом случае нет необходимости настраивать IP-адрес вручную.

MTU

Диапазон: 68~9600

Конфигурация по умолчанию: 1500

Функция: Настройте максимальную длину пакета, который может пройти на уровне IP.

4. Конфигурация IPv6 для интерфейса VLAN.

VLAN ID

Диапазон: 1~4093

Функция: Настройте атрибуты VLAN IP-интерфейса так, чтобы только порты-члены VLAN могли получить доступ к текущему IP-интерфейсу.

5. Настройка дополнительного IP адреса.

Настройте вручную дополнительный IP-адрес для IP-интерфейса коммутатора.

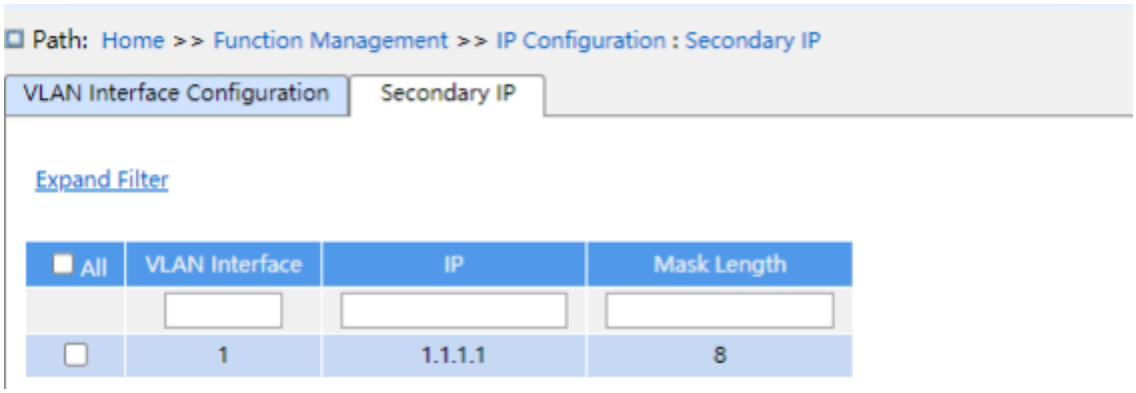


Рис. 100. Настройка вторичного IP адреса

VLAN Interface

Функция: Настройте атрибуты VLAN IP-интерфейса так, чтобы только порты-члены VLAN могли получить доступ к текущему IP-интерфейсу.

IP

Формат: A.B.C.D

Функция: Настроить IP-адрес вручную.

Mask Length

Функция: Маска подсети - это 32-битное число, состоящее из последовательности «1» и последовательности «0». «1» соответствует полю номера сети и полю номера подсети, а «0» соответствует полю номера хоста. Mask Length - это число единиц в маске.

- Каждый IP-интерфейс соответствует основному IP-адресу и может соответствовать нескольким вторичным IP-адресам;
- Различные IP-интерфейсы должны быть настроены с использованием первичных/вторичных IP-адресов для разных сегментов сети.

7.4 Агрегация портов

7.4.1 Статическая агрегация

7.4.1.1 Введение

Агрегация портов объединяет группу портов с одинаковой конфигурацией в логический порт для увеличения полосы пропускания и скорости передачи. Каждый порт-участник в одной группе агрегации реализует разделение трафика и динамическое резервирование между собой для повышения надежности соединения.

Группа агрегации - это физическая группа портов с одинаковой конфигурацией. Физические порты, настроенные в группе агрегации, могут участвовать в агрегации каналов и становиться портами-членами группы агрегации. Когда физические порты, добавленные в группу агрегации, соответствуют определенным условиям, они объединяются в независимый логический порт группы агрегации. Пользователи могут использовать эту группу агрегации в качестве порта, что позволяет не только увеличить пропускную способность сети, но и обеспечить функцию резервного копирования каналов.

7.4.1.2 Реализация

Как показано на рисунке далее, три порта на коммутаторе A и коммутаторе B объединяются, образуя канал порта (port channel). Пропускная способность канала порта равна общей пропускной способности этих трех портов.

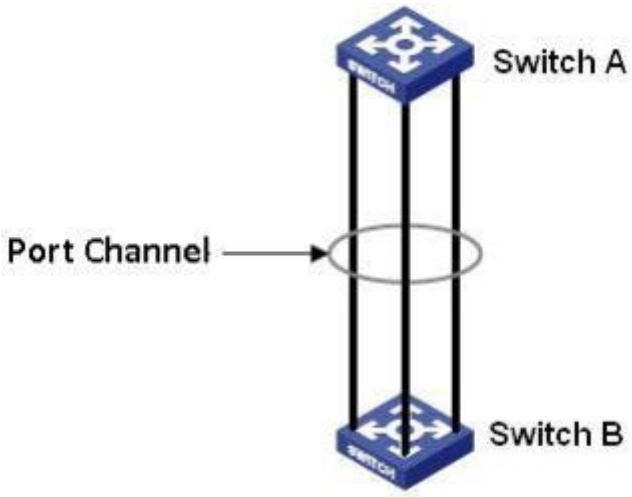


Рис. 101. Пример Port Channel

Если коммутатор A отправляет пакеты коммутатору B через канал порта, коммутатор A определяет порт-участник для передачи трафика на основе результата расчета распределения нагрузки. При выходе из строя одного порта (входящего в канал порта) трафик, передаваемый через порт, передается другому порту на основе алгоритма распределения нагрузки.

- Порт может присоединиться только к одной группе агрегации;
- Порт с включенным протоколом LACP нельзя добавить в статическую группу агрегации, а порт, добавленный в статическую группу агрегации, нельзя включить с помощью протокола LACP;
- Агрегация портов и резервные порты являются взаимоисключающими. Порт, добавленный в группу агрегации, не может быть настроен как резервный порт. Порт, настроенный как резервный порт, не может быть добавлен в группу агрегации;
- Упомянутые резервные порты относятся к кольцевым портам STRP, резервным портам STRP, портам STP, портам RSTP и портам MSTP.

7.4.1.3 Web конфигурация

1. Конфигурация статической агрегации.

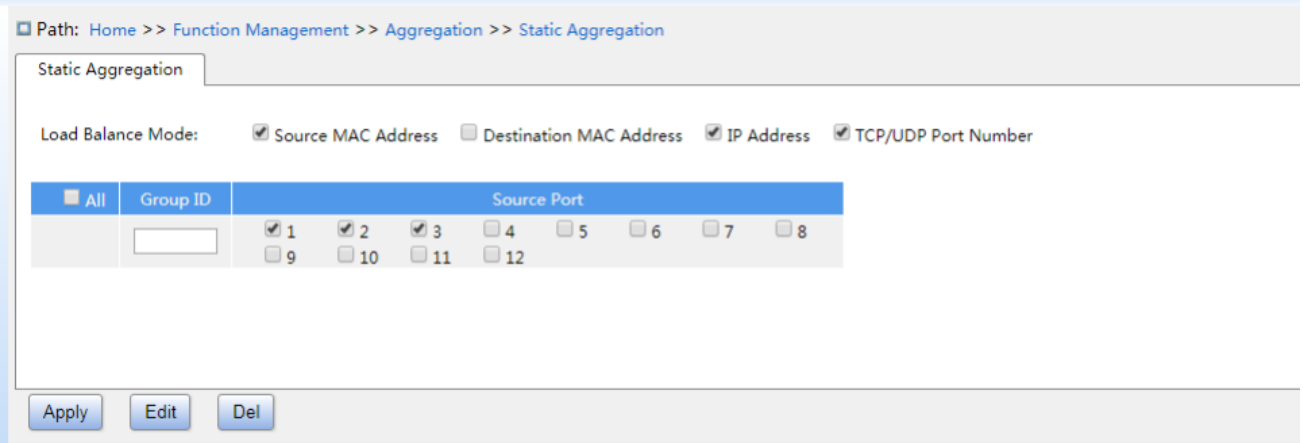


Рис. 102. Конфигурация статической агрегации

Load Balance Mode

Варианты конфигурации: Source MAC address / destination MAC / IP address / TCP/UDP port number

Конфигурация по умолчанию: Source MAC address + IP address + TCP/UDP port number

Функция: Настройка режима распределения нагрузки для группы агрегации.

Описание: Source MAC address выполняет балансировку трафика на основе MAC-адреса источника; destination MAC выполняет балансировку трафика на основе MAC-адреса назначения; IP address выполняет балансировку трафика на основе IP-адреса; TCP/UDP port number выполняет балансировку трафика на основе номера порта TCP/UDP.

Group ID

Диапазон: 1~N (N - количество портов/2)

Функция: Настройка номера для группы агрегации.

Описание: Порты входящие одну группу агрегации имеют одинаковые свойства портов. Количество групп агрегации зависит от порта устройства, каждая группа агрегации поддерживает до 8 портов.

Source Port

Варианты конфигурации: Enable/ Disable

Функция: Выбор порта для присоединения к указанной группе агрегации.

7.4.1.4 Пример конфигурации

Как показано на рис. 101, три порта (порты 1, 2 и 3) коммутатор A соответственно подключены к трем портам (порты 1, 2 и 3) коммутатора B, образуя группу агрегации 1, тем самым реализуя распределение трафика между портами (предположим, что три совокупных порта коммутатора имеют одинаковые атрибуты).

Конфигурация коммутаторов:

1. Выберите порты 1, 2 и 3 в коммутаторе A, чтобы присоединиться к группе агрегации 1, см. рис. 102.
2. Выберите порты 1, 2 и 3 в коммутаторе B, чтобы присоединиться к группе агрегации 1, см. рис. 102.

7.4.2 LACP

7.4.2.1 Введение

Протокол управления агрегацией каналов (Link Aggregation Control Protocol, LACP) основан на стандарте IEEE802.3ad. Он используется для обмена информацией с одноранговым портом через Link Aggregation Control Protocol Data Unit (LACPDU), для выбора порта участника в группе динамической агрегации.

7.4.2.2 Реализация

Порт с включенным LACP сообщает партнеру (peer port) о приоритете LACP своего устройства, MAC-адресе устройства, приоритете LACP порта, номере порта и значении ключа путем отправки сообщений LACPDU. После получения сообщения LACPDU партнер (peer port) согласовывает с локальной стороной (локальным портом):

1. Сравнивает идентификаторы устройств на обоих концах (идентификатор устройства equipment ID = приоритет LACP устройства + MAC устройства). Сначала

сравнивает приоритет LACP устройства. Если они одинаковы, сравнивает MAC-адреса устройств и выбирает устройство с меньшим идентификатором устройства в качестве основного устройства (master equipment).

2. Сравнивает идентификатор порта основного устройства (идентификатор порта port ID = приоритет порта LACP + номер порта). Сначала сравнивает приоритет порта LACP. Если они одинаковы, сравнивает номер порта и выбирает порт с меньшим идентификатором порта в качестве референсного порта (reference port).

3. Если значение ключа и конфигурация атрибутов порта и reference port совпадают и порты находятся в активном состоянии (Up), а значение ключа и конфигурации атрибутов peer port и reference port также совпадают, то порт может стать портом участником в группе динамической агрегации.

7.4.2.3 Web конфигурация

1. Настройка приоритета LACP.

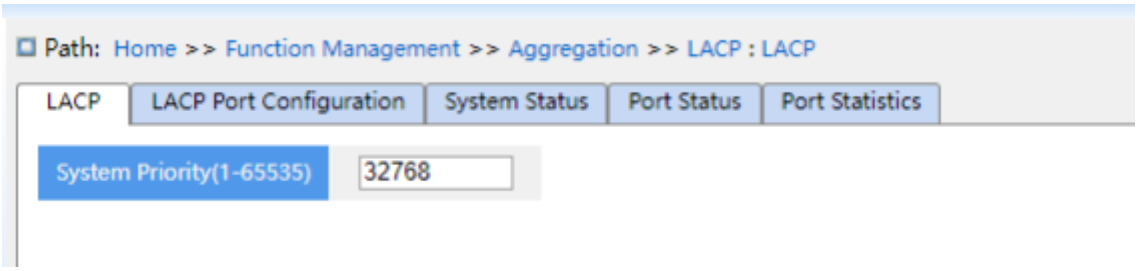


Рис. 103. Настройка приоритета LACP

LACP

Диапазон: 1~65535

Конфигурация по умолчанию: 32768

Функция: Настройка приоритета LACP, используемого для выбора основного устройства (master equipment) при согласовании LACP.

2. Конфигурация портов LACP.

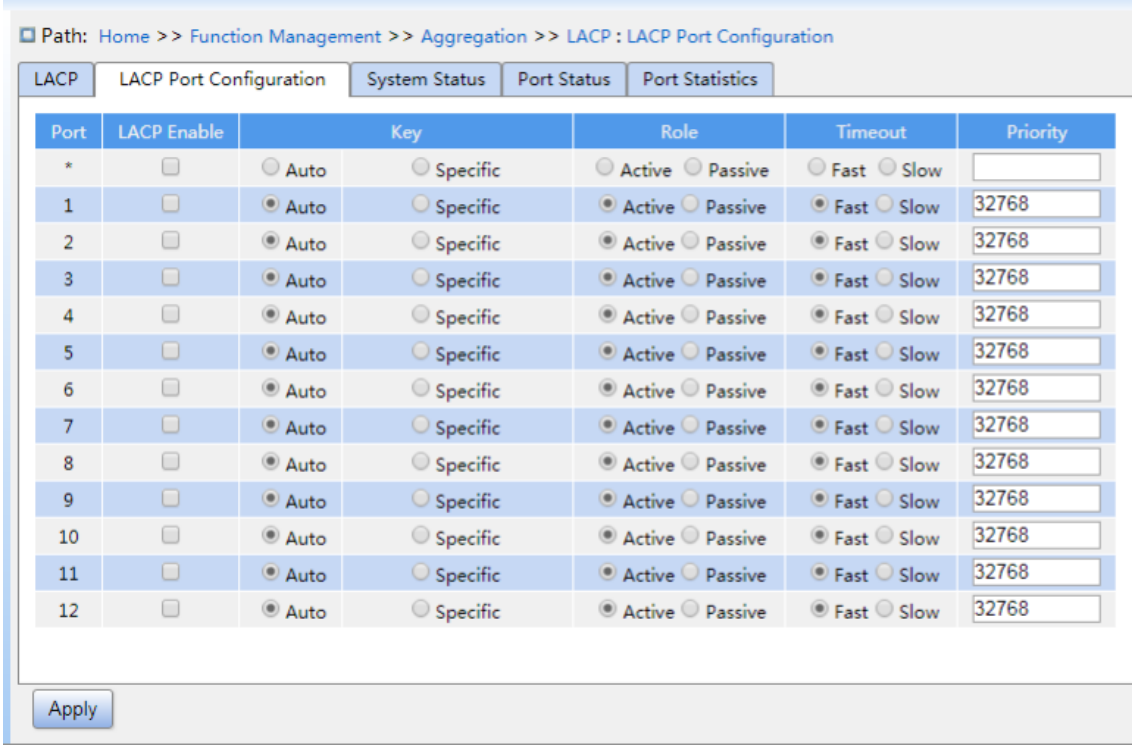


Рис. 104. Настройка портов LACP

LACP Enable

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включение LACP протокола для порта.

Key

Варианты конфигурации: Auto / Specific（1~65535）

Конфигурация по умолчанию: Auto

Функция: Настройка значение ключа для порта. При выборе Auto значение ключа определяется скоростью порта, key=1 (10Mb); key=2 (100Mb); key=3 (1000Mb). Порты с разными значениями ключа не могут быть добавлены в группу динамической агрегации.

Role

Варианты конфигурации: Active/passtive

Конфигурация по умолчанию: Active

Функция: Выберите статус роли LACP. Активный порт будет активно отправлять

сообщения LACPDU на противоположный порт; пассивный порт будет отправлять сообщения LACPDU на противоположный порт только после получения сообщений LACPDU от противоположного порта.

По крайней мере один из двух подключенных портов должен быть Active, иначе два порта не смогут обмениваться информацией.

Timeout

Варианты конфигурации: Fast / slow

Конфигурация по умолчанию: Fast

Функция: Active порт, настойка временного интервала для отправки сообщения LACPDU. Fast относится к интервалу времени, равному 1 сек., а slow относится к интервалу времени, равному 30 сек.

Priority

Диапазон: 1~65535

Конфигурация по умолчанию: 32768

Функция: Настройте приоритет порта LACP для использования при выборе reference port. Порт с наименьшим приоритетом в главном устройстве выбирается в качестве reference port.

3. Просмотр состояния LACP.

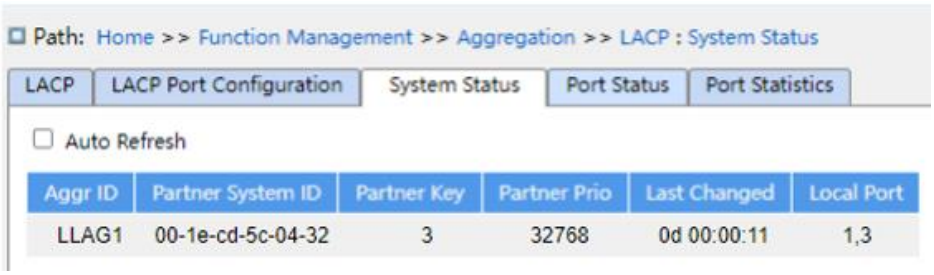
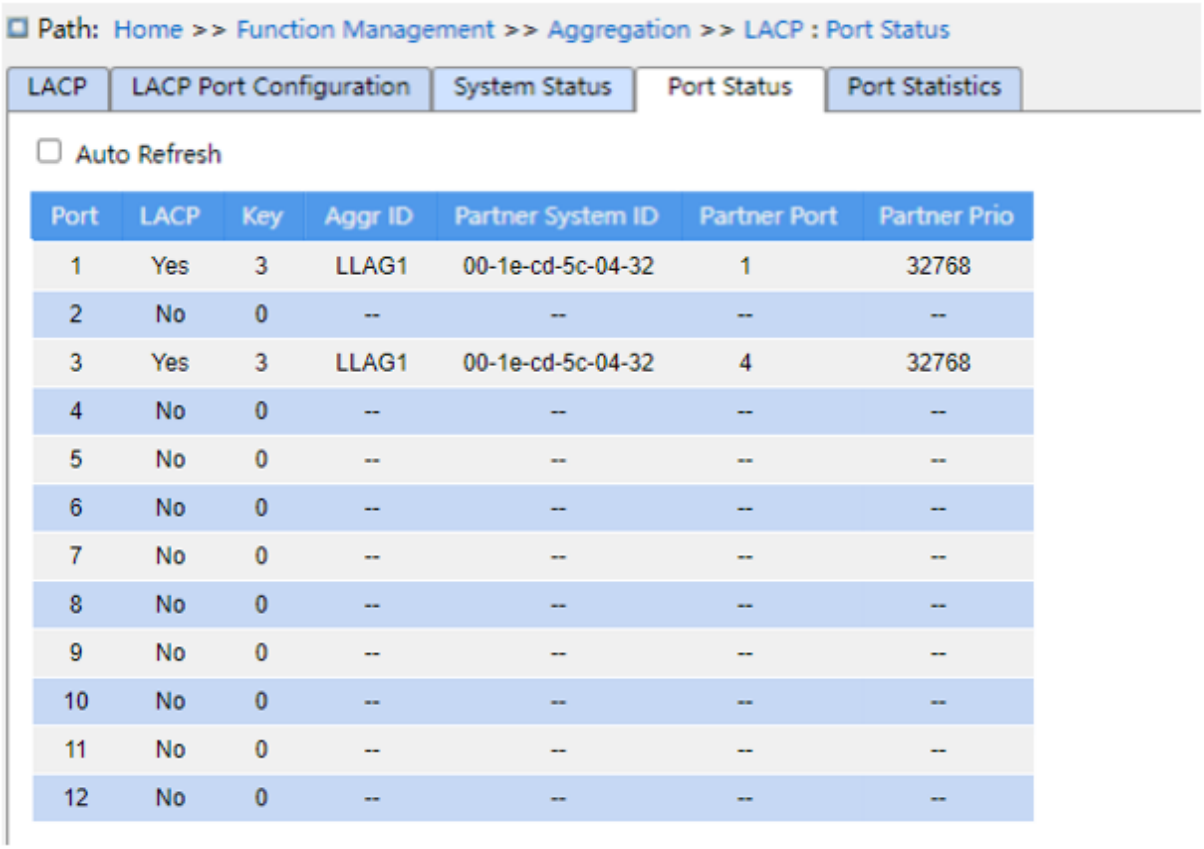


Рис. 105. Просмотр состояния LACP

4. Просмотр состояния портов LACP



Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	Yes	3	LLAG1	00-1e-cd-5c-04-32	1	32768
2	No	0	--	--	--	--
3	Yes	3	LLAG1	00-1e-cd-5c-04-32	4	32768
4	No	0	--	--	--	--
5	No	0	--	--	--	--
6	No	0	--	--	--	--
7	No	0	--	--	--	--
8	No	0	--	--	--	--
9	No	0	--	--	--	--
10	No	0	--	--	--	--
11	No	0	--	--	--	--
12	No	0	--	--	--	--

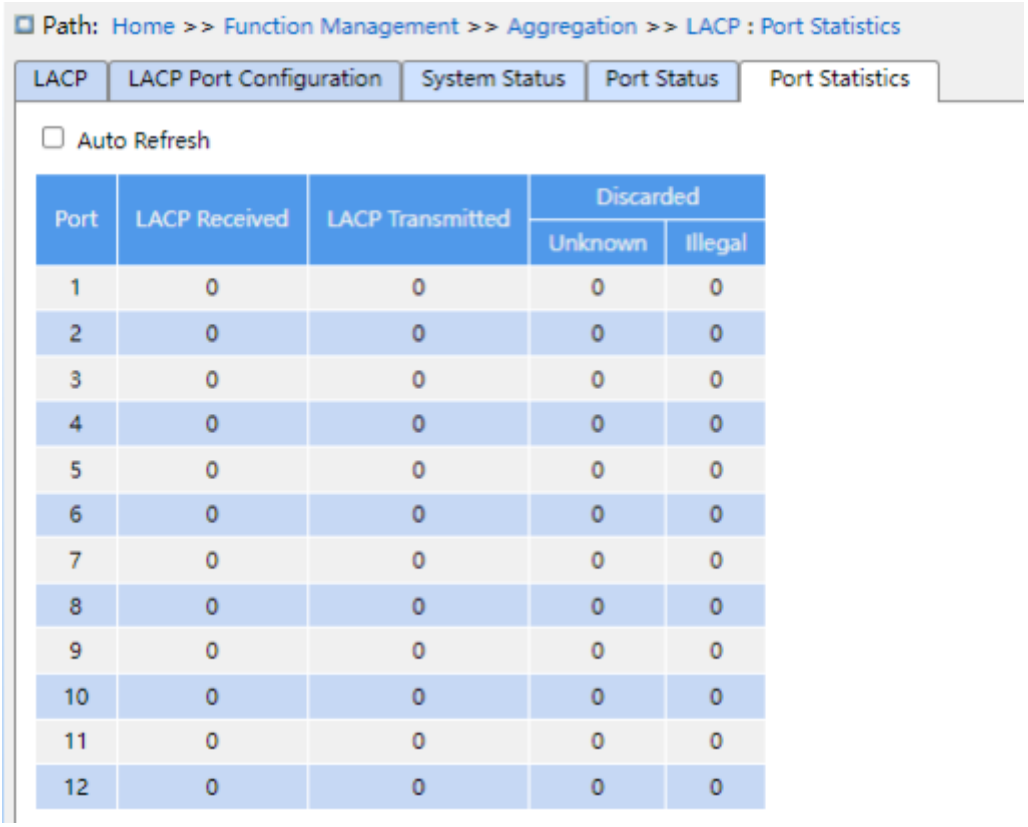
Рис. 106. Просмотр состояния портов LACP

LACP Status

Варианты отображения: Yes/No

Функция: Отобразить статус LACP порта. Yes означает, что LACP включен и порт включен. No означает, что LACP отключен и порт не работает.

5. Просмотр статистики портов LACP.



Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0

Рис. 107. Просмотр статистика портов LACP

7.4.2.4 Пример конфигурации

Как показано на рис. 101, добавьте три порта (порт 1, 2 и 3) коммутатора A в группу портов 1 и три порта (порт 1, 2 и 3) коммутатора B в группу портов 1. Используйте сетевые кабели для соединения этих портов, чтобы сформировать port channel, реализующий распределение нагрузки между портами. (Предполагается, что три порта коммутатора A и B имеют одинаковые атрибуты соответственно).

Конфигурация коммутаторов:

1. Включите LACP на портах 1, 2 и 3 на коммутаторе A, см. 104;
2. Включите LACP на портах 1, 2 и 3 на коммутаторе B, см. 104.

7.5 Резервирование

7.5.1 Протокол ST-Ring

7.5.1.1 Введение

ST-Ring и ST-Ring+ являются проприетарными протоколами резервирования СТЭЗ. Они позволяют сети восстанавливаться в течение 50 мс при сбое соединения, обеспечивая стабильную и надежную связь. ST кольца делятся на два типа: основанные на порте (ST-Ring-Port) и основанные на VLAN (ST-Ring-VLAN).

ST-Ring-Port: указывает порт для пересылки или блокирования пакетов.

ST-Ring-VLAN: указывает порт для пересылки или блокирования пакетов определенной VLAN. Это позволяет использовать несколько VLAN на одном касательном tangent порте, то есть один порт является частью разных резервных колец, основанных на разных VLAN.

7.5.1.2 Принцип работы

Ведущий (Master): У одного кольца есть только один master. Master отправляет пакеты протокола ST-Ring и определяет статус кольца. Когда кольцо замкнуто, два кольцевых порта на главном устройстве находятся в состоянии работы (Forwarding) и блокировки (Blocking) соответственно.

Первый порт, статус соединения которого изменяется на Up при образовании кольца, находится в состоянии forwarding. Другой кольцевой порт находится в состоянии blocking.

Подчиненный (Slave): Кольцо может включать в себя несколько подчиненных Slave устройств. Slave устройства прослушивают и пересылают пакеты протокола ST-Ring и сообщают информацию о неисправностях ведущему Master устройству.

Резервный порт (Backup port): Порт для связи между ST-кольцами называется резервным портом.

Главный резервный порт (Master backup port): Когда кольцо имеет несколько

резервных портов (backup port), резервный порт с большим MAC-адресом является главным резервным портом. Он находится в состоянии forwarding.

Подчиненный резервный порт (Slave backup port): Когда кольцо имеет несколько резервных портов, все резервные порты, кроме главного резервного порта, являются подчиненными резервными портами. Они находятся в blocking состоянии.

Состояние forwarding: Если порт находится в состоянии передачи данных (forwarding), то порт может как принимать, так и отправлять данные.

Состояние blocking: Если порт находится в состоянии блокировки (blocking), порт может принимать и пересылать только пакеты протокола ST-Ring, но не другие пакеты.

7.5.1.3 Реализация

Реализация ST-Ring-Port

Forwarding порт на главном устройстве (master) периодически отправляет пакеты протокола ST-Ring для определения состояния соединения. Если блокирующий (blocking) порт ведущего устройства принимает пакеты, кольцо замыкается; в противном случае кольцо открыто.

Процесс работы коммутатора A, коммутатора B, коммутатора C и коммутатора D:

1. Сконфигурируйте коммутатор A в качестве ведущего, а другие коммутаторы - в качестве подчиненных;

2. Кольцевой порт 1 на главном устройстве находится в состоянии передачи (forwarding), в то время как кольцевой порт 2 находится в состоянии блокировки (blocking). Оба порта на подчиненных устройствах находятся в состоянии передачи (forwarding).

3. Если соединение CD не работает, как показано далее на рисунке, то:

a) Когда соединение CD не работает, то порты 6 и 7 на ведомых устройствах находятся в состоянии блокировки (blocking). Порт 2 ведущего устройства переходит в состояние передачи forwarding, обеспечивая нормальную связь;

b) Когда неисправность устранена, порты 6 и 7 ведомых устройств переходят в состояние передачи (forwarding). Порт 2 ведущего устройства переходит в

состояние блокировки (blocking). Происходит переключение каналов, и каналы восстанавливаются до состояния, существовавшего до неисправности CD.

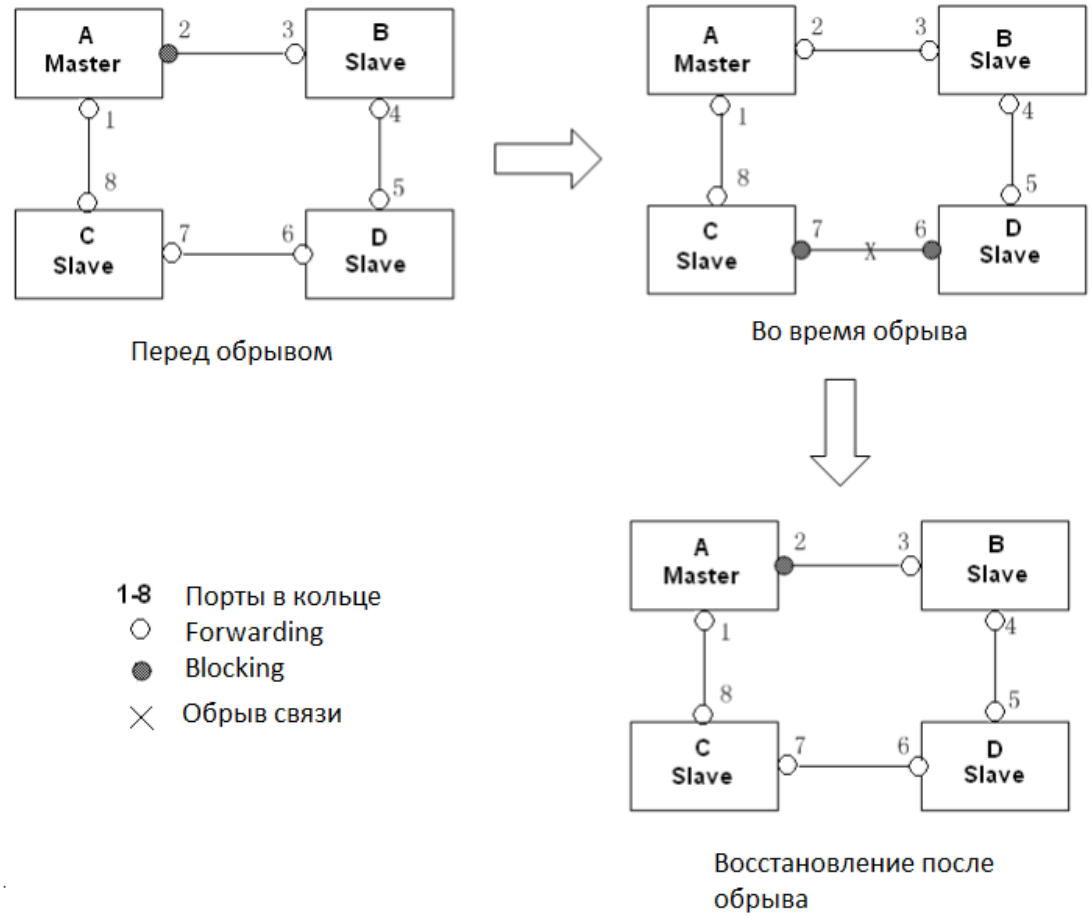


Рис. 108. Обрыв соединения CD

4. Если соединение AC не работает, как показано далее на рисунке, то:

a) Когда соединение AC не работает, порт 1 находится в состоянии блокировки (blocking), а порт 2 переходит в состояние передачи (forwarding), обеспечивая нормальную связь по каналу.

b) После устранения неисправности порт 1 по-прежнему находится в состоянии блокировки (blocking), а порт 8 в состоянии передачи (forwarding). Переключения не происходит.

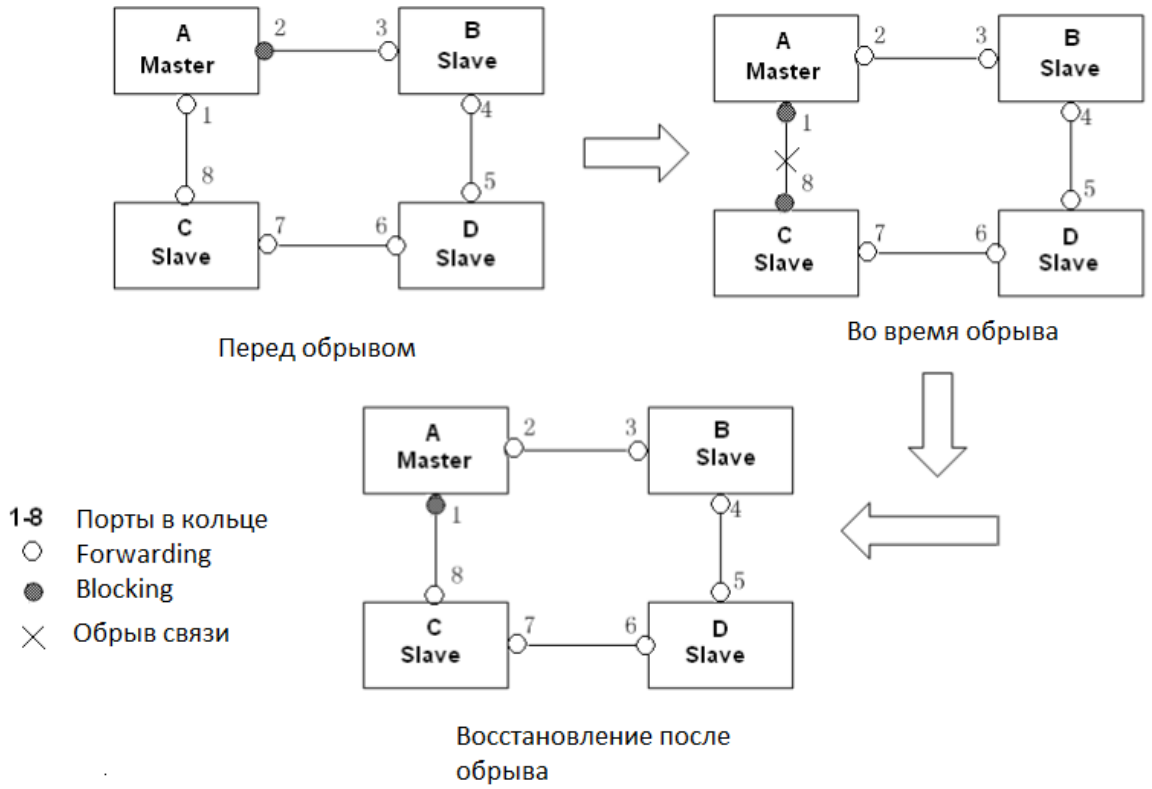


Рис. 109. Обрыв соединения AC

Изменение статуса соединения (link status) портов влияет на статус кольцевых backup портов.

ST-Ring-VLAN реализация

ST-Ring-VLAN позволяет пересылать пакеты из разных VLAN по разным путям. Каждый путь пересылки для VLAN образует ST-Ring-VLAN. Разные кольца ST-VLAN могут иметь разных мастеров. Как показано на рисунке далее, настроены две сети ST-Ring-VLAN.

Кольцевые соединения ST-Ring-VLAN 10: AB-BC-CD-DE-EA.

Кольцевые соединения ST-Ring-VLAN 20: FB-BC-CD-DE-EF.

Два кольца имеют tangent порты BC, CD и DE. Коммутаторы C и D используют одни и те же порты в двух кольцах, но используют разные логические каналы на основе VLAN.

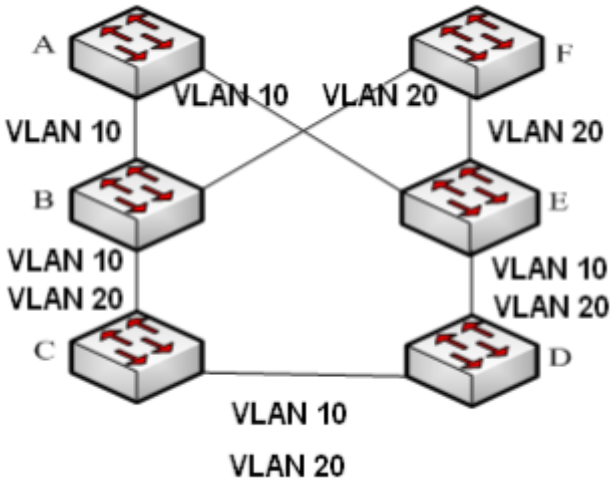


Рис. 110. Реализация ST-Ring-VLAN

В каждом логическом кольце ST-Ring-VLAN реализация идентична реализации ST-Ring-Port.

ST-Ring+ реализация

ST-Ring+ может обеспечить резервирование для двух колец ST-Ring, как показано на рисунке далее. Один резервный (backup) порт настроен соответственно на коммутаторе C и коммутаторе D. Какой порт является главным резервным портом (master backup port), зависит от MAC-адресов двух портов. Если главный резервный порт или его соединение выходят из строя, подчиненный резервный порт (slave backup port) будет пересылать пакеты, предотвращая петли и обеспечивая нормальную связь между резервными кольцами.

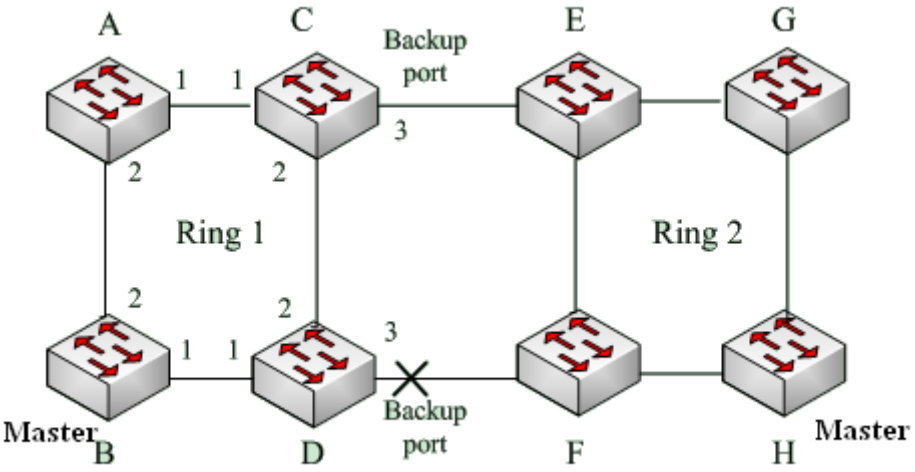


Рис. 111. Реализация ST-Ring+

Изменение статуса соединения (link status) портов влияет на статус кольцевых backup портов.

7.5.1.4 Принцип работы

Конфигурация ST-Ring должна соответствовать следующим условиям:

- Все коммутаторы в одном кольце должны иметь одинаковый номер домена (domain number).
- Каждое кольцо может иметь только одного ведущего (master) и несколько ведомых (slave).
- На каждом коммутаторе для кольца можно настроить только два порта.
- Для двух связанных колец резервные (backup) порты можно настроить только в одном кольце.
- В одном кольце можно настроить максимум два резервных (backup) порта.
- На коммутаторе для одного кольца можно настроить только один резервный (backup) порт.
- ST-Ring-Port и ST-Ring-VLAN нельзя настроить на одном коммутаторе одновременно.

7.5.1.5 Web конфигурация

1. Настройка кольцевого резервирования ST-Ring.

Перейдите

[Home] → [Function Management] → [Redundancy] → [ST-Ring]

Redundancy Mode

Варианты конфигурации: Port Based/Vlan Based

Конфигурация по умолчанию: Port Based

Функция: Выбор режима кольцевого резервирования ST-Ring.

- К кольцевым протоколам на основе портов относятся RSTP, ST-Ring-Port и STRP-Port, а к кольцевым протоколам на основе VLAN относятся MSTP, ST-Ring-VLAN и STRP-VLAN.
- Кольцевые протоколы на основе VLAN являются взаимоисключающими, и для одного устройства можно настроить только один тип кольцевого протокола на основе VLAN.
- Кольцевой протокол на основе порта и кольцевой протокол на основе VLAN являются взаимоисключающими, и для одного устройства можно выбрать только один режим кольцевого протокола.

2. Настройка ST-Ring-Port и ST-Ring-VLAN.

Перейдите

[Home] → [Function Management] → [Redundancy] → [ST-Ring]

Domain ID

Диапазон: 1~32

Функция: Domain ID используется для различения колец. Один коммутатор поддерживает максимум 16 колец на основе VLAN, количество колец на основе портов зависит от количества портов коммутатора.

Domain Name

Диапазон: 1~31 символов

Функция: Сконфигурируйте имя для обозначения кольца.

Station Type

Варианты конфигурации: Master/Slave

Значение по умолчанию: Master

Функция: Выбор роли коммутатора в кольце. Ведущий или подчиненный.

Ring Port-1/Ring Port-2

Варианты конфигурации: все порты коммутатора.

Функция: Выбор двух кольцевых портов.

- Кольцевые порты ST-Ring и агрегация портов являются взаимоисключающими. Кольцевые порты ST-Ring не могут быть добавлены в группу агрегации; порты, добавленные в группу агрегации, не могут быть настроены как кольцевые порты ST-Ring;
- Кольцевые порты на основе RSTP, ST-Ring-Port и STRP-Port являются взаимоисключающими, то есть на коммутаторе может быть настроен только один из протоколов одновременно;
- Не следует настраивать порты в группе изоляции и как порты кольца ST-Ring одновременно.

ST-Ring+

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включение / выключение поддержки ST-Ring+ для кольца.

Backup Port

Варианты конфигурации: все порты коммутатора

Функция: Назначить резервный (backup) порт.

Описание: Перед включением резервного порта необходимо включить функцию ST-Ring+.

Выберите резервный порт, отличный от кольцевого порта.

VLAN List

Варианты конфигурации: Все созданные VLAN на коммутаторе

Функция: Выберите VLAN для кольцевого порта. При наличии нескольких VLAN вы можете разделить VLAN запятой (,) и дефисом (-), где (-) используется для разделения двух последовательных идентификаторов VLAN, а (,) используется для разделения двух непоследовательных идентификаторов VLAN.

3. Просмотр и изменение конфигурации ST-Ring.

Перейдите

[Home] → [Function Management] → [Redundancy] → [ST-Ring]

Нажмите <Edit> для изменения конфигурации для выбранной записи ST-Ring.

Нажмите <Del> для удаления конфигурации для выбранной записи ST-Ring.

Пример конфигурации:

Global ST-Ring Configuration									
Redundancy Mode:		Port Based							
ST-Ring Configuration:									
All	**Domian ID**	**Domian Name**	**Station Type**	**Ring Port-1**	**Ring Port-2**	**ST-Ring+**	**Backup Port**	**Vlan List**	**Details**
	1	aaa	Master	2	3	Enable	---	---	
	2	bbb	Slave	4	5	Disable	---	---	

4. Просмотр статуса состояния ST-Ring.

Перейдите

[Home] → [Function Management] → [Redundancy] → [ST-Ring]

Далее перейдите в [Details] для выбранного кольца.

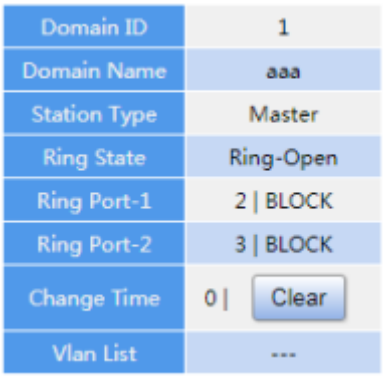


Рис. 112. Отображение состояния ST-Ring

7.5.1.6 Пример конфигурации

Как показано на рис. 111, коммутаторы A, B, C и D образуют кольцо 1 (Ring1); коммутаторы E, F, G и H образуют кольцо 2 (Ring2). Соединения CE и DF являются резервными соединениями между Ring1 и Ring2.

Конфигурация коммутатора A:

1. Настройте domain ID "1", domain name "a", ring port "1", "2", station type "slave", ST-Ring+ "disable", backup port не назначен;

Конфигурация коммутатора B:

2. Настройте domain ID "1", domain name "a", ring port "1", "2", station type "master", ST-Ring+ "disable", backup port не назначен;

Конфигурация коммутатора C и коммутатора D:

3. Настройте domain ID "1", domain name "a", ring port "1", "2", station type "master", ST-Ring+ "enable", backup port "3";

Конфигурация коммутатора E, коммутатора F, коммутатора G:

4. Настройте domain ID "2", domain name "b", ring port "1", "2", station type "slave", ST-Ring+ "disable", backup port не назначен;

Конфигурация коммутатора H:

5. Настройте domain ID "2", domain name "b", ring port "1", "2", station type "master", ST-Ring+ "disable", backup port не назначен.

7.5.2 STRP

7.5.2.1 Введение

STRP - протокол для передачи данных в сетях с кольцевой топологией. STRP позволяет предотвращать широковещательные штормы в кольцевых сетях; если канал или узел неисправен, резервный канал может взять на себя обслуживание сети в режиме реального времени, чтобы обеспечить непрерывную передачу данных.

STRP использует механизм выбора ведущего устройства без фиксированного ведущего устройства.

Протокол STRP предоставляет следующие возможности:

- Время восстановления, независимое от масштаба сети

Оптимизируя механизм пересылки данных сообщений об обнаружении кольцевой сети, протокол STRP может достичь времени восстановления после сбоя, которое не зависит от масштаба сети. Благодаря внедрению таких механизмов, как отчеты о прерываниях в реальном времени, время восстановления после сбоя STRP может достигать 20 мс, тем самым значительно улучшая реальную производительность. Эта функция позволяет коммутаторам обеспечить более высокую надежность приложений в энергетике, железнодорожном транспорте и многих других отраслях, где требуется управление в реальном времени.

- Разнообразные функции контроля подключения

Для повышения стабильности сети STRP предоставляет разнообразные функции обнаружения типичных сбоев в сети, включая обнаружение быстрого отключения, обнаружение однонаправленного соединения по оптоволокну, проверку качества соединения и исправности оборудования, обеспечивая надлежащую передачу данных.

- Применимо к различным сетевым топологиям

Помимо быстрого восстановления для простых кольцевых сетей, STRP также поддерживает сложные кольцевые топологии, такие как пересекающиеся кольца и касательные кольца. Кроме того, STRP поддерживает несколько экземпляров на основе VLAN, тем самым обеспечивая гибкую работу в сети для различных сетевых

приложений.

- Мощные функции диагностики и технического обслуживания

STRP предоставляет мощные механизмы запроса состояния и сигнализации для диагностики и обслуживания сети, помогающие поддерживать и диагностировать сеть, а также предоставляет механизмы для предотвращения штормов кольцевой сети и других проблем, вызванных неправильной работой или ошибками конфигурации.

7.5.2.2 Принцип работы

1. Режимы работы STRP

STRP -VLAN: пересылает или блокирует пакеты на основе VLAN. Если порт находится в состоянии блокировки (blocking), блокируются только пакеты данных указанной VLAN. Таким образом, на касательных кольцевых портах можно настроить несколько VLAN. Порт может принадлежать разным кольцам STRP в соответствии с конфигурациями VLAN.

2. Статусы портов STRP

Состояние forwarding: Если порт находится в состоянии передачи (forwarding), он может принимать и пересылать пакеты данных.

Состояние blocking: Если порт находится в состоянии блокировки (blocking), он может принимать и пересылать пакеты STRP, но не другие пакеты данных.

Главный (primary) порт: кольцевой порт в root, который принудительно переходит в состояние передачи (forwarding) при замыкании петли. Этот порт должен быть настроен пользователем.

- Если в root не настроен основной (primary) порт, то первый порт, статус соединения которого изменяется на up при замыкании кольца, перейдет в состояние forwarding. Другой кольцевой порт перейдет в состояние blocking.
- Порт, находящийся в состоянии блокировки (blocking) в root, может активно отправлять STRP пакеты.

3. STRP роли

STRP определяет роли коммутаторов путем пересылки пакетов Announce, предотвращая образование замкнутых колец.

INIT: указывает устройство, на котором включена функция STRP, и два кольцевых порта находятся в состоянии отключения соединения (Link down).

Root: указывает устройство, на котором включен STRP и по крайней мере один кольцевой порт находится в состоянии подключения (Link up state). В кольце Root выбирается в соответствии с векторами пакетов Announce и может меняться в зависимости от топологии сети. Root периодически отправляет свои пакеты Announce на другие устройства. Статусы кольцевых портов: Один кольцевой порт находится в состоянии forwarding, а другой - в состоянии blocking. При получении пакета Announce от другого устройства Root сравнивает вектор пакета с вектором своего собственного пакета Announce. Если вектор полученного пакета больше, Root изменяет свою роль на Normal или B-Root в соответствии со статусом канала и наличием CRC деградации на портах.

B-Root: указывает устройство, на котором включен STRP, удовлетворяющее по крайней мере одному из следующих условий: один кольцевой порт находится в состоянии подключения (Link up state), в то время как другой находится в состоянии отключения, наличие CRC деградации, приоритет не менее 200. B-Root сравнивает и пересылает пакеты Announce. Если вектор полученного пакета Announce меньше вектора его собственного пакета announce, B-Root изменяет свою роль на Root; в противном случае он пересылает полученный пакет и не меняет свою собственную роль. Статусы кольцевых портов: Один кольцевой порт находится в состоянии forwarding.

Normal: указывает устройство, на котором включен STRP, и оба кольцевых порта находятся в состоянии соединения (Link up) без деградации CRC, а приоритет превышает 200. Normal только пересылает пакеты Announce, но не проверяет содержимое пакетов. Статусы кольцевых портов: Оба кольцевых порта находятся в состоянии forwarding.

CRC деградация: указывает, что количество пакетов CRC превышает пороговое значение в течение 30 минут.

7.5.2.3 Реализация

Каждый коммутатор рассчитывает свой собственный вектор пакета Announce. Коммутатор с набольшим вектором будет выбран в качестве Root.

Вектор пакета Announce содержит следующую информацию для назначения роли.

Таблица 5. Вектор Announce пакета

Link status (статус подключения)	CRC деградация		Role priority	IP адрес устройства	MAC адрес устройства
	CRC деградация статус	CRC деградация показатель			

Link status: Значение устанавливается равным 1, если один кольцевой порт находится в состоянии отключения соединения (Link down), и устанавливается равным 0, если оба кольцевых порта находятся в состоянии подключения (Link up).

Статус деградации CRC: Если деградация CRC происходит на одном порте, значение устанавливается равным 1. Если деградация CRC не происходит на двух кольцевых портах, значение устанавливается равным 0.

Скорость деградации CRC: отношение количества пакетов CRC к пороговому значению за 30 минут.

Role priority: Значение может быть установлено в веб-интерфейсе.

Параметры (в таблице 5) для вектора пакета Announce сравниваются по следующей процедуре:

1. Сначала проверяется значение статуса соединения. Считается, что устройство с большим значением статуса соединения имеет больший вектор.

2. Если два сравниваемых устройства имеют одинаковое значение статуса

соединения, сравниваются значения статуса деградации CRC. Считается, что устройство с большим значением статуса деградации CRC имеет больший вектор. Если значение CRC degradation status для всех сравниваемых устройств равно 1, считается, что устройство с большим значением CRC degradation rate имеет больший вектор.

3. Если два сравниваемых устройства имеют одинаковое значение статуса соединения и значение CRC degradation value, значения приоритета роли, IP-адресов и MAC-адресов сравниваются последовательно. Считается, что устройство с большим значением имеет больший вектор.

4. В качестве Root выбирается устройство с большим вектором.

Только когда значение статуса деградации CRC равно 1, значение скорости деградации CRC участвует в векторном сравнении. В противном случае векторы сравниваются независимо от значения скорости деградации CRC.

- Реализация режима STRP-Port-Based

Роли коммутаторов:

1. При запуске все коммутаторы находятся в состоянии INIT. Когда состояние одного порта изменяется на Link up, коммутатор становится Root и отправляет пакеты Announce другим коммутаторам в кольце для выбора роли.

2. В качестве Root выбирается коммутатор с наибольшим вектором пакета Announce. Кольцевой порт, который подключается (link up) первым к Root, находится в состоянии forwarding, а другой кольцевой порт находится в состоянии blocking. Среди других коммутаторов в кольце коммутатор с одним кольцевым портом в состоянии Link down или деградации CRC является B-Root. Коммутатор с обоими кольцевыми портами в состоянии link up и без деградации CRC является Normal.

Процедура устранения неисправности (fault recovery) при работе протокола STRP показана далее.

1. В исходной топологии A является Root; порт 1 находится в состоянии

forwarding, а порт 2 - в состоянии blocking. B, C и D являются Normal, и их кольцевые порты находятся в состоянии forwarding.

2. Когда соединение CD неисправно, STRP изменяет статусы портов 6 и 7 на blocking. В результате C и D становятся Root. Поскольку A, C и D в данный момент являются Root, все они отправляют пакеты Announce. Векторы C и D больше, чем у A, потому что порты 7 и 6 находятся в состоянии отключения соединения (Link down). В этом случае, если вектор D больше вектора C, то D выбирается в качестве Root, а C становится B-Root. При получении пакета o Announce D, A обнаруживает, что вектор D больше, чем его собственный вектор, и оба его кольцевых порта находятся в состоянии подключен (Link up). Таким образом, A становится Normal и изменяет статус порта 2 на forwarding.

3. При восстановлении подключения CD, D по-прежнему является Root, поскольку его вектор больше вектора C.

- Если на D не настроен ни один primary порт, то порт 7 по-прежнему находится в состоянии blocking, а порт 8 - в состоянии forwarding.
- Если порт 7 на D настроен как primary порт, то порт 7 переходит в состояние forwarding, а порт 8 находится в состоянии blocking.

STRP изменяет состояние порта 6 на forwarding. В результате C становится Normal. Таким образом, роли коммутаторов при восстановлении соединения не меняются.

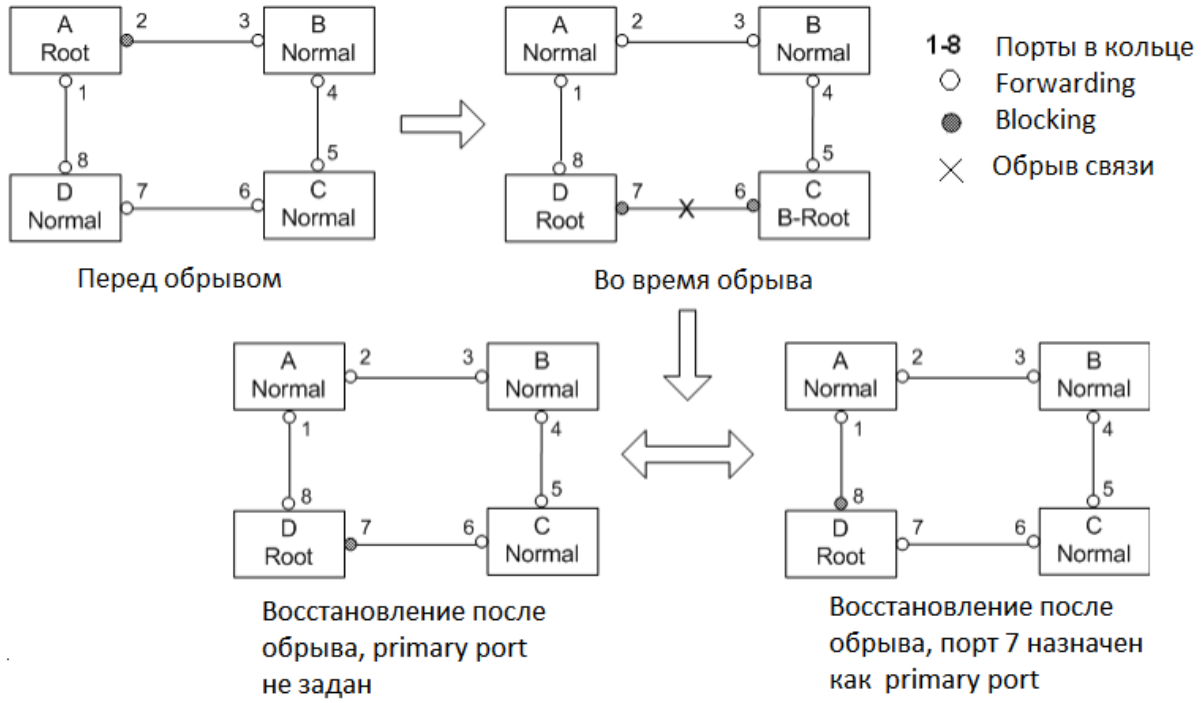


Рис. 113. Обрыв соединения при работе STRP

В кольцевой сети STRP, роли коммутаторов меняются при сбое соединения, но не меняются при восстановлении соединения. Этот механизм повышает безопасность сети и надежность передачи данных.

➢ Реализация STRP-VLAN-Based режима

STRP-VLAN-Based кольца позволяют пересылать пакеты из разных VLAN по разным путям. Каждый путь пересылки для VLAN формирует STRP-VLAN-Based протокол. Разные STRP-VLAN-Based кольца могут иметь разные корни (root).

Как показано на рисунке далее, сконфигурировано два STRP-VLAN-Based кольца:

Кольцевое соединение STRP-VLAN10/20-Based: AB-BC-CD-DE-EA;

Кольцевое соединение STRP-VLAN30-Based: FB-BC-CD-DE-EF.

Эти два кольца имеют tangent соединения BC, CD и DE. Коммутатор C и коммутатор D используют одни и те же порты в двух кольцах, но используют разные логические соединения на основе VLAN.

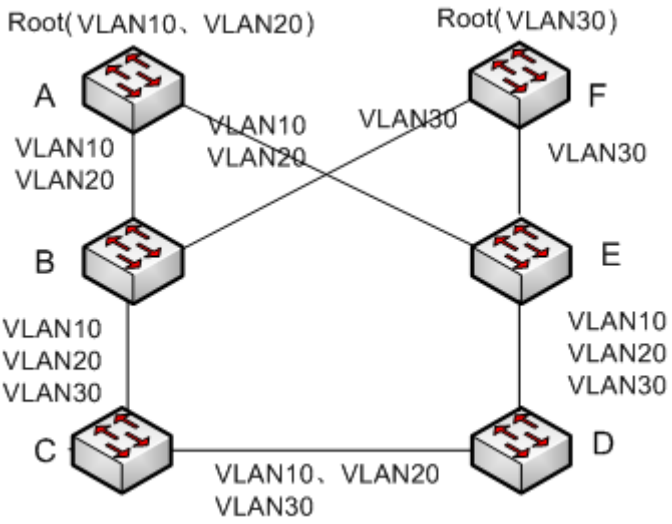


Рис. 114. STRP-VLAN-Based кольцевые соединения

Статус порта и назначение ролей для каждого STRP-VLAN-Based кольца такие же, как и для кольца на основе STRP-Port-Based порта.

- STRP резервирование двух колец

STRP может обеспечить резервирование для двух STRP колец, предотвращая образование петель между кольцами.

Backup port: указывает порт связи между кольцами STRP. Можно настроить несколько резервных портов, но они должны находиться в одном кольце. Первый подключаемый резервный порт (backup) - это ведущий резервный порт (master backup), который находится в состоянии передачи (forwarding). Все остальные резервные порты являются подчиненными (slave backup). Они находятся в блокирующем (blocking) состоянии.

Как показано на рисунке далее, на каждом коммутаторе можно настроить один резервный (backup) порт. Ведущий резервный (master backup) порт находится в состоянии forwarding, а другие резервные (backup) порты - в состоянии блокировки (blocking). Если ведущий резервный (master backup) порт или его соединение неисправны, для пересылки данных будет выбран подчиненный резервный (slave backup) порт.

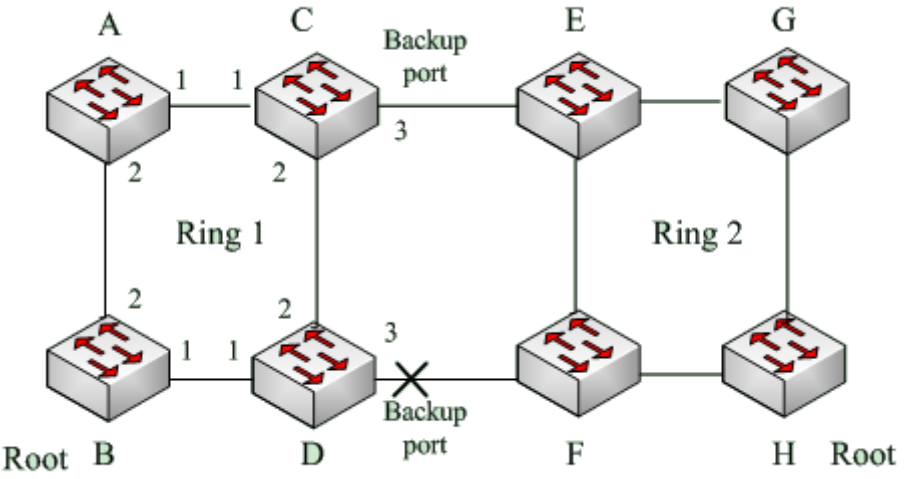


Рис. 115. Резервирование STRP

Изменение статуса соединения влияет на состояние резервных (backup) портов.

7.5.3 DHP

7.5.3.1 Введение

Как показано на рисунке далее, коммутаторы DHP A, B, C, и D соединены в кольцо. Протокол Dual Homing Protocol (DHP) обеспечивает следующие функции:

- Коммутаторы A, B, C и D могут взаимодействовать друг с другом, не влияя на правильную работу устройств в кольце;
- В случае обрыва связи между A и B, то A может взаимодействовать с B, C и D посредством коммутаторов Device 1 и Device 2.

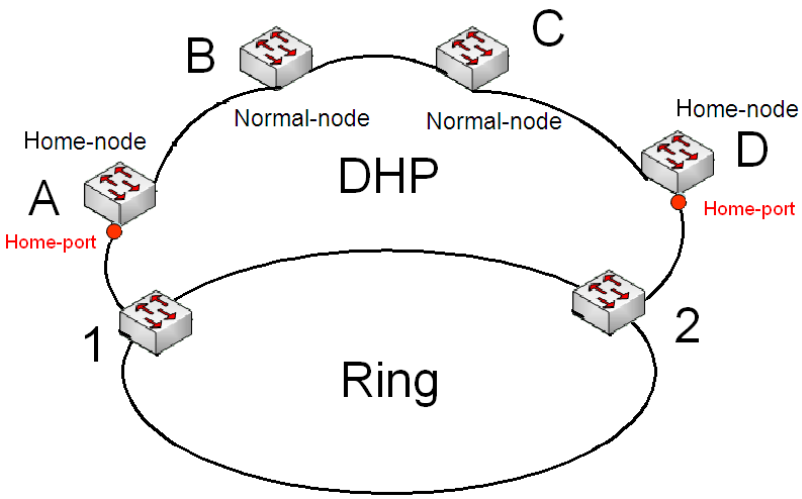


Рис. 116. Применение DHP протокола

7.5.3.2 Реализация DHP

Реализация DHP основана на протоколе STRP. Механизм выбора и назначения ролей в DHP такой же, как и в STRP. DHP обеспечивает резервирование канала связи с помощью конфигурации домашнего узла (Home-node), стандартного узла (Normal-node) и домашнего порта (Home-port).

Home-node: указывает устройства на обоих концах DHP-канала и завершает передачу пакетов STRP.

Home-port: указывает порт, соединяющий Home node с внешней сетью. Home-port обеспечивает следующие функции:

- Отправка ответных пакетов в Root после получения пакетов Announce от Root. Root идентифицирует статус кольца как замкнутое, если он получает ответные (response) пакеты. Если Root не получает ответных пакетов, он определяет статус кольца как разомкнутое.
- Блокирование STRP-пакетов внешних сетей и изоляция DHP-канала от внешних сетей.
- Отправка пакетов для очистки записей (entry clearing packets) подключенным устройствам во внешних сетях при изменении топологии DHP-канала.

Normal-node: указывает устройства в канале DHP, исключая устройства на обоих концах. Normal-node узлы передают ответные пакеты от Home-nodes.

7.5.3.3 Реализация

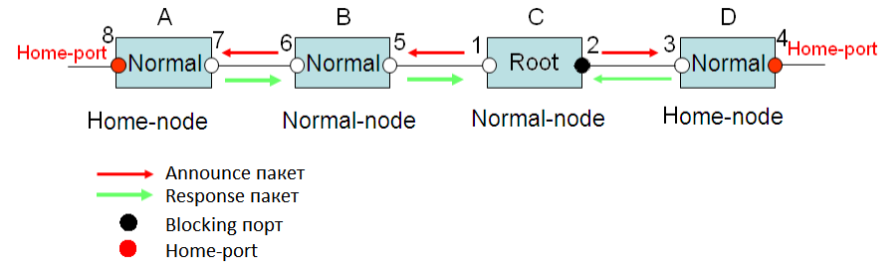


Рис. 117. Конфигурация DHP

Коммутаторы A, B, C и D подключены согласно рис. 116, 117. Конфигурация коммутаторов следующая:

- Конфигурация STRP: коммутатор C настроен как Root; порт 2 находится в состоянии blocking; коммутаторы A, B и D настроены как Normal; все остальные кольцевые порты находятся в состоянии forwarding;
- Конфигурация DHP: коммутаторы A и D настроены как Home-node; порт 8 и порт 4 - Home-port; коммутаторы B и C настроены как Normal-node.

Реализация:

1. Коммутатор C, настроен как Root, отправляет пакеты Announce через два своих кольцевых порта. Home-port 8 и Home-port 4 завершают прием пакетов Announce и отправляют ответные (response) пакеты на коммутатор C. Коммутатор C определяет статус кольца как замкнуты. Порт 2 находится в состоянии блокировки (blocking).

2. Когда соединение между коммутаторами A и B разорвано, топология включает в себя два соединения: A и B-C-D.

- Коммутатор A выбирается в качестве Root. Порт 7 находится в состоянии blocking.
- В группе коммутаторов B-C-D в качестве корневого выбирается B. Порт 6 находится в состоянии блокировки (blocking). Коммутатор C становится Normal. Порт 2 находится в состоянии передачи (forwarding). Коммутатор A может взаимодействовать с B, C и D посредством коммутаторов Device 1 и

Device 2. Принцип работы показан на рисунке далее.

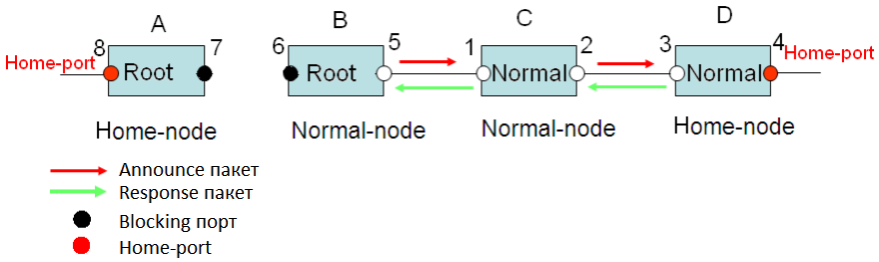


Рис. 118. Работа DHP при обрыве

7.5.3.4 Принцип работы

При конфигурации STRP необходимо выполнять следующие условия:

- Все коммутаторы в одном кольце должны иметь одинаковый domain number.
- Одно кольцо содержит только один коммутатор Root, но может содержать несколько B-Roots или Normal коммутаторов.
- На каждом коммутаторе можно настроить только два порта для одного кольца.
- Для двух подключенных колец резервные (backup) порты могут быть настроены только в одном кольце.
- В одном кольце можно настроить несколько резервных (backup) портов.
- На коммутаторе только один резервный (backup) порт можно настроить для определенного кольца.

7.5.3.5 Web конфигурация STRP

1. Выбор режима резервирования STRP показано на рисунке далее.

[Home] → [Function Management] → [Redundancy] → [STRP]

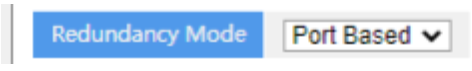


Рис. 119. Режим работы STRP на коммутаторе

Redundancy Mode

Варианты конфигурации: Port Based/Vlan Based

Конфигурация по умолчанию: Port Based

Функция: Выбор режима работы STRP

- К кольцевым протоколам на основе портов (Port-based) относятся RSTP, ST-Ring-Port и STRP-Port, а к кольцевым протоколам на основе VLAN (VLAN-based) относятся MSTP, ST-Ring-VLAN и STRP-VLAN.
- VLAN-based кольцевые протоколы являются взаимоисключающими, и только один тип VLAN-based протокола может быть настроен на одном устройстве.
- Port-based протоколы и VLAN-based протоколы являются взаимоисключающими, и для одного устройства можно выбрать только один режим кольцевого протокола.

2. Настройка STRP-Port-Based и STRP-VLAN-Based протоколов показано на рисунках далее.

Рис. 120. Конфигурация STRP-Port-Based

Рис. 121. Конфигурация STRP-VLAN-Based

Domain ID

Диапазон: 1~32

Функция: Каждое кольцо имеет уникальный идентификатор домена (Domain ID). Один коммутатор поддерживает максимум 8 колец на базе VLAN, количество колец на основе портов зависит от количества портов коммутатора.

Domain Name

Диапазон: 1~31 символов

Функция: Настройка имени домена (Domain Name).

Ring Port-1/Ring Port-2

Варианты конфигурации: все порты коммутатора

Функция: выберите два кольцевых порта.

- Конфигурация кольцевого порта STRP и конфигурации резервного порта (backup port) являются взаимоисключающими с агрегацией портов.
- Кольцевые протоколы на основе портов RSTP, ST-Ring-Port и STRP-Port являются взаимоисключающими.
- Не настраивать порты в группе изоляции одновременно как порты кольца STRP и резервные (backup) порты.

Primary Port

Варианты конфигурации: --/Ring Port-1/Ring Port-2

Конфигурация по умолчанию: --

Функция: Настройте основной (primary) порт. Когда кольцо замкнуто, основной порт корневого узла (root) находится в состоянии передачи (forwarding).

DHP Mode

Варианты конфигурации: Disable /Normal-Node/Home-Node

Конфигурация по умолчанию: Disable

Функция: Отключить режим DHP. Или настроить режим DHP.

DHP Home Port

Варианты конфигурации: Ring-Port-1/Ring-Port-2/Ring-Port-1-2

Функция: Настройте Home-port для Home-node протокола DHP.

Описание: Если в канале DHP имеется только одно устройство, оба кольцевых порта для Home-node должны быть настроены как Home-port.

CRC Threshold

Диапазон: 25~65535

Конфигурация по умолчанию: 100

Функция: Настройка порога срабатывания CRC.

Описание: Этот параметр используется при выборе root . Система подсчитывает количество полученных CRC. Если количество CRC одного кольцевого порта превышает пороговое значение, система считает, что порт имеет CRC degradation. В

результате значение CRC degradation устанавливается равным 1 в векторе пакета Announce порта.

Role Priority

Диапазон: 0~255

Конфигурация по умолчанию: 128

Функция: Параметр устанавливает значение приоритета для протокола STRP.

Backup Port

Варианты конфигурации: Все порты коммутатора.

Функция: Выбор резервного (backup) порта.

Выберите резервный (backup) порт, отличный от кольцевого порта.

VLAN List

Варианты конфигурации: все созданные VLAN

Функция: Выберите VLAN для работы по протоколу STRP-VLAN-Based

Protocol Vlan ID

Диапазон: 1~4093

Описание: Идентификатор VLAN следует выбрать из приведенного выше списка VLAN ID.

Функция: Пакеты STRP с VLAN ID служат основой для диагностики и обслуживания кольца на основе STRP-VLAN.

Protocol Enable

Варианты конфигурации: Enable / Disable

Функция: Включение STRP протокола для указанного домена.

3. Конфигурация STRP:

All	Domain ID	Domain Name	Ring Port-1	Ring Port-2	Primary Port	DHP Mode	DHP Home Port	CRC Threshold	Role Priority	Backup Port	Vlan List	Protocol Vlan ID	Protocol Enable	
			1	1	---	Disable	---	100	128	---				
	1	bbb	1	2	Ring Port-1	Normal-Node	---	100	128	---	1	1	Disable	Details

Рис. 122. Конфигурация STRP

Выберите запись STRP, нажмите <Modify>, чтобы изменить конфигурацию записи STRP; нажмите <Delete>, чтобы удалить назначенную запись STRP.

4. Out-Home-Port конфигурация.

Рис. 123. Конфигурация Out-Home-Port

Port

Диапазон: Все порты коммутатора.

Функция: Когда порт DHP включен, кольцо, образованное нисходящей линией связи (down-link) и основным кольцом (main ring), будет находиться в состоянии замкнутого кольца ring-close, обеспечивая нормальную связь между всеми устройствами.

5. Нажмите <Details> для записи STRP для просмотра статуса коммутатора в кольце STRP ring.

[Home] → [Function Management] → [Redundancy] → [STRP] → [STRP Information]

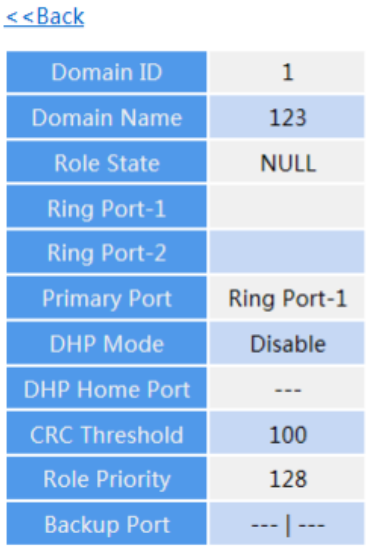


Рис. 124. Состояние STRP

7.5.3.6 Пример конфигурации

Коммутаторы A, B, C, и D включены в кольцо Ring 1; коммутаторы E, F, G, и H включены в кольцо Ring 2; CE и DF - это резервированные соединения (backup links) между Ring 1 и Ring 2. Пример показан на рис. 115.

Конфигурация коммутаторов A, B:

1. Установите Domain ID равным 1, Domain name a. Выберите кольцевой порт 1 и кольцевой порт 2. Сохраните значения по умолчанию для role priority и backup port. Пример настройки показан на рис. 120.

Конфигурация коммутаторов C, D:

2. Установите Domain ID равным 1, Domain name a, порт backup port выберите 3. Выберите кольцевой порт 1 и кольцевой порт 2. Сохраните значения по умолчанию для role priority. Пример настройки показан на рис. 120.

Конфигурация коммутаторов E, F, G, H:

3. Установите Domain ID равным 2, Domain name b. Выберите кольцевой порт 1 и кольцевой порт 2. Сохраните значения по умолчанию для role priority и backup port. Пример настройки показан на рис. 120.

7.5.4 Протокол RSTP/STP

7.5.4.1 Введение

Spanning Tree Protocol (STP), основанный на стандарте IEEE802.1D, - это протокол локальной сети, используемый для предотвращения широковещательных штормов, вызванных образованием петель, и предназначен для обеспечения резервного соединения каналов. Устройства с поддержкой STP обмениваются пакетами и блокируют определенные порты, чтобы преобразовать «петли» в «деревья», предотвращая распространение бесконечных петель. Недостаток STP заключается в том, что порт должен ждать задержку пересылки forwarding delay, чтобы перейти в состояние пересылки (forwarding).

Чтобы преодолеть этот недостаток, IEEE создает стандарт 802.1w в дополнение к

802.1D. IEEE802.1w определяет Rapid Spanning Tree Protocol (RSTP). По сравнению с STP, RSTP обеспечивает гораздо более быструю конвергенцию за счет добавления альтернативного (alternate) порта и резервного (backup) порта для корневого (root) порта и назначенного (designated) порта соответственно. Если корневой (root) порт недействителен, альтернативный (alternate) порт может быстро перейти в состояние пересылки (forwarding).

7.5.4.2 Принцип работы

Корневой мост (Root bridge): служит корнем для дерева. Сеть имеет только один корневой мост. Корневой мост меняется в зависимости от топологии сети. Корневой мост периодически отправляет BPDU другим устройствам, которые пересылают BPDU для обеспечения стабильности топологии.

Корневой порт (Root port) : указывает наилучший порт для передачи данных с некорневых мостов (non-root bridges) на корневой мост (root bridge). Лучший порт - это порт с наименьшими затратами для корневого моста. Некорневой мост взаимодействует с корневым мостом через корневой порт. Некорневой мост имеет только один корневой порт. Корневой мост не имеет корневого порта.

Назначенный порт (designated): указывает порт для пересылки BPDU на другие устройства или локальные сети. Все порты на корневом мосту являются назначенными портами.

Альтернативный (alternate) порт: указывает резервный порт корневого порта. Если корневой порт выходит из строя, альтернативный порт становится новым корневым портом.

Резервный (backup) порт: указывает резервный порт назначенного порта. Когда назначенный порт выходит из строя, резервный порт становится новым назначенным портом и пересылает данные.

7.5.4.3 BPDU сообщения

Чтобы предотвратить образование петель, все мосты локальной сети

рассчитывают связующее дерево. Процесс расчета включает передачу BPDU между устройствами для определения топологии сети. В таблице 6 показана структура данных BPDU.

Таблица 6. Сообщение BPDU

...	Root bridge ID	Root path cost	Designated bridge ID	Designated port ID	Message age	Max age	Hello time	Forward delay	...
...	8 байт	4 байта	8 байт	2 байта	2 байта	2 байта	2 байта	2 байта	...

Root bridge ID: приоритет корневого моста (2 байта) + MAC-адрес корневого моста (6 байт);

Root path cost: стоимость пути к корневому мосту；

Designated bridge ID: приоритет назначенного моста (2 байта) + MAC-адрес назначенного моста (6 байт);

Designated port ID: приоритет порта+номер порта;

Message age: продолжительность времени, в течение которой BPDU может быть распространен в сети;

Max age：максимальная продолжительность времени, в течение которой BPDU может храниться на устройстве. Когда Message age больше Max age, BPDU отбрасывается;

Hello time: интервал отправки BPDU;

Forward delay: задержка смены статуса (discarding--learning или learning--forwarding).

7.5.4.4 Реализация протокола

Процесс вычисления связующего дерева для всех мостов с помощью BPDU выглядит следующим образом:

1. На начальном этапе каждый порт всех устройств генерирует BPDU с самим собой в качестве корневого моста (root bridge); как ID корневого моста, так и

назначенный ID моста являются идентификатором локального устройства; стоимость корневого пути (Root path cost) равна 0; назначенный (designated) порт является локальным портом.

2. Лучший выбор BPDU. Все устройства отправляют свои собственные BPDU и получают BPDU от других устройств.

При получении BPDU каждый порт сравнивает полученный BPDU со своим собственным:

- Если приоритет его собственного BPDU выше, то порт не выполняет никаких операций;
- Если приоритет полученного BPDU выше, то порт заменяет локальный BPDU на полученный.

Устройства сравнивают BPDU всех портов и определяют наилучший BPDU.

Принципы сравнения BPDU следующие:

- BPDU с меньшим ID корневого моста имеет более высокий приоритет;
- Если ID корневого моста двух BPDU совпадают, сравниваются затраты на их корневой путь. Если стоимость корневого пути в BPDU плюс стоимость пути к локальному порте меньше, то приоритет BPDU выше;
- Если стоимость корневого пути для двух BPDU также одинакова, ID назначенного моста, ID назначенного порта и ID порта, принимающего BPDU, дополнительно сравниваются по порядку. BPDU с меньшим идентификатором имеет более высокий приоритет. BPDU с меньшим ID корневого моста имеет более высокий приоритет.

3. Выбор корневого моста. Корневой мост (root bridge) связующего дерева - это мост с наименьшим ID моста.

4. Выбор корневого порта. Устройство, не являющееся корневым мостом, выбирает порт, принимающий наилучший BPDU, в качестве корневого порта (root port).

5. Расчет BPDU для назначенного (designated) порта. Основываясь на BPDU корневого порта и стоимости пути к корневому порту, устройство вычисляет BPDU

назначенного порта для каждого порта следующим образом:

- ID корневого моста заменяется ID корневого моста BPDU корневого порта;
- стоимость корневого пути заменяется стоимостью корневого пути корневого порта BPDU плюс стоимость пути корневого порта;
- назначенный ID моста заменяется ID локального устройства;
- назначенный ID порта заменяется ID локального порта.

6. Выбор назначенного (designated) порта. Если вычисленный BPDU лучше, то устройство выбирает порт в качестве назначенного, заменяет порт BPDU на вычисленный BPDU и отправляет вычисленный BPDU. Если порт BPDU лучше, то устройство не обновляет порт BPDU и блокирует порт. Заблокированные порты (blocked) могут принимать и пересылать только пакеты RSTP, но не другие пакеты.

7.5.4.5 Web конфигурация

Настройка параметров моста STP/RSTP.

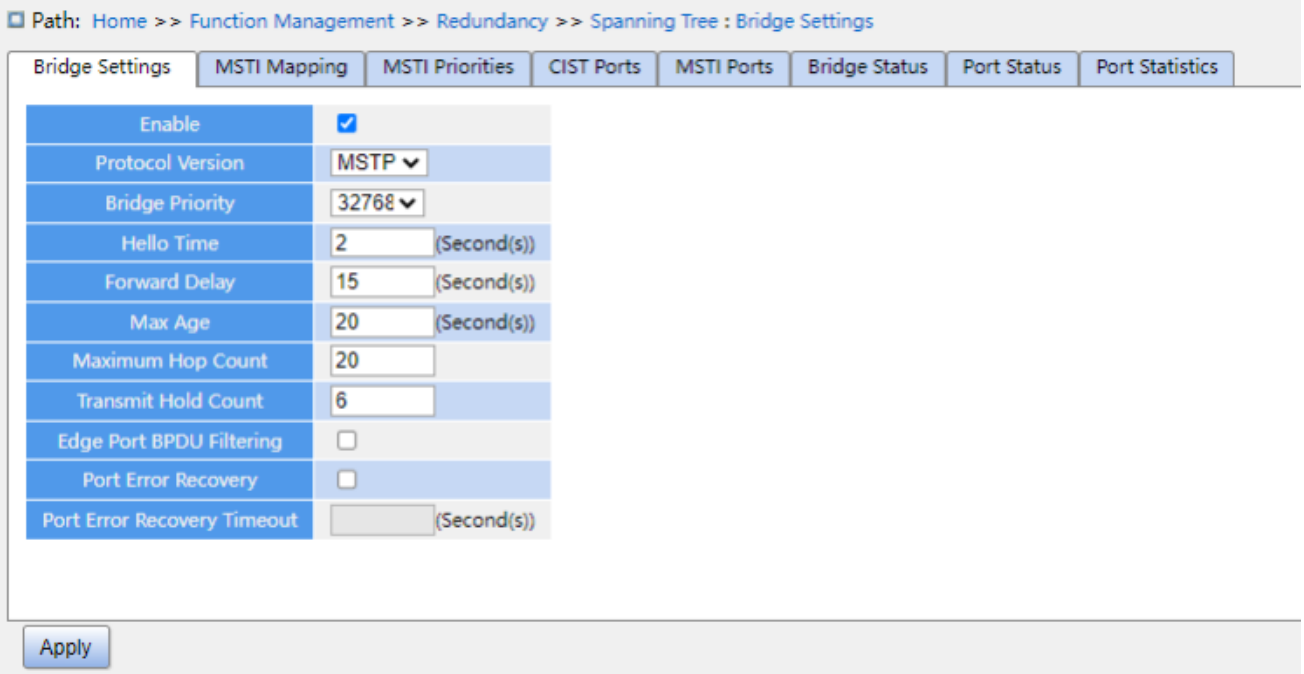


Рис. 125. Настройка параметров моста RSTP/STP

Global Configuration

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение или выключение протоколов связующего дерева (ST).

- Кольцевые протоколы на основе портов включают RSTP, а кольцевые протоколы на основе VLAN включают MSTP и STRP-VLAN;
- Кольцевой протокол на основе порта и кольцевой протокол на основе VLAN являются взаимоисключающими, и для одного устройства может быть выбран только один режим кольцевого протокола.

Protocol Priority

Варианты конфигурации: MSTP/RSTP/STP

Конфигурация по умолчанию: MSTP

Функция: Выбор протокола связующего дерева (ST).

Brigde Priority

Диапазон: 0~61440, Шаг 4096

Конфигурация по умолчанию: 32768

Функция: Настройка приоритета сетевого моста.

Описание: Приоритет используется для выбора корневого моста. Чем меньше значение, тем выше приоритет.

Hello Time

Диапазон: 1~10 сек.

Конфигурация по умолчанию: 2 сек.

Функция: Настройте интервал для отправки BPDU.

Forward Delay

Диапазон: 4~30 сек.

Конфигурация по умолчанию: 15 сек.

Функция: Настройте время изменения статуса с Discarding на Learning или с Learning на Forwarding.

Max Age

Диапазон: 6~40 сек.

Конфигурация по умолчанию: 20 сек.

Функция: Максимальная продолжительность, в течение которой BPDU может быть сохранен на устройстве.

Описание: Если значение message age в BPDU больше указанного значения, то BPDU отбрасывается.

- Значения Forward Delay Time, Hello Time и Max Age Time должны соответствовать следующим требованиям: 2*(Forward Delay Time – 1,0 сек.) >= Max Age Time; Max Age Time >= 2*(Hello Time + 1,0 сек.);
- Рекомендуется использовать настройку по умолчанию.

Maximum Hop Count

Диапазон: 6~40

Конфигурация по умолчанию: 20

Функция: Максимальное количество прыжков в регионе MST ограничивает размер региона MST. Максимальное количество прыжков, настроенное в корне региона, используется как максимальное количество прыжков в регионе MST.

Описание: Начиная с корневого моста связующего дерева в домене MST, каждый раз, когда устройство пересылает сообщение конфигурации в домене, количество переходов уменьшается на 1, и устройство отбрасывает полученное сообщение конфигурации с количеством переходов 0.

- Конфигурация максимального количества переходов действительна для устройства корневого моста в домене MST. Устройства некорневого моста используют конфигурацию корневого моста;
- Рекомендуется использовать настройку по умолчанию.

Transmit Hold Count

Диапазон: 1~10

Конфигурация по умолчанию: 6

Функция: Установите максимальное количество пакетов BPDU, которые могут быть отправлены портом в течение каждого Hello Time.

Edge Port BPDU Filtering

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение/ выключение пересылки пакетов BPDU для пограничного порта.

Port Error Recovery

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Определяет, может ли порт автоматически восстановиться из состояния ошибки в нормальное состояние.

Port Error Recovery Timeout

Диапазон: 30~86400 сек.

Функция: Установите время восстановления порта из состояния ошибки в нормальное состояние.

2. Настройка порта RSTP.

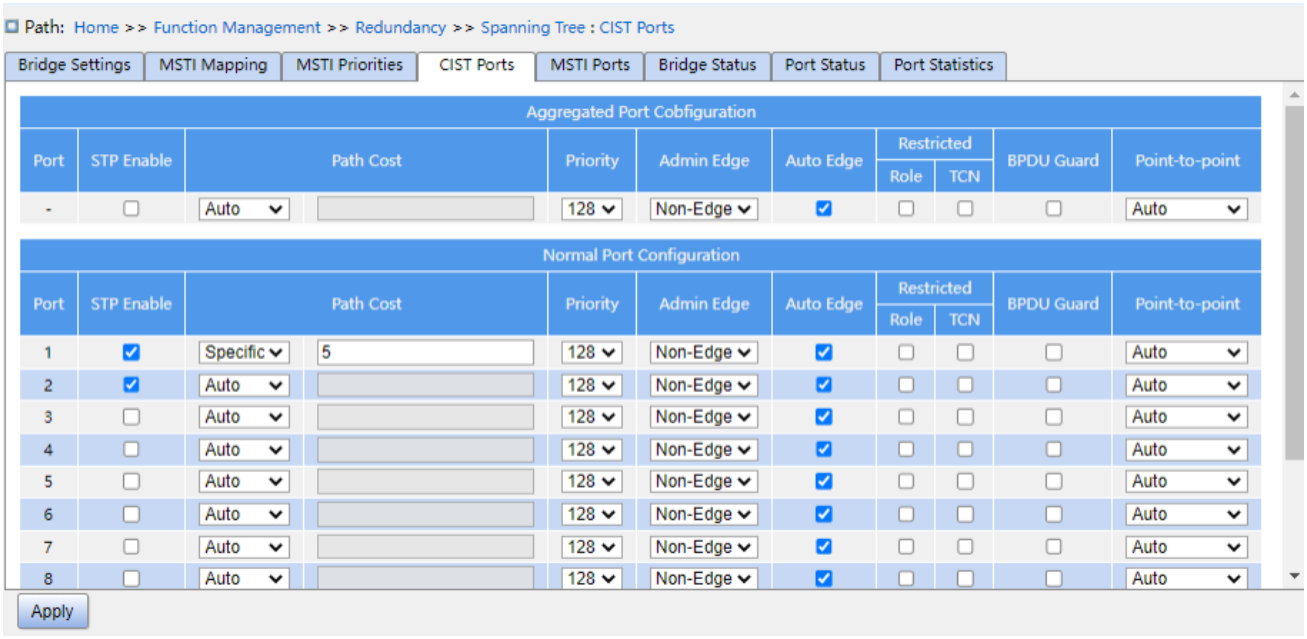


Рис. 126. Настройка RSTP порта

CIST Ports

Функция: Используйте группу агрегации в качестве порта CIST и настройте стоимость и приоритет ее пути в указанном экземпляре.

STP Enabled

Варианты конфигурации: Enable/ Disable

Конфигурация по умолчанию: Disable

Функция: Включите или отключите STP/RSTP на портах.

- Порты RSTP и агрегация портов являются взаимоисключающими;
- Кольцевые порты между кольцевыми протоколами RSTP и STRP являются взаимоисключающими;

- Рекомендуется не настраивать порты в одной группе изоляции одновременно с портами RSTP; не добавляйте порты RSTP в одну группу изоляции.

Path Cost

Варианты конфигурации: Auto/Specific（1~200000000）

Конфигурация по умолчанию: Auto

Функция: Настройте стоимость пути порта.

Описание: Стоимость пути к порту используется для расчета оптимального пути. Этот параметр зависит от пропускной способности. Чем больше пропускная способность, тем ниже стоимость. Изменяя стоимость пути к порту, вы можете изменить путь передачи от текущего устройства к корневому мосту, тем самым изменив роль порта.

Priority

Диапазон: 0~240, шаг изменения 16

Конфигурация по умолчанию: 128

Функция: Настройте приоритет порта, который определяет роли портов.

Admin Edge

Варианты конфигурации: Non-Edge/Edge

Конфигурация по умолчанию: Non-Edge

Функция: Установите, является ли текущий порт пограничным (Edge) портом.

Описание: Если порт напрямую подключен к терминалу и не подключен к другим устройствам или общему сегменту сети, порт считается пограничным (edge) портом. Пограничный порт может быстро перейти из состояния blocking в состояние forwarding без задержки ожидания. После того, как пограничный порт получает пакеты BPDU, он становится не-пограничным (non-edge) портом.

Restricted Role

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Порт с ограниченным доступом никогда не будет выбран в качестве корневого узла, даже если ему присвоен наивысший приоритет.

Restricted TCN

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Порт с ограниченным TCN не будет активно отправлять сообщения TCN.

BPDU Guard

Варианты конфигурации: Enable/ Disable

Конфигурация по умолчанию: Disable

Функция: Контролировать, переходит ли пограничный порт в состояние Error-Disable и отключается ли он при получении пакетов BPDU.

Point-to-point

Варианты конфигурации: Auto/Forced True/Forced False

Конфигурация по умолчанию: Auto

Функция: Установите тип соединения для порта. Если порт подключен как «точка-точка» (point-to-point), порт может быстро перейти в другое состояние.

Описание: Auto означает, что коммутатор автоматически определяет подключения на основе дуплексного статуса порта. Когда порт находится в полнодуплексном режиме, коммутатор считает, что тип подключения является "точка-точка"; когда порт находится в полудуплексном режиме, коммутатор считает, что тип подключения является общим. Принудительный выбор (Forced True) "точка-точка" означает, что для подключения выбран тип "точка-точка", а принудительный выбор (Forced False) означает, что выбран общий тип подключения.

7.5.4.6 Пример конфигурации

Приоритеты коммутаторов A, B и C равны 0, 4096 и 8192. Стоимость пути (path cost) для соединений составляет 4, 5 и 10. Подключение показано на рисунке далее.

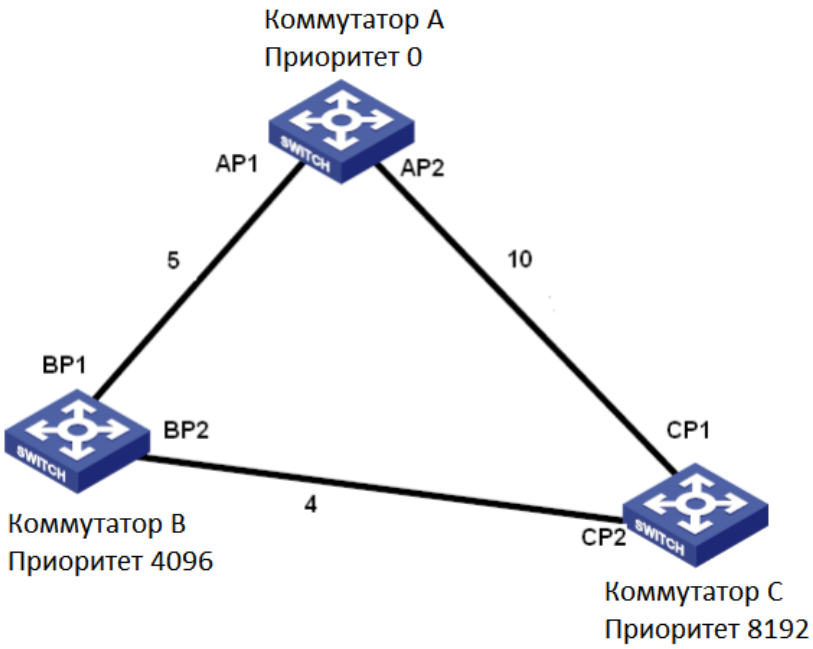


Рис. 127. Пример конфигурации RSTP

Конфигурация коммутатора A:

1. Установите bridge priority равным 0, остальные параметры оставить по умолчанию. Настройка параметров показана на рис. 125.

2. Установите path cost порта 1 равным 5, path cost для порта 2 равным 10. Настройка параметров показана на рис. 126.

Конфигурация коммутатора B:

1. Установите bridge priority равным 4096, остальные параметры оставить по умолчанию. Настройка параметров показана на рис. 125.

2. Установите path cost порта 1 равным 5, path cost для порта 2 равным 4. Настройка параметров показана на рис. 126.

Конфигурация коммутатора C:

1. Установите bridge priority равным 8192, остальные параметры оставить по умолчанию. Настройка параметров показана на рис. 125.

2. Установите path cost порта 1 равным 10, path cost для порта 2 равным 4. Настройка параметров показана на рис. 126.

- Приоритет коммутатора A равен 0, его корневой ID (root ID) является

наименьшим. Следовательно, коммутатор A является корневым мостом (root bridge).

- Стоимость пути от AP1 до BP1 равна 5, а от AP2 до BP2 равна 14. Следовательно, BP1 является корневым портом (root port).
- Стоимость пути от AP1 до CP2 равна 9, а от AP2 до CP1 равна 10. Следовательно, CP2 является корневым портом (root port), а BP2 является назначенным портом (designated port).

7.5.5 MSTP

7.5.5.1 Введение

Хотя RSTP обеспечивает быструю конвергенцию, он также, как и STP, имеет следующий недостаток: все мосты в локальной сети используют одно связующее дерево, и пакеты всех VLAN пересылаются по связующему дереву. Как показано на рис. 128, определенные конфигурации могут блокировать соединение между Switch A и Switch C. Поскольку Switch B и Switch D не находятся в VLAN 1, они не могут пересылать пакеты VLAN 1. В результате порт VLAN 1 Switch A не может взаимодействовать с портом Switch C.

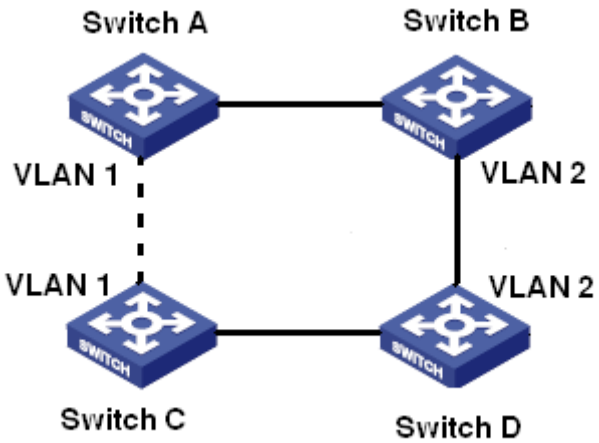


Рис. 128. Недостаток RSTP при работе с VLAN

Чтобы решить эту проблему, был создан Multiple Spanning Tree Protocol (MSTP). Он

обеспечивает как быструю конвергенцию, так и отдельные пути пересылки для трафика различных VLAN, обеспечивая лучший механизм распределения нагрузки для резервированных соединений.

Протокол MSTP сопоставляет одну или несколько сетей VLAN в один экземпляр. Коммутаторы с одинаковой конфигурацией образуют регион. Каждый регион содержит несколько взаимно независимых связующих деревьев. Регион служит узлом коммутатора. Он участвует в вычислениях с другими регионами на основе алгоритма связующего дерева, вычисляя общее связующее дерево. Основываясь на этом алгоритме, сеть на рис. 128 формирует топологию, показанную на рис. 129. Switch A и Switch C находятся в Region1. Ни одно соединение не заблокировано, поскольку регион не содержит петель. То же самое для Region2. Region1 и Region2 аналогичны узлам коммутатора. Эти два "коммутатора" образуют петлю. Следовательно, соединение должно быть заблокировано.

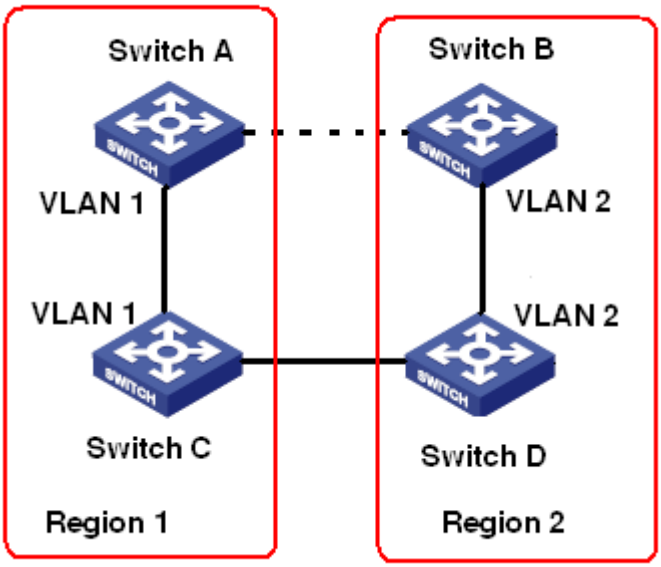


Рис. 129. Топология MSTP

7.5.5.2 Основные понятия

Концепция работы MSTP показана на рис. 130-133.

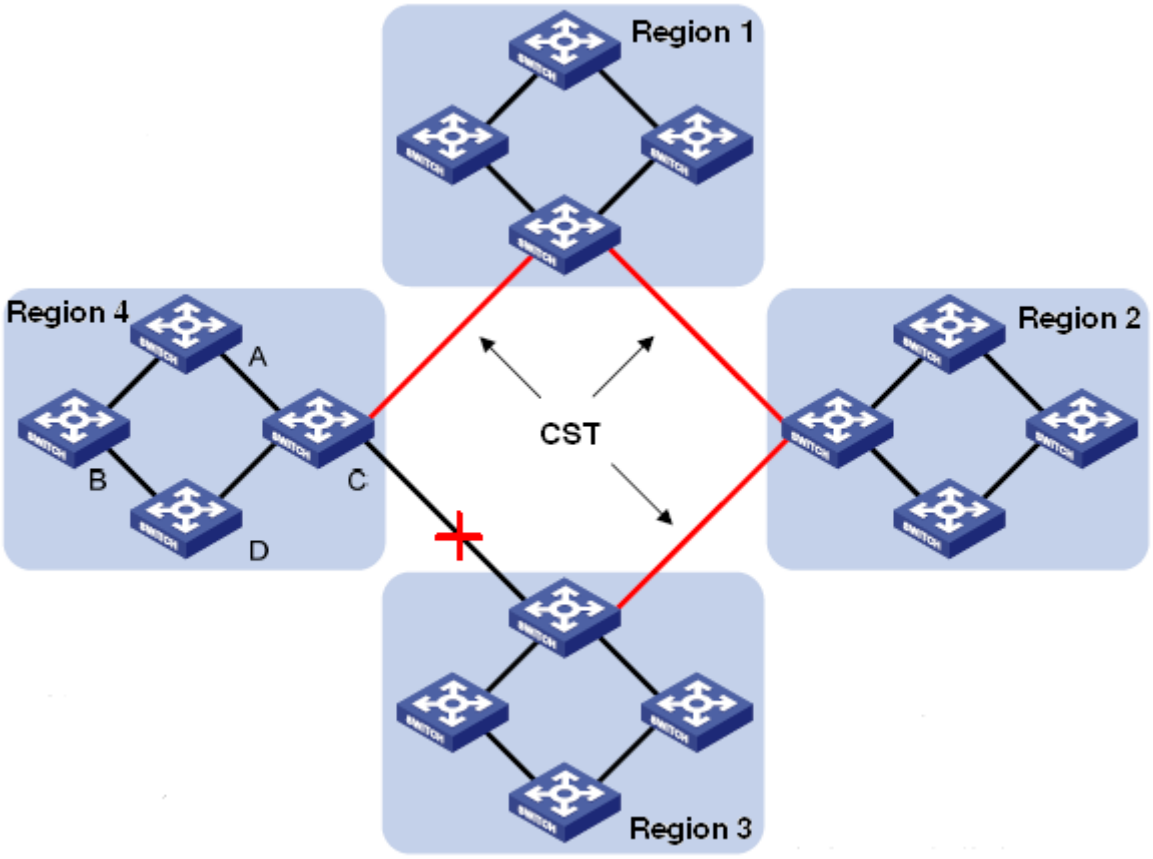


Рис. 130. Концепция MSTP

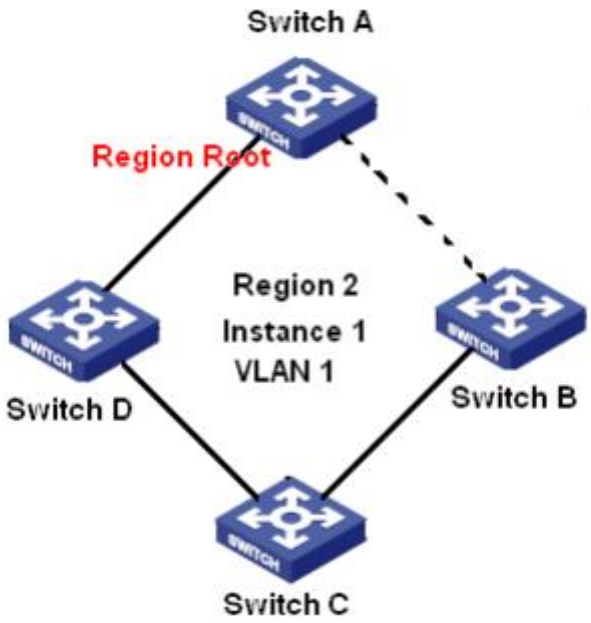


Рис. 131. VLAN1

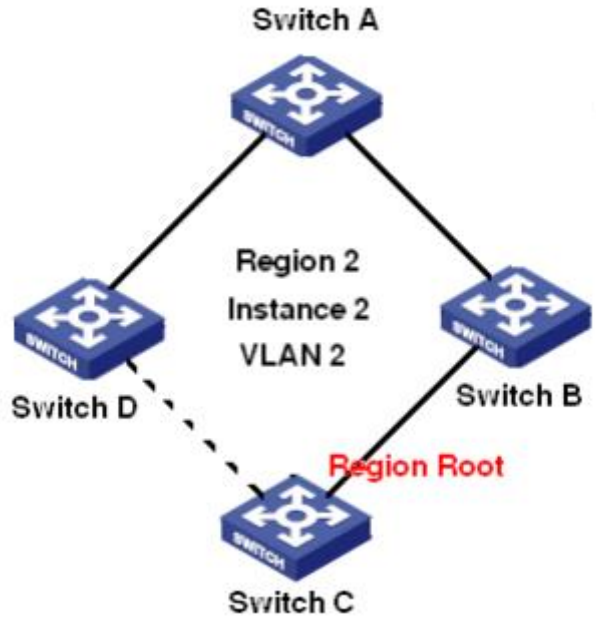


Рис. 132. VLAN 2 сопоставлена с Instance 2

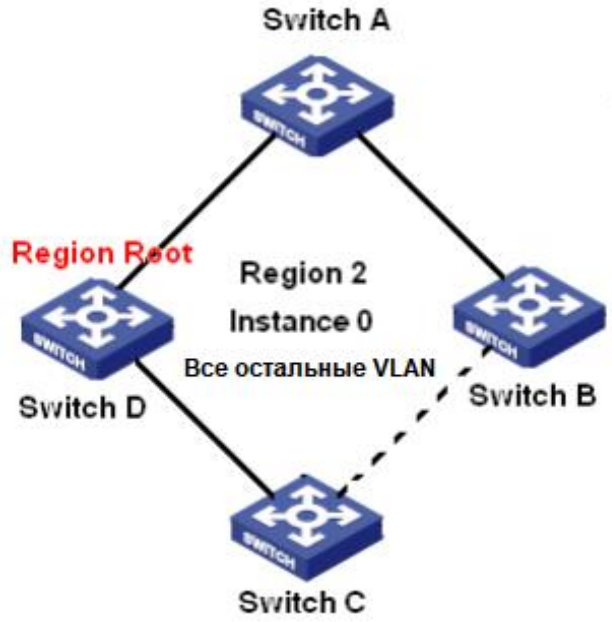


Рис. 133. Остальные VLAN сопоставляются с Instance 0

Экземпляр (instance): коллекция из нескольких VLAN. Одна VLAN (как показано на рис. 131 и рис. 132) или несколько VLAN с одинаковой топологией (как показано на рис. 133) могут быть сопоставлены одному instance; то есть одна VLAN может образовывать связующее дерево, а несколько VLAN могут совместно использовать одно связующее дерево. Разные instance сопоставляются с разными связующими деревьями. Instance 0 является связующим деревом для устройств всех регионов (regions), в то время как

другие instance являются связующими деревьями для устройств определенного региона (region).

Регион MST (MST region): Коммутаторы с одинаковым именем региона MSTP, уровнем ревизии и VLAN-to-instance сопоставлением находятся в одном регионе MST. Как показано на рис. 130, Region1, Region2, Region3 и Region4 - это четыре разных региона MST. Таблица сопоставления (mapping table) VLAN: состоит из сопоставления между VLAN и связующими деревьями. На рис. 131 таблица сопоставления VLAN Region 2 представляет собой сопоставление между VLAN 1 и Instance 1. Как показано на рис. 132, VLAN 2 сопоставлена с Instance 2. Другие VLAN сопоставляются с Instance 0, как показано на рис. 133.

Таблица сопоставления VLAN (VLAN mapping table): состоит из сопоставления между VLAN и связующими деревьями. На рис. 131 таблица сопоставления VLAN региона 2 представляет собой сопоставление между VLAN 1 и instance 1; VLAN 2 сопоставлена с instance 2, как показано на рис. 132. Другие VLAN сопоставляются с instance 0, как показано на рис. 133.

Общее и внутреннее связующее дерево (CIST): указывает instance 0, то есть связующее дерево, охватывающее все устройства в сети. Как показано на рис. Рис. 130 , включает IST и CST.

Внутреннее связующее дерево (IST): указывает CIST сегмент в регионе MST, то есть instance 0 каждого региона, как показано на рис. 133.

Общее связующее дерево (CST): указывает связующее дерево, соединяющее все регионы MST в коммутационной сети. Если каждая область MST является узлом устройства, CST - это связующее дерево, вычисляемое на основе STP/RSTP этими узлами устройства. Как показано на рис. 130, красные линии указывают на связующее дерево.

MSTI (Multiple Spanning Tree Instance): одна область MST может образовывать несколько связующих деревьев, и они независимы друг от друга. Каждое связующее дерево является MSTI, как показано на рис. 131 и 132. IST является специальным MSTI.

Общий корень (Common root): указывает корневой мост CIST. Коммутатор с наименьшим идентификатором корневого моста в сети является common root.

В регионе MST связующие деревья имеют разную топологию, и их региональные корни также могут быть разными. Как показано на рисунках 131, 132 и 133, эти три экземпляра имеют разные региональные корни (region root). Корневой мост MSTI вычисляется на основе STP/RSTP в текущем регионе MST. Корневой мост IST - это устройство, подключенное к другому региону MST и выбранное на основе полученной информации о приоритете.

Граничный порт (Boundary port): указывает порт, который соединяет регион MST с другим регионом MST, работающим регионом STP или работающим регионом RSTP.

Состояние порта (Port state): Порт может находиться в любом из указанных ниже состояний в зависимости от того, запоминает ли он MAC-адреса и перенаправляет ли трафик.

Состояние пересылки (Forwarding state): указывает, что порт запоминает MAC-адреса и перенаправляет трафик.

Состояние обучения (Learning state): указывает, что порт запоминает MAC-адреса, но не пересылает трафик.

Состояние отбрасывания (Discarding state): указывает, что порт не запоминает MAC-адреса и не пересылает трафик.

Корневой порт (Root port): указывает наилучший порт от некорневого моста к корневому мосту, то есть порт с наименьшими затратами для корневого моста. Некорневой мост взаимодействует с корневым мостом через корневой порт. Некорневой мост имеет только один корневой порт. Корневой мост не имеет корневого порта. Корневой порт может находиться в состоянии переадресации, обучения или отбрасывания.

Назначенный порт (Designated port): указывает порт для переадресации BPDU на другие устройства или локальные сети. Все порты на корневом мосту являются назначенными портами. Назначенный порт может находиться в состоянии

переадресации, обучения или отбрасывания.

Главный порт (Master port): указывает порт, который соединяет область MST с общим корнем. Порт находится на кратчайшем пути к общему корню. С точки зрения CST, главный порт является корневым портом региона (как узла). Главный порт является специальным граничным портом. Это корневой порт для CIST и главный порт для других экземпляров. Главный порт может находиться в состоянии переадресации, обучения или отбрасывания.

Альтернативный порт (Alternate port): указывает резервный порт корневого порта или главного порта. Когда корневой порт или главный порт выходит из строя, альтернативный порт становится новым корневым портом или главным портом. Главный порт может находиться только в состоянии discarding.

Резервный порт (Backup port): указывает резервный порт назначенного порта. Когда назначенный порт выходит из строя, резервный порт становится назначенным портом и пересылает данные без какой-либо задержки. Резервный порт может находиться только в состоянии discarding.

7.5.5.3 Реализация MSTP

Протокол MSTP делит сеть на несколько регионов MST. CST рассчитывается между регионами. В регионе вычисляется несколько связующих деревьев. Каждое связующее дерево является MSTI. Экземпляр 0 - это IST, а другие экземпляры - MSTI.

1. Вычисление CIST (Общее и внутреннее связующее дерево)

- Устройство отправляет и принимает пакеты BPDU. На основе сравнения сообщений конфигурации MSTP, устройство с наивысшим приоритетом выбирается в качестве общего корня (common root) CIST;
- IST рассчитывается в каждом регионе MST;
- Каждая область MST рассматривается как единое устройство, а CST вычисляется между регионами;
- CST и IST составляют CIST всей сети.

2. Вычисление MSTI (экземпляр множественного связующего дерева)

В регионе MST MSTP создает различные связующие деревья для VLAN. Каждое связующее дерево вычисляется независимо. Процесс вычисления аналогичен процессу в STP.

В регионе MST пакеты VLAN пересылаются по соответствующему MSTI. Между регионами MST пакеты VLAN пересылаются по CST.

7.5.5.4 Web конфигурация

1. Установка параметров для работы MSTP показана далее.

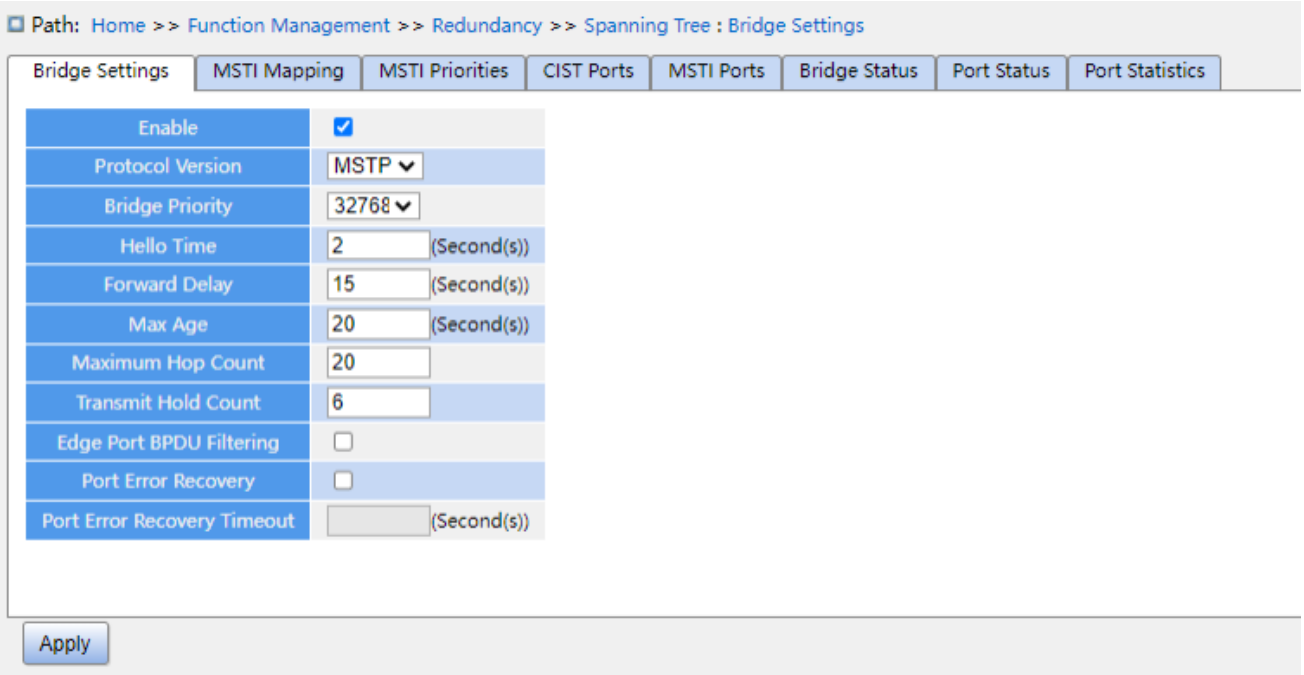


Рис. 134. Настройка Bridge MSTP

Global Configuration

Варианты конфигурации: Disable / Enable

Конфигурация по умолчанию: Disable

Функция: Отключите или включите связующее дерево.

- Кольцевые протоколы на основе портов включают RSTP и STRP-port, а кольцевые протоколы на основе VLAN включают MSTP и STRP-VLAN.
- Кольцевой протокол на основе порта и кольцевой протокол на основе VLAN являются взаимоисключающими, и для одного устройства может быть выбран

только один режим кольцевого протокола.

Protocol Priority

Варианты конфигурации: MSTP/RSTP/STP

Конфигурация по умолчанию: MSTP

Функция: Выберите протокол связующего дерева.

Bridge Priority

Диапазон: 0~61440, шаг настройки 4096

Конфигурация по умолчанию: 32768

Функция: Настройте приоритет сетевого моста (коммутатора).

Описание: Приоритет используется для выбора корневого моста. Чем меньше значение, тем выше приоритет.

Hello Time

Диапазон: 1~10 сек.

Конфигурация по умолчанию: 2 сек.

Функция: Настройте интервал для отправки BPDU сообщений.

Forward Delay

Диапазон: 4~30 сек.

Конфигурация по умолчанию: 15 сек.

Функция: Настройте время изменения статуса с отбрасывания (Discarding) на обучение (Learning) или с обучения (Learning) на пересылку (Forwarding).

Max Age

Диапазон: 6~40 сек.

Конфигурация по умолчанию: 20 сек.

Функция: Максимальная продолжительность, в течение которой BPDU может быть сохранен на устройстве.

Описание: Если значение message age в BPDU больше указанного значения, то BPDU отбрасывается.

- Значения Forward Delay Time, Hello Time и Max Age Time должны соответствовать следующим требованиям: 2*(Forward Delay Time – 1,0 сек.) >= Max Age Time; Max Age Time >= 2*(Hello Time + 1,0 сек.);
- Рекомендуется использовать настройку по умолчанию.

Maximum Hop Count

Диапазон: 6~40

Конфигурация по умолчанию: 20

Функция: Максимальное количество прыжков в регионе MST ограничивает размер региона MST. Максимальное количество прыжков, настроенное в корне региона, используется как максимальное количество прыжков в регионе MST.

Описание: Начиная с корневого моста связующего дерева в домене MST, каждый раз, когда устройство пересылает сообщение конфигурации в домене, количество переходов уменьшается на 1, и устройство отбрасывает полученное сообщение конфигурации с количеством переходов 0.

- Конфигурация максимального количества переходов действительна для устройства корневого моста в домене MST. Устройства некорневого моста используют конфигурацию корневого моста;
- Рекомендуется использовать настройку по умолчанию.

Transmit Hold Count

Диапазон: 1~10

Конфигурация по умолчанию: 6

Функция: Установите максимальное количество пакетов BPDU, которые могут быть отправлены портом в течение каждого Hello Time.

Edge Port BPDU Filtering

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение/ выключение пересылки пакетов BPDU для пограничного порта.

Port Error Recovery

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Определяет, может ли порт автоматически восстановиться из состояния ошибки в нормальное состояние.

Port Error Recovery Timeout

Диапазон: 30~86400 сек.

Функция: Установите время восстановления порта из состояния ошибки в нормальное состояние.

2. Настройка MSTI Mapping показана далее.

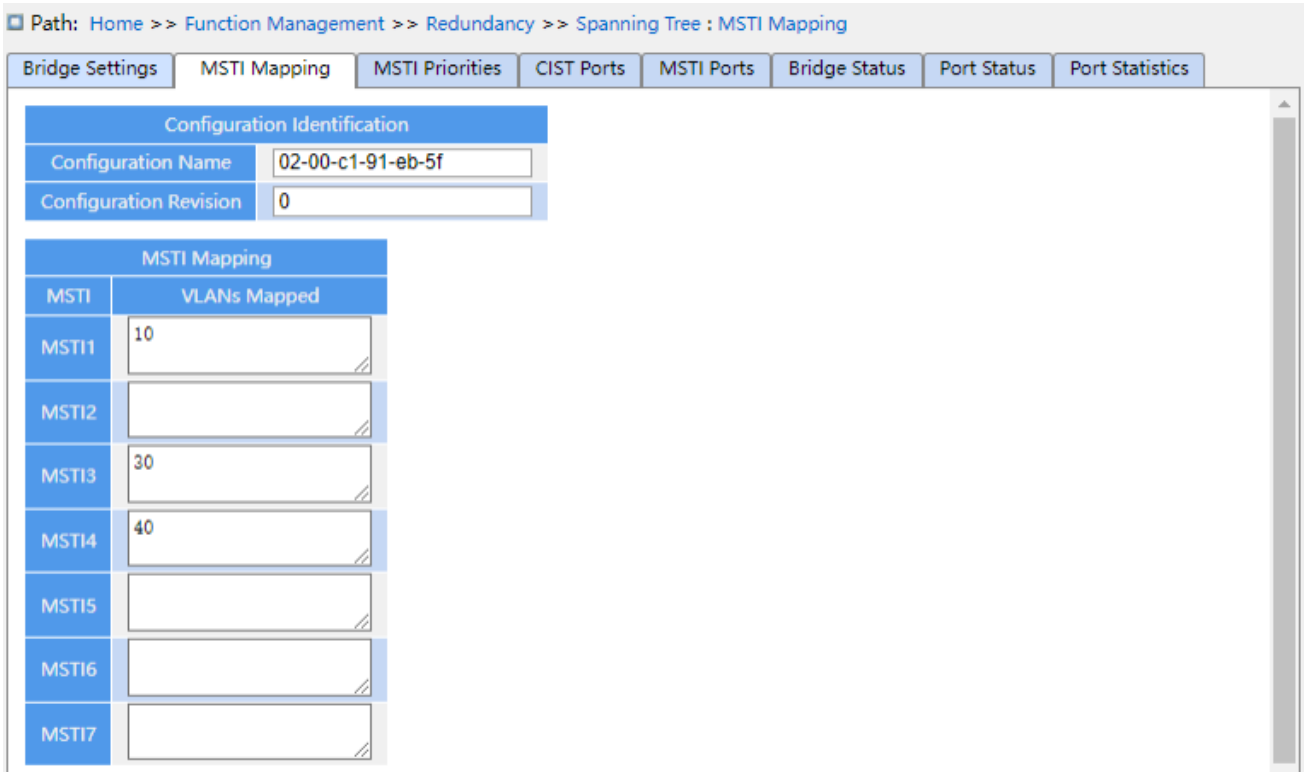


Рис. 135. Настройка MSTP Mapping

Configuration Name

Диапазон: 1~32 символа

Конфигурация по умолчанию: MAC-адрес устройства

Функция: Настройка названия региона MST (MST region).

Configuration Revision

Диапазон: 0~65535

Конфигурация по умолчанию: 0

Функция: Настройте параметр ревизии (revision) региона MSTP.

Описание: Параметр ревизии, имя региона MST и таблица сопоставления VLAN определяют MST region, к которому принадлежит устройство. Когда все конфигурации одинаковы, устройства находятся в одном регионе MST.

VLANs Mapped

Диапазон: 1~4093

Функция: Настройте таблицу сопоставления VLAN в регионе MST. При наличии нескольких VLAN вы можете разделить VLAN запятой (,) и дефисом (-), где дефис используется для разделения двух последовательных VLAN ID, а запятая используется для разделения двух непоследовательных VLAN ID.

Описание: По умолчанию все VLAN сопоставляются с экземпляром instance 0. Одна VLAN сопоставляется только с одним экземпляром связующего дерева. Если VLAN с существующим сопоставлением сопоставляется с другим экземпляром, предыдущее сопоставление отменяется. Если сопоставление между назначенной VLAN и экземпляром удалено, эта VLAN будет сопоставлена instance 0.

3. Настройка MSTI приоритета в указанном экземпляре.

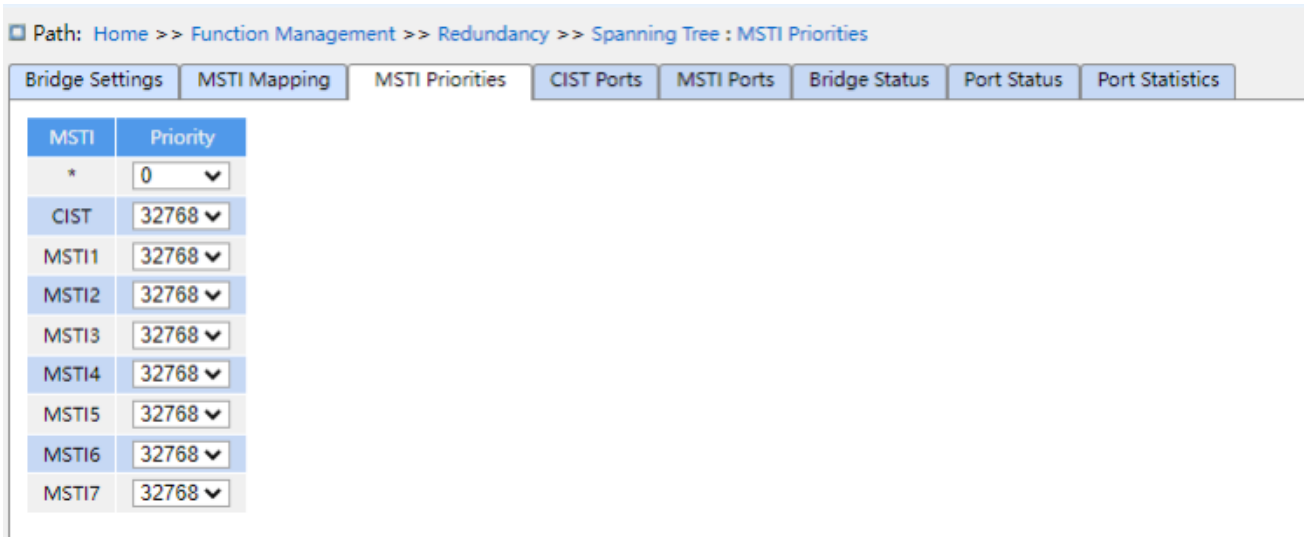


Рис. 136. Настройка MSTI приоритета

Priority

Диапазон: 0~61440, шаг настройки 4096

Конфигурация по умолчанию: 32768

Функция: Настройте приоритет моста коммутатора в указанном экземпляре.

Описание: Приоритет моста определяет, может ли коммутатор быть выбран региональным корнем (regional root) экземпляра связующего дерева. Чем меньше значение, тем выше приоритет. Установив более низкий приоритет, определенное устройство может быть назначено корневым мостом (root bridge) связующего дерева. Устройство MSTP может быть сконфигурировано с разными приоритетами в разных экземплярах связующего дерева.

Нажмите <Apply>, чтобы текущие настройки вступили в силу.

4. Настройка портов CIST показана далее.

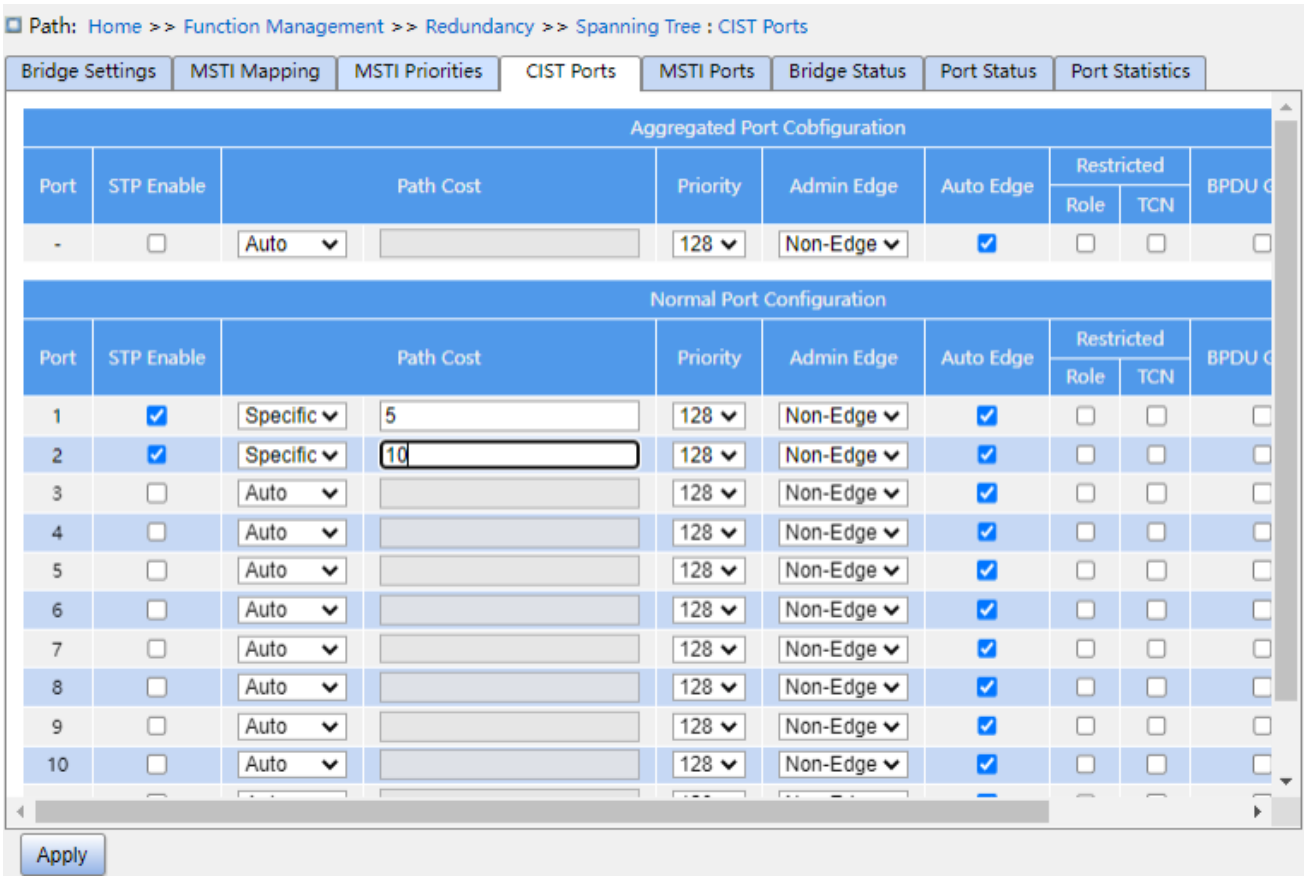


Рис. 137. Настройка портов CIST

CIST Aggregated Port Configuration

Функция: Используйте группу агрегации в качестве порта CIST и настройте ее служебные данные и приоритет в указанном экземпляре.

STP Enable

Варианты конфигурации: Enable/ Disable

Конфигурация по умолчанию: Disable

Функция: Включить или отключить STP/RSTP на портах.

- Поскольку порт MSTP и агрегация портов являются взаимоисключающими, порт MSTP не может быть добавлен в группу агрегации.
- Порты MSTP не следует добавлять в одну и ту же группу изоляции.

Path Cost

Варианты конфигурации: Auto/Specific（1~200000000）

Конфигурация по умолчанию: Auto

Функция: Настройте path cost на путь к порту.

Описание: Стоимость пути (path cost) используется для расчета наилучшего пути. Значение параметра зависит от полосы пропускания. Чем больше значение, тем ниже стоимость. Вы можете изменить роль порта, изменив значение параметра path cost.

Priority

Диапазон: 0~240，шаг настройки 16

Конфигурация по умолчанию: 128

Функция: Настройте приоритет порта, который определяет роль порта.

Admin Edge

Варианты конфигурации: Non-Edge/Edge

Конфигурация по умолчанию: Non-Edge

Функция: Установите, является ли текущий порт пограничным (Edge) портом.

Описание: Если порт напрямую подключен к терминалу и не подключен к другим устройствам или общему сегменту сети, порт считается пограничным (edge) портом. Пограничный порт может быстро перейти из состояния blocking в состояние forwarding без задержки ожидания. После того, как пограничный порт получает пакеты BPDU, он становится не-пограничным (non-edge) портом.

Auto Edge

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Enable

Функция: включение функции автоматического обнаружения пограничного порта.

Restricted Role

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Порт с ограниченным доступом никогда не будет выбран в качестве корневого узла, даже если ему присвоен наивысший приоритет.

Restricted TCN

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Порт с ограниченным TCN не будет активно отправлять сообщения TCN.

BPDU Guard

Варианты конфигурации: Enable/ Disable

Конфигурация по умолчанию: Disable

Функция: Контролировать, переходит ли пограничный порт в состояние Error-Disable и отключается ли он при получении пакетов BPDU.

Point-to-point

Варианты конфигурации: Auto/Forced True/Forced False

Конфигурация по умолчанию: Auto

Функция: Установите тип соединения для порта. Если порт подключен как «точка-точка» (point-to-point), порт может быстро перейти в другое состояние.

Описание: Auto означает, что коммутатор автоматически определяет подключения на основе дуплексного статуса порта. Когда порт находится в полнодуплексном режиме, коммутатор считает, что тип подключения является "точка-точка"; когда порт находится в полудуплексном режиме, коммутатор считает, что тип подключения является общим. Принудительный выбор (Forced True) "точка-точка" означает, что для подключения выбран тип "точка-точка", а принудительный выбор (Forced False) означает, что выбран общий тип подключения.

5. Настройка портов MSTI показана далее.

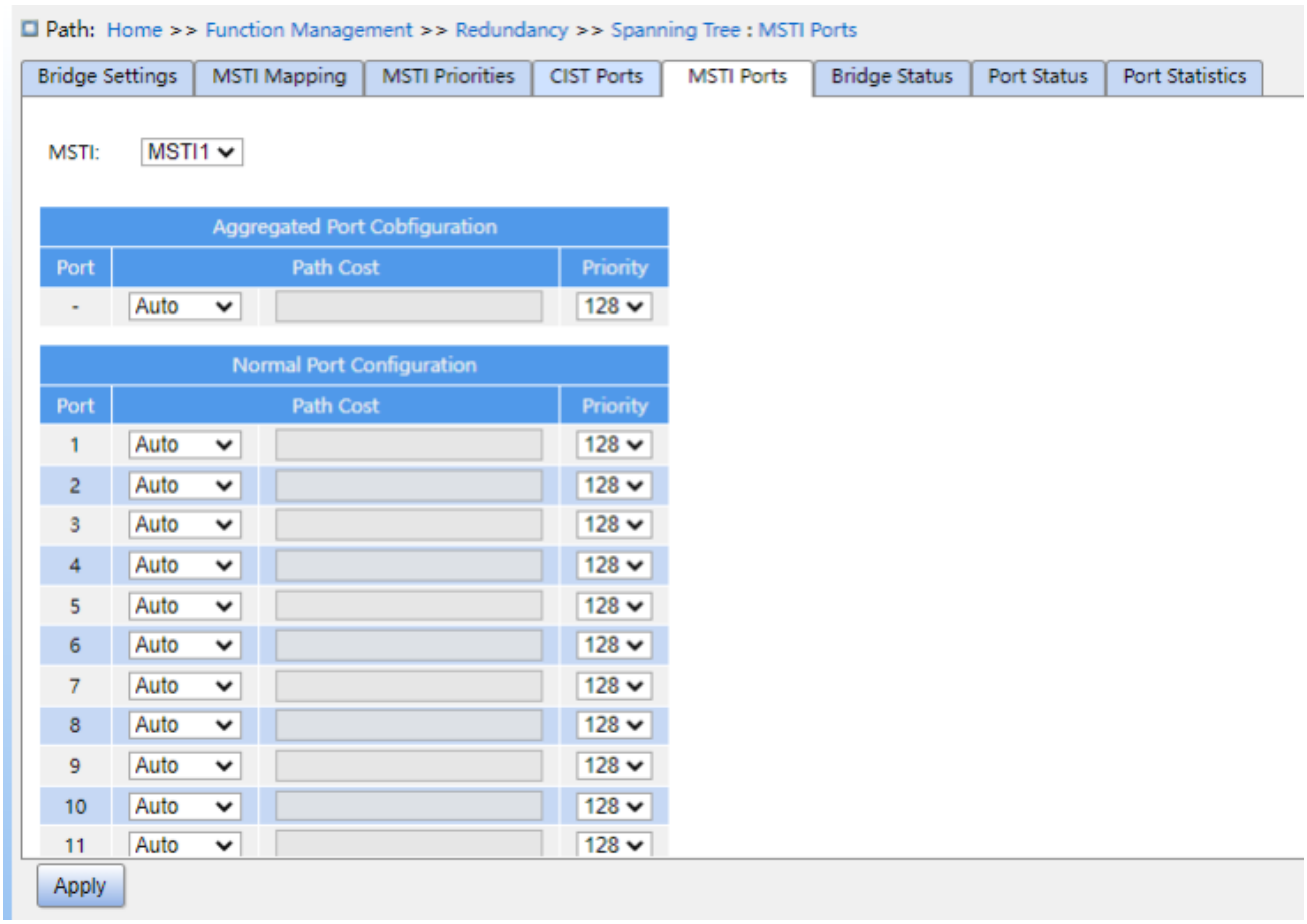


Рис. 138. Настройка портов MSTI

Select MSTI

Варианты конфигурации: MST1~MST7

Конфигурация по умолчанию: MST1

Функция: Выбор MSTI для дальнейшей настройки.

MSTI Aggregated Port Configuration

Функция: Сконфигурируйте группу агрегации в качестве порта MSTP и настройте ее path cost и приоритет (priority) в указанном экземпляре.

Path Cost

Варианты конфигурации: Auto/Specific (1~200000000)

Конфигурация по умолчанию: Auto

Функция: Настройте стоимость пути (path cost) в назначенном экземпляре.

Описание: Стоимость пути (path cost) используется для расчета наилучшего пути. Значение параметра зависит от полосы пропускания. Чем больше значение, тем ниже

стоимость. Вы можете изменить роль порта, изменив значение параметра path cost.

Priority

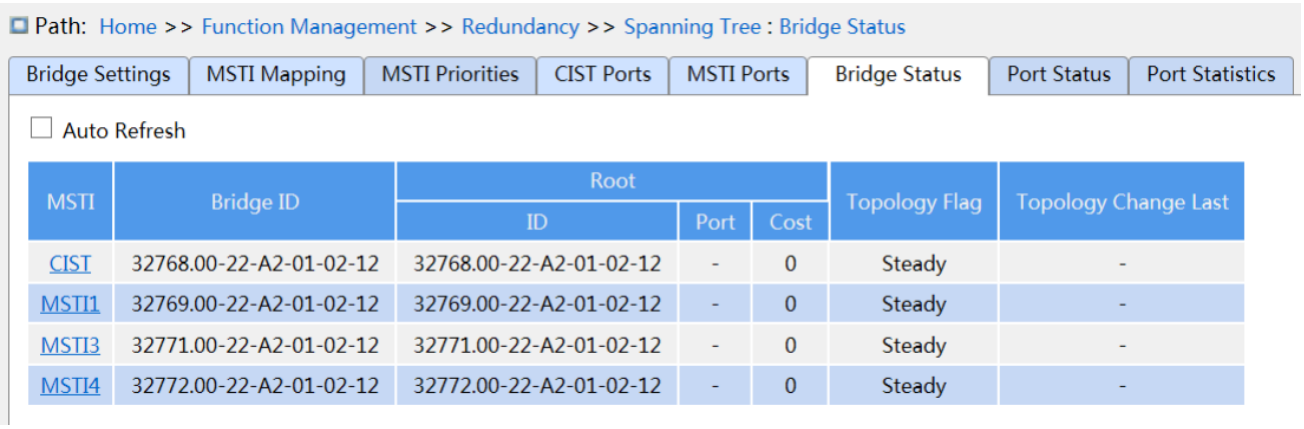
Диапазон: 0~240，шаг настройки 16

Конфигурация по умолчанию: 128

Функция: Настройте приоритет порта, который определяет роль порта.

Описание: Приоритет порта определяет, будет ли он выбран в качестве корневого порта. При том же условии порт с более низким приоритетом будет выбран в качестве корневого порта. Порты с поддержкой MSTP могут быть сконфигурированы с разными приоритетами и играть разные роли портов в разных экземплярах связующего дерева.

6. Просмотр статуса Bridge Status.



MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-22-A2-01-02-12	32768.00-22-A2-01-02-12	-	0	Steady	-
MSTI1	32769.00-22-A2-01-02-12	32769.00-22-A2-01-02-12	-	0	Steady	-
MSTI3	32771.00-22-A2-01-02-12	32771.00-22-A2-01-02-12	-	0	Steady	-
MSTI4	32772.00-22-A2-01-02-12	32772.00-22-A2-01-02-12	-	0	Steady	-

Рис. 139. Просмотр статуса Bridge Status

MSTI

Функция: Указывает экземпляр связующего дерева.

cist: Указывает экземпляр CIST по умолчанию при использовании протокола STP/RSTP;

MSTI: Указывает экземпляр каждого связующего дерева при использовании MSTP.

Bridge ID

Функция: Указывает идентификатор моста текущего экземпляра связующего дерева этого устройства, состоящий из приоритета моста и MAC-адреса моста.

Root

Функция: Указывает информацию о корневом мосте в текущем экземпляре связующего дерева этого устройства. id: Указывает идентификатор моста корневого моста в текущем экземпляре связующего дерева. port: Указывает корневой порт в текущем

экземпляре связующего дерева. Overhead: Указывает стоимость пути от корневого порта до корневого моста в текущем экземпляре связующего дерева.

Topology Flag

Функция: Указывает текущее состояние экземпляра связующего дерева.

Duration after topology change

Функция: Указывает интервал времени с момента последнего изменения топологии до настоящего времени.

7. Просмотр статус STP портов.

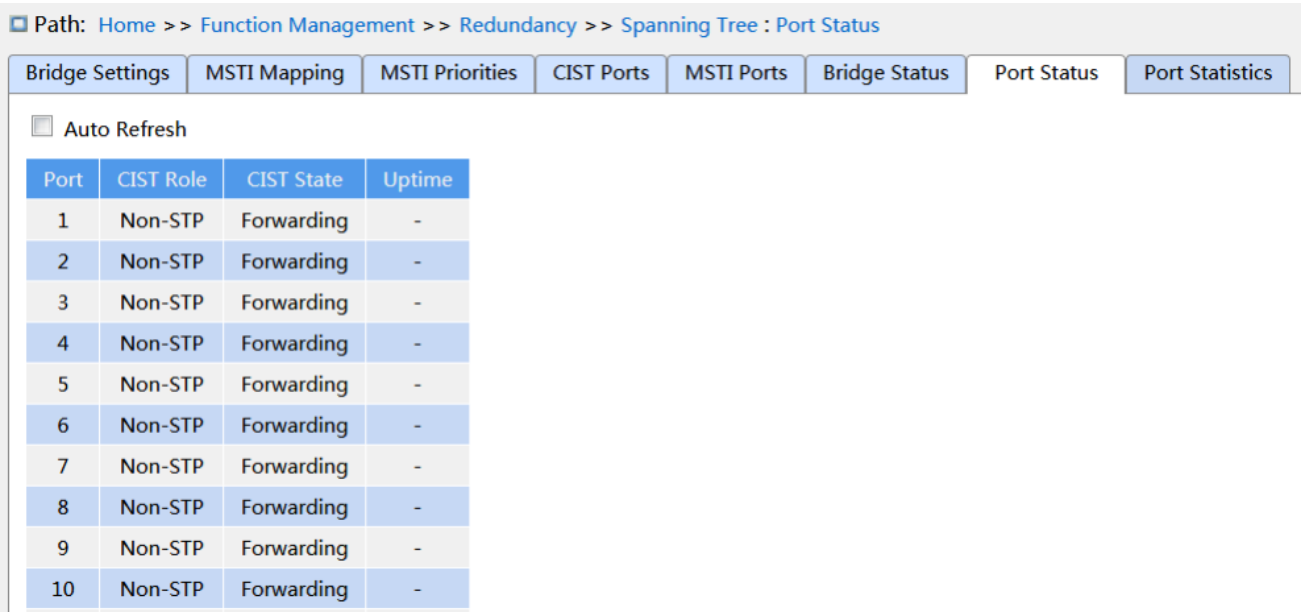


Рис. 140. Просмотр статуса Bridge Status

8. Просмотр статистики по STP портам.

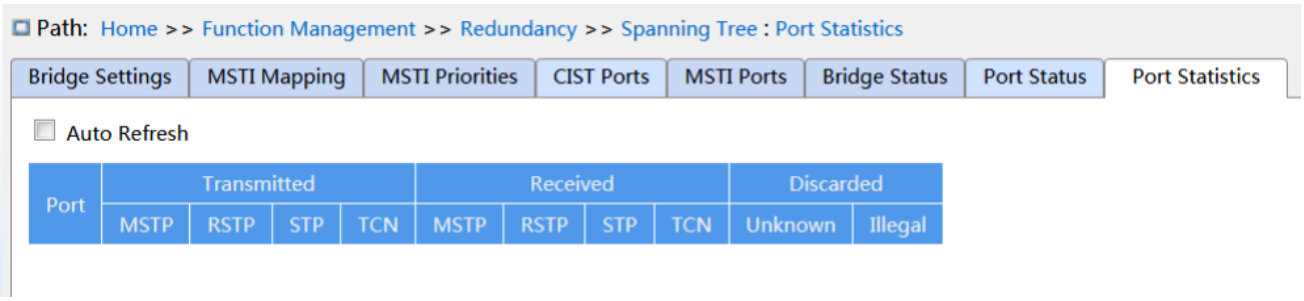


Рис. 141. Просмотр статистики по STP портам

Функция: Количество сообщений MSTP/RSTP/STP/TCN, отправленных/полученных через порт.

7.5.5.5 Пример конфигурации

Коммутаторы A, B, C и D принадлежат к одному и тому же региону MST. Сети VLAN, отмеченные красным цветом, указывают, что пакеты VLAN могут передаваться указанным соединениям. После завершения конфигурирования пакеты VLAN могут пересылаться по разным instance (экземплярам) связующего дерева. Пакеты VLAN 10 пересылаются по instance 1, а корневым мостом (root bridge) для instance 1 является коммутатор A; Пакеты VLAN 30 пересылаются по instance 3, а корневым мостом instance 3 является коммутатор B. Пакеты VLAN 40 пересылаются по instance 4, а корневым мостом экземпляра 4 является коммутатор C. Пакеты VLAN 20 пересылаются по instance 0, а корневым мостом экземпляра 0 является коммутатор B. Подключение показано на рис. 142.

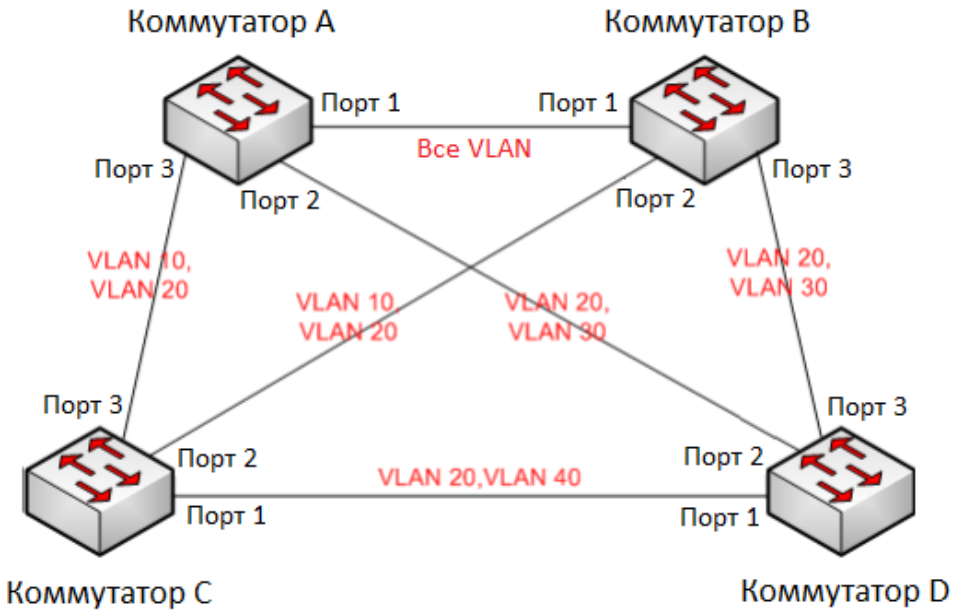


Рис. 142. Пример конфигурации MSTP

Конфигурация коммутатора A:

1. Создайте VLAN 10, 20 и 30 на коммутаторе A; установите порты и разрешите прохождение пакетов соответствующих VLAN.

2. Включите глобальный протокол MSTP, как показано на рис. 134.

3. Установите для названия региона MST значение Region, а для параметра

revision значение 0, как показано на рис. 135.

4. Создайте MSTI 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с экземплярами (instance) 1, 3 и 4 соответственно, как показано на рис. 135.

5. Установите приоритет моста коммутатора в MSTI 1 на 4096 и сохраните приоритет по умолчанию в других экземплярах, как показано на рис. 136.

Конфигурация коммутатора B:

6. Создайте VLAN 10, 20 и 30 на коммутаторе B; установите порты и разрешите прохождение пакетов соответствующих VLAN.

7. Включите глобальный протокол MSTP, как показано на рис. 134.

8. Установите для названия региона MST значение Region, а для параметра revision значение 0, как показано на рис. 135.

9. Создайте MSTI 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с экземплярами (instance) 1, 3 и 4 соответственно, как показано на рис. 135.

10. Установите приоритет моста коммутатора в MSTI 3 и MSTI 0 на 4096 и сохраните приоритет по умолчанию в других экземплярах, как показано на рис. 136.

Конфигурация коммутатора C:

11. Создайте VLAN 10, 20 и 40 на коммутаторе C; установите порты и разрешите прохождение пакетов соответствующих VLAN.

12. Включите глобальный протокол MSTP, как показано на рис. 134.

13. Установите для названия региона MST значение Region, а для параметра revision значение 0, как показано на рис. 135.

14. Создайте MSTI 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с экземплярами (instance) 1, 3 и 4 соответственно, как показано на рис. 135.

15. Установите приоритет моста коммутатора в MSTI 4 на 4096 и сохраните приоритет по умолчанию в других экземплярах, как показано на рис. 136.

Конфигурация коммутатора D:

16. Создайте VLAN 20, 30 и 40 на коммутаторе D; установите порты и разрешите прохождение пакетов соответствующих VLAN.

17. Включите глобальный протокол MSTP, как показано на рис. 134.

18. Установите для названия региона MST значение Region, а для параметра revision значение 0, как показано на рис. 135.

19. Создайте MSTI 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с экземплярами (instance) 1, 3 и 4 соответственно, как показано на рис. 135.

Когда расчет MSTP завершен, MSTI каждой VLAN выглядит следующим образом:

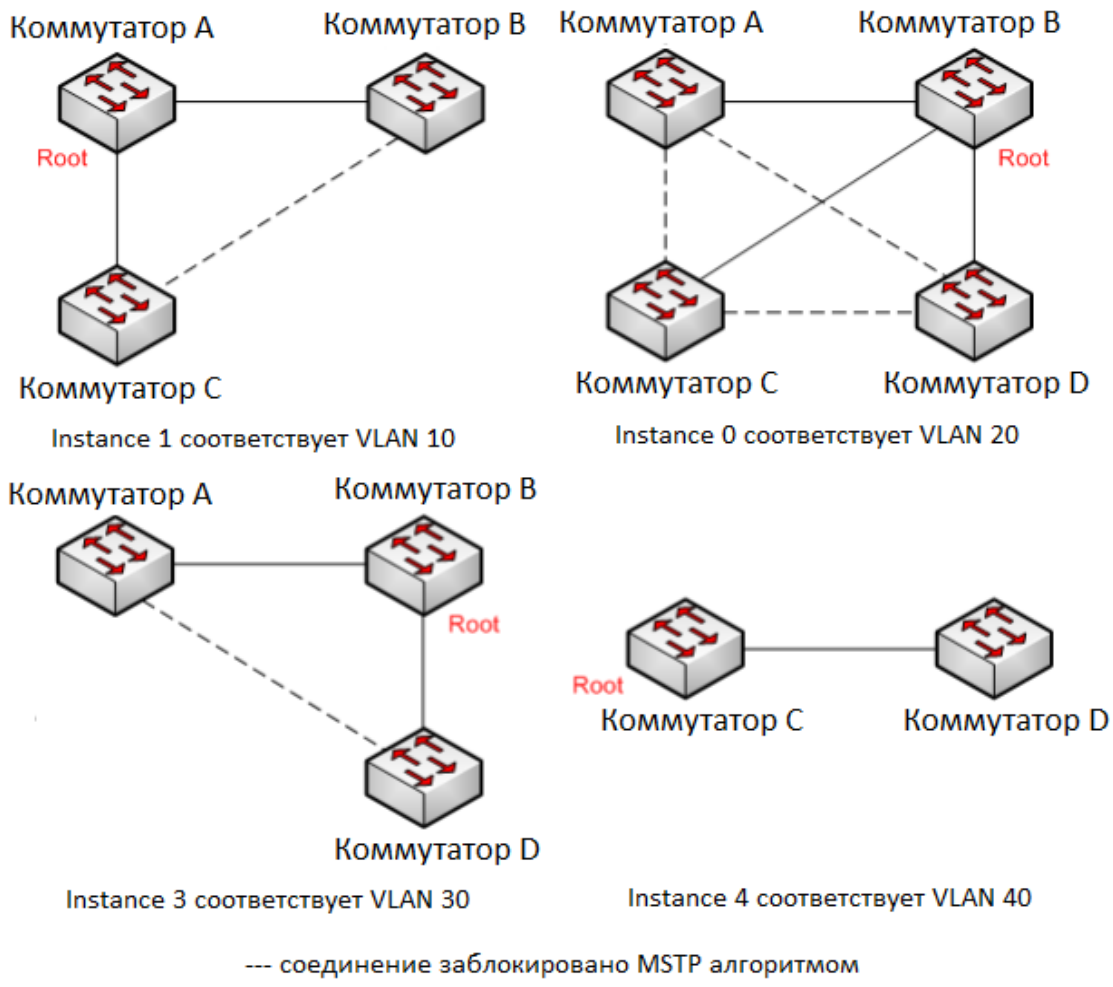


Рис. 143. Spanning Tree Instance для каждого VLAN

7.6 Конфигурация ARP

7.6.1 Введение

Address Resolution Protocol (ARP) - это протокол разрешения адресов, который выполняет сопоставление между IP-адресами и MAC-адресами с помощью механизма запроса и ответа на адрес. Коммутатор может динамически устанавливать взаимосвязь между IP-адресами и MAC-адресами хостов в сегменте сети, также поддерживаются статические записи ARP, с возможностью указания фиксированной взаимосвязи между IP-адресами и MAC-адресами.

7.6.2 Принцип работы

Элементы таблицы ARP делятся на динамические элементы таблицы ARP и статические элементы таблицы ARP. Элементы динамической таблицы генерируются и поддерживаются автоматически посредством взаимодействия с сообщениями ARP, которые устаревать, обновляться новыми сообщениями ARP и перезаписываться статическими элементами таблицы ARP. Статические элементы таблицы настраиваются и обслуживаются вручную и не устаревают и не перезаписываются динамическими элементами таблицы ARP.

7.6.3 Прокси ARP

Если запрос ARP отправляется с хоста в сети на другой хост в том же сегменте сети, но не в той же физической сети, то шлюз с функцией прокси (proxy) ARP, напрямую подключенный к исходному хосту, может ответить на пакет запроса. Этот процесс называется proxy ARP.

Процесс использования прокси-сервера ARP заключается в следующем:

1. Исходный хост отправляет ARP-запрос узлу другой физической сети;

2. Шлюз, напрямую подключенный к исходному хосту, включает функцию прокси-ARP интерфейса VLAN. Если существует маршрут к хосту назначения, то прокси-ARP

ответит MAC-адресом своего собственного интерфейса от имени хоста назначения;

3. IP-пакеты, отправленные с исходного хоста на целевой хост, передаются на прокси-устройство с поддержкой ARP;

4. Шлюз выполняет IP-маршрутизацию и пересылку пакетов.

5. IP-пакет, отправленный на хост назначения, проходит через сеть и, достигает хоста назначения.

7.6.4 Web конфигурация

1. Настройка таблицы статических адресов ARP.

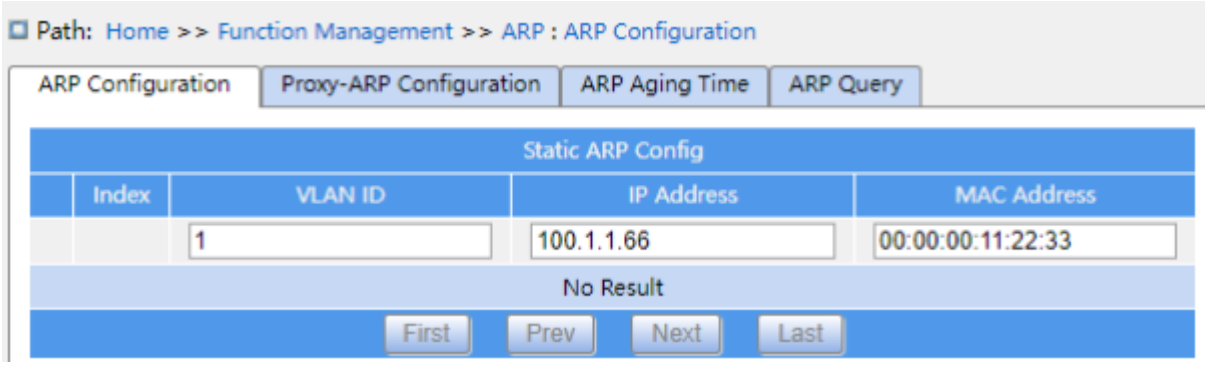


Рис. 144. Конфигурация статической таблицы ARP

VLAN ID

Конфигурация: Созданный интерфейс L3 VLAN，диапазон 1~4093

Функция: Выбор интерфейса L3 VLAN для текущего элемента таблицы ARP.

IP address

Формат: A.B.C.D

Функция: Настройка IP-адресов для статических элементов таблицы ARP.

MAC address

Формат: HH-HH-HH-HH-HH-HH (H - шестнадцатеричное число)

Функция: Настройте mac-адрес элементов статической таблицы ARP.

Type

Варианты конфигурации: port/Lag

Конфигурация по умолчанию: 1/1

Функция: Этот тип указывает тип порта или тип LAG (группы агрегации), где настроены статические записи ARP. Тип порта используется для статической настройки ARP на фактическом физическом порте. Тип LAG указывает, что статический ARP настроен в группе агрегации и используется, когда устройство имеет агрегацию. Настройте статические записи ARP для всей группы агрегации.

В обычных условиях коммутатор автоматически запоминает записи ARP и не требует от администратора настройки статических записей.

2. Конфигурация ARP прокси-сервера.

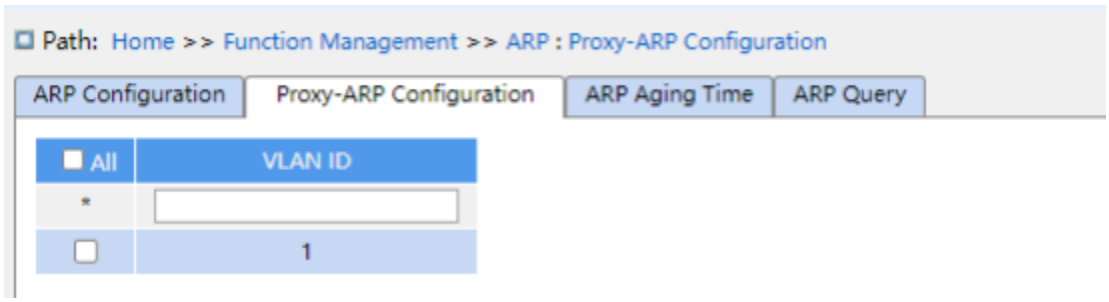


Рис. 145. Конфигурация ARP прокси-сервера

VLAN ID

Диапазон: 1~4093

Функция: Выберите интерфейс L3 прокси-сервера ARP.

3. Настройка времени устаревания ARP

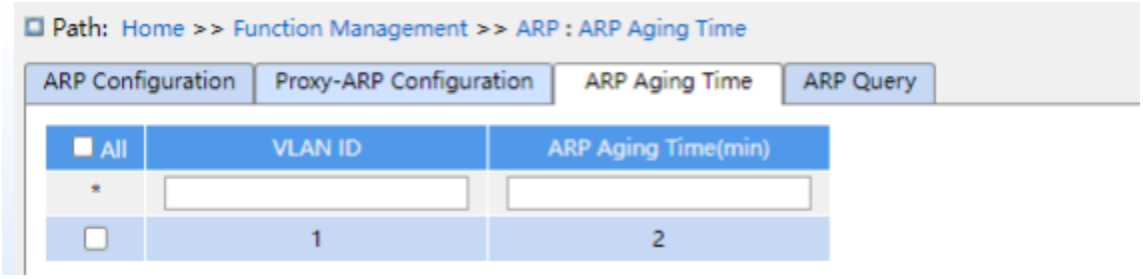


Рис. 146. Настройка времени устаревания ARP

VLAN ID

Диапазон: 1~4093

Функция: Укажите интерфейс уровня L3.

ARP Aging Time

Диапазон: 1 ~ 60min

Конфигурация по умолчанию: 5min

Функция: настройка времени устаревания (aging time) ARP.

Описание: По истечении срока действия запись динамического адреса будет удалена из списка ARP.

4. ARP-запрос.

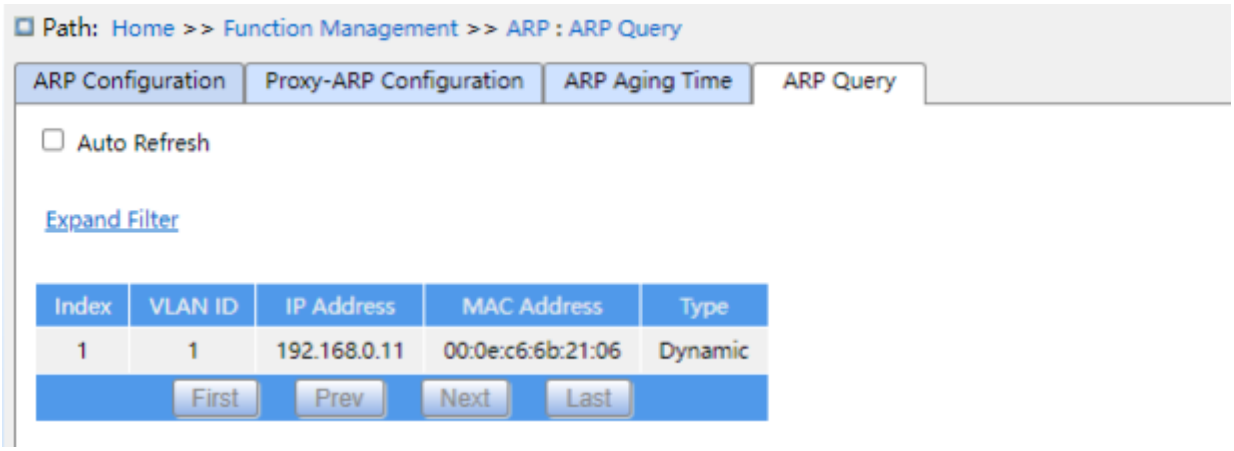


Рис. 147. ARP-запрос

ARP Query

Отображаемое значение: {index, VLAN ID, IP address, MAC address, type}

Функция: отображение элемента таблицы ARP

Описание: В списке отображаются все записи ARP, с портом в состоянии LinkUp, включая статические и динамические записи.

7.7 Конфигураци ACL

7.7.1 Введение

С развитием сетевых технологий проблемы безопасности становятся все более актуальными, требуя механизма контроля доступа.

Access Control List (ACL) - список управления доступом, реализует фильтрацию пакетов путем сопоставления информации в пакетах во входящем направлении

коммутатора с параметрами таблицы доступа.

7.7.2 Реализация

Фильтрация пакетов реализуется путем сопоставления записей конфигурации ACL. Каждая запись конфигурации ACL состоит из нескольких условий ACL. Эти условия находятся в отношениях «и» (&). Пакеты, полученные портом, считаются сопоставленными только тогда, когда они соответствуют всем условия записи ACL. Между различными записями конфигурации ACL нет зависимости.

При наличии нескольких записей ACL устройство сравнивает пакет с записями ACL одну за другой. Как только пакет встречает первую соответствующую запись ACL, он немедленно выполняет соответствующее действие и больше не подвергается воздействию последующих записей ACL.

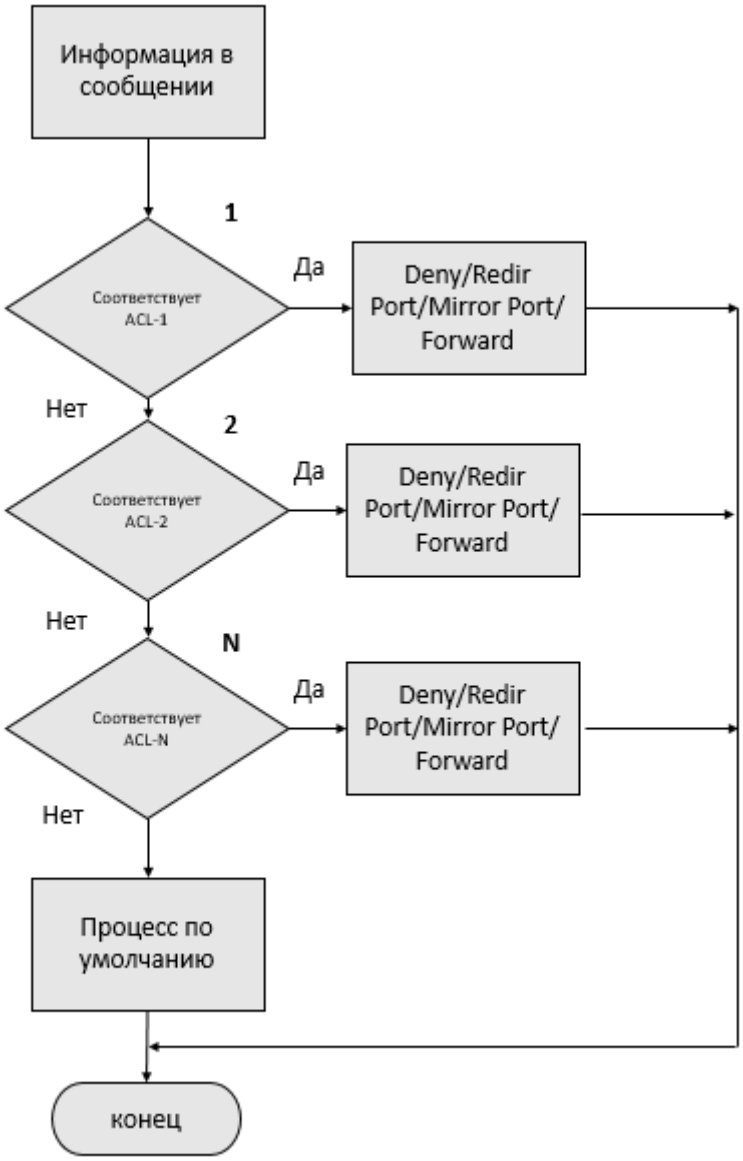


Рис. 148. Алгоритм работы ACL

Процесс «обработки по умолчанию» - это то, как порт обрабатывает пакеты, когда записи ACL не настроены.

7.7.3 Web конфигурация

1. Настройка записей таблицы ACL.

Перейдите [Home] → [Function Management] → [ACL] в дереве навигации.

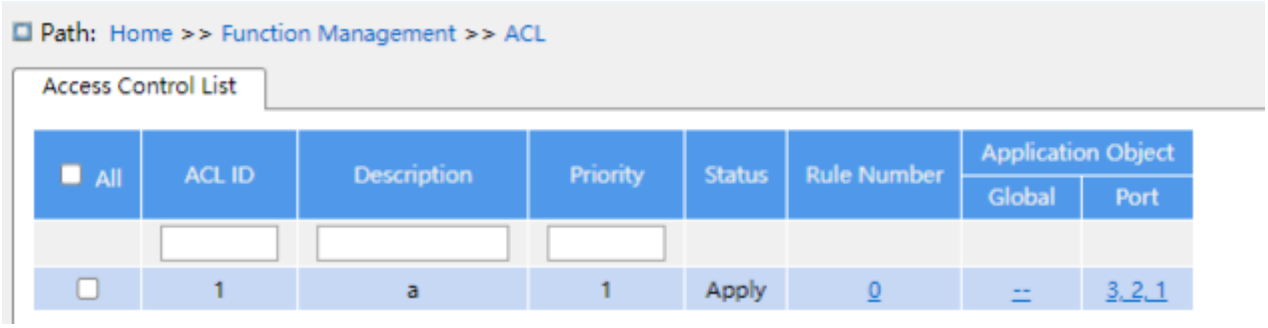


Рис. 149. Настройка записей таблицы ACL

ACL ID

Диапазон: 1~1024

Функция: Настройте идентификатор записи (ACL ID) для таблицы ACL.

Описание: Коммутатор поддерживает до 512 записей таблицы ACL. Если записи таблицы применяются к нескольким портам, то применение для каждого порта представляет собой одну запись таблицы ACL.

Поскольку коммутатор имеет некоторые системные записи ACL, количество записей ACL, которые фактически может настроить пользователь, составляет менее 1024.

Description

Диапазон: 1~127 символов

Функция: Добавьте описание к записи таблицы ACL.

Priority

Диапазон: 1~1024

Функция: Чем меньше число, тем выше приоритет записи.

2. Нажмите на одну из записей таблицы, чтобы войти в интерфейс, показанный на рисунке далее, и нажмите на кнопку <Add Rule>, чтобы настроить правила таблицы ACL.

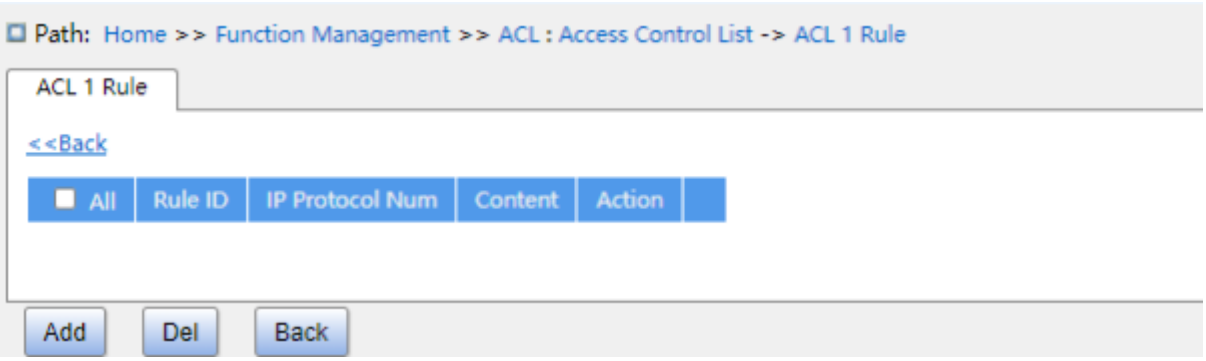


Рис. 150. Редактирование записи ACL

3. Настройте правила для записи в таблице ACL1, как показано на следующем рисунке.

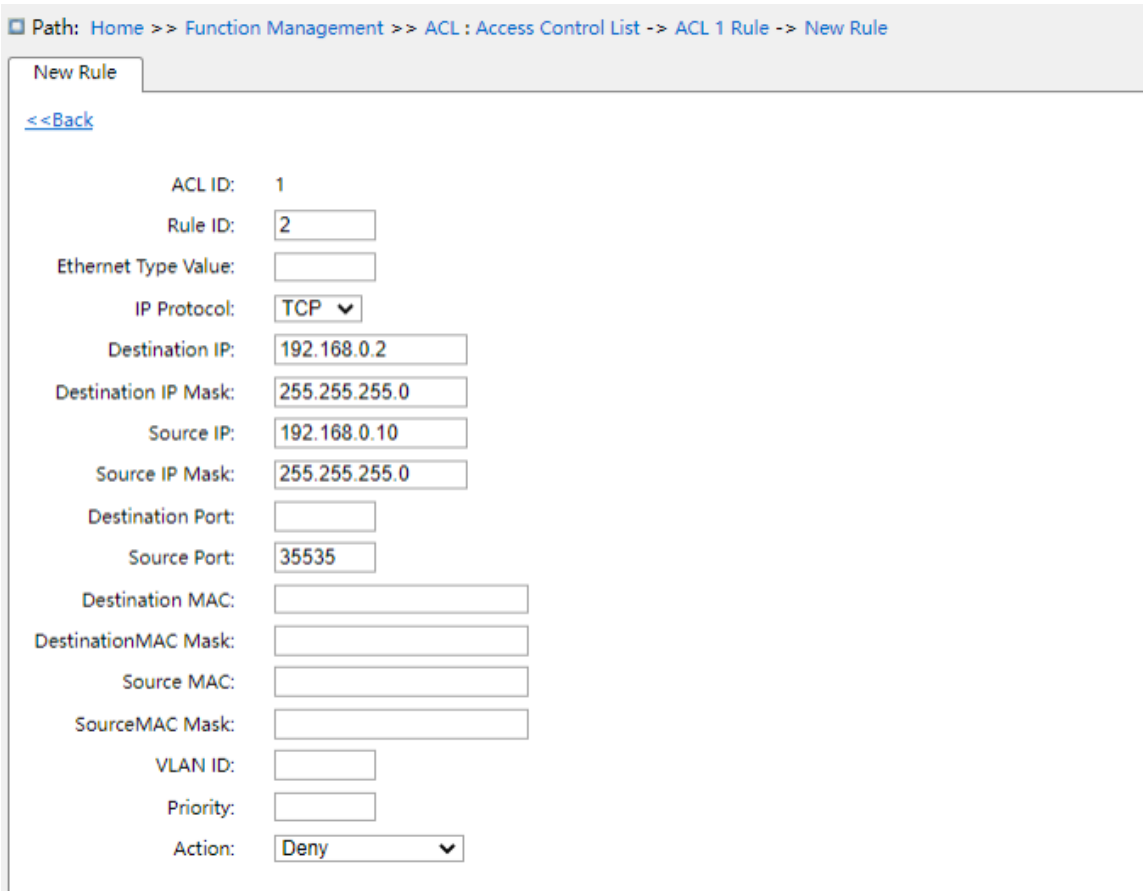


Рис. 151. Настройка правила ACL

Rule ID

Диапазон: 1~1024

Функция: Настройка номера правила для записи в таблице ACL.

Описание: Каждая запись ACL поддерживает максимум 512 правил, а общее количество правил во всех списках контроля доступа не может превышать 512.

Ethernet Type Value

Диапазон: 0x600~0xFFFF

Функция: Настройка типа протокола для правила.

IP Protocol

Варианты конфигурации: Any /ICMP/TCP/UDP/Other

Конфигурация по умолчанию: Any

Функция: Настройте параметр - тип протокола передачи сообщений IPv4. При выборе ICMP/ UDP/TCP необходимо настроить соответствующий параметр; при выборе Other необходимо настроить номер протокола.

Если тип протокола в сообщении IPv4, полученном входящим портом, соответствует конфигурации этого параметра, условие считается выполненным успешно.

Destination IP / Destination IP Mask

Функция: Настройте информацию об IP-адресе назначения в правиле destination IP.

Значение «1» в маске IP-адреса (destination IP mask) представляет интересующий бит IP-адреса, а «0» представляет бит IP-адреса, который следует игнорировать.

Source IP / Source IP Mask

Функция: Настройте информацию об IP-адресе источника в правиле Source IP. Значение «1» в маске IP-адреса (Source IP Mask) представляет интересующий бит IP-адреса, а «0» представляет бит IP-адреса, который следует игнорировать.

Destination port

Диапазон: 0~65535

Функция: Настройка номера порта назначения TCP/UDP.

Source Port

Диапазон: 0~65535

Функция: Настройте номер порта источника TCP/UDP.

Destination MAC / DestinationMAC Mask

Формат: HH:HH:HH:HH:HH:HH (H — шестнадцатеричное число) /A.B.C.D

Функция: Настройте информацию о MAC-адресе назначения. Значение «1» в маске MAC-адреса (DestinationMAC Mask) представляет интересующий бит IP-адреса, а «0» представляет бит IP-адреса, который следует игнорировать.

Source MAC / SourceMAC Mask

Формат: HH:HH:HH:HH:HH:HH (H — шестнадцатеричное число) /A.B.C.D

Функция: Настройте информацию о MAC-адресе источника . Значение «1» в маске MAC-адреса (SourceMAC Mask) представляет интересующий бит IP-адреса, а «0» представляет бит IP-адреса, который следует игнорировать.

VLAN ID

Варианты конфигурации: 1~4093

Функция: Настройте идентификатор VLAN ID для правила.

Priority

Варианты конфигурации: 0~7 (значение COS)

Функция: Настроить значение приоритета для повторной маркировки (re-tagging).

Описание: Если значение приоритета в пакете соответствует priority, будет принята стратегия повторной маркировки (re-tagging).

Action

Варианты конфигурации: Permit/Deny/Mirror to CPU/ Mirror to Port/Redirect to CPU/ Redirect to Port/Redirect to nexthop/Limit To kbps/Limit To mbps/Modify DSCP/Modify Queue /Modify Cos

Конфигурация по умолчанию: Permit

Функция: Настройте обработку успешно сопоставленных сообщений.

Описание: Permit означает получение успешно совпавшего сообщения; Deny означает отбрасывание успешно совпавшего сообщения; Mirror to CPU означает получение успешно совпавшего сообщения и его зеркальное отображение на CPU; Mirror to Port означает получение успешно совпавшего сообщения и его зеркальное отображение на указанный порт; Redirect to CPU означает означает перенаправление успешно совпавших сообщений на CPU; Redirect to Port означает перенаправление

означает перенаправление успешно совпавших сообщений на указанный порт. Redirect to Nexthop используется для создания действия, которое перенаправляет сообщения на один IP-адрес следующего перехода. Limit To kbps означает ограничение скорости кбит/с для успешно сопоставленных сообщений. Limit To mbps означает ограничение скорости успешно сопоставленных сообщений в Мбит/с. Modify DSCP означает изменение значения DSCP успешно сопоставленных сообщений. Modify Queue представляет собой изменение значения очереди успешно сопоставленных сообщений. Modify Cos представляет собой изменение значения CoS успешно сопоставленных пакетов.

4. Настройка таблицы ACL1.

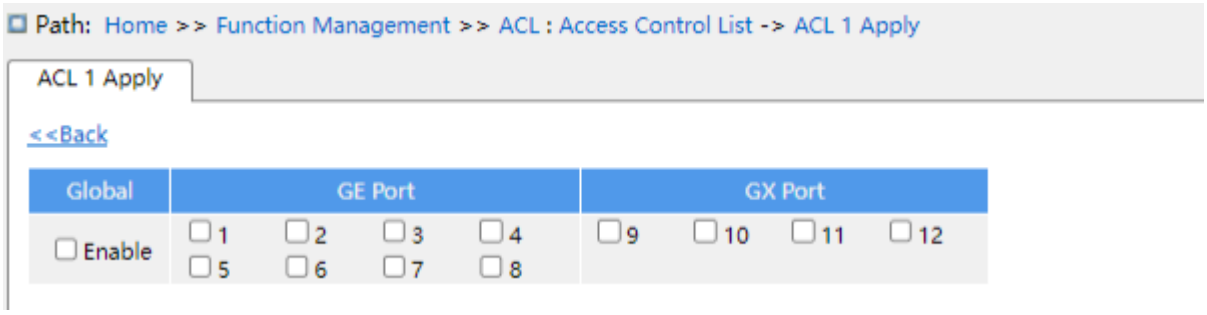


Рис. 152. Настройка таблицы ACL1

ACL1 Application object

Варианты конфигурации: Global/FE port/FX port

Функция: Применять правила ACL глобально или к портам.

7.8 Конфигурация MAC адресов

7.8.1 Введение

При пересылке пакета коммутатор выполняет поиск порта пересылки в таблице MAC-адресов на основе MAC-адреса назначения пакета.

MAC-адрес может быть как статическим, так и динамическим.

Статический MAC-адрес настраивается пользователем. Он имеет наивысший приоритет (не переопределяется динамическими MAC-адресами) и действителен

постоянно.

Динамические MAC-адреса запоминаются коммутатором при пересылке данных. Они действительны только в течение определенного периода. Коммутатор периодически обновляет свою таблицу MAC-адресов. При получении фрейма данных, подлежащего пересылке, коммутатор запоминает MAC-адрес источника кадра, устанавливает сопоставление с принимающим портом и запрашивает порт пересылки в таблице MAC-адресов на основе MAC-адреса назначения кадра. Если найдено совпадение, коммутатор пересылает кадр данных с соответствующего порта. Если совпадение не найдено, коммутатор транслирует кадр в своем широковещательном домене.

Время устаревания (Aging time) начинается с момента добавления динамического MAC-адреса в таблицу MAC-адресов. Если ни один порт не получает кадр с MAC-адресом в течение 1-2 кратного времени устаревания, коммутатор удаляет запись MAC-адреса из таблицы динамических адресов пересылки. Статические MAC-адреса не учитывают концепцию времени устаревания.

7.8.2 Web конфигурация

1. Настройка времени устаревания MAC адреса.

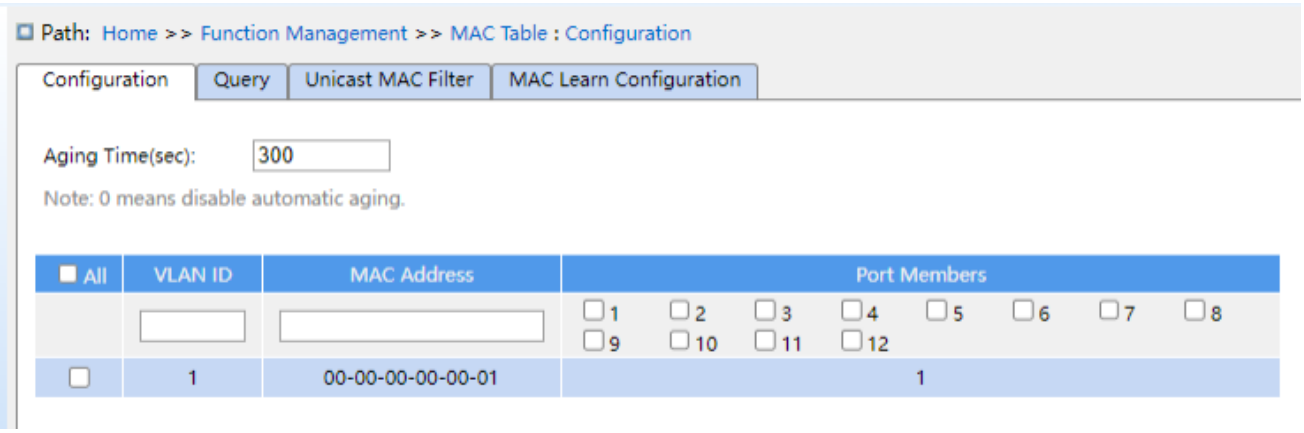


Рис. 153. . Настройка времени устаревания MAC адреса

Aging Time

Диапазон: 0 или 10~1000000 сек.

Конфигурация по умолчанию: 300 сек.

Функция: Установите время устаревания (Aging Time) для динамического MAC-адреса.

VLAN ID

Варианты конфигурации: все созданные VLAN ID.

Функция: Сопоставляет статический MAC адрес и VLAN ID.

MAC address

Формат: HH-HH-HH-HH-HH-HH (H - шестнадцатеричное число)

Функция: Настройте MAC-адрес. Для одноадресного (unicast) MAC-адреса младший бит в первом байте равен 0. Для многоадресного (multicast) MAC-адреса младший бит в первом байте равен 1.

Port Members

Функция: Выберите порты для пересылки пакетов с этим MAC-адресом назначения. Устройство поддерживает до 64 записей статической таблицы MAC-адресов.

2. Просмотр таблицы MAC адресов.

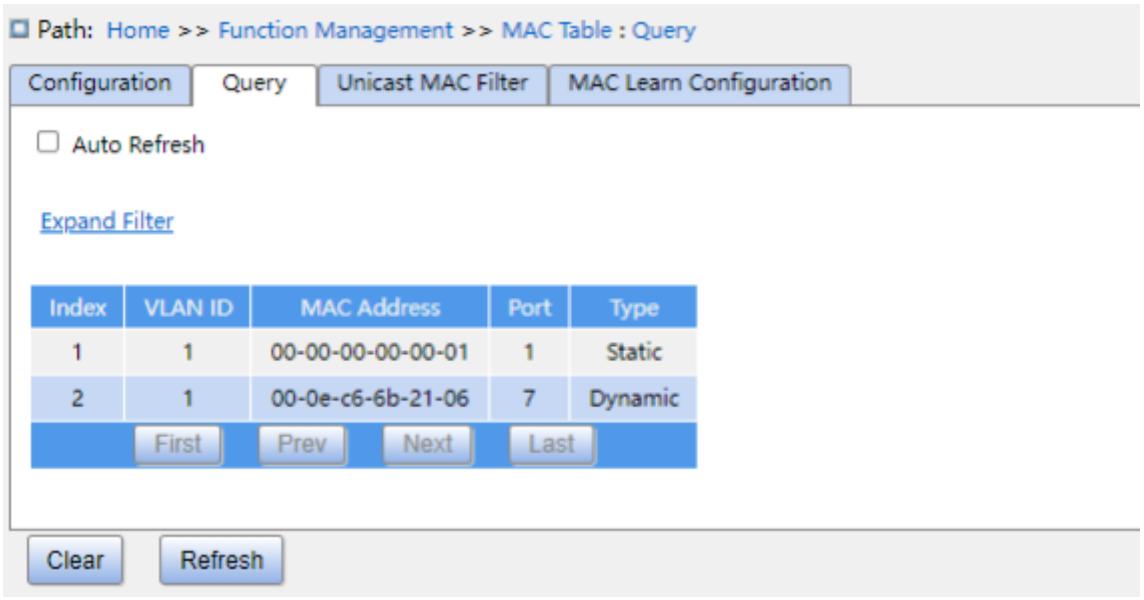


Рис. 154. Просмотр таблицы MAC адресов

VLAN ID

Варианты конфигурации: * / >= / <= / select range

Конфигурация по умолчанию: *

Функция: Отображение таблицы MAC в соответствии с настроенным VLAN ID.

MAC Address

Варианты конфигурации: * / >= / <= / select range

Конфигурация по умолчанию: *

Функция: Отображение таблицы MAC в соответствии с настроенным MAC-адресом.

Port

Варианты конфигурации: * / include/ not include

Конфигурация по умолчанию: *

Функция: Отображение таблицы MAC в соответствии с настроенным портом.

Type

Варианты конфигурации: * / static / dynamic

Конфигурация по умолчанию: *

Функция: Отображение таблицы MAC в соответствии с настроенным типом.

3. Настройка таблица фильтрации одноадресных (unicast) MAC-адресов.

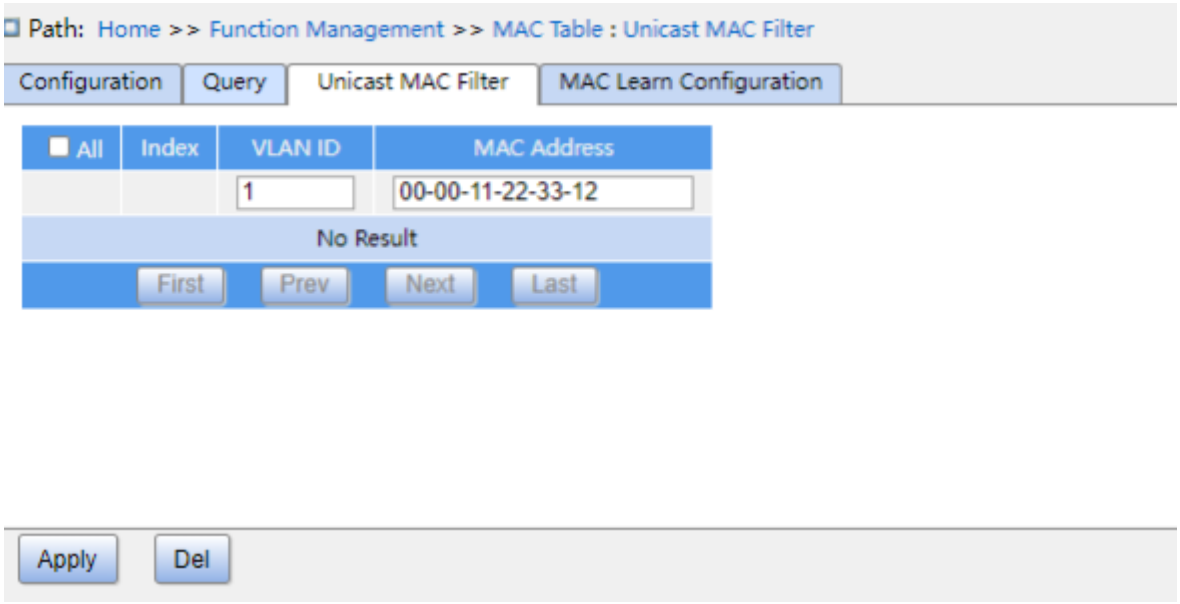


Рис. 155. Настройка таблица фильтрации unicast MAC-адресов

VLAN ID

Варианты конфигурации: все созданные VLAN ID

Функция: Настройте VLAN ID для статических адресов MAC.

MAC Address

Формат: HH-HH-HH-HH-HH-HH (H - шестнадцатеричное число)

Функция: Настройте MAC-адрес. Для одноадресного (unicast) MAC-адреса младший бит в первом байте равен 0. Для многоадресного (multicast) MAC-адреса младший бит в первом байте равен 1.

4. Настройка функции MAC Learning показана на следующем рисунке.

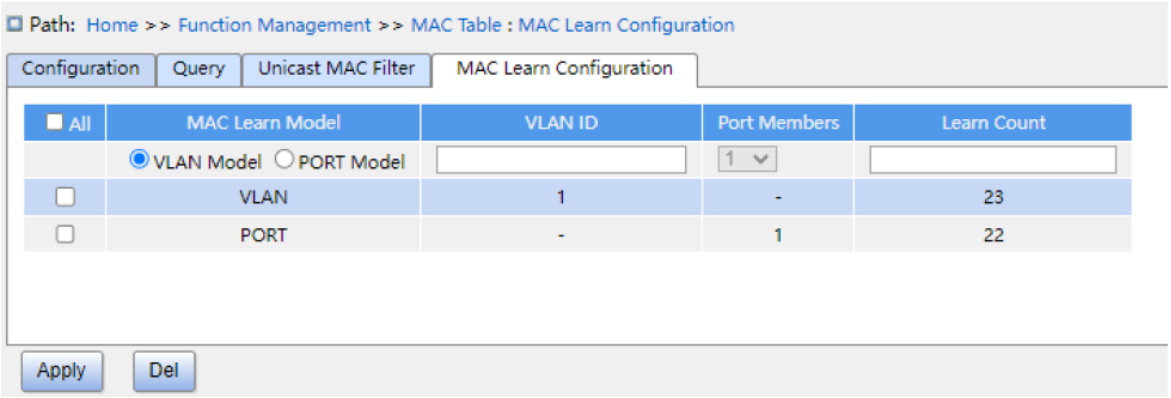


Рис. 156. Настройка функции MAC Learning

MAC Learn Model

Варианты конфигурации: VLAN mode / PORT mode

Функция: Настройте режим ограничения обучения MAC, который может ограничить количество учетных записей MAC в VLAN или порту.

VLAN ID

Варианты конфигурации: 1-4093

Функция: Настройка VLAN для функции ограничения MAC learning .

Port Members

Варианты конфигурации: все порты коммутатора

Функция: Включает функция ограничения адресов для функции MAC learning.

Learn Count

Диапазон: 1~8192

Функция: Настройте количество адресов для функции MAC learning.

7.9 PoE

7.9.1 Введение

POE (Power Over Ethernet) означает, что коммутатор может подавать питание по витой паре удаленно через порт Ethernet, а надежное расстояние подачи питания составляет до 100 м. Это эффективно решает проблему централизованного электроснабжения IP-видеокамер, беспроводных точек доступа, устройств сбора данных и так далее, без учета проводки внутренней системы электроснабжения, оно может подавать питание на оборудование одновременно с подключением к сети.

Стандарт IEEE 802.3at включает в себя PSE и PD, PSE (Power Sourcing quipment) - это устройство, которое подает питание на другое устройство, а PD (Powered Device) - это устройство, которое питается от системы питания PoE.

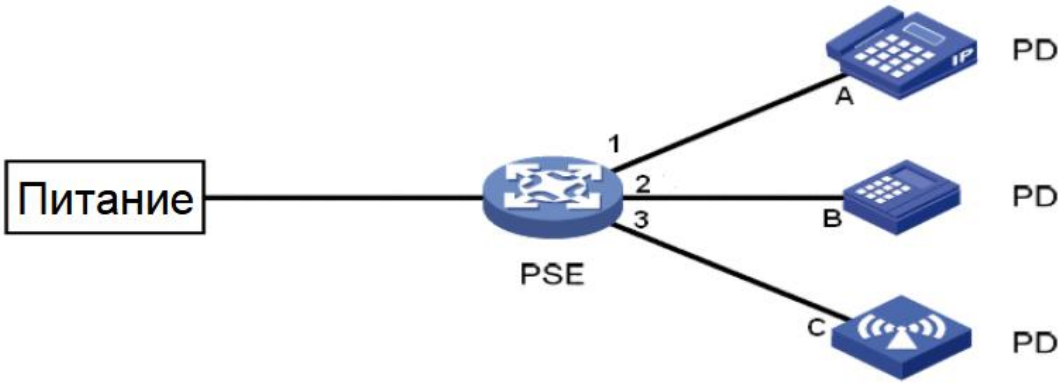


Рис. 157. Система питания PoE

7.9.2 Web конфигурация

1. Настройка функции PoE для портов коммутатора показано на рисунке далее.

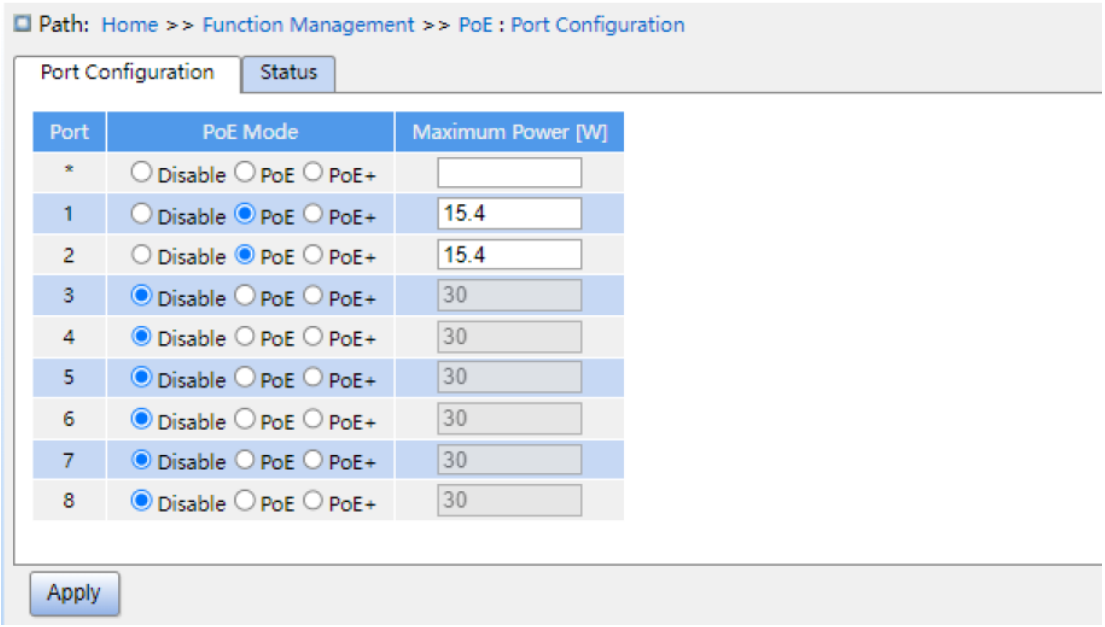


Рис. 158. Настройка функции PoE для портов коммутатора

PoE Mode

Варианты конфигурации: Disable/PoE/PoE+

Конфигурация по умолчанию: Disable

Функция: Включен ли POE для порта. PoE: выход, соответствующий стандарту IEEE802.3af; PoE+: выход, соответствующий стандарту IEEE802.3at.

Maximum Power [W]

Варианты конфигурации: 1~15.4w（PoE）/1~30.0w（PoE+）

Функция: настройте максимальную выходную мощность порта PoE. Если энергопотребление подключенного к порту PD-устройства превышает это значение конфигурации, питание PD-устройства невозможно. В соответствии с фактическими требованиями пользователь может настроить предельную выходную мощность каждого порта коммутатора.

2. Просмотр статута PoE для коммутатора показано далее.

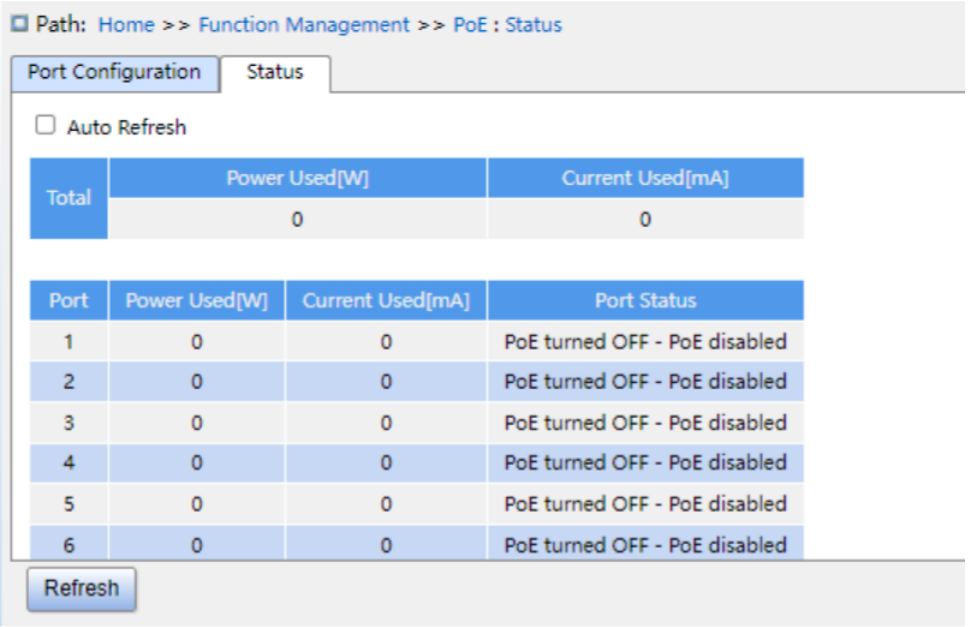


Рис. 159. Просмотр статута PoE

Power Used/Current Used

Функция: Отображает параметры энергопотребления, тока для портов PoE.

Port Status

Варианты отображения: No PD detected/Invalid PD/PoE turned ON/PoE turned OFF-PoE disabled/ PoE turned OFF-Power budget exceeded/PoE turned OFF-PD overload/ PoE turned ON-PD forced ON

Функция: Отображает состояние PoE порта.

Пояснение:

"No PD detected" обозначает включение PoE, но не обнаружение устройства PD.

"Invalid PD" обозначает, что функция PoE включена, обнаружен PD, но источник питания неисправен. Т.е. источник питания, подключенный к коммутатору, выдает выходное напряжения не соответствующее необходимому диапазону.

"PoE turned ON" обозначает, что функция PoE включена, обнаружен PD, источник питания в норме.

"PoE turned OFF-PoE disabled" обозначает, что функция PoE отключена.

"PoE turned OFF-Power budget exceeded" указывает на то, что функция PoE включена на порту, обнаружен PD, но подача питания на PD не производится, если общее

энергопотребление всех PD превышает максимальное энергопотребление PSE после подключения PD.

"PoE turned OFF-PD overload" указывает, что функция PoE включена на порту, обнаружен PD и подача питания на PD не производится, если общее энергопотребление всех PD не превышает максимальное энергопотребление PSE, но энергопотребление PD превышает максимальную выходную мощность порта PoE.

"PoE turned ON-PD forced ON" относится к включению PoE и принудительному питанию.

7.10 IGMP Snooping

7.10.1 Введение

Internet Group Management Protocol Snooping (IGMP Snooping) - это протокол многоадресной рассылки на канальном уровне. Он используется для управления группами многоадресной рассылки. Коммутаторы с поддержкой IGMP Snooping (IGMP отслеживания) анализируют принятые пакеты IGMP, устанавливают сопоставление между портами и MAC-адресами многоадресной рассылки и пересылают многоадресные пакеты в соответствии с этим сопоставлением.

Существует три версии протокола Internet Group Message Protocol (IGMP): IGMPv1, IGMPv2 и IGMPv3. IGMPv1 определен в RFC 1112, IGMPv2 определен в RFC 2236, а IGMPv3 определен в RFC 3376.

Версия IGMPv1 имеет только два сообщения: сообщения отчета (report) и сообщения запроса (query), которые определяют базовый процесс запроса членов группы и отчета.

IGMPv2 основан на IGMPv1 и добавляет сообщение о выходе для быстрого выхода (leave) членов группы. Преимущество этого механизма заключается в том, что когда последний член группы многоадресной рассылки покидает группу многоадресной рассылки, он может уведомить маршрутизатор о необходимости провести быструю

конвергенцию.

Еще одно отличие от IGMPv1 заключается в том, что существует два типа сообщений запроса IGMPv2. Один - обычное сообщение запроса. Устройство периодически отправляет сообщение общего запроса (general query packet) группы для запроса членства, а другой – конкретную многоадресную группу. Сообщение запроса. Когда хост покидает группу многоадресной рассылки, после того как устройство получает сообщение о выходе, устройство отправляет конкретное сообщение запроса группы многоадресной рассылки, чтобы определить, все ли члены группы многоадресной рассылки покинули группу. По сравнению с IGMPv1, IGMPv2 поддерживает два типа пакетов запросов: общий пакет запросов (general query packet) и пакет запросов для конкретной группы (group-specific query packet). Коммутатор периодически отправляет общий пакет запросов для запроса членства. Когда хост покидает группу многоадресной рассылки (multicast group), после получения коммутатором сообщения об уходе (leave message) коммутатор отправляет пакет запроса для конкретной группы (group-specific query packet), чтобы определить, все ли участники покидают группу многоадресной рассылки.

IGMPv3 добавляет функцию фильтрации источника хоста. Хост может указать, получать или не получать сообщения от определенных источников групп многоадресной рассылки.

7.10.2 Основные понятия

Отправитель запроса (Querier): периодически отправляет пакеты общих запросов IGMP для запроса статуса участников группы многоадресной рассылки, сохраняя информацию о группе многоадресной рассылки. Когда в сети существует несколько querier, то автоматически выбирается тот, у которого наименьший IP-адрес, в качестве отправителя запроса. Только выбранный querier периодически отправляет пакеты общих запросов IGMP. Другие querier получают и пересылают пакеты запросов IGMP.

Порт маршрутизации (Router port): получает пакеты общего запроса (на

коммутаторе с поддержкой IGMP) от отправителя запроса (querier). При получении отчета IGMP коммутатор устанавливает запись многоадресной рассылки и добавляет порт, который получает отчет IGMP, в список портов-участников. Если порт маршрутизации существует, он также добавляется в список портов-участников. Затем коммутатор пересылает отчет IGMP другим устройствам через порт маршрутизации, чтобы другие устройства установили ту же запись многоадресной рассылки.

Прокси-сервер IGMP Snooping: Функция IGMP Snooping Proxy настраивается на пограничном устройстве для того, чтобы уменьшить количество report пакетов и leave пакетов и оставлять пакеты, полученные вышестоящим устройством (upstream), тем самым повышая общую производительность вышестоящего устройства. Устройство, на котором настроена функция IGMP snooping proxy, функционирует как хост для своего вышестоящего устройства и как querier для своего нижестоящего (downstream) хоста.

7.10.3 Принцип работы

IGMP Snooping управляет участниками группы многоадресной рассылки путем обмена пакетами между устройствами с поддержкой IGMP. Управление производится с помощью следующих пакетов:

General query packet: Querier периодически отправляет пакеты общего запроса (IP-адрес назначения: 224.0.0.1), чтобы подтвердить, есть ли в группе многоадресной рассылки (multicast group) порты-участники. После получения General query packet сторона, не отправляющая запрос, также пересылает сообщение запроса на все подключенные порты.

Specific query packet: Если устройство хочет покинуть группу многоадресной рассылки, оно отправляет пакет IGMP leave. После получения пакета leave отправитель запроса (querier) отправляет специальный пакет запроса (IP-адрес назначения: IP-адрес группы многоадресной рассылки), чтобы подтвердить, содержит ли группа другие порты-члены.

Membership report packet: если устройство присоединилось к группе многоадресной рассылки, то после получения пакета запроса IGMP оно отправит пакет отчета IGMP (IP-адрес назначения: IP-адрес группы многоадресной рассылки) в ответ на пакет запроса. Если устройство хочет присоединиться к группе многоадресной рассылки, оно отправит пакет отчета IGMP отправителю запросов IGMP (querier), чтобы присоединиться к интересующей группе многоадресной рассылки.

Leave packet: Если устройство хочет покинуть группу многоадресной рассылки, оно отправит пакет выхода IGMP (IP-адрес назначения: 224.0.0.2).

7.10.4 Web конфигурация

1. Включение протокола IGMP Snooping.

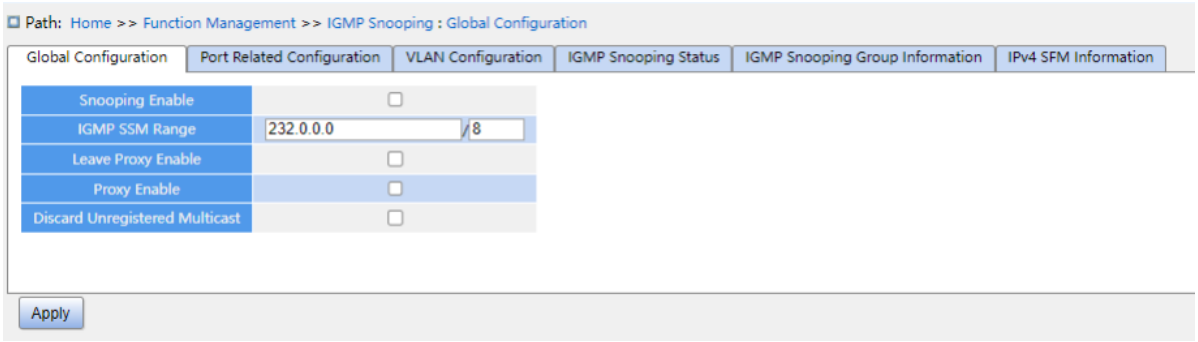


Рис. 160. Настройка IGMP Snooping

Snooping Enable

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение или отключение протокола IGMP Snooping на коммутаторе.

IGMP SSM Range

Формат: A.B.C.D/ 4~32

Конфигурация по умолчанию: 232.0.0.0/8

Функция: Только хосты и маршрутизаторы с адресом в пределах значения этого параметра могут запускать сервисную модель многоадресной рассылки IGMP (IGMP SSM) при условии, что хосты и маршрутизаторы поддерживают сервисную модель

IGMP SSM.

Leave Proxy Enabled

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Укажите, следует ли пересылать пакеты leave отправителю запроса. Когда функция включена, пакеты leave не пересылаются.

Proxy Enabled

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Укажите, следует ли пересылать отправителю запроса пакеты leave и пакеты отчетов участников. Когда это включено, пакеты leave и пакеты отчетов участников не пересылаются.

Discard Unregistered Multicast

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Отбрасывает ли коммутатор неизвестные многоадресные пакеты при их получении.

2. Настройка портов IGMP.

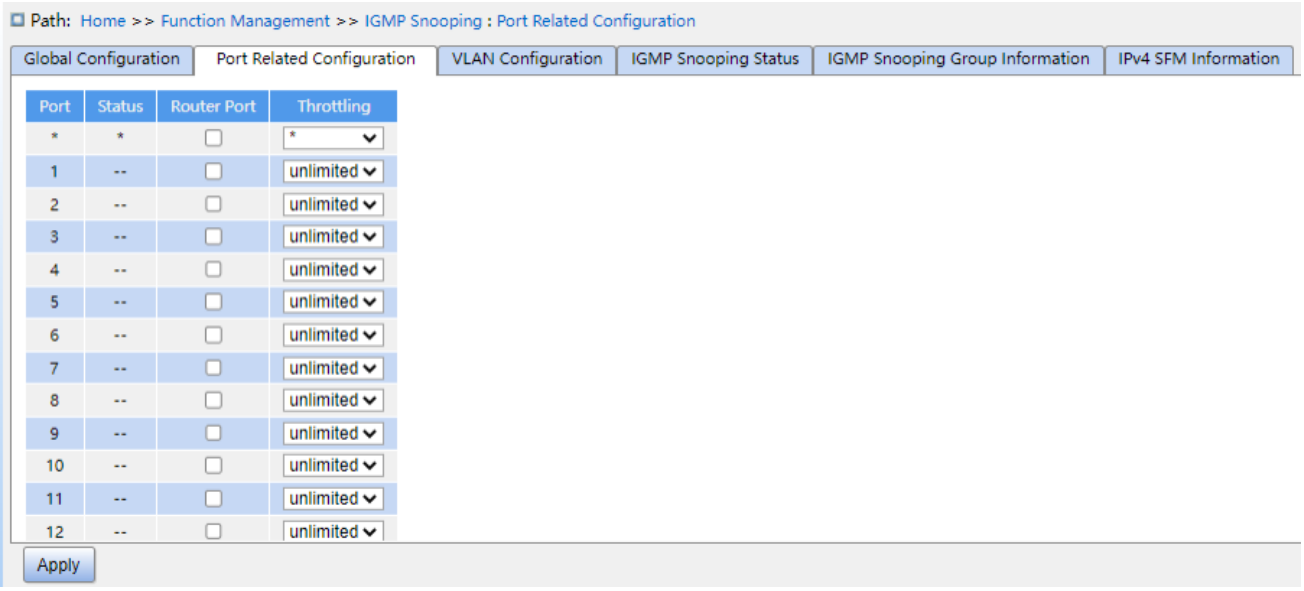


Рис. 161. Настройка IGMP портов

Status

Варианты конфигурации: --/static/dynamic

Функция: Отображает состояние порта маршрутизатора. static означает, что порт статически настроен как порт маршрутизации; dynamic означает, что порт динамически определяется как порт маршрутизации.

Router Port

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Настройка порта маршрутизации.

Throttling

Варианты конфигурации: unlimited /1~10

Конфигурация по умолчанию: unlimited

Функция: Ограничивать ли количество записей многоадресной рассылки, полученных портом.

3. Настройка IGMP Snooping VLAN.

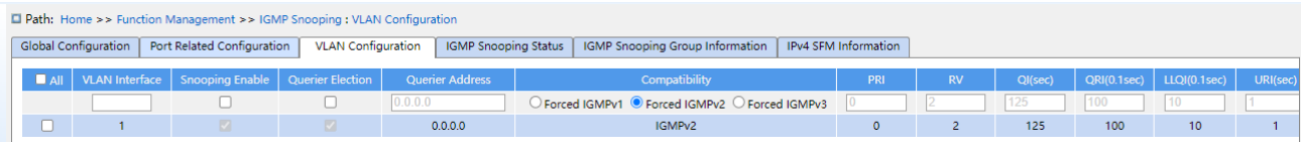


Рис. 162. Настройка IGMP Snooping VLAN

VLAN Interface

Варианты конфигурации: Все созданныеVLAN ID

Snooping Enabled

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включите или отключите функцию VLAN IGMP Snooping. Предварительным условием для этой функции является включение глобальной функции IGMP Snooping.

Querier Election

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включить ли функцию IGMP query для этой VLAN.

Описание: Если в сети несколько querier, они автоматически выберут в качестве querier тот, у которого наименьший IP-адрес. Если есть только одно устройство, которое поддерживает функцию запроса IGMP, оно будет querier.

Querier Address

Формат: A.B.C.D

Функция: Настройка IP-адреса источника для отправки пакета запроса. Если задано значение 0.0.0.0, IP-адрес порта VLAN используется в качестве адреса querier.

Compatibility

Варианты конфигурации: Forced IGMPv1 / Forced IGMPv2 / Forced IGMPv3

Конфигурация по умолчанию: Forced IGMPv2

Функция: Настройка версии IGMP.

PRI（Priority of Interface）

Диапазон: 0~7

Конфигурация по умолчанию: 0

Функция: Настройте приоритет управляющего пакета IGMP.

RV（Robustness Variable）

Диапазон: 2~255

Конфигурация по умолчанию: 2

Функция: Укажите параметр надежности функции IGMP Query.

Описание: Чем больше параметр, тем хуже сетевое окружение. Пользователь может установить подходящий параметр надежности в соответствии с реальной сетью.

QI（Query Interval）

Диапазон: 1~31744 сек.

Конфигурация по умолчанию: 125 сек.

Функция: Настройка интервала времени для отправки запроса general query packet.

QRI（Query Response Interval）

Диапазон: ~31744 (единица измерения 0,1 сек.)

Конфигурация по умолчанию: 100

Функция: Настройка максимального времени для отправки ответа general query packet.

LLQI（Last Member Query Interval）

Диапазон: 0~31744 (единица измерения 0,1 сек.)

Конфигурация по умолчанию: 10

Функция: Настройка максимального времени для отправки ответа specific query packet.

Конфигурация QI, QRI и LLQI действительна только для querier.

URI（Unsolicited Report Interval）

Диапазон: 0~31744 сек.

Конфигурация по умолчанию: 1 сек.

Функция: Установите интервал для повторной отправки хостом пакета отчета о присоединении к группе многоадресной рассылки.

Нажмите < Add New IGMP VLAN >, чтобы настроить запись IGMP Snooping VLAN.

Это устройство поддерживает до 32 записей IGMP Snooping VLAN.

4. Просмотр статуса IGMP Snooping.

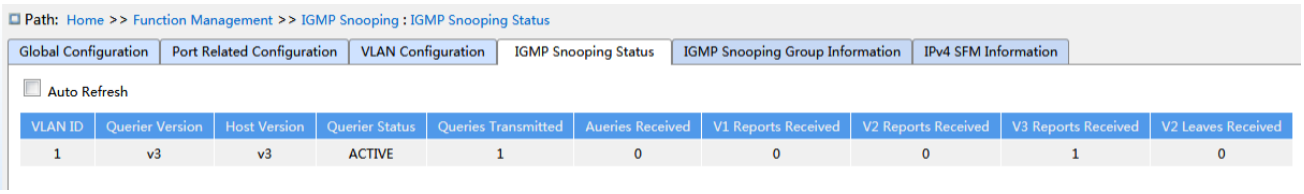


Рис. 163. Просмотр статуса IGMP Snooping

Функция: На этой странице показаны подробности отслеживания IGMP Snooping VLAN.

5. Просмотр списка участников многоадресной рассылки.

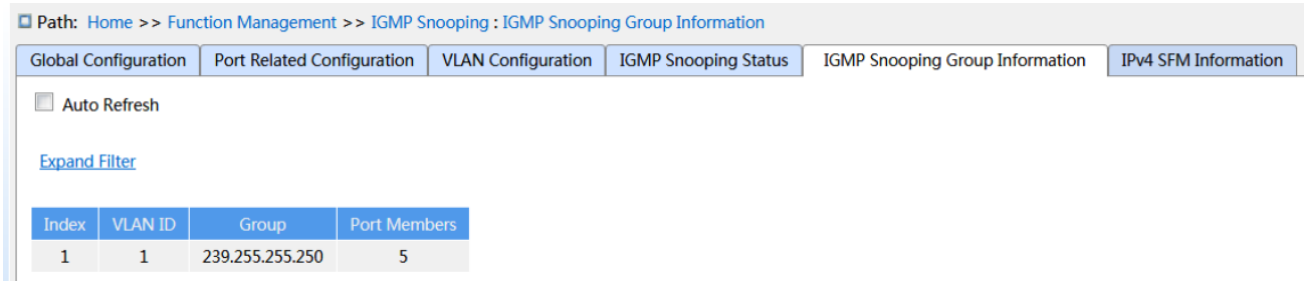


Рис. 164. Список участников IGMP Snooping

VLAN ID

Варианты конфигурации: * / >= / <= / selection range

Конфигурация по умолчанию: *

Функция: Отображение информацию о группе в соответствии с VLAN ID.

Group

Варианты конфигурации: * / >= / <= / selection range

Конфигурация по умолчанию: *

Функция: Отображение информации о группе в соответствии с настроенным адресом.

Port

Варианты конфигурации: */include/not include

Конфигурация по умолчанию: *

Функция: Отображение информации о группе в соответствии с настроенным портом.

6. Просмотр информации об IPv4 SMF.

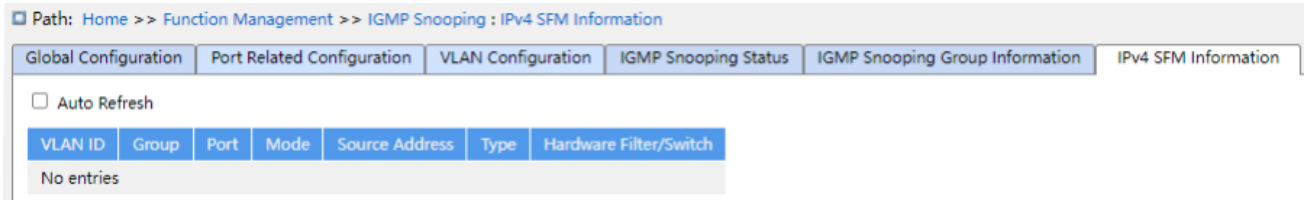


Рис. 165. Информация IGMP Snooping IPv4 SFM

Когда устройство использует протокол v3, хосты могут явно запрашивать получение или непринятие данных многоадресной рассылки от определенного

источника многоадресной рассылки.

7.10.5 Пример конфигурации

Как показано на рис. 166, включите функцию IGMP Snooping Коммутаторах 1, 2 и 3. Включите автоматический запрос (Querier Election) на Коммутаторах 2 и 3.

IP-адрес коммутатора 2 - 192.168.1.2; IP-адрес Коммутатора 3 - 192.168.0.2. Поэтому Коммутатор 3 выбран в качестве querier.

1. Включите IGMP Snooping для Коммутатора 1.
2. Включите IGMP Snooping и автоматический запрос (auto-query) для Коммутатора 2.
3. Включите IGMP Snooping и автоматический запрос (auto-query) для Коммутатора 3.

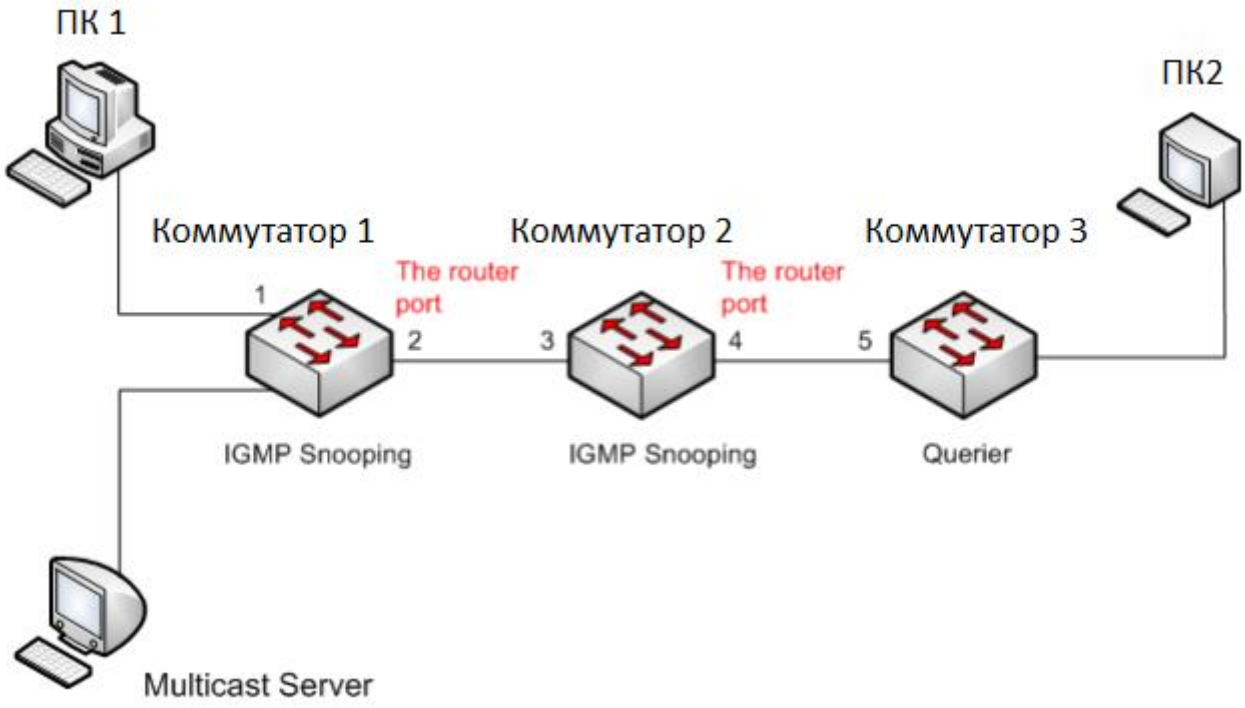


Рис. 166. Пример IGMP Snooping

- Поскольку Коммутатор 3 выбран в качестве querier, он периодически отправляет сообщение general query message.
- Порт 4 Коммутатора 2 получает сообщение запроса (query message). Он становится router port. Тем временем Коммутатор 2 пересылает сообщение запроса с порта 3. Затем порт 2 коммутатора 1 выбирается в качестве router

port, как только он получает сообщение запроса от Коммутатора 2.

- Когда ПК 1 присоединится к мультикаст группе 225.1.1.1, он отправит IGMP report message. Поэтому порт 1 и router port 2 Коммутатора 1 также присоединятся к мультикаст группе 225.1.1.1. Затем IGMP report message будет перенаправлено на Коммутатор 2 через router port 2, поэтому порт 3 и порт 4 Коммутатора 2 также присоединится к 225.1.1.1. Затем сообщение отчета IGMP report message будет перенаправлено на Коммутатор 3 через router port 4. Поэтому порт 5 Коммутатора 3 также присоединится к 225.1.1.1.
- Когда данные мультикаст рассылки достигают Коммутатора 1, данные будут перенаправлены на ПК1 через порт 1; поскольку router port 2 также является членом группы многоадресной рассылки, поэтому данные многоадресной рассылки будут перенаправлены через router port. Таким образом, когда данные достигнут порта 5 Коммутатора 3, они прекратят пересылку, поскольку получателя больше нет, но если ПК2 также присоединится к группе 255.1.1.1, то данные многоадресной рассылки будут перенаправлены на ПК2.

7.11 DHCP Конфигурация

С непрерывным расширением масштаба сетей и ростом сложности сетей, в условиях частого перемещения компьютеров (таких как ноутбуки или беспроводная сеть) протокол BootP (Bootstrap Protocol), разработанный специально для статической конфигурации конечных устройств, становится все более неспособным удовлетворять фактическим потребностям. Для быстрого доступа к сети и выхода из нее, а также повышения коэффициента использования ресурсов IP-адресов требуется автоматический механизм назначения IP-адресов на основе BootP. Для решения этих проблем был введен Dynamic Host Configuration Protocol (DHCP).

DHCP использует модель взаимодействия клиент-сервер. Клиент (DHCP Client) отправляет запрос конфигурации серверу (DHCP Server), а затем сервер отвечает

клиенту параметрами конфигурации, такими как IP-адрес, обеспечивая динамическую настройку IP-адресов. Структура типичного приложения DHCP показана на рисунке далее.

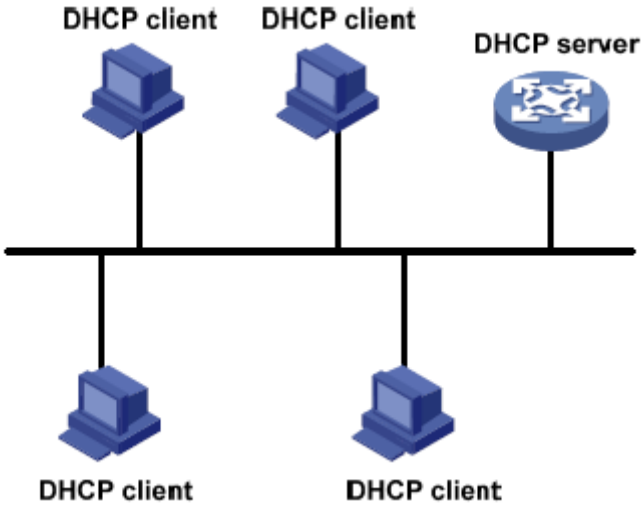


Рис. 167. Типовое применение DHCP

Поскольку пакеты отправляются в широковещательном режиме во время процесса получения динамического IP-адреса, DHCP-клиент и DHCP-сервер должны находиться в одном сегменте сети. Если они находятся в разных сегментах сети, клиент может взаимодействовать с сервером через DHCP relay.

DHCP поддерживает два типа распределения IP-адресов:

Статическое распределение (Static allocation): администратор сети статически привязывает фиксированные IP-адреса к нескольким конкретным клиентам, таким как WWW-сервер, и отправляет привязанные IP-адреса клиентам по DHCP. Срок аренды для статического распределения является постоянным.

Динамическое распределение (Dynamic allocation): DHCP-сервер динамически выделяет IP-адрес клиенту. Этот механизм распределения может выделять клиенту постоянный IP-адрес или IP-адрес с ограниченным сроком аренды. По истечении срока аренды клиенту необходимо повторно назначить IP-адрес. Сетевой администратор может выбрать механизм распределения DHCP для каждого клиента.

7.11.1 Конфигурация DHCP сервера

7.11.1.1 Введение

DHCP-сервер является поставщиком служб DHCP. Он использует DHCP-сообщения для связи с DHCP-клиентом, чтобы выделить клиенту подходящий IP-адрес и назначить клиенту другие сетевые параметры по мере необходимости. В следующих условиях DHCP-сервер обычно используется для распределения IP-адресов:

- Большой масштаб сети. Нагрузка, связанная с настройкой вручную, велика, и управлять всей сетью сложно.
- Число хостов превышает количество назначаемых IP-адресов, и он не может выделить фиксированный IP-адрес каждому хосту.
- Лишь немногим узлам в сети требуются фиксированные IP-адреса, а большинству узлов фиксированные IP-адреса не требуются.

7.11.1.2 Пул адресов DHCP

DHCP-сервер выбирает IP-адрес из пула адресов и распределяет его вместе с другими параметрами клиенту. Последовательность распределения IP-адресов следующая:

1. IP-адрес, статически привязанный к MAC-адресу клиента.

2. IP-адрес, записанный на DHCP-сервере, который когда-либо был выделен клиенту.

3. IP-адрес, указанный в сообщении запроса, отправленном от клиента.

4. Первый допустимый IP-адрес, найденный в пуле адресов.

5. Если доступного IP-адреса нет, проверьте IP-адрес, срок аренды которого истекает и у которого были конфликты, по порядку. Если найден, выделите IP-адрес. Если нет, процесс не выполняется.

7.11.1.3 Web конфигурация

1. Включение DHCP-сервера.

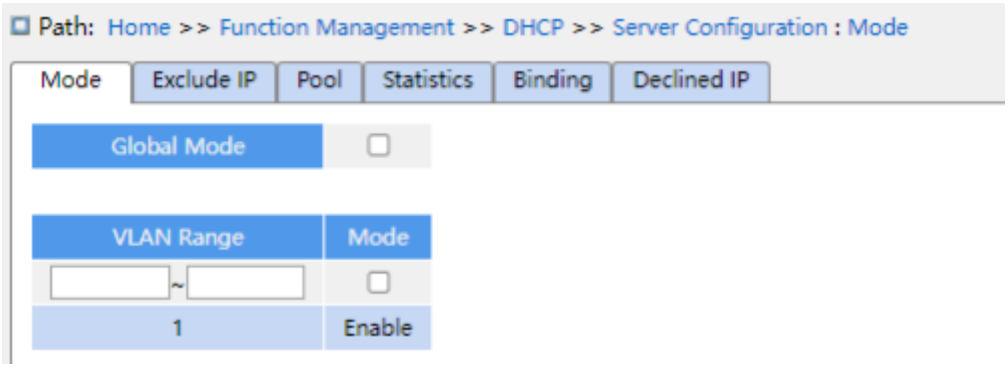


Рис. 168. Включение DHCP сервера

Global Mode

Варианты конфигурации: Disable/Enable

Конфигурация по умолчанию: Disable

Функция: Включение DHCP сервера на коммутаторе.

{VLAN Range, Mode}

Диапазон: {1~4093, Enable/Disable }

Функция: Если для VLAN клиента, который запрашивает IP-адрес, установлено значение Enable, DHCP-сервер выделяет IP-адрес клиенту. В противном случае DHCP-сервер не выделяет IP-адрес клиенту.

2. Создание пула DHCP-адресов

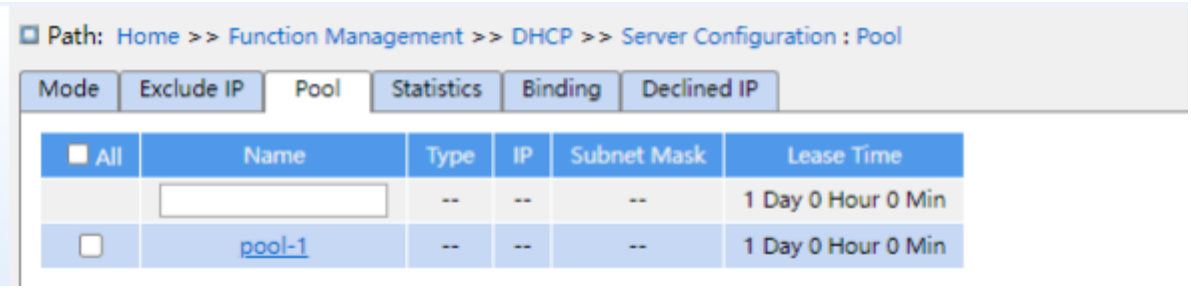


Рис. 169. Создание пула DHCP-адресов

Name

Диапазон: 1~32 символа

Функция: Настройка имени пула IP-адресов.

Нажмите < Apply >, чтобы создать новый пул DHCP-адресов.

3. Настройка пула DHCP-адресов.

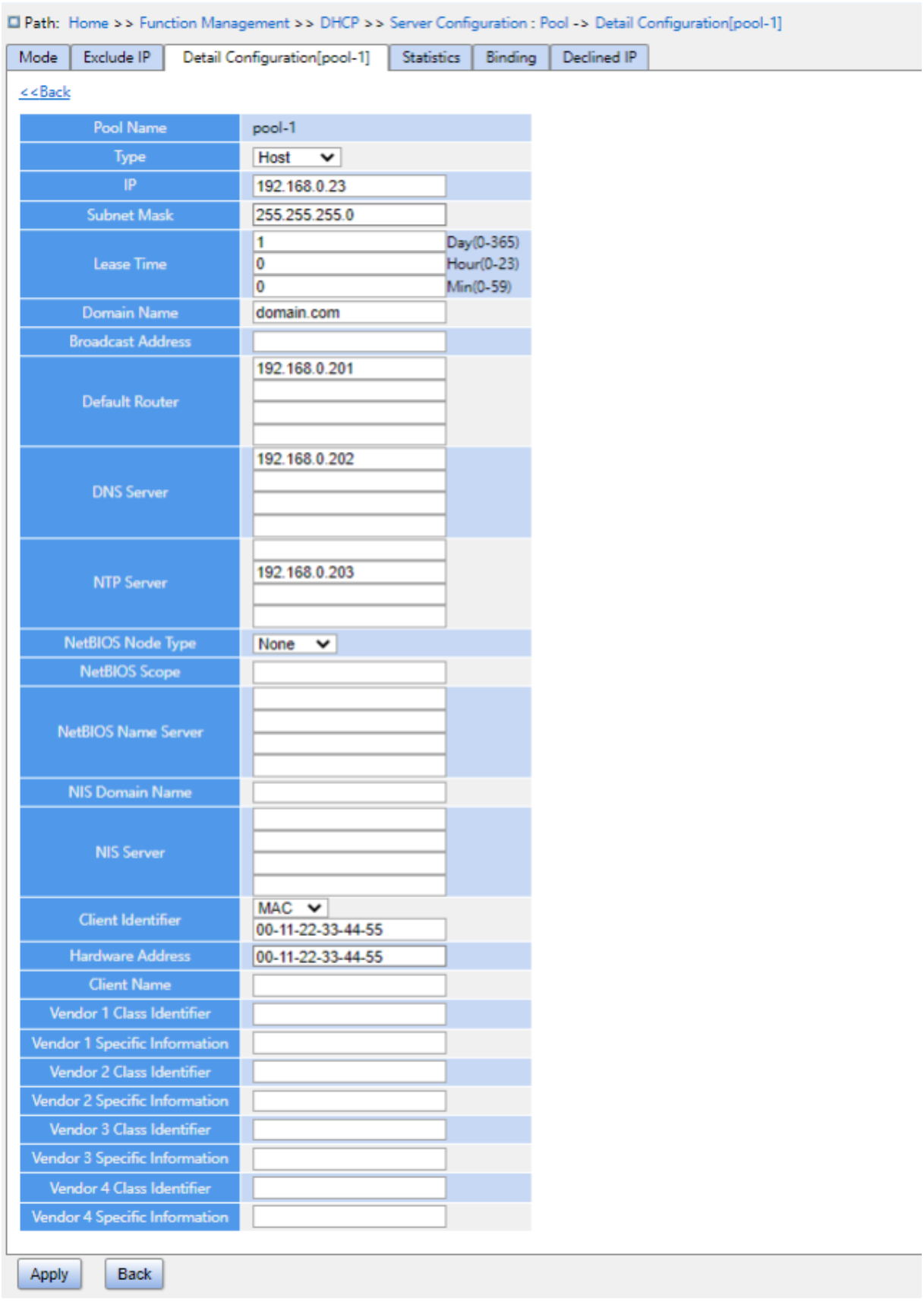


Рис. 170. Настройка пула IP-адресов

Type

Варианты конфигурации: None/Network/Host

Конфигурация по умолчанию: None

Функция: Настройте тип пула адресов. Network: коммутатор динамически распределяет IP-адреса нескольким DHCP-клиентам. Host: коммутатор поддерживает статическое распределение IP-адресов специальным DHCP-клиентам.

{IP, Subnet Mask}

Функция: Сеть указывает, что вы можете настроить диапазон пула IP-адресов, а диапазон адресов определяется маской подсети. Маска подсети представляет собой число длиной 32 бита и состоит из строки, равной 1, и строки, равной 0. "1" соответствует полям номера сети и полям номера подсети, в то время как "0" соответствует полям номера хоста.

Хост (Type Host) указывает, что вы можете настроить статически ограниченный IP-адрес клиента. Статическое распределение IP-адресов реализуется путем ограничения MAC-адреса и IP-адреса клиента. Когда клиент с этим MAC-адресом запрашивает IP-адрес, DHCP-сервер находит IP-адрес, соответствующий MAC-адресу клиента, и выделяет IP-адрес клиенту. Приоритет этого режима распределения выше, чем у динамического распределения IP-адресов, и срок аренды является постоянным.

Lease Time

Диапазон: 0 day 0 hour 0 minute~365 days 23 hours 59 minutes

(0 день 0 час 0 минута ~ 365 дней 23 часов 59 минут)

Конфигурация по умолчанию: 1 day 0 hour 0 minute

Описание: Настройте время ожидания динамического распределения. Для разных пулов адресов DHCP-сервер может устанавливать разное время аренды адресов.

Domain Name

Диапазон: 1~32 символа

Функция: Настройка доменного имени для пула IP-адресов. При выделении IP-адреса клиенту также отправляется суффикс доменного имени.

Broadcast Address

Формат: A.B.C.D

Функция: Настройка широковещательного адреса клиента, выделяемого DHCP-сервером.

Default Router

Формат: A.B.C.D

Функция: Настройка адреса клиентского шлюза, выделяемого DHCP-сервером.

Описание: Когда DHCP-клиент посещает хост, который находится в другом сегменте, данные должны пересылаться через шлюзы. Когда DHCP-сервер распределяет IP-адреса клиентам, он может одновременно указывать адреса шлюзов. Пул адресов DHCP можно настраивать на максимум 4 шлюза.

DNS Server

Формат: A.B.C.D

Функция: Настройка адреса клиентского шлюза, выделяемого DHCP-сервером.

Описание: Пул DHCP-адресов можно настраивать на максимум 4 DNS-сервера.

NTP Server

Формат: A.B.C.D

Функция: Настройка адреса клиентского NTP-сервера, выделяемого DHCP-сервером.

NetBIOS Node Type

Варианты конфигурации: None / B-node / P-node / M-node / H-node

Конфигурация по умолчанию: None

Функция: Настройка типа клиентского узла NetBIOS, выделяемого DHCP-сервером.

Описание: B-node получает сопоставление в режиме широковещательной передачи. P-node получает сопоставление, отправляя одноадресный пакет для связи с WINS-сервером. M-node получает сопоставление, отправляя широковещательный пакет в первый раз. Если M-node не удается получить сопоставление с первого раза, он получает сопоставление, отправляя одноадресный пакет для связи с WINS-

сервером во второй раз. H-node получает сопоставление, отправляя одноадресный пакет для связи с WINS-сервером в первый раз. Если H-node не удается получить сопоставление в первый раз, он получает сопоставление, отправляя широковещательный пакет во второй раз.

NetBIOS Scope

Диапазон: 1~32 символа

Функция: Настройка имени NetBIOS.

NetBIOS Name Server

Формат: A.B.C.D

Функция: Настройка адреса клиентского WINS-сервера, выделяемого DHCP-сервером.

Описание: Для клиента, работающего под управлением операционной системы Microsoft Windows (OS), сервер Windows Internet Naming Service (WINS) предоставляет услугу преобразования имени хоста в IP-адрес для хоста, который использует протокол NetBIOS для связи. Поэтому большинству клиентов на базе ОС Windows требуется настройка WINS. Чтобы разрешить DHCP-клиенту преобразовывать имя хоста в IP-адрес, укажите адрес WINS-сервера, когда DHCP-сервер выделяет IP-адрес клиенту. В пуле DHCP-адресов можно настроить максимум 4 WINS-сервера.

NIS Domain Name

Диапазон: 1~32 символа

Функция: Настройка доменного имени NIS клиента, выделяемого DHCP-сервером.

NIS Server

Формат: A.B.C.D

Функция: Настройка адреса клиентского NIS-сервера, выделяемого DHCP-сервером.

Client Identifier

Варианты конфигурации: None / FQDN / MAC

Конфигурация по умолчанию: None

Функция: Если тип пула - host, укажите уникальный идентификатор клиента.

Hardware Address

Формат: HH-HH-HH-HH-HH-HH (H - шестнадцатеричное число)

Функция: Если тип пула - host, настройте статически привязанный MAC-адрес клиента.

Client Name

Диапазон: 1~32 символа

Функция: Настройка имени пользователя для клиента.

Vendor i Class Identifier

Диапазон: 1~64 символа

Функция: Настройка Vendor Class Identifier для клиента, назначаемого DHCP-сервером.

Vendor I Specific Information

Диапазон: 1~64 шестнадцатеричное число

Функция: Настройка Vendor Specific Information для клиента, назначаемого DHCP-сервером.

4. Настройка исключенных (excluded) IP-адресов (IP-адреса не распределяются динамически в пуле DHCP-адресов).

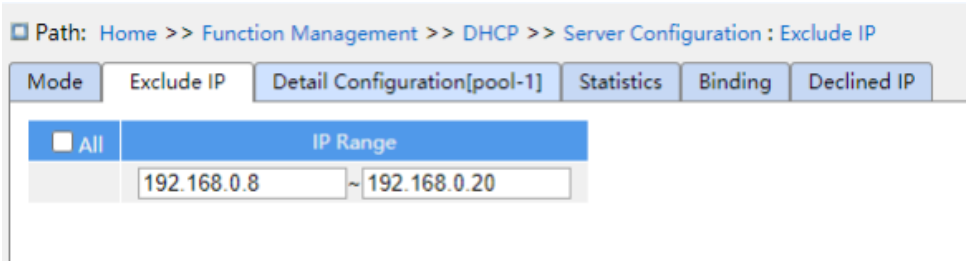


Рис. 171. Настройка excluded IP-адресов

IP Range

Функция: Настройка диапазона IP-адресов, которые не распределяются динамически в пуле DHCP-адресов. При распределении IP-адресов DHCP-сервер должен исключить занятый IP-адрес (например, IP-адреса шлюза и DNS-сервера).

5. Просмотр статистической информации DHCP-сервера.

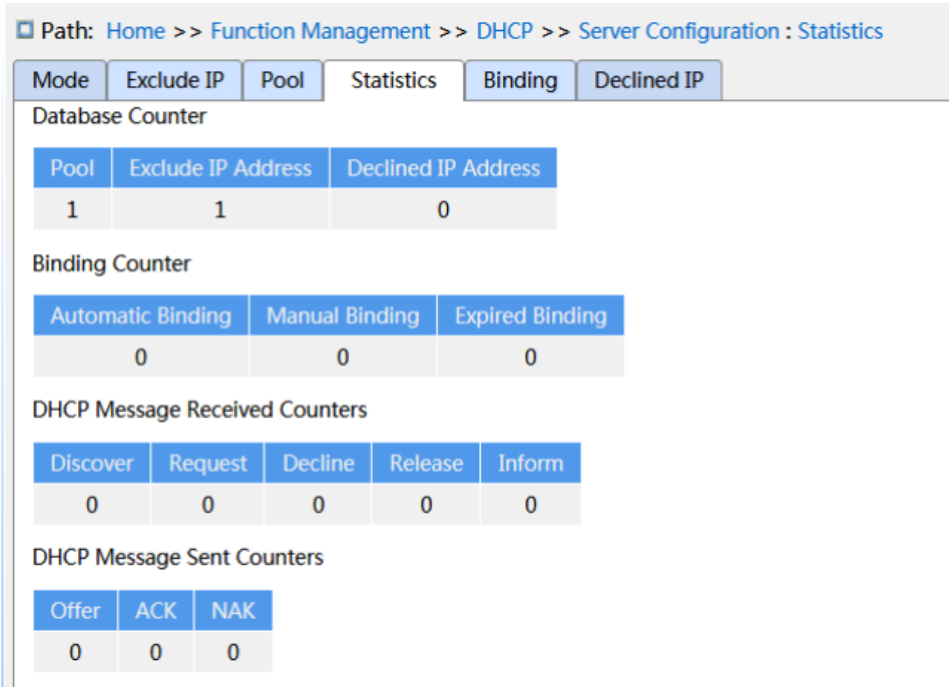


Рис. 172. Просмотр статистики DHCP-сервера

6. Просмотр информации об IP-адресах, выделенных DHCP-сервером.

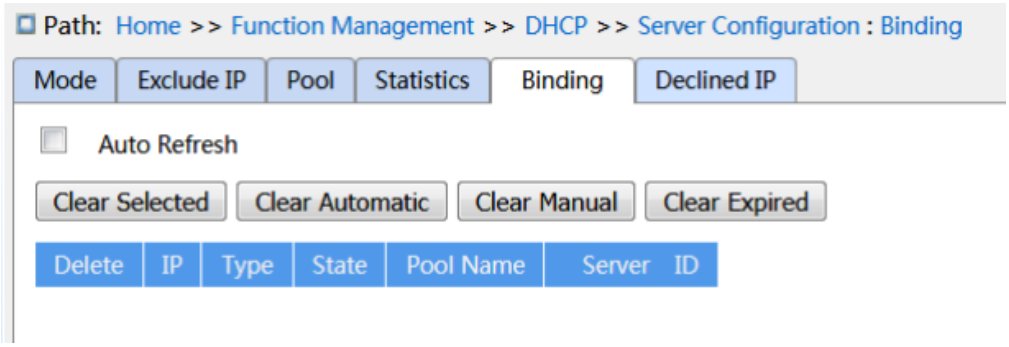


Рис. 173. Просмотр Bindind для DHCP-сервера

7. Просмотр IP-адресов, отклоненных DHCP-клиентами.

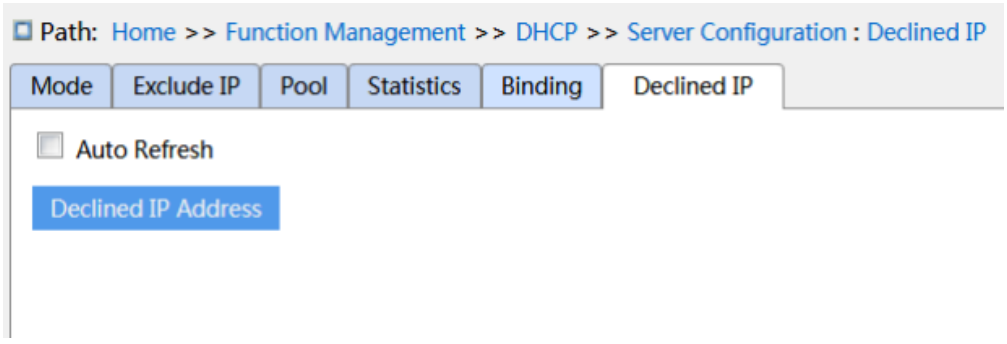


Рис. 174. Просмотр Declined IP для DHCP-сервера

Когда клиент обнаруживает, что IP-адрес, назначенный сервером, конфликтует со статическим IP-адресом в сегменте сети, он отправляет серверу сообщение об отказе

от получения IP-адреса. Сервер записывает IP-адрес, который клиент отклоняет, и не будет выделять IP-адрес другим клиентам в течение определенного периода времени.

7.11.1.4 Пример конфигурации

Как показано на рис. 175, Коммутатор A работает как DHCP-сервер, а Коммутатор B работает как DHCP-клиент. Порт 3 коммутатора A соединяется с портом 4 коммутатора B. Клиент отправляет сообщения с запросом IP-адреса, и сервер может назначить IP-адрес клиенту двумя способами. Когда DHCP-сервер динамически выделяет IP-адрес, исключенный диапазон IP-адресов составляет 192.168.0.1~192.168.0.10.

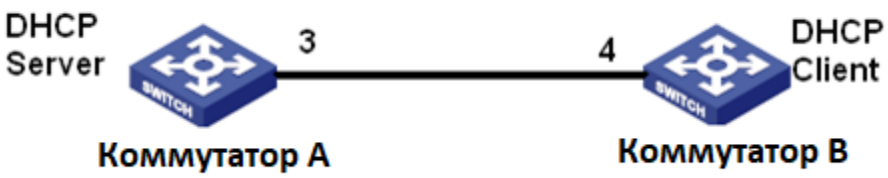


Рис. 175. Пример конфигурации DHCP

Статически выделяемые IP-адреса

➢ Конфигурация Коммутатора A:

1. Включите статус DHCP-сервера в соответствующих VLAN, как показано на рис. 168.

2. Создайте пул IP DHCP: pool-1, как показано на рис. 169.

3. Установите тип пула как Host; IP-адрес как 192.168.0.6; маску как 255.255.255.0; Привяжите MAC-адрес Коммутатора B: 00-11-22-33-44-55, как показано на рис. 170.

➢ Конфигурация Коммутатора B:

1. Настройте Коммутатор B на автоматическое получение IP-адреса через DHCP.

2. Коммутатор B получает IP-адрес 192.168.0.6 и маску подсети 255.255.255.0 от DHCP-сервера, как показано на рис. 176.

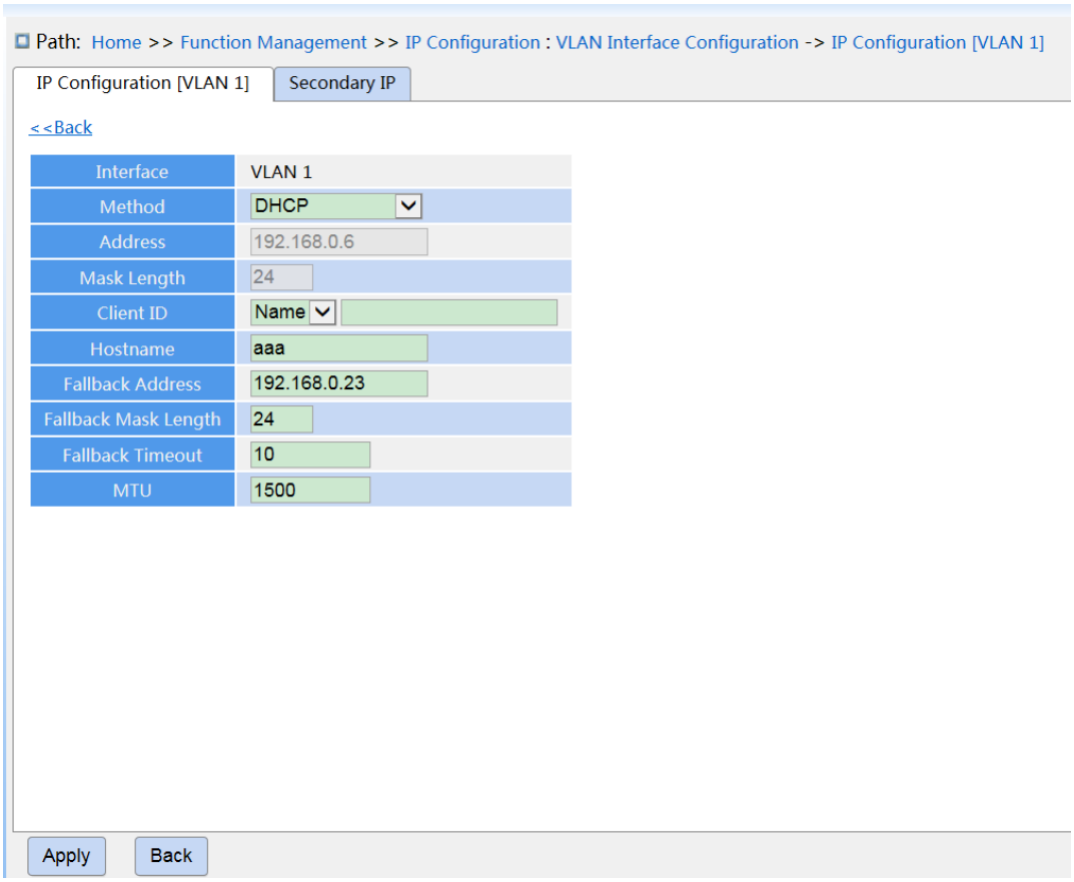


Рис. 176. Пример DHCP

Динамически выделяемые IP адреса

➢ Конфигурация Коммутатора A:

1. Включите статус DHCP-сервера в соответствующих VLAN, как показано на рис. 168.

2. Создайте пул IP DHCP: pool-2, как показано на рис. 169.

3. Установите тип пула как Network; IP-адрес как 192.168.0.6; маску как 255.255.255.0, остальное - конфигурация по умолчанию, как показано на рис. 170.

4. Настройте диапазон исключенных IP-адресов как 192.168.0.1~192.168.0.10, как показано на рис. 171.

➢ Конфигурация Коммутатора B:

1. Настройте Коммутатор B на автоматическое получение IP-адреса через DHCP.

2. DHCP-сервер выполняет поиск назначаемых IP-адресов в пуле адресов по порядку и выделяет Коммутатору B первый найденный назначаемый IP-адрес и другие

сетевые параметры. Маска подсети - 255.255.255.0.

Настройки, как показано на рис. 177.

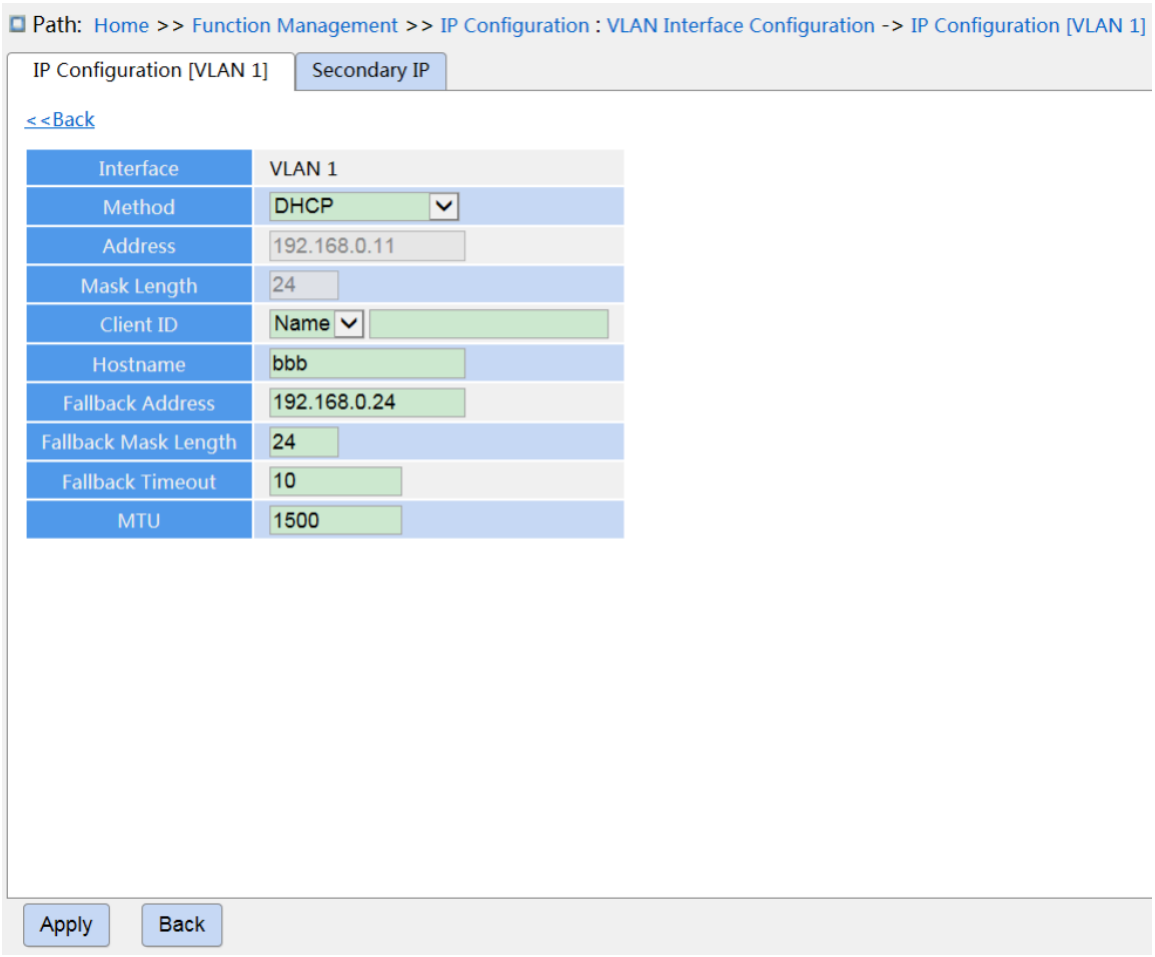


Рис. 177. Пример DHCP

7.11.2 DHCP Snooping

7.11.2.1 Введение

DHCP Snooping - это функция мониторинга служб DHCP на уровне layer 2 и функция безопасности DHCP. Механизм безопасности DHCP Snooping может контролировать, чтобы только доверенный порт мог пересылать сообщение запроса DHCP-клиента на легальный сервер, в то же время он может контролировать источник ответного сообщения DHCP-сервера, гарантируя клиенту получение IP-адреса с действительного сервера. Механизм безопасности DHCP Snooping разделяет порт на доверенный порт и ненадежный порт.

Доверенный порт (trusted port): это порт, который напрямую или косвенно

подключается к действительному DHCP-серверу. Доверенный порт обычно пересылает сообщения запроса DHCP-клиентов и ответные сообщения DHCP-серверов, чтобы гарантировать, что DHCP-клиенты могут получать действительные IP-адреса.

Ненадежный порт (untrusted port): это порт, который соединяется с недействительным DHCP-сервером. Ненадежный порт не пересылает сообщения запроса DHCP-клиентов и ответные сообщения DHCP-серверов, чтобы предотвратить получение DHCP-клиентами недопустимых IP-адресов.

7.11.2.2 Web конфигурация

1. Конфигурация функции DHCP Snooping

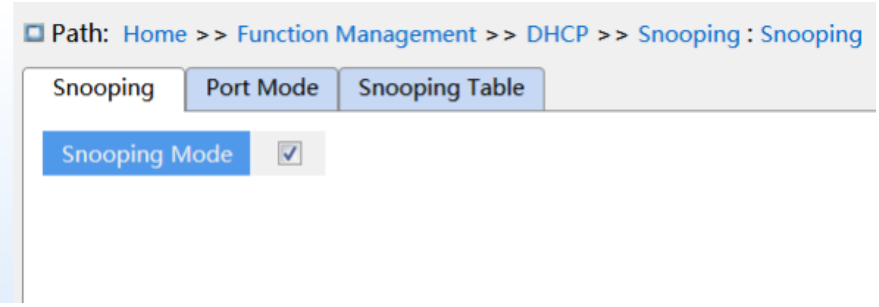


Рис. 178. Включение DHCP Snooping

DHCP Snooping Mode

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение DHCP Snooping.

Коммутатор, работающий как DHCP-сервер и клиент, не может включить функцию DHCP Snooping.

2. Конфигурация доверенных (trusted) портов.

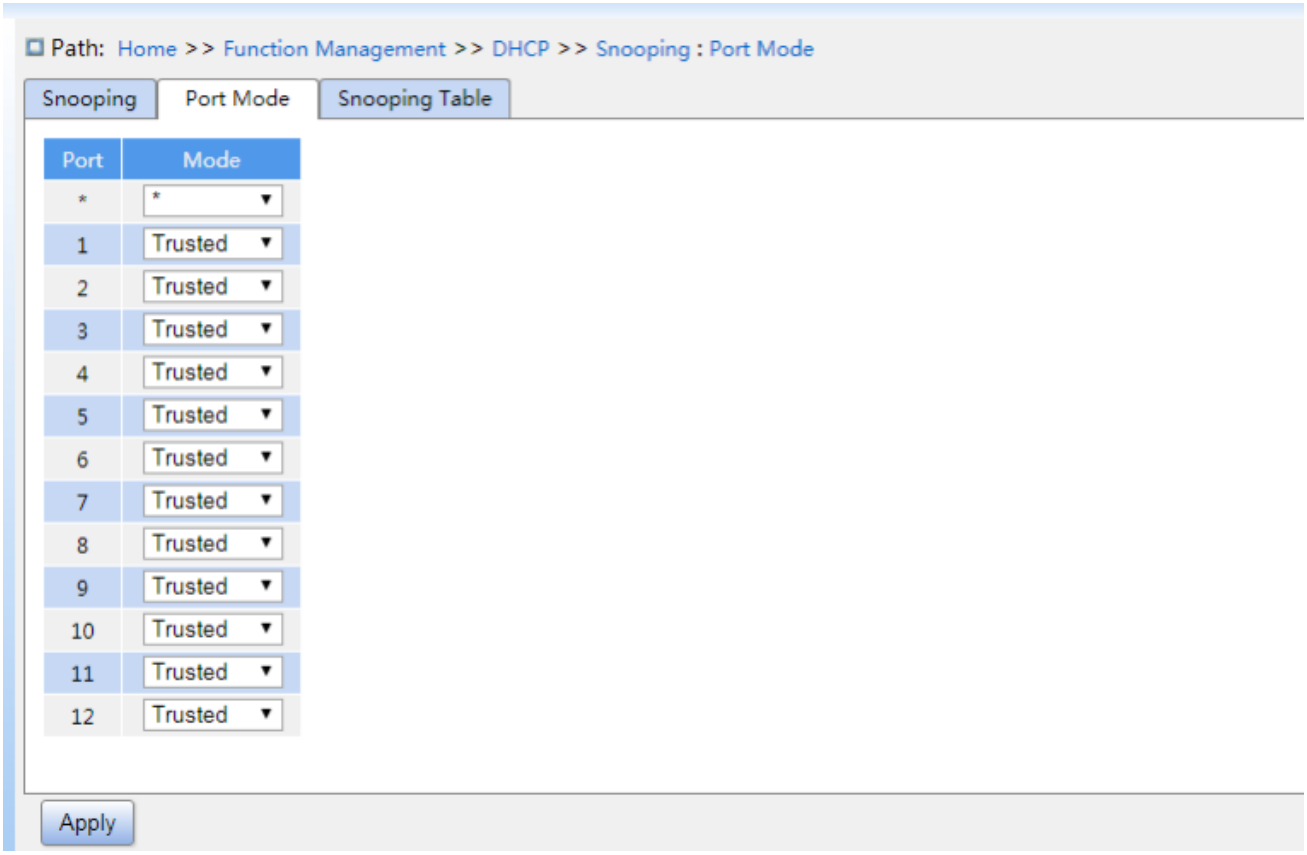


Рис. 179. Конфигурация trusted портов

Mode

Варианты конфигурации: Trusted/Untrusted

Конфигурация по умолчанию: Trusted

Функция: Установите для порта значение доверенный порт или ненадежный порт. Порты, которые прямо или косвенно подключаются к действительным DHCP-серверам, являются доверенными портами.

3. Просмотр записей DHCP snooping.

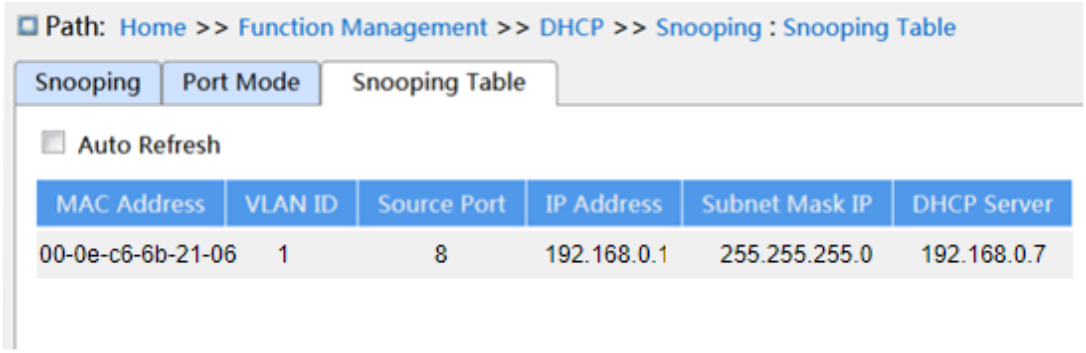


Рис. 180. Просмотр сосотяния DHCP snooping

7.11.2.3 Пример конфигурации

DHCP-клиент запрашивает IP-адрес у DHCP-сервера. В сети существует неавторизованный DHCP-сервер. Установите порт 1 в качестве доверенного порта с помощью DHCP Snooping, чтобы переслать сообщение запроса DHCP-клиента на DHCP-сервер и переслать ответное сообщение DHCP-сервера DHCP-клиенту. Установите порт 3 на ненадежный порт, который не может переслать сообщение запроса DHCP-клиента и ответное сообщение неавторизованного DHCP-сервера, гарантируя, что клиент сможет получить действительный IP-адрес от действительного DHCP-сервера.

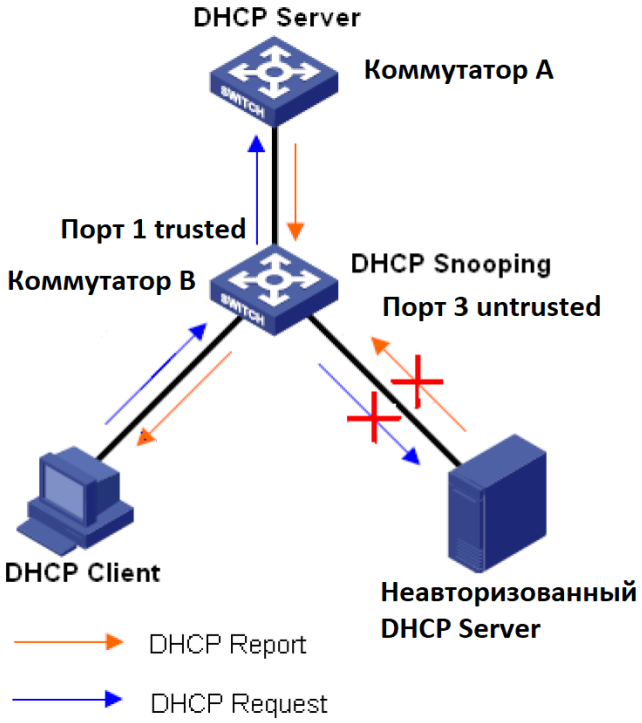


Рис. 181. Пример конфигурации DHCP Snooping

Конфигурация Коммутатора B:

Включите функцию отслеживания DHCP, как показано на рис. 178.

Установите порт 1 коммутатора B на доверенный (trusted) порт и установите порт 3 доверенный (trusted) порт, как показано на рис. 179.

7.11.3 DHCP Relay

7.11.3.1 Введение

1. DHCP Realy

DHCP relay (ретрансляция) - это пересылка DHCP-пакетов между DHCP сервером и клиентом. Если DHCP-клиент находится не в той же подсети, что и сервер, должен быть DHCP ретранслятор для пересылки сообщений запроса DHCP и ответа на них. Переадресация данных DHCP ретранслятора отличается от обычной маршрутной переадресации. Обычная маршрутная переадресация относительно прозрачна, и устройство, как правило, не изменяет содержимое IP-пакета. Однако после получения DHCP сообщения DHCP ретранслятор восстановит DHCP сообщение и затем переадресует его. С точки зрения DHCP клиента агент ретрансляции DHCP подобен DHCP серверу; с точки зрения DHCP сервера агент ретрансляции DHCP подобен DHCP клиенту.

DHCP ретранслятор (relay) пересылает полученный пакет запроса DHCP на DHCP сервер в режиме одноадресной рассылки и пересылает полученный пакет ответа DHCP DHCP клиенту. DHCP ретранслятор отвечает за связь DHCP клиентов и DHCP серверов, расположенных в разных сегментах сети. Он реализует динамическое управление IP-адресами для нескольких сегментов сети, то есть динамическое управление IP-адресами DHCP в режиме клиент-ретранслятор-сервер, как показано далее.

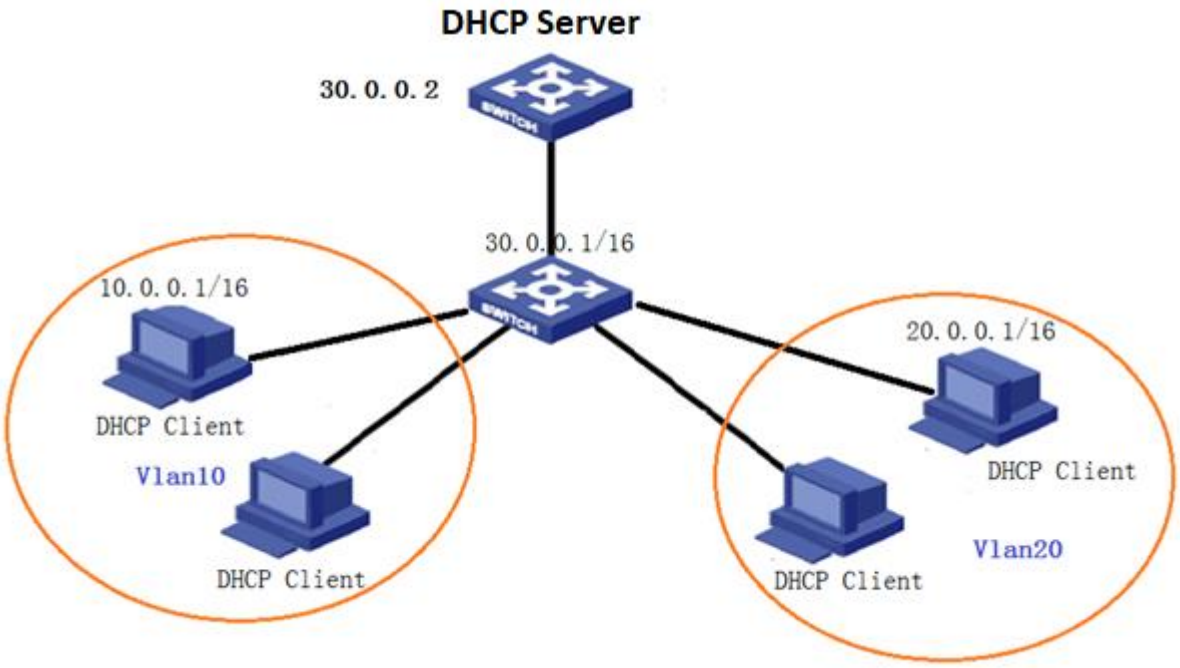


Рис. 182. Режим Client-Relay-Server

2. DHCP Relay Agent Information(option 82)

Когда relay выполняет DHCP-ретрансляцию, есть возможность добавить некоторые опции для указания некоторой сетевой информации DHCP-клиента, чтобы сервер мог назначать пользователям разные IP-адреса в соответствии с более точной информацией. Согласно RFC 3046, номер используемого параметра option равен 82.

Option 82 (Relay Agent Information Entry) записывает информацию о клиенте. Когда функция отслеживания DHCP, поддерживаемая Option 82, получает сообщение запроса от DHCP-клиента, она добавляет соответствующее поле Option 82 в сообщения и затем пересылает сообщение на DHCP-сервер. Сервер, поддерживающий Option 82, может гибко распределять адреса в соответствии с сообщением Option 82.

Поле Option 82 коммутаторов данной серии содержит дополнительные опции: Sub-option 1 (Circuit ID) и Sub-option 2 (Remote ID). Форматы опций показаны далее.

- Дополнительная опция 1 (Sub-option 1) содержит VLAN ID и номер порта, на который поступает сообщение запроса от DHCP-клиента, как показано в таблице далее.
-

Таблица 7. Формат Sub-option 1

Sub-option type（0x01）	Length（0x04）	VLAN ID	Port number
1 байт	1 байт	2 байта	2 байта

Sub-option type: тип дополнительной опции 1 равен 1.

Length: количество байт, которые занимают VLAN ID и номер порта.

VLAN ID: На устройстве DHCP Realy VLAN ID порта, который получает сообщение запроса от DHCP клиента.

Port number: На устройстве DHCP Realy номер порта, на который поступает сообщение запроса от DHCP клиента.

- Sub-option2 содержит MAC-адрес устройства DHCP Relay, которое получает сообщение запроса от DHCP клиента, как показано в таблице далее.

Таблица 8. Формат Sub-option 2

Sub-option type（0x02）	Length（0x06）	MAC адрес
1 байт	1 байт	6 байт

Sub-option type: тип дополнительной опции 2 равен 2

Length: количество байт, которое занимает содержимое sub-option2. MAC-адрес занимает 6 байт, а символьная строка - 16 байт.

MAC-адрес: содержимое sub-option2 - это MAC-адрес устройства DHCP Realy, которое получает сообщение запроса от DHCP-клиента.

Если DHCP Relay поддерживает функцию Option 82, когда DHCP Relay получает сообщение с запросом DHCP, он обработает сообщение с запросом в соответствии с тем, содержит ли сообщение Option 82 и политику клиента, а затем перенаправит обработанное сообщение на DHCP-сервер. Метод обработки показан в таблице далее.

Таблица 9. DHCP Relay обработка запросов

Запрос от DHCP клиента	**Конфигурация политики**	**DHCP Relay обработка запроса**
Сообщение содержит Option 82	Drop	Отбросить сообщение
	Keep	Сохраните формат сообщения без изменений и переслать сообщение
	Replace	Заменить поле Option 82 в сообщении полем Option 82 отслеживающего устройства и переслать новое сообщение
Сообщение не содержит Option 82	Drop/Keep/Replace	Добавить поле Option 82 устройства DHCP Relay в сообщение и переслать его

Когда устройство DHCP Relay получает сообщение от DHCP-сервера, и если сообщение содержит поле Option 82, то устройство удалит поле Option 82 и перешлет сообщение клиенту.

7.11.3.2 Web конфигурация

1. Включение функции DHCP Relay на коммутаторе.

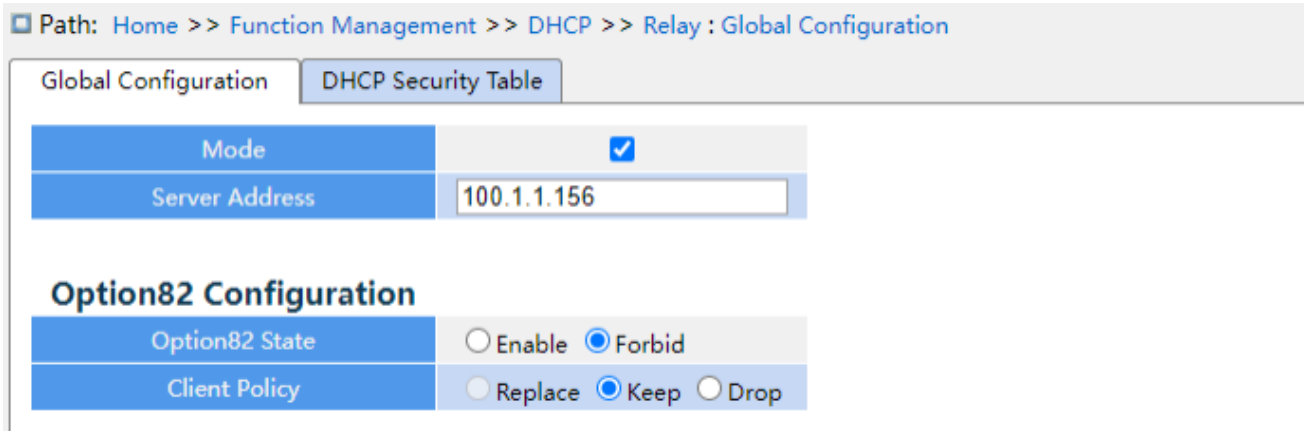


Рис. 183. Включение функции DHCP Relay

Mode

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включение DHCP Relay на коммутаторе.

Server Address

Функция: Настройте адрес DHCP-сервера.

Option82 Sate

Варианты конфигурации: Enable/forbid

Конфигурация по умолчанию: Forbid

Функция: Включить option82 для DHCP-ретрансляции (relay).

Client Policy

Варианты конфигурации: Replace/keep/drop

Конфигурация по умолчанию: Keep

Функция: Настройте политику клиента. DHCP relay обработает сообщение запроса, отправленное клиентом, в соответствии с политикой клиента.

2. Просмотр таблицы безопасности DHCP.

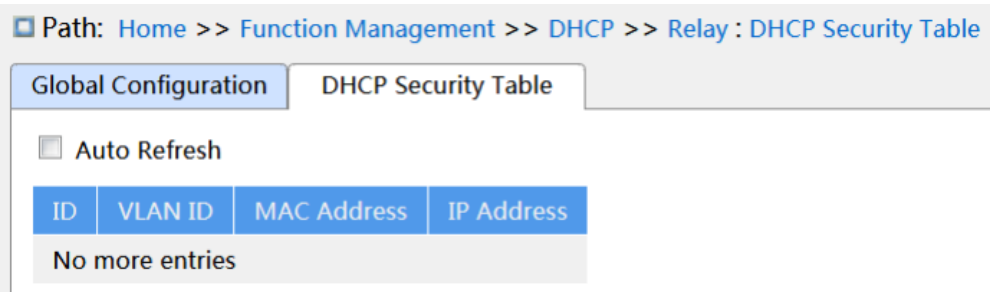


Рис. 184. Просмотр таблицы безопасности DHCP

7.11.3.3 Пример конфигурации

Коммутатор A в качестве DHCP-сервера, коммутатор B в качестве DHCP relay, коммутатор C в качестве DHCP-клиента и порт 1 коммутатора A подключаются к порту 1 коммутатора B, порт 2 коммутатора B подключается к порту 2 коммутатора C. DHCP-сервер находится не в той же локальной сети, что и DHCP-клиент. Клиент динамически получает IP-адрес и другие сетевые параметры в режиме DHCP через DHCP relay.

Рис. 185. Пример конфигурации DHCP Relay

Конфигурация Коммутатора A:

1. Создайте VLAN1 и настройте IP: 100.1.1.156, как показано на рис. 99;

2. Откройте состояние DHCP сервера в VLAN 1, как показано на рис.99 ;

3. Создайте пул адресов pool-33, как показано на рис. 169;

4. выберите тип пула адресов как Network; IP-адрес: 33.1.1.6; Маска: 255.0.0.0;

Конфигурация Коммутатора B:

1. Создайте VLAN1 и настройте IP: 100.1.1.180, как показано на рис. 99;

2. Создайте VLAN 33 и настройте IP: 33.1.1.2, как показано на рис. 99;

3. Включите DHCP relay, как показано на рис. 183;

4. Настройте IP-адрес сервера: 100.1.1.156, как показано на рис. 183;

Конфигурация Коммутатора C:

1. Создайте VLAN 33 и включите DHCP клиент, как показано на рис. 99;

2. Коммутатор A назначает IP-адрес 33.0.0.1 коммутатору C.

7.12 Конфигурация IEEE802.1X

7.12.1 Введение

В качестве общего механизма контроля доступа к портам локальной сети протокол 802.1X реализует аутентификацию и безопасность в сети Ethernet. 802.1X - это управление доступом в сети на основе портов (Port Based Network Access Control). Управление доступом в сети на основе портов предназначено для реализации аутентификации и контроля портов для устройств в локальной сети. Если пользователь проходит аутентификацию, он может получить доступ к ресурсам в локальной сети. Системы стандарта 802.1X используют структуру Клиент/сервер (Client/Server), как

показано далее. Для аутентификации пользователя и авторизации управления доступом на основе портов требуются следующие элементы:

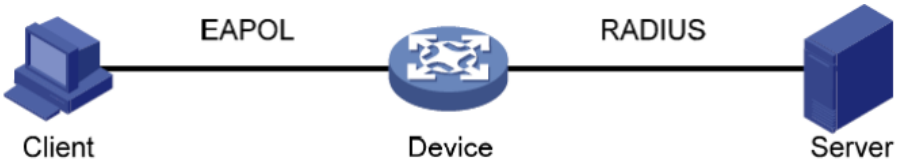


Рис. 186. Структура IEEE802.1X

Client (клиент): обычно представляет собой пользовательский терминал. Когда пользователь хочет выйти в Интернет, он запускает клиентскую программу и вводит требуемые имя пользователя и пароль. Клиентская программа отправит запрос на подключение. Клиент должен поддерживать EAPOL (Extensible Authentication Protocol over LAN).

Device (устройство): представляет собой коммутатор аутентификации в сети Ethernet. Он загружает и доставляет информацию об аутентификации пользователя, а также включает или отключает порт в зависимости от результата аутентификации.

Authentication server (сервер аутентификации): представляет из себя службу аутентификации для устройств. Проверяет, есть ли у пользователей разрешения на использование сетевых служб в соответствии с идентификаторами (именами пользователей и паролями), отправляемыми клиентами, и включает или отключает порты в соответствии с результатами аутентификации.

7.12.2 Web конфигурация

1. Конфигурация диспетчера задач (Task Manager) для 802.1X.

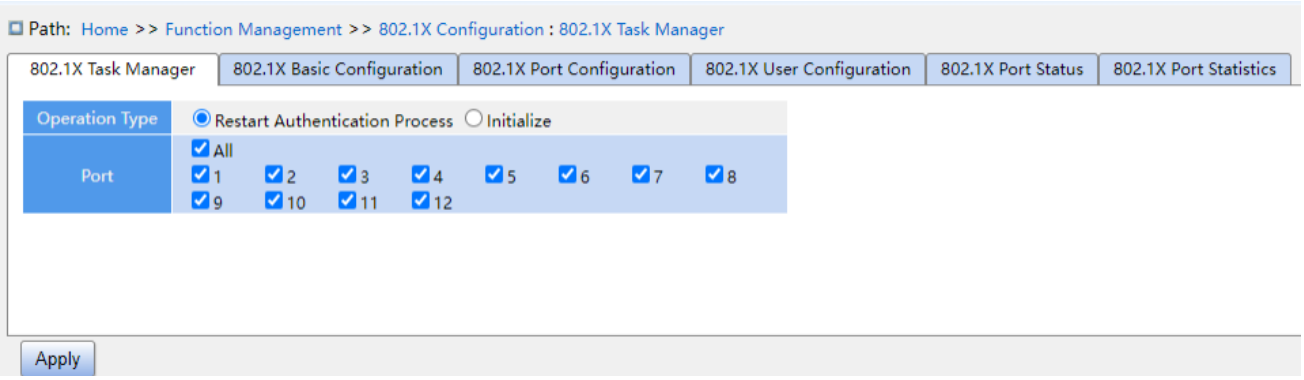


Рис. 187. Конфигурация Task Manager

Operation Type

Варианты конфигурации: Restart Authentication Process / initialize

Функция: Когда для порта выбирается режим аутентификации на основе Mac (Mac-Based) и 802.1X на основе порта (port-based), вы можете выбрать <Restart Authentication Process>/<Initialize> для повторной аутентификации. Во время процесса повторной аутентификации статус порта переключается в состояние не прошедший проверку подлинности (unauthenticated state).

Port

Функция: Выберите порт, который необходимо Restart Authentication Process / initialize.

2. Базовая конфигурация IEEE802.1X.

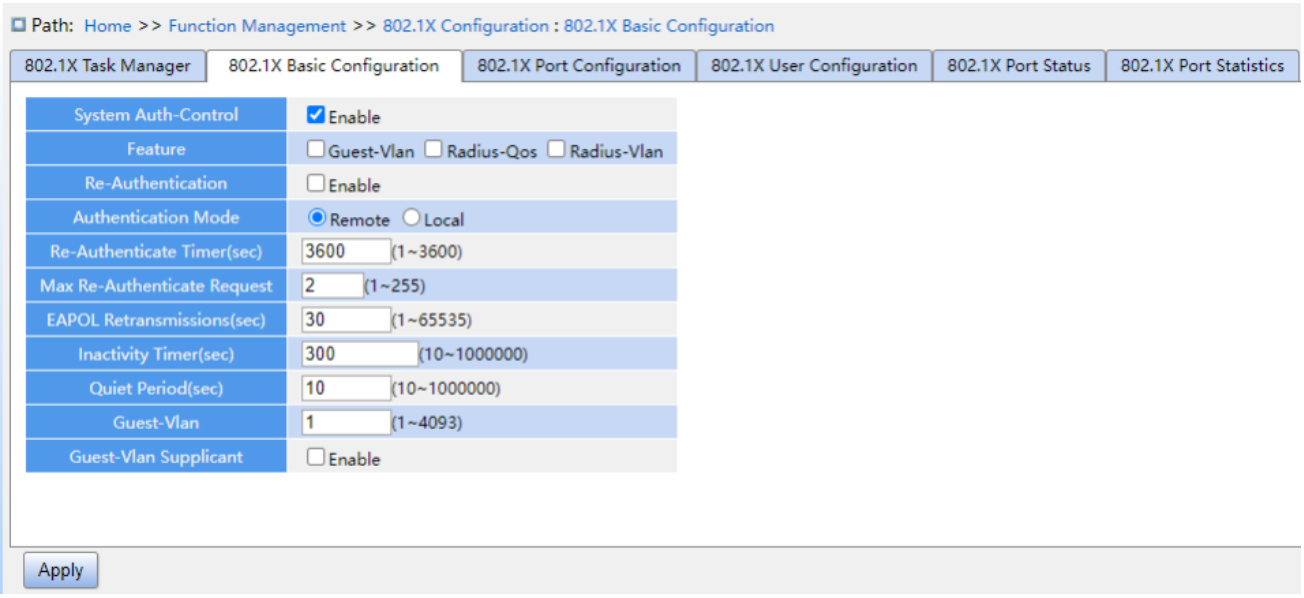


Рис. 188. Базовая конфигурация IEEE802.1X

System Auth-Control

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включение/выключение протокола безопасности IEEE802.1x.

Guest-VLAN

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: При включении, если пользователь не аутентифицирован или ему не удается пройти аутентификацию, устройство добавляет порт аутентификации клиента в гостевую (guest) VLAN. Все пользователи, которые обращаются к этому порту, авторизованы для доступа к ресурсам в гостевой VLAN.

RADIUS-QOS

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: При включении, после прохождения клиентом аутентификации, сервер передает информацию авторизации на устройство. Если на сервере настроена функция RADIUS-QOS, то информация авторизации включает информацию CoS. Устройство изменит значение CoS порта аутентификации клиента в соответствии с назначенным значением.

RADIUS-VLAN

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: При включении, после прохождения клиентом аутентификации, сервер передает информацию авторизации на устройство. Если на сервере настроена функция RADIUS-VLAN, то информация авторизации включает информацию VLAN. Устройство добавляет порт аутентификации клиента в назначенную VLAN.

Re-Authentication

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Настройте, требуется ли регулярная повторная аутентификация при аутентификации (чтобы регулярно определять онлайн-статус пользователя).

Authentication Mode

Варианты конфигурации: Remote/Local

Конфигурация по умолчанию: Remote

Функция: Настройте режим аутентификации RADIUS как удаленную аутентификацию или локальную аутентификацию.

Re-Authenticate Timer

Диапазон: 1~3600 сек.

Конфигурация по умолчанию: 3600 сек.

Функция: При успешной аутентификации установите временной интервал для повторной аутентификации. Только если Re-Authentication в Enable.

Max Re-Authenticate Request

Диапазон: 1~255

Конфигурация по умолчанию: 2

Функция: Установите максимальное количество попыток повторной передачи для пакетов запроса идентификации EAPOL. Если устройство по-прежнему не получает ответных пакетов от клиента после максимального количества попыток повторной передачи, устройство будет считать, что аутентификация завершилась неудачно.

EAPOL Retransmissions

Диапазон: 1~65535 сек.

Конфигурация по умолчанию: 30 сек.

Функция: Установите время ожидания ответа от клиента. После отправки запроса Identity EAPOL устройство повторно передаст запрос Identity EAPOL, если по истечении указанного времени оно по-прежнему не получит ответа от клиента.

Inactivity Timer

Диапазон: 10~1000000 сек.

Конфигурация по умолчанию: 300 сек.

Функция: При аутентификации на основе MAC, если после успешной аутентификации в течение этого времени не пройдет ни одного пакета, соответствующая запись безопасности будет удалена.

Quiet Period

Диапазон: 10~1000000 сек.

Конфигурация по умолчанию: 10 сек.

Функция: Если аутентификация завершается неудачно, устройство переходит в режим ожидания. Во время периода ожидания устройство не отвечает на запросы аутентификации от клиента.

Guest-VLAN

Варианты конфигурации: 1~4093

Конфигурация по умолчанию: 1

Функция: Настройка гостевой VLAN ID.

Guest-VLAN Supplicant

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: При Enable, если пользователь не аутентифицирован или ему не удается пройти аутентификацию, устройство добавляет порт аутентификации клиента в гостевую VLAN. При Disable устройство добавляет порт в гостевую VLAN только в том случае, если на этом порте нет записи EAPOL.

- Обязательным условием для настройки параметров Guest-VLAN , Max Re-Authenticate Request, Guest-Vlan Supplicant является включение гостевой VLAN.
- Если тип порта аутентификации клиента Trunk или Hybrid, не рекомендуется включать RADIUS-VLAN и Guest-VLAN.
- CoS, назначенный авторизацией, не меняет конфигурацию порта. Однако CoS,

назначенный авторизацией, имеет более высокий приоритет, чем CoS, настроенный пользователем. Действительным после аутентификации является значение CoS, назначенное для авторизации. Если пользователь не проходит аутентификацию или переходит в автономный режим, значение CoS, настроенное пользователем, вступает в силу.

- VLAN, назначенная для авторизации, или гостевая VLAN не изменяют конфигурацию порта. Однако VLAN, назначенная для авторизации, или гостевая VLAN имеет более высокий приоритет, чем VLAN, настроенная пользователем.

После того, как пользователь начинает аутентификацию, и если аутентификация прошла успешно:

Если порт включает RADIUS-VLAN, порт добавляется к VLAN, назначенной сервером RADIUS.

Если порт не включает RADIUS-VLAN, порт добавляется к VLAN, настроенной пользователем.

Если пользователю не удается пройти аутентификацию или он переходит в автономный режим:

Если порт поддерживает Guest-VLAN и Guest-Vlan Supplicant, порт добавляется в VLAN.

Если порт включает Guest-VLAN, но не включает Guest-Vlan Supplicant, порт добавляется в гостевую VLAN, когда запись EAPOL недоступна. И добавляется в VLAN, настроенную пользователем, когда доступна запись EAPOL.

Если порт не поддерживает Guest-VLAN, порт добавляется к VLAN, настроенной пользователем.

3. Настройка портов IEEE802.1X.

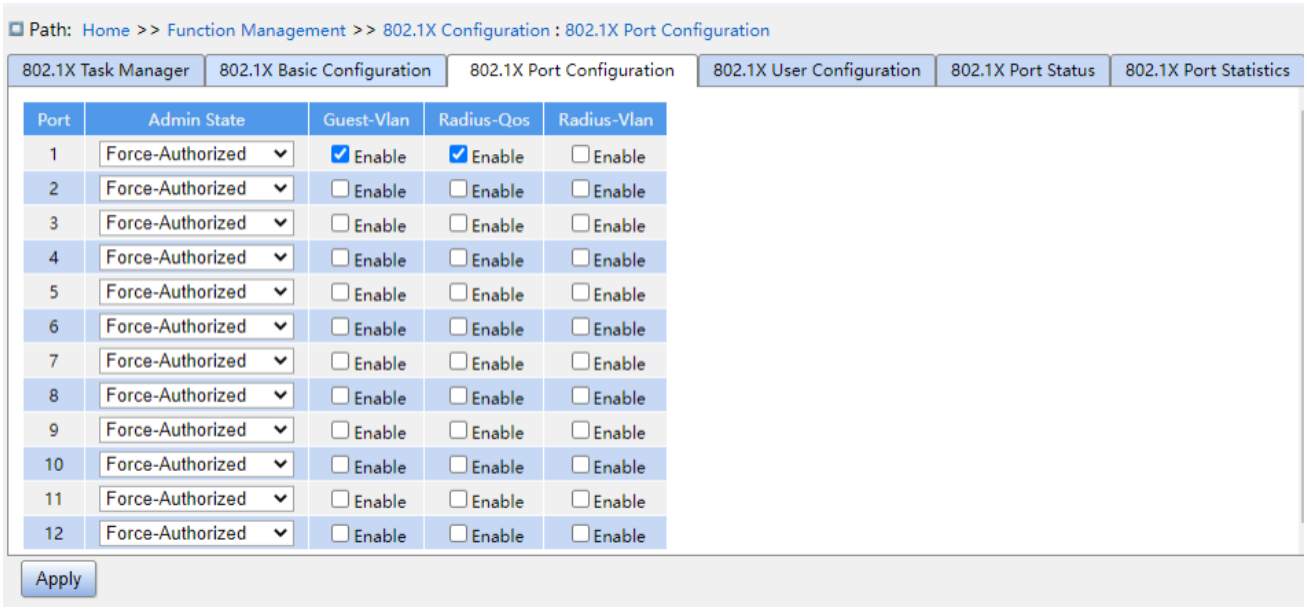


Рис. 189. Настройка портов IEEE802.1X

Port

Варианты конфигурации: все порты коммутатора

Admin State

Варианты конфигурации: Force Authorized / Force Unauthorized / Port-based / MAC-based

Конфигурация по умолчанию: Force Authorized

Функция: Выберите режим проверки подлинности порта.

Описание: Force Authorized означает, что порт всегда находится в авторизованном состоянии и позволяет пользователям получать доступ к сетевому ресурсу без аутентификации. Force Unauthorized означает, что порт всегда находится в неавторизованном состоянии и не позволяет пользователям проводить аутентификацию, а коммутатор не предоставляет услуги аутентификации клиентам, которые обращаются к коммутатору с этого порта. MAC-based означает, что все пользователи для доступа к этому порту должны пройти индивидуальную аутентификацию. Когда пользователь отключается от сети, только этот пользователь не может использовать сеть. Port-based указывает, что аутентификация пользователей осуществляется на основе порта. После того, как первый пользователь, использующий

порт, пройдет аутентификацию, аутентификация всех остальных пользователей, использующих порт, не требуется. Однако, когда первый пользователь находится в автономном режиме, порт отключен, и все остальные пользователи, использующие порт, не могут пользоваться сетью.

RADIUS-QOS

Варианты конфигурации: Enable/ Disable

Конфигурация по умолчанию: Disable

Функция: Включение или отключение QoS, назначенного RADIUS, для указанного порта.

RADIUS-VLAN

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включение или отключите VLAN, назначенного RADIUS, для указанного порта.

Guest-VLAN

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включить ли Guest-VLAN на порте.

Эта функция доступна только в том случае, если RADIUS-QOS, RADIUS-VLAN и Guest-VLAN включены как на глобальном уровне, так и на уровне портов.

4. Конфигурация пользователей IEEE802.1X.

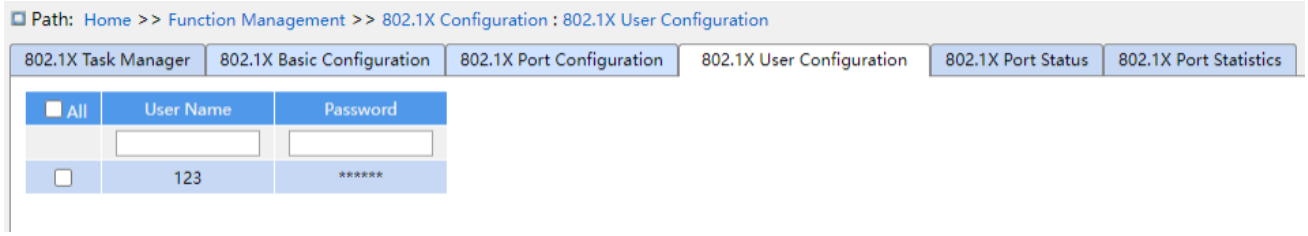


Рис. 190. Конфигурация пользователей IEEE802.1X

User Name

Варианты конфигурации: 1~16 символов

Конфигурация по умолчанию: None

Функция: Настройте имя пользователя для локальной аутентификации.

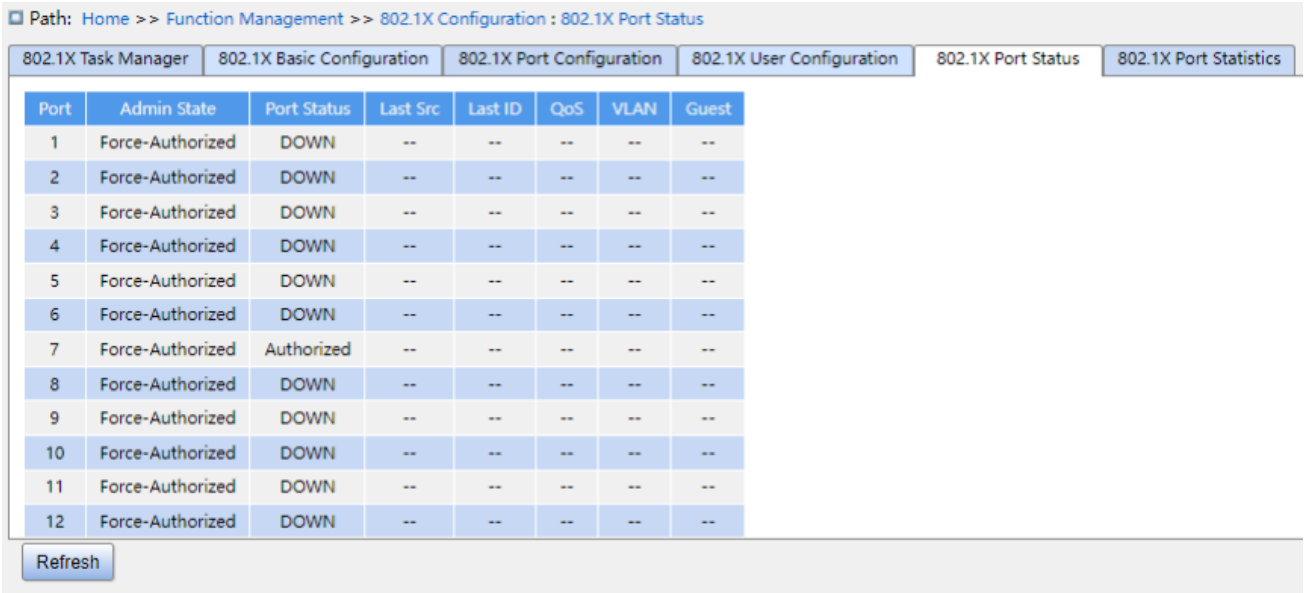
Password

Варианты конфигурации: 1~16 символов

Конфигурация по умолчанию: None

Функция: Настройте пароль для локальной аутентификации.

5. Просмотр статуса портов IEEE802.1X.



Port	Admin State	Port Status	Last Src	Last ID	QoS	VLAN	Guest
1	Force-Authorized	DOWN	--	--	--	--	--
2	Force-Authorized	DOWN	--	--	--	--	--
3	Force-Authorized	DOWN	--	--	--	--	--
4	Force-Authorized	DOWN	--	--	--	--	--
5	Force-Authorized	DOWN	--	--	--	--	--
6	Force-Authorized	DOWN	--	--	--	--	--
7	Force-Authorized	Authorized	--	--	--	--	--
8	Force-Authorized	DOWN	--	--	--	--	--
9	Force-Authorized	DOWN	--	--	--	--	--
10	Force-Authorized	DOWN	--	--	--	--	--
11	Force-Authorized	DOWN	--	--	--	--	--
12	Force-Authorized	DOWN	--	--	--	--	--

Рис. 191. Просмотр статуса портов IEEE802.1X

Port Status

Варианты конфигурации: Disable / AuthUnAuth / down / x A/y UnA

Функция: Disable указывает, что IEEE802.1X отключен глобально; Auth указывает, что пользователь, подключенный к порту, проходит аутентификацию; UnAuth указывает, что пользователь, подключенный к порту, не проходит аутентификацию; DOWN указывает, что порт отключен; x A/y UnA указывает, что x пользователей авторизованы, а y пользователей неавторизованы при аутентификации MAC-based Auth.

6. Статистика портов IEEE802.1X.

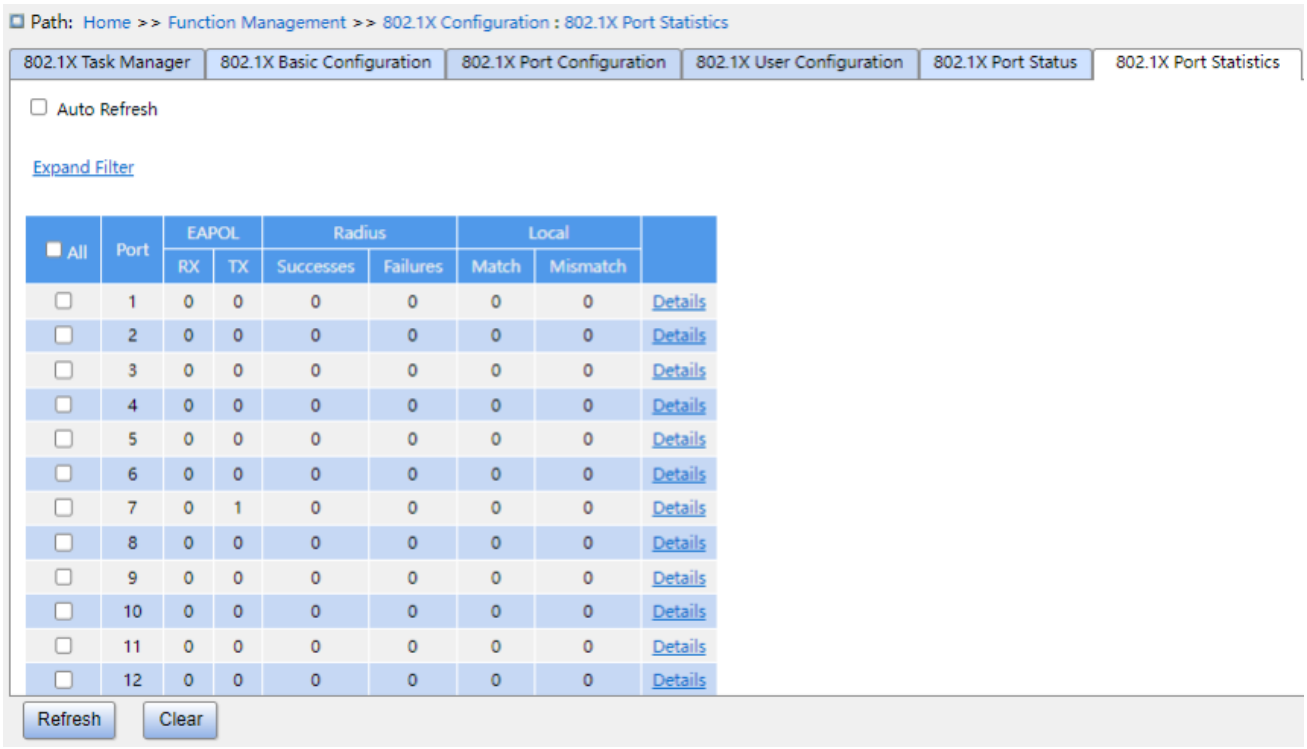


Рис. 192. Просмотр статистики портов IEEE802.1X

Нажмите <Details>, чтобы войти в интерфейс информационной статистики IEEE802.1X соответствующего порта, как показано далее.

<<Back

Statistics		
Eapol	Rx Total	0
	Tx Total	0
	Rx RespId	0
	Tx ReqId	0
	Rx RespMD5	0
	Tx ReqMD5	0
	Rx Resp	0
	Tx Req	0
	Rx Start	0
	Rx LogOff	0
	Rx Invalid Type	0
	Rx Invalid Len	0
Radius	Rx Access Challenges	0
	Rx Other Requests	0
	Rx Auth Successes	0
	Rx Auth Failures	0
	Tx Responses	0
	Mac Address	--
Local	MD5-Challenge Match	0
	MD5-Challenge Mismatch	0
	Error User	0
	Error Decode	0
	Error InvalidNethod	0

Рис. 193. Просмотр детальной статистики портов IEEE802.1X

7.12.3 Пример конфигурации

Как показано далее, client подключен к порту 1 коммутатора. Включите IEEE802.1x на порте 1 и выберите режим аутентификации на основе порта (Port-based). Имя пользователя и пароль для удаленной аутентификации являются ddd, остальная конфигурация используется по умолчанию. См. пример конфигурации RADIUS.

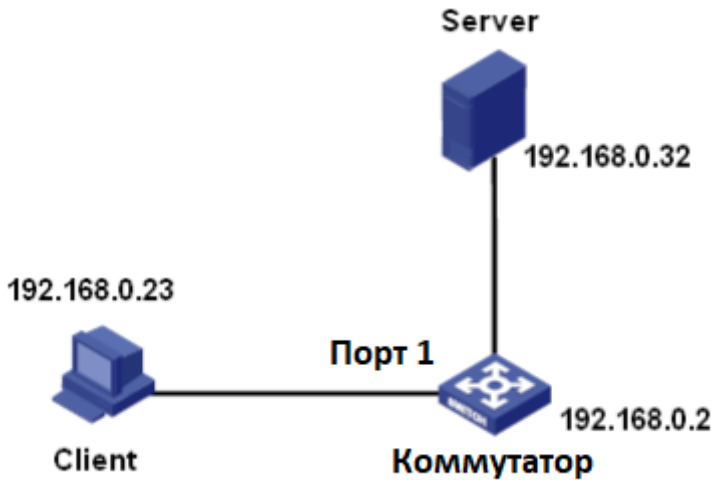


Рис. 194. Пример конфигурации IEEE802.1X

7.13 GMRP

7.13.1 Введение GARP

Generic Attribute Registration Protocol (GARP) используется для распространения, регистрации и отмены определенной информации (VLAN, адрес многоадресной рассылки) между коммутаторами в одной сети.

С помощью GARP информация о конфигурации участника (member) GARP будет распространяться на всю коммутационную сеть. Участник GARP инструктирует других участников GARP зарегистрировать или отменить свою собственную информацию о конфигурации посредством сообщения о присоединении/выходе (join/leave). Участник также регистрирует или отменяет информацию о конфигурации других участников на основе сообщений о присоединении/выходе (join/leave).

GARP включает в себя три типа сообщений: Join, Leave и LeaveAll.

- Когда объект приложения GARP хочет зарегистрировать свою собственную информацию на других коммутаторах, объект отправляет сообщение о присоединении. Сообщения о присоединении делятся на два типа: JoinEmpty и JoinIn. Сообщение JoinIn отправляется для объявления зарегистрированного атрибута, в то время как сообщение JoinEmpty отправляется для объявления атрибута, который еще не зарегистрирован.

- Когда объект GARP хочет отменить свою собственную информацию на других коммутаторах, объект отправляет сообщение Leave message. Leave message делятся на два типа: LeaveEmpty и LeaveIn. Сообщение LeaveIn отправляется для отмены зарегистрированного атрибута, в то время как сообщение LeaveEmpty отправляется для отмены атрибута, который еще не зарегистрирован.
- После запуска объекта GARP запускается таймер LeaveAll. Когда таймер истекает, объект отправляет сообщение LeaveAll.

Объект приложения указывает порт с поддержкой GARP (GARP-enabled port).

Таймеры GARP включают Hold timer, Join timer, Leave timer, LeaveAll timer.

Hold Timer: когда коммутатор с поддержкой GARP получает сообщение о регистрации, он запускает таймер удержания (Hold Timer), а не немедленно отправляет сообщение о присоединении. Когда таймер удержания истечет, он поместит всю регистрационную информацию, полученную за это время, в одно сообщение о присоединении и отправит его, уменьшив тем самым количество отправляемых сообщений.

Join Timer: чтобы гарантировать, что сообщение о присоединении может быть надежно передано другим коммутаторам, коммутатор с поддержкой GARP будет ожидать временной интервал таймера присоединения (Join Timer) после отправки первого сообщения о присоединении. Если коммутатор не получит сообщение о присоединении в течение этого времени, он снова отправит сообщение о присоединении, в противном случае он не отправит второе сообщение.

Leave Timer: когда коммутатору с поддержкой GARP необходимо, чтобы другие коммутаторы аннулировали информацию его атрибута, он отправляет сообщение Leave. Другие коммутаторы с поддержкой GARP, получившие это сообщение, активируют (Leave Timer). Если коммутаторы не получат сообщение о присоединении

(Join message) до истечения времени таймера, они аннулируют эту информацию атрибута.

LeaveAll Timer: когда коммутатор включает GARP, он одновременно запускает таймер LeaveAll. По истечении времени таймера коммутатор отправит сообщение LeaveAll другим коммутаторам с поддержкой GARP и позволит им повторно зарегистрировать всю информацию об их атрибутах, а затем перезапустит таймер LeaveAll, чтобы начать новый цикл.

7.13.2 Протокол GMRP

GARP Multicast Registration Protocol (GMRP) - это протокол регистрации многоадресной рассылки, основанный на GARP. GMRP используется для поддержания информации о регистрации многоадресной рассылки коммутаторов. Все коммутаторы с поддержкой GMRP могут получать информацию о регистрации многоадресной рассылки от других коммутаторов, динамически обновлять и распространять информацию о регистрации локальной многоадресной рассылки между коммутаторами. Этот механизм обмена информацией обеспечивает согласованность информации о многоадресной рассылке, поддерживаемой всеми коммутаторами с поддержкой GMRP в сети.

Если коммутатор или терминал хочет присоединиться к группе многоадресной рассылки или покинуть ее, порт с поддержкой GMRP передает информацию на все порты в одной и той же VLAN.

7.13.3 Принцип работы

Порт агента (agent): указывает порт, на котором включены GMRP и функция агента.

Порт распространения (propagation): указывает порт, на котором включен только GMRP.

Динамически полученные от порта агента (agent) записи перенаправляются с помощью порта распросранения (propagation) на порты распространения более

низкого уровня.

Все таймеры GMRP в одной сети должны быть согласованными, чтобы предотвратить взаимные влияния.

Таймеры должны соответствовать следующим правилам: Hold timer < Join timer, 2*Join timer < Leave timer, и Leave timer <LeaveAll timer.

7.13.4 Web конфигурация

1. Включение глобального протокола GMRP и настройка таймеров.

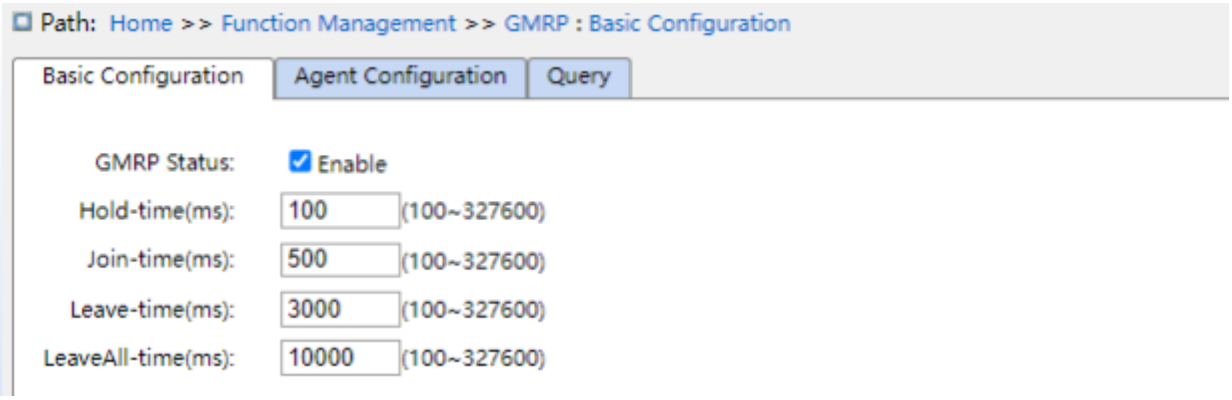


Рис. 195. GMRP Global конфигурация

GMRP Status

Варианты конфигурации: Enable/ Disable

Конфигурация по умолчанию: Disable

Функция: Включение/выключение глобальной функции GMRP. Эту функцию нельзя использовать вместе с функцией отслеживания IGMP.

Hold-timer

Диапазон: 100~327600 миллисек.

Конфигурация по умолчанию: 100 миллисек.

Описание: Это значение должно быть кратно 100. Лучше установить одинаковое время ожидания (Hold-timer) на всех портах с поддержкой GMRP.

Join-timer

Диапазон: 100~327600 миллисек.

Конфигурация по умолчанию: 500 миллисек.

Описание: Это значение должно быть кратно 100. Лучше установить одинаковое время таймеров присоединения (Join-timer) на всех портах с поддержкой GMRP.

Leave-timer

Диапазон: 100~327600 миллисек.

Конфигурация по умолчанию: 3000 миллисек.

Описание: Это значение должно быть кратно 100. Лучше установить одинаковое время выхода (Leave-timer) на всех портах с поддержкой GMRP.

LeaveAll-timer

Диапазон: 100~327600 миллисек.

Конфигурация по умолчанию: 10000 миллисек.

Функция: Временной интервал отправки пакетов LeaveAll. Значение должно быть кратно 100.

Описание: если время таймера LeaveAll для разных устройств истекает одновременно, одновременно отправляется несколько сообщений LeaveAll, что увеличивает нагрузку на сеть. Чтобы избежать одновременного истечения таймера LeaveAll на разных устройствах, значение фактического LeaveAll тамера - это случайное значение, которое больше значения LeaveAll таймера в 1,5 раза.

2. Настройка функции GMRP для портов.

Port	GMRP Enable	GMRP Agent Enable	Last PDU Origin
1	☑	☑	00-00-00-00-00-00
2	☑	☐	00-00-00-00-00-00
3	☐	☐	--
4	☐	☐	--
5	☐	☐	--
6	☐	☐	--
7	☐	☐	--
8	☐	☐	--
9	☐	☐	--
10	☐	☐	--
11	☐	☐	--
12	☐	☐	--

Рис. 196. GMRP конфигурация портов

GMRP Enable

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение функции GMRP для порта.

GMRP Agent Enable

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включение функции агента GMRP на порте.

Last PDU Origin

Функция: Исходный MAC-адрес последнего пакета протокола, полученного этим портом.

- Порт agent не может распространять записи agent .
- Предварительным условием для включения функции agent GMRP является включение функции порта GMRP.

3. Настройка записей агентов (agent) GMRP.

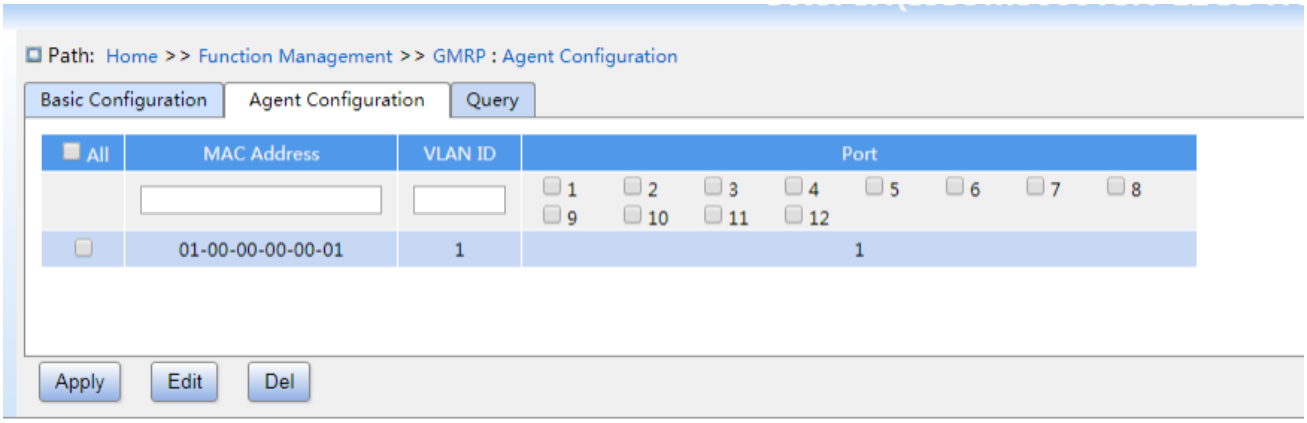


Рис. 197. Конфигурация Agent Entry GMRP

MAC address

Формат: HH-HH-HH-HH-HH-HH (H - шестнадцатеричное число)

Функция: Настройте MAC-адрес для группы многоадресной рассылки. Младший бит в первом байте равен 1.

VLAN ID

Варианты конфигурации: все созданные VLAN

Функция: Настройте идентификатор VLAN для записи агента GMRP.

Описание: Запись агента GMRP может пересылаться только с порта распространения (propagation) с VLAN ID, совпадающим с VLAN ID этой записи.

Port

Варианты конфигурации: все настроенные agent порты.

4. Просмотр конфигурации GMRP.

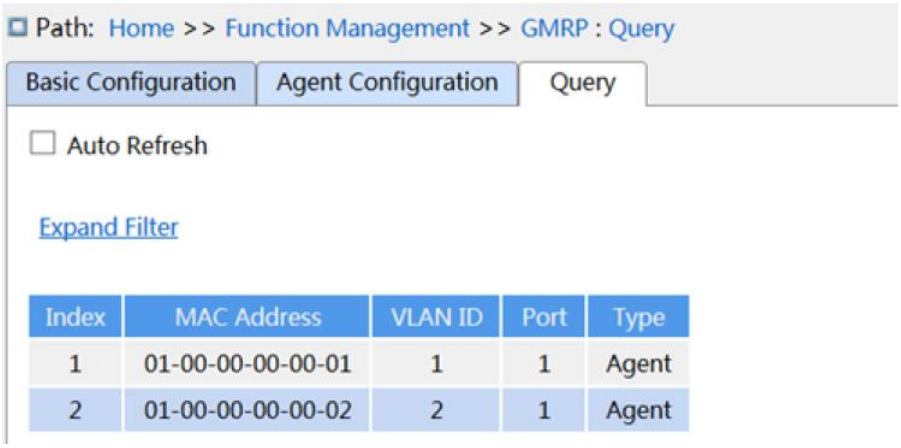


Рис. 198. Информация о работе GMRP

7.13.5 Пример конфигурации

Коммутатор A и Коммутатор B соединены портом 2. Порт 1 Коммутатора A настроен на порт агента и генерирует две записи многоадресной рассылки：

MAC-адрес: 01-00-00-00-00-01, VLAN: 1

MAC-адрес: 01-00-00-00-00-02, VLAN: 2

После настройки различных атрибутов VLAN для портов обратите внимание на динамическую регистрацию между коммутаторами и обновление информации о многоадресной рассылке.

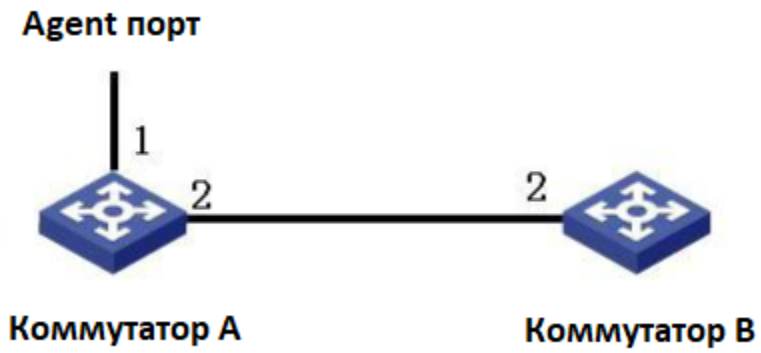


Рис. 199. GMRP сеть

Конфигурация Коммутатора A:

1. Включите глобальную функцию GMRP на коммутаторе A; установите таймер на значение по умолчанию, как показано на рис. 195.

2. Включите функцию GMRP и функцию агента на порте 1; включите только функцию GMRP на порте 2; как показано на рис. 196.

3. Настройте запись многоадресной рассылки агента. Установите <MAC address, VLAN ID, Member port> на <01-00-00-00-00-01, 1, 1> и <01-00-00-00-00-02, 2, 1>, как показано на рис. 194.

Конфигурация Коммутатора B:

4. Включите глобальную функцию GMRP на коммутаторе B; установите таймер на значение по умолчанию, как показано на рис. 195.

5. Включите функцию GMPR на порте 2; установите таймеры на значения по умолчанию, как показано на рис. 196. В таблице далее перечислены динамически определяемые записи многоадресной рассылки GMRP в коммутаторе B.

Таблица 10. Записи динамической таблицы

Атрибуты порта 2 на Коммутаторе A	**Атрибуты порта 2 на Коммутаторе B**	**Записи мультикаст, полученные на Коммутаторе B**
Access VID=1	Access VID=1	MAC: 01-00-00-00-00-01 VLAN ID: 1 Member порт: 2
Access VID=2	Access VID= 2	MAC: 01-00-00-00-00-02 VLAN ID: 2 Member порт: 2
Access VID= 1	Access VID= 2	MAC: 01-00-00-00-00-01 VLAN ID: 2 Member порт: 2

7.14 Маршрутизация

Чтобы получить доступ к удаленному хосту в Интернете, хост должен выбрать соответствующий маршрут с помощью маршрутизаторов или Layer-3 коммутаторов. В процессе выбора пути каждый Layer-3 коммутатор выбирает путь к следующему Layer-3 коммутатору в соответствии с адресом назначения полученного пакета, пока последний Layer-3 коммутатор не отправит пакет на узел назначения. Путь, который выбирает каждый Layer-3 коммутатор, называется маршрутом. Маршруты делятся на следующие типы:

Прямой маршрут (direct route): указывает маршрут, обнаруженный протоколом канального уровня.

Статический маршрут (static route): указывает маршрут, настроенный сетевым администратором вручную.

Динамический маршрут (dynamic route): указывает маршрут, обнаруженный протоколом маршрутизации.

Примечание: Функция Layer-3 протокола маршрутизации поддерживается в коммутаторах этой серии.

7.14.1 Таблица маршрутизации

7.14.1.1 Введение

Статические маршруты настраиваются вручную. Если топология сети проста, вам нужно только настроить статические маршруты для правильной работы сети. Статические маршруты просты в настройке и стабильны. Их можно использовать для балансировки нагрузки и резервирования маршрутов. Недостатком использования статических маршрутов является то, что они не могут адаптироваться к изменениям топологии сети. Если в сети произойдет сбой или топологическое изменение, то соответствующие маршруты будут недоступны и сеть прервется. Когда это произойдет, сетевой администратор должен изменить статические маршруты вручную.

7.14.1.2 Таблица маршрутизации

Каждый Layer-3 коммутатор поддерживает таблицу маршрутизации, в которой записываются все маршруты, используемые коммутатором. Каждая запись в таблице указывает, через какой интерфейс VLAN должен пройти пакет, предназначенный для определенной подсети или хоста, чтобы достичь следующего маршрутизатора или непосредственно подключенного пункта назначения. Запись маршрута включает в себя следующие элементы:

Пункт назначения (destination): указывает IP-адрес или сеть назначения.

Маска сети (network mask): указывает, наряду с адресом назначения, сеть, в которой находится узел назначения или Layer-3 коммутатор. Логическая операция И между адресом назначения и маской сети дает адрес сети назначения. Например, если адрес назначения равен 129.102.8.10, а маска 255.255.0.0, адрес сети назначения равен 129.102.0.0. Сетевая маска состоит из определенного числа последовательных единиц. Она может быть выражена в десятичном формате с точками или количеством «1».

Исходящий (egress): указывает интерфейс, через который должен быть перенаправлен соответствующий IP-пакет.

IP-адрес следующего Layer-3 коммутатора (next hop): указывает новый Layer-3 коммутатор, через который будет проходить IP-пакет.

Приоритет (priority): Маршруты, ведущие к одному и тому же пункту назначения, но имеющие разные последующие переходы, могут иметь разные приоритеты и могут быть найдены различными протоколами маршрутизации или настроены вручную. Оптимальный маршрут - это маршрут с наивысшим приоритетом.

7.14.1.3 Маршрут по умолчанию

Чтобы предотвратить слишком большое количество записей в таблице маршрутизации, вы можете настроить маршрут по умолчанию. Маршрут по умолчанию

- статический маршрут. Если пакету данных не удается найти соответствие в таблице маршрутизации, он пересылается в соответствии с маршрутом по умолчанию. В таблице маршрутизации маршрутом по умолчанию является маршрут, в котором как пункт назначения, так и маска равны 0.0.0.0. Если пакет не соответствует какой-либо записи в таблице маршрутизации и маршрут по умолчанию не настроен, коммутатор отбрасывает пакет и возвращает ICMP-пакет, указывающий, что адрес назначения или сеть недоступны.

7.14.1.4 Web конфигурация

1. Конфигурация статической маршрутизации.

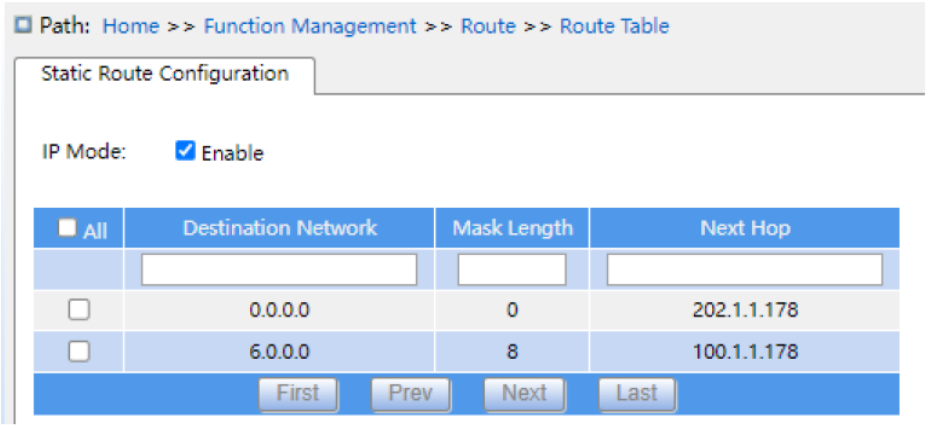


Рис. 200. Конфигурация Static routing

IP Mode

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Enable

(для устройств Layer 3 значение по умолчанию включено. Для устройств Layer 2 значение по умолчанию выключено)

Функция: Следует ли включать режим IP.

Destination Network

Формат: A.B.C.D

Функция: настройте сетевой адрес для пункта назначения в таблице статических маршрутов.

Mask Length

Функция: маска подсети представляет собой 32-разрядное число, состоящее из последовательности "1" и последовательности "0". "1" соответствует полю номера сети и полю номера подсети, в то время как "0" соответствует полю номера хоста. Длина маски - это число, равное количеству "1" в маске.

Next Hop

Формат: A.B.C.D

Функция: Настройте IP-адрес следующего коммутатора.

7.14.1.5 Пример конфигурации

Сетевые маски всех Layer-3 коммутаторов и хостов в сети равны 255.255.255.0. Требуется настроить статические маршруты, чтобы позволить любому из хостов взаимодействовать друг с другом.

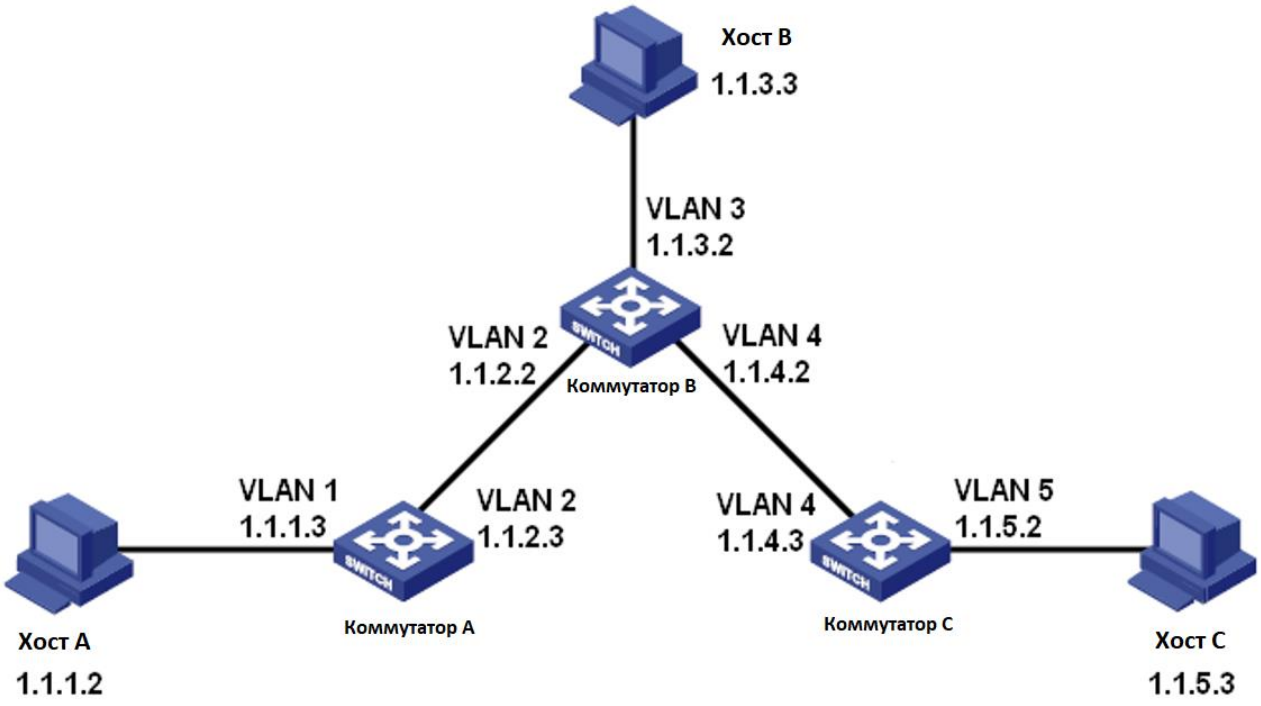


Рис. 201. Пример конфигурации статических маршрутов

Настройка коммутатора A:

1. Установите IP-адреса для интерфейсов VLAN.

2. IP-адрес назначения: 1.1.3.0; маска адреса назначения: 255.255.255.0; следующий переход: 1.1.2.2;

IP-адрес назначения: 1.1.5.0; маска адреса назначения: 255.255.255.0; следующий переход: 1.1.2.2; как показано на рис. 200.

Настройка коммутатора B:

3. Установите IP-адреса для интерфейсов VLAN.

4. Настройте статический маршрут со следующими параметрами:

IP-адрес назначения: 1.1.1.0, маска адреса назначения: 255.255.255.0, следующий переход: 1.1.2.3;

IP-адрес назначения: 1.1.5.0, маска адреса назначения: 255.255.255.0, следующий переход: 1.1.4.3; как показано на рис. 200.

Настройка коммутатора C:

5. Установите IP-адреса для интерфейсов VLAN.

6. Настройте статический маршрут со следующими параметрами:

IP-адрес назначения: 0.0.0.0, маска адреса назначения: 0.0.0.0, следующий переход: 1.1.4.2;

IP-адрес назначения: 1.1.5.0, маска адреса назначения: 255.255.255.0, следующий переход: 1.1.4.3; как показано на рис. 200.

Настройте шлюз по умолчанию хоста A на 1.1.1.3, шлюз по умолчанию хоста B на 1.1.3.2 и шлюз по умолчанию хоста C на 1.1.5.2.

7.15 Конфигурация QoS

7.15.1 Введение

Quality of Service (QoS) обеспечивают дифференцированные услуги, основанные на различных требованиях, в условиях ограниченной полосы пропускания посредством управления трафиком и распределения ресурсов в IP-сетях.

QoS пытаются обеспечить работу различных сервисов, чтобы уменьшить перегрузку сети и свести к минимуму влияние перегрузки на службы с высоким

приоритетом.

Классификация трафика (traffic classification), контроль траффика (traffic policing), формирование трафика (traffic shaping), управление нагрузкой (congestion management) и предотвращение потерь данных - вот основные концепции развертывания QoS. В основном они выполняют следующие функции:

Traffic classification: идентифицирует объект на основе определенных правил сопоставления. Это основа и предварительное условие для работы QoS.

Traffic policing: контролирует скорость трафика пакетов, передаваемых на устройство. Когда скорость трафика превышает заданную скорость трафика, устройство принимает меры ограничения для защиты сетевых ресурсов от повреждения. Контроль трафика подразделяется на контроль трафика на основе портов и контроль трафика на основе очередей.

Traffic shaping: упреждающая настройка скорости вывода трафика. Она направлена на адаптацию трафика к доступным сетевым ресурсам устройства, находящегося ниже по потоку, для предотвращения ненужного отбрасывания пакетов и перегрузки. Формирование трафика подразделяется на формирование трафика на основе портов и формирование трафика на основе очередей.

Congestion management: это обязательно для решения проблемы конкуренции за ресурсы. Управление перегрузкой кэширует пакеты в очередях и определяет последовательность пересылки пакетов на основе определенного алгоритма планирования, обеспечивая преимущественную пересылку для ключевых служб.

Congestion avoidance: чрезмерная перегрузка может привести к повреждению сетевых ресурсов. Предотвращение перегрузки отслеживает использование сетевых ресурсов. При обнаружении растущей перегрузки функция использует упреждающее отбрасывание пакетов и настраивает объем трафика для устранения перегрузки.

Traffic policing, traffic shaping, congestion management, and congestion avoidance контролируют сетевой трафик и выделяемые ресурсы с разных сторон. Они являются конкретным воплощением QoS. Например, коммутатор контролирует пакеты, которые

передаются в сеть, на основе зафиксированной скорости. Коммутатор осуществляет управление расписанием очередей QoS и в случае перегрузки принимает меры по предотвращению перегрузки.

7.15.2 Принцип работы

Каждый порт коммутаторов этой серии поддерживает 8 очередей кэширования, от 0 до 7 в порядке возрастания приоритета.

Когда кадр достигает порта, коммутатор определяет очередь для кадра в соответствии с информацией о кадре и порте. Коммутаторы этой серии поддерживают классификацию трафика в следующих режимах отображения очередей: порт, 802.1Q информация о заголовке, differentiated services code point (DSCP), и QoS control list (QCL), с приоритетом в порядке возрастания. При пересылке данных порт использует режим планирования для распределения данных по 8 очередям и пропускной способности каждой очереди. Коммутаторы этой серии поддерживают два режима планирования: взвешенный (Weighted) по 6 очередям и SP (Strict Priority).

WRR (Weighted Round Robin) планирует потоки данных на основе весового коэффициента. Очереди получают свою пропускную способность в зависимости от их весового соотношения. WRR отдает приоритет очередям с высоким соотношением веса. Очередям с более высоким весовым коэффициентом выделяется больше полосы пропускания. Режим SP предпочтительно пересылает пакеты с высоким приоритетом. Он в основном используется для передачи чувствительных сигналов. Если кадр попадает в очередь с высоким приоритетом, коммутатор прекращает планирование очередей с низким приоритетом и начинает обрабатывать данные очереди с высоким приоритетом. Когда очередь с высоким приоритетом не содержит данных, коммутатор начинает обрабатывать данные очереди с более низким приоритетом.

6 Queues Weighted указывает, что очереди 6 и 7 используют режим планирования со строгим приоритетом (Strict Priority), и очередь 0 ~ очередь 5 используют режим WRR. Данные в очереди 7 обрабатываются до данных в очереди 6. Когда и очередь 7, и

очередь 6 пусты, данные в очереди 0 ~ очереди 5 обрабатываются в зависимости от весового соотношения.

7.15.3 Web конфигурация

1. Настройте режим перемаркировки 802.1p в соответствии с отображением (Mapped), как показано ниже.

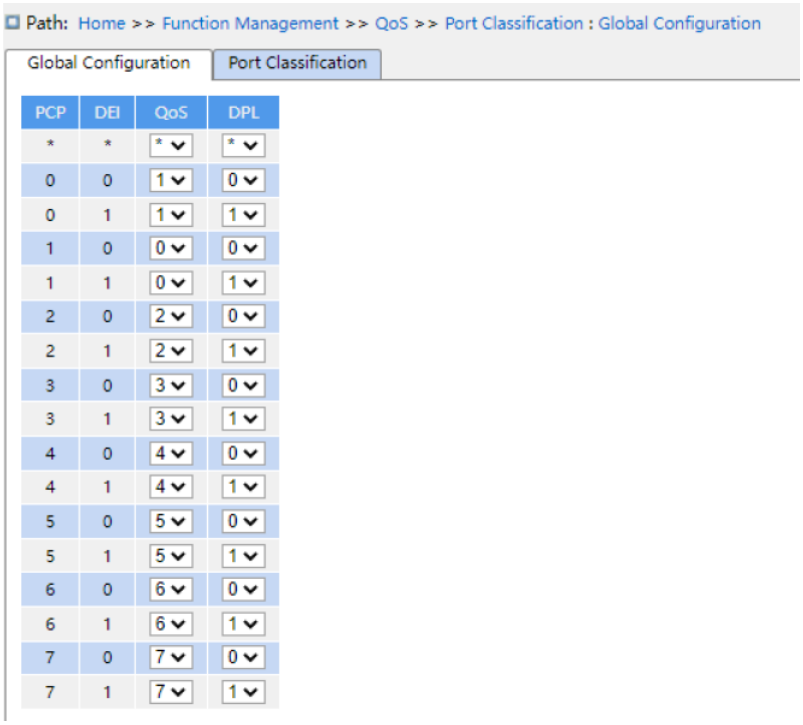


Рис. 202. Настройка режима Mapped Remarking

Режим отображения очереди, основанный на информации заголовка 802.1Q, подходит только для полученных сообщений с тегом.

(PCP, DEI) в (QoS class, DP level) mapping (перемаркировка)

Диапазон: 0~7 (QoS type) 0~1 (DP level)

Конфигурация по умолчанию: значение PCP 0, 1, 2, 3, 4, 5, 6, 7 mapping (перемаркировка) QoS class 1, 0, 2, 3, 4, 5, 6, 7.

DEI значение 0, 1 перемаркировка в DP level 0, 1.

Функция: Сконфигурируйте сопоставление (PCP, DEI) с (CoS, DPL) в соответствии

со значениями PCP и DEI в сообщении.

Описание: Класс QoS равен значению CoS, которое определяет очередь хранения сообщения, соответствующую очереди 0 - 7. Когда сообщение поступает на коммутатор, коммутатор присваивает сообщению значения CoS и DPI. Если тип сообщения - tag и включен класс тэгов, значения CoS и DPI сообщения являются значением сопоставления от (PCP, DEI) до (CoS, DPL).

2. Включение режима иерархии портов, как показано далее

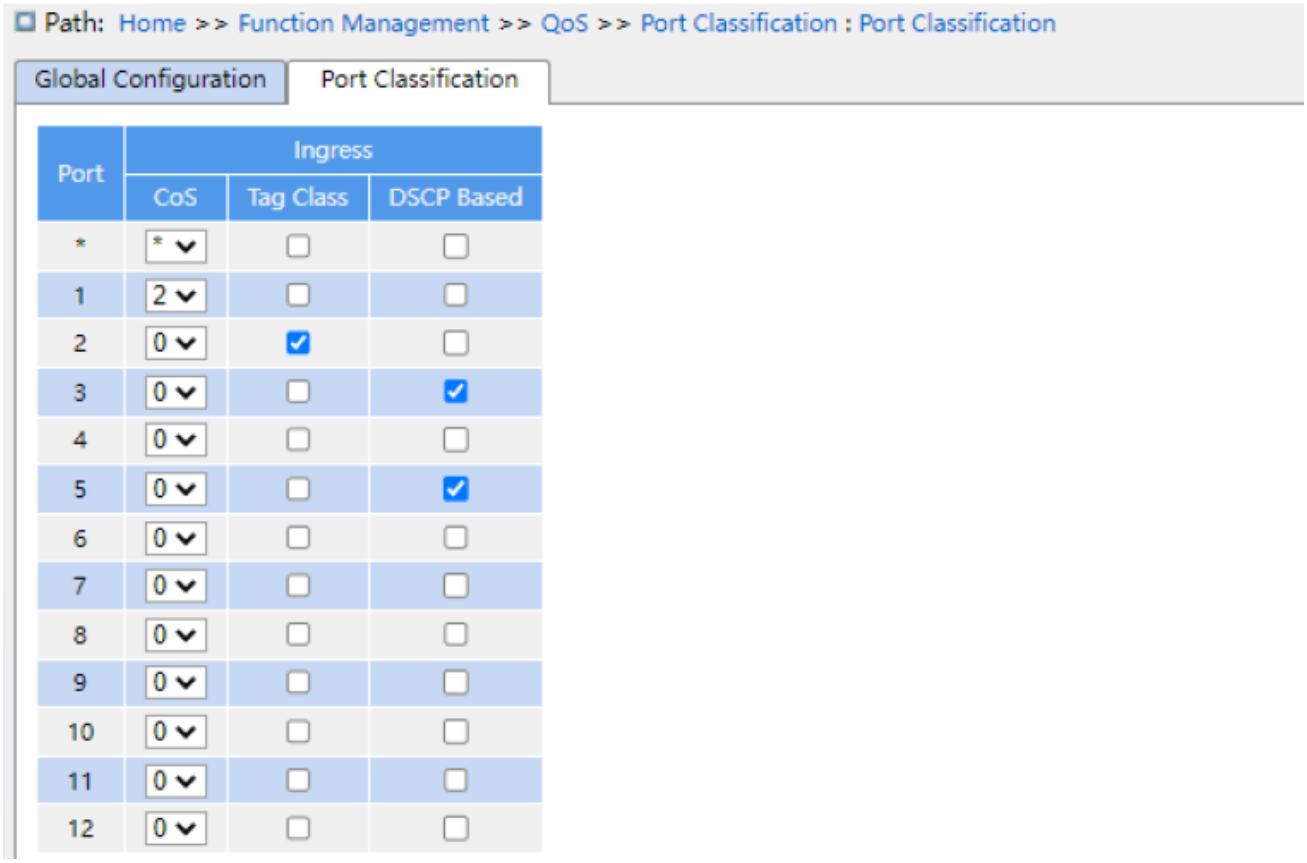


Рис. 203. Настройка hierarchy mode для портов

DSCP Based

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: Включает или отключает режим отображения очередей на основе DSCP, который имеет более высокий приоритет, чем режим отображения очереди на основе

заголовка 802.1Q.

CoS

Диапазон: 0~7

Конфигурация по умолчанию: 0

Функция: Настройте значение CoS порта по умолчанию.

Tag Class

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: Включает или отключает режим отображения очереди (mapping) на основе информации заголовка 802.1Q.

3. Включение глобального режима 802.1p перемаркировки (re-tagging) показано на рисунке далее; на этом экране показан режим повторной пометки 802.1p, когда порт пересылает сообщения. Повторная пометка 802.1p указывает, что порт обновляет значения PCP и DEI в сообщении при пересылке сообщения.

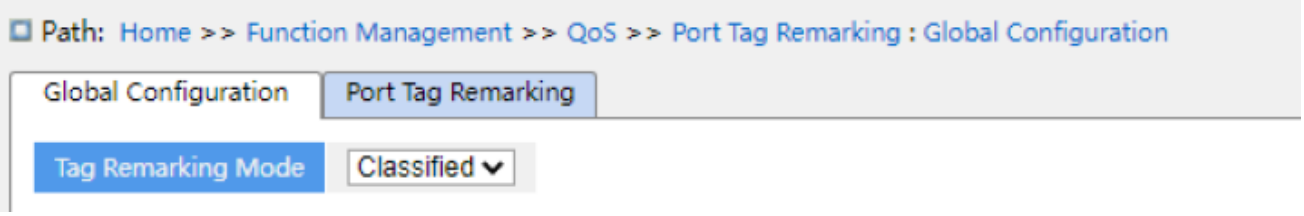


Рис. 204. Включение глобального режима 802.1p перемаркировки (re-tagging)

Функция перемаркировки 802.1p недействительна, если исходящий порт пересылает сообщения, которые не содержат метки (Tag).

Настройте режим повторной пометки 802.1p на Classified, как показано на рис. 204.

Tag Remark Mode

Варианты конфигурации: Classified /Default

Конфигурация по умолчанию: Classified

Режим Classified: Значения PCP и DEI не обновляются, когда исходящий порт пересылает сообщение.

Настройте режим перемаркировки 802.1p по умолчанию (Default Remarking Mode), как показано на рисунке далее.

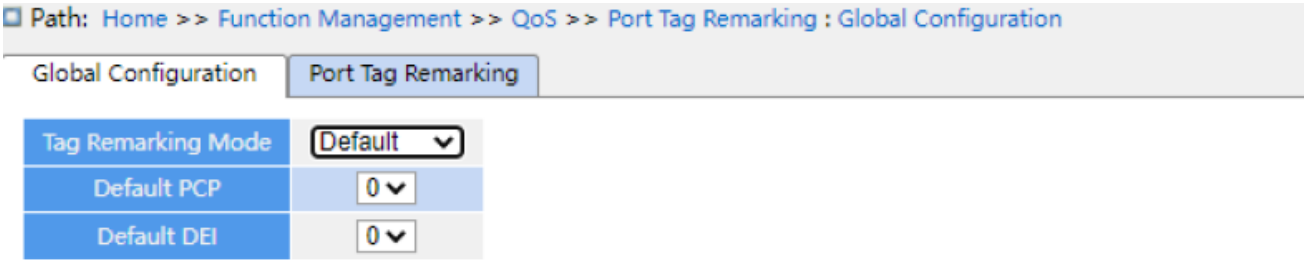


Рис. 205. Настройка режима Default Remarking

Tag Remarking Mode

Варианты конфигурации: Classified/ Default

Конфигурация по умолчанию: Classified

Функция: настройка режима перемаркировки 802.1p. Режим Default: Когда выходной порт пересылает сообщение, значения PCP и DEI в обновленном сообщении являются значениями по умолчанию для выходного порта (конфигурация приведена ниже).

Default PCP

Диапазон: 0~7

Конфигурация по умолчанию: 0

Функция: настройте значение PCP по умолчанию для исходящего (egress) порта.

Default DEI

Диапазон: 0~1

Конфигурация по умолчанию: 0

Функция: настройте значение DEI по умолчанию для исходящего (egress) порта.

4. Настройте перемаркировку 802.1p, как показано далее.

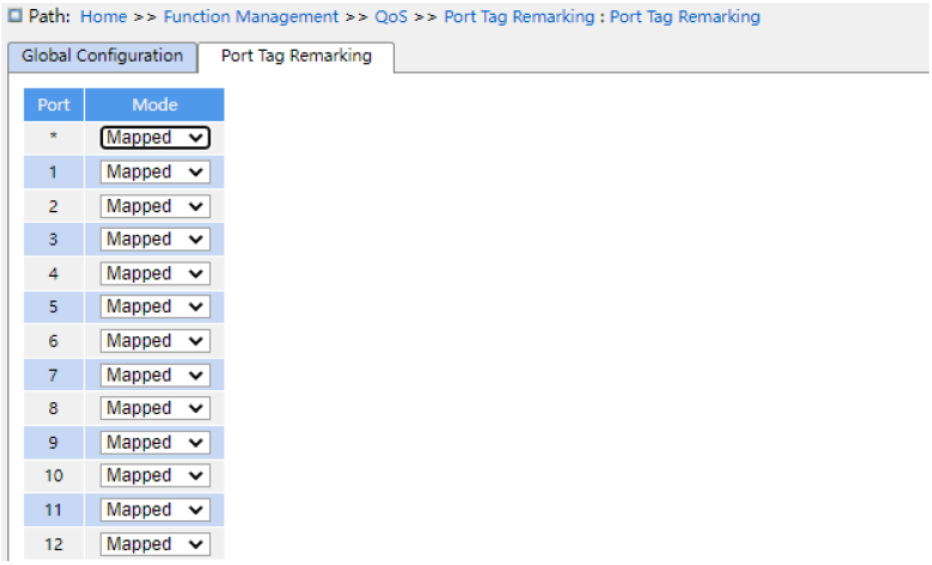


Рис. 206. Настройка перемаркировки 802.1p для выбранного порта

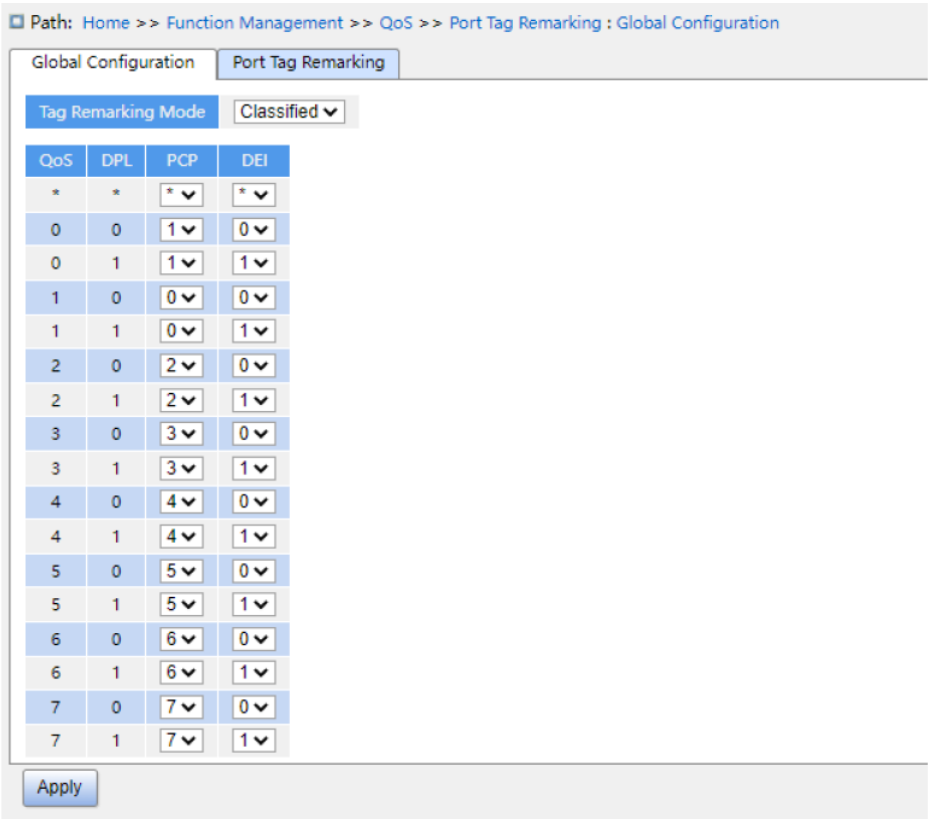


Рис. 207. Настройка режима Mapped Remarking

Tag Remarking Mode

Варианты конфигурации: Classified/Mapped/Default

Конфигурация по умолчанию: Classified

Функция: настройка режима перемаркировки 802.1p. Режим Mapped: Когда выходной

порт пересылает сообщение, значения PCP и DEI в обновленном сообщении отображают (mapping) значение из (CoS, DPL) в (PCP, DEI) (конфигурация отображения, как показано ниже).

(QoS class, DP level) в (PCP, DEI) отображение (mapping)

Варианты конфигурации: 0~7 (PCP) 0~1 (DEI)

Конфигурация по умолчанию: QoS class 0, 1, 2, 3, 4, 5, 6, 7 отображение в PCP значение 1, 0, 2, 3, 4, 5, 6, 7;

DP level 0, 1 отображение в DEI значение 0, 1.

Функция: в соответствии со значениями CoS и DPL в сообщении сконфигурируйте сопоставление (CoS, DPL) с (PCP, DEI).

5. Включение Translate для входящего (ingress) порта, перезапись входящего (ingress) порта, как показано далее.

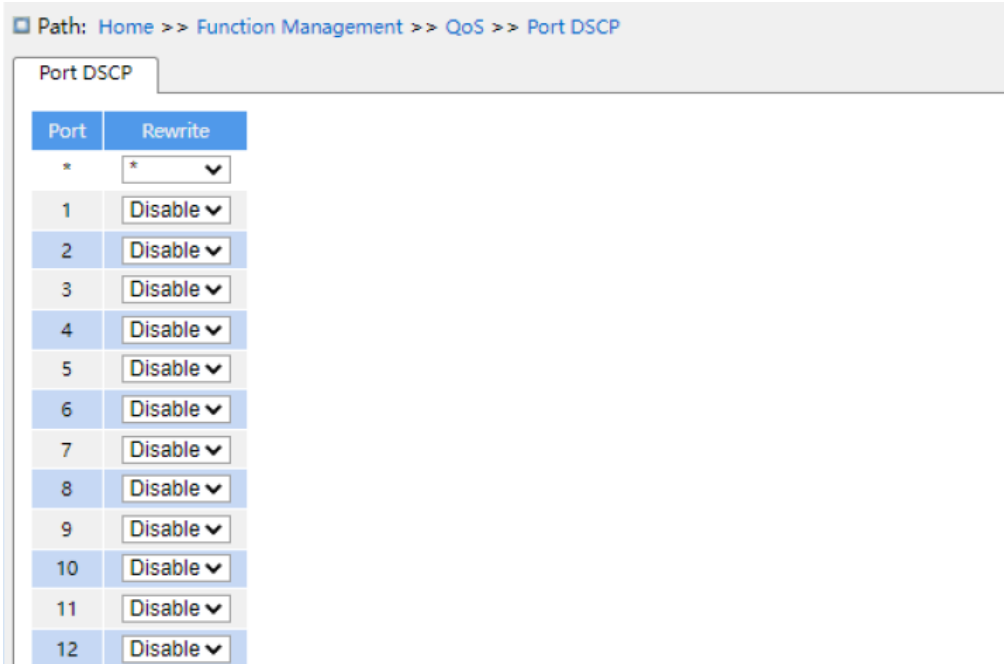


Рис. 208. Настройка DSCP для порта

Rewrite

Варианты конфигурации: Disable/enable/remap

Конфигурация по умолчанию: Disable

Функция: Настройте режим перезаписи значения DSCP, когда исходящий (egress) порт пересылает сообщение.

Disable: Когда исходящий (egress) порт пересылает сообщение, значение DSCP в сообщении не перезаписывается;

Enable: Когда исходящий (egress) порт пересылает сообщение, следует ли переписывать значение DSCP в сообщении в соответствии с конфигурацией.

Remap: Когда исходящий (egress) порт пересылает сообщение, DSCP в сообщении переписывается в соответствии с отображением (DSCP, DPL) в DSCP.

6. Настройка режима отображения очереди на основе DSCP, как показано ниже.

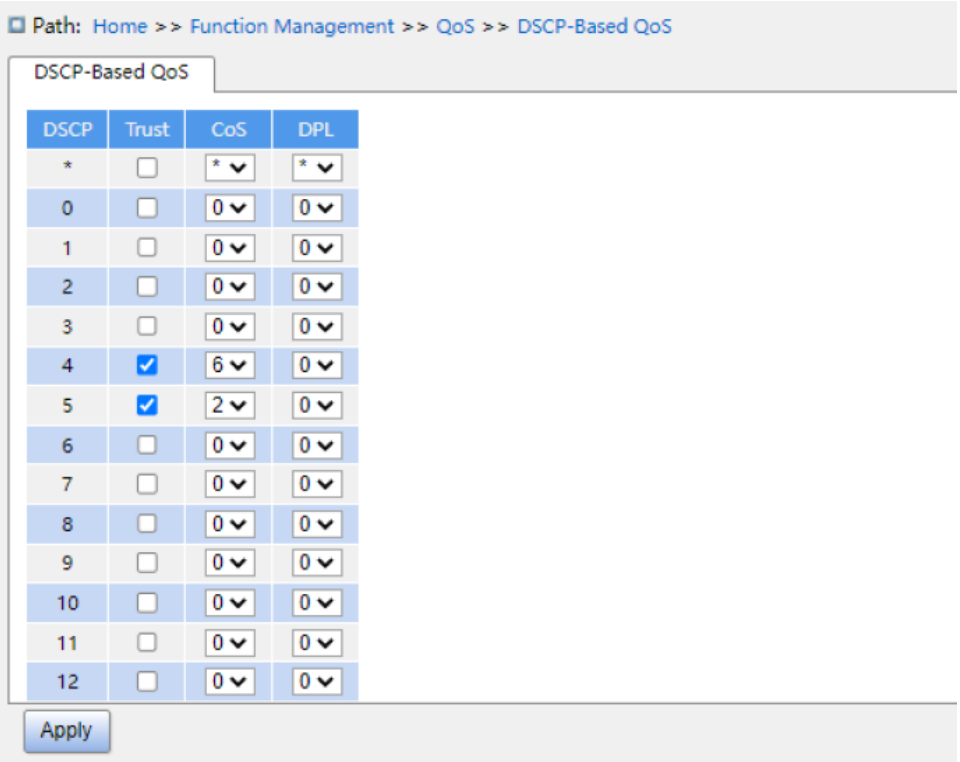


Рис. 209. Настройка режима отображения очереди на основе DSCP

Trust

Варианты конфигурации: Enable/disable

Конфигурация по умолчанию: Disable

Функция: следует ли доверять значению DSCP.

Режим отображения очереди, основанный на DSCP, применяется только к значению DSCP сообщения, полученного портом в качестве значения доверия (trust value).

COS

Варианты конфигурации: 0~7

Конфигурация по умолчанию: 0

Функция: Настройте сопоставление DSCP с CoS.

Описание: Значение CoS определяет сохраненную очередь сообщений, значение CoS 0 ~ 7, в свою очередь, соответствует очереди 0~7. Когда сообщение со значением DSCP в качестве trust поступает на коммутатор, коммутатор присваивает сообщению значение CoS в соответствии с сопоставлением DSCP с CoS.

Когда входящий (ingress) порт включает функцию translate, коммутатор присваивает значение CoS в соответствии с переведенным значением DSCP; в противном случае коммутатор присваивает значение CoS в соответствии с исходным значением DSCP в сообщении.

DPL

Варианты конфигурации: 0~1

Конфигурация по умолчанию: 0

Функция: Настройка сопоставления DSCP с DPL

Описание: После того, как сообщение со значением DSCP в качестве trust поступает на коммутатор, коммутатор присваивает сообщению значение DPI в соответствии с сопоставлением DSCP с DPL.

7. Настройка DSCP translation, как показано далее.

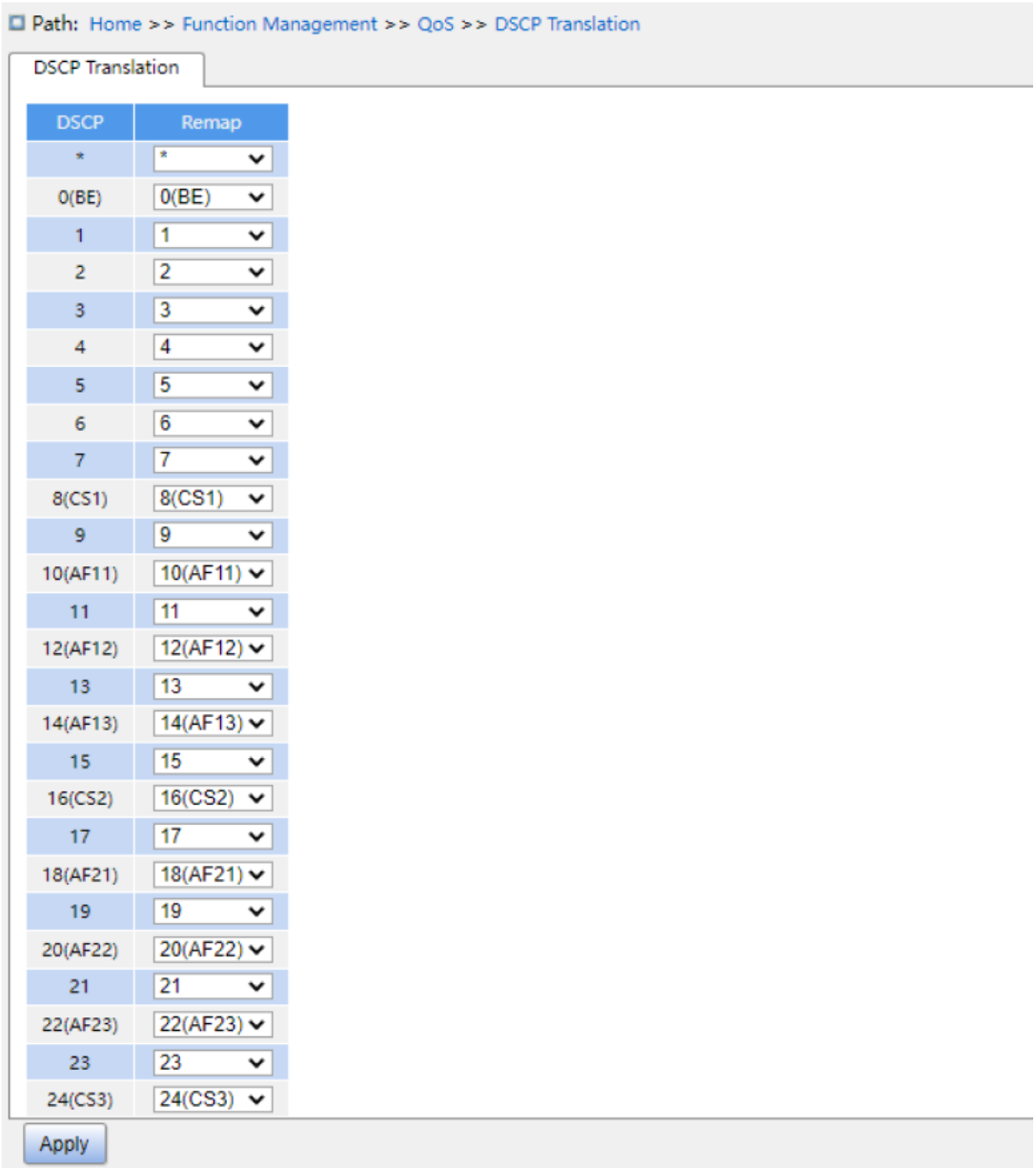


Рис. 210. Настройка DSCP translation

Translate

Диапазон: 0~63

Функция: настройка таблицы преобразования значения dscp.

Когда входящий (ingress) порт включает “translate”, выбранное значение является преобразованным значением. В противном случае выбранное значение DSCP является исходным значением DHCP в сообщении.

Remap DP0

Диапазон: 0~63

Функция: Настройка (DSCP, DPL) для сопоставления с DSCP.

8. Настройка режима планировщика очереди портов, как показано далее.

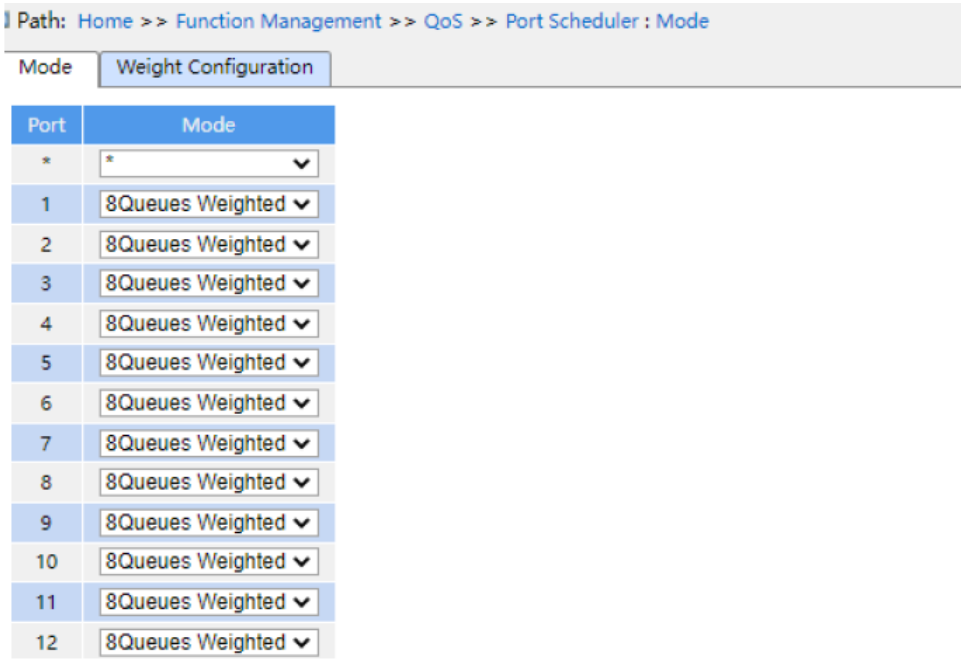


Рис. 211. Настройка режима планировщика очереди портов

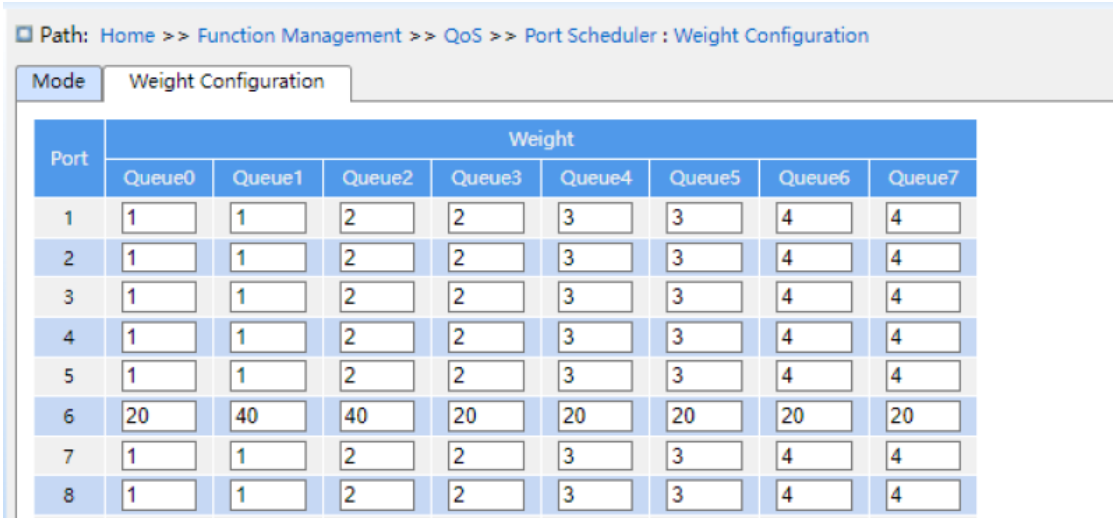


Рис. 212. Настройка таблицы весов для планировщика

Scheduler Mode

Варианты конфигурации: Strict Priority /2-8 взвешенные очереди

Конфигурация по умолчанию: Strict Priority

Функция: Настройте режим планировщика очереди портов.

Weight

Диапазон: 1~100

Конфигурация по умолчанию: 17

Функция: Настройка веса очереди.

9. Настройка Port Shaping, как показано далее.

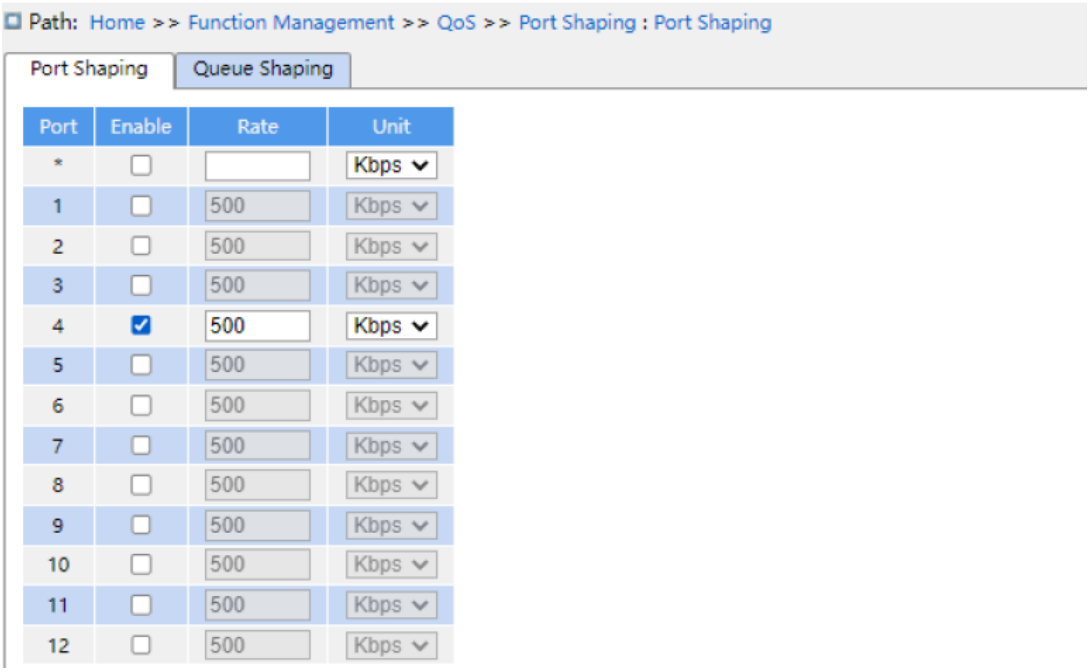


Рис. 213. Настройка Port Shaping

Enable

Варианты конфигурации: Enable/disable

Конфигурация по умолчанию: disable

Функция: включение функции shaping для порта. Port shaping устанавливает лимит скорости для выбранного порта.

Rate, Unit

Диапазон:16~1000000kbps/ 1~1000Mbps

Функция: Ограничьте скорость передачи количества кадров по порту и отбрасывайте кадры, превышающие ограниченное значение.

10. Настройка Queue shaping, как показано далее.

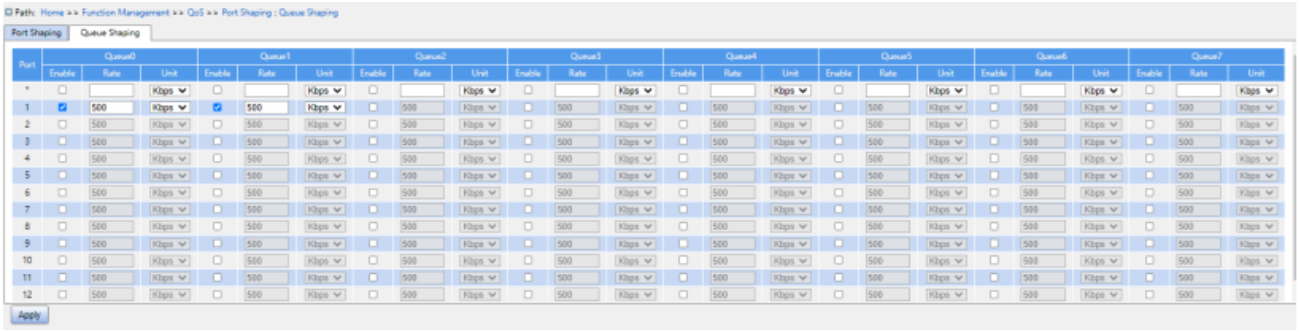


Рис. 214. Настройка Queue shaping

Enable

Варианты конфигурации: Enable/disable

Конфигурация по умолчанию: disable

Функция: включить ли режим shaping для очереди.

Rate, Unit

Диапазон: 16~1000000kbps/ 1~1000Mbps

Конфигурация по умолчанию: 500kbps

Функция: Ограничьте скорость кадров, передаваемых очередью на порт, и отбрасывайте кадры, превышающие заданное значение.

7.15.4 Пример конфигурации

Как показано на рис. 215, порт1~порт5 пересылают пакеты на порт 6. Среди них пакеты, полученные портом 1, являются Untag, пакеты, поступающие в порт 1, сопоставляются с очередью 2.

Значение PCP принятого пакета порта 2 равно 0, значение DEI равно 1, и пакеты, поступающие на порт 2, сопоставляются с очередью 3.

Значение DSCP полученного пакета на порту 3 равно 4, и пакеты, поступающие на порт 3, сопоставляются с очередью 6.

Порт 4 включен для тестирования и функции traffic shaping, и поскольку traffic shaping вступает в силу в направлении исходящего порта, конфигурация передается на

порт 6.

Значение DSCP для полученного пакета через порт 5 равно 5, и пакеты, поступающие на порт 5, сопоставляются с очередью 2.

Порт 6 использует режим планирования SP+WRR.

Процесс настройки:

1. Установите значение CoS для порта 1 равным 2, как показано на рис. 203.

2. Включите Tag Class порта 2 и сопоставьте (PCP=0, DEI=1) с CoS=3, как показано на рис. 202.

3. Включите DSCP на основе портов 3 и 5, как показано на рис. 203.

4. Значение Trust DSCP 4 и 5, сопоставьте значение DSCP 4 с очередью 6, а значение DSCP 5 с очередью 2, как показано на рис. 209.

5. Включите traffic shaping на порту 6, чтобы ограничить сообщения, отправляемые на порт 4, до 500 Кбит/с, например, рис. 213.

6. Настройте режим queue scheduling для порта 6 на взвешивание 6 очередей, вес очереди Q0~Q5 принимает значения 20, 40, 40, 20, 20, 20, как показано на рис. 211 и рис. 212.

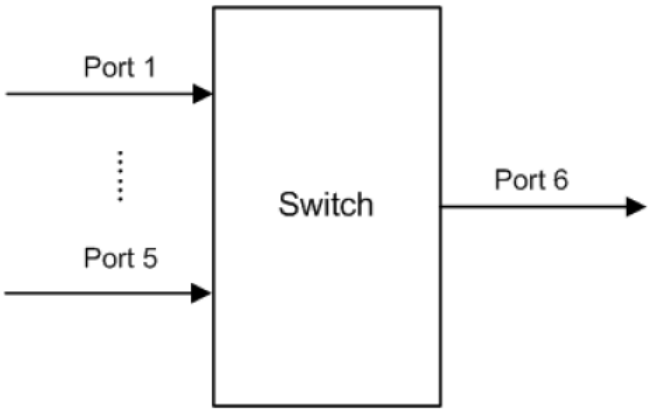


Рис. 215. Пример конфигурации QoS

Пакеты портов 1 и 5 входят в очередь 2, пакеты портов 2 входят в очередь 3, пакеты портов 3 входят в очередь 6, пакеты портов 4 входят в очередь 5.

Очереди 6 и 7 используют режим планирования со строгим приоритетом, а очереди

с 0 по 5 используют режим планирования WRR. Данные в очереди 6 обрабатываются первыми. Когда очередь 6 пуста, данные в очередях с 0 по 5 планируются с учетом весового коэффициента.

Вес очереди равен 20, 40, 40, 20, 20, 20. Таким образом, доля полосы пропускания, выделяемая пакетам во входной очереди 2, равна 40/（20+40+40+20+20+20）=25%, который распределяется между пакетами во входной очереди 3, равен 20/（20+40+40+20+20+20）=13%, и это, выделенное пакетам во входной очереди 5, равно 20/（20+40+40+20+20+20）=13%. Среди них пакеты с порта 1 и порта 5 поступают в очередь 2, таким образом, они пересылаются в соответствии с правилом "первым вошёл-первым ушёл " (FIFO), но общая доля пропускной способности портов 1 и 5 должна составлять 25%.

8 Конфигурация Loop Detect

8.1 Введение

После того, как для порта включено обнаружение петель (loop detect), пакеты обнаружения петель будут отправляться через порт, чтобы определить, существуют ли замкнутые петли в сети, подключенной к порту. Цикл отправки CPU коммутатора периодически обнаруживает пакеты, поступающие в порт. Если какой-либо порт коммутатора принимает пакеты обнаружения петель, то коммутатор определяет, что петли существуют в сети. Далее происходит отключение порта, который отправляет пакеты обнаружения петель, и порт будет подключен автоматически через некоторое время и продолжит обнаружение. Временной интервал для отправки пакетов обнаружения петель и время восстановления порта могут быть сконфигурированы.

Обнаружение петель и ST-Ring/STRP/RSTP/MSTP являются взаимоисключающими. Порт с включенным обнаружением петель не может быть сконфигурирован как кольцевой порт; на кольцевом порту не может быть включено обнаружение петель.

8.2 Web конфигурация

1. Сконфигурируйте функцию обнаружения петли порта, как показано на рис. 216.

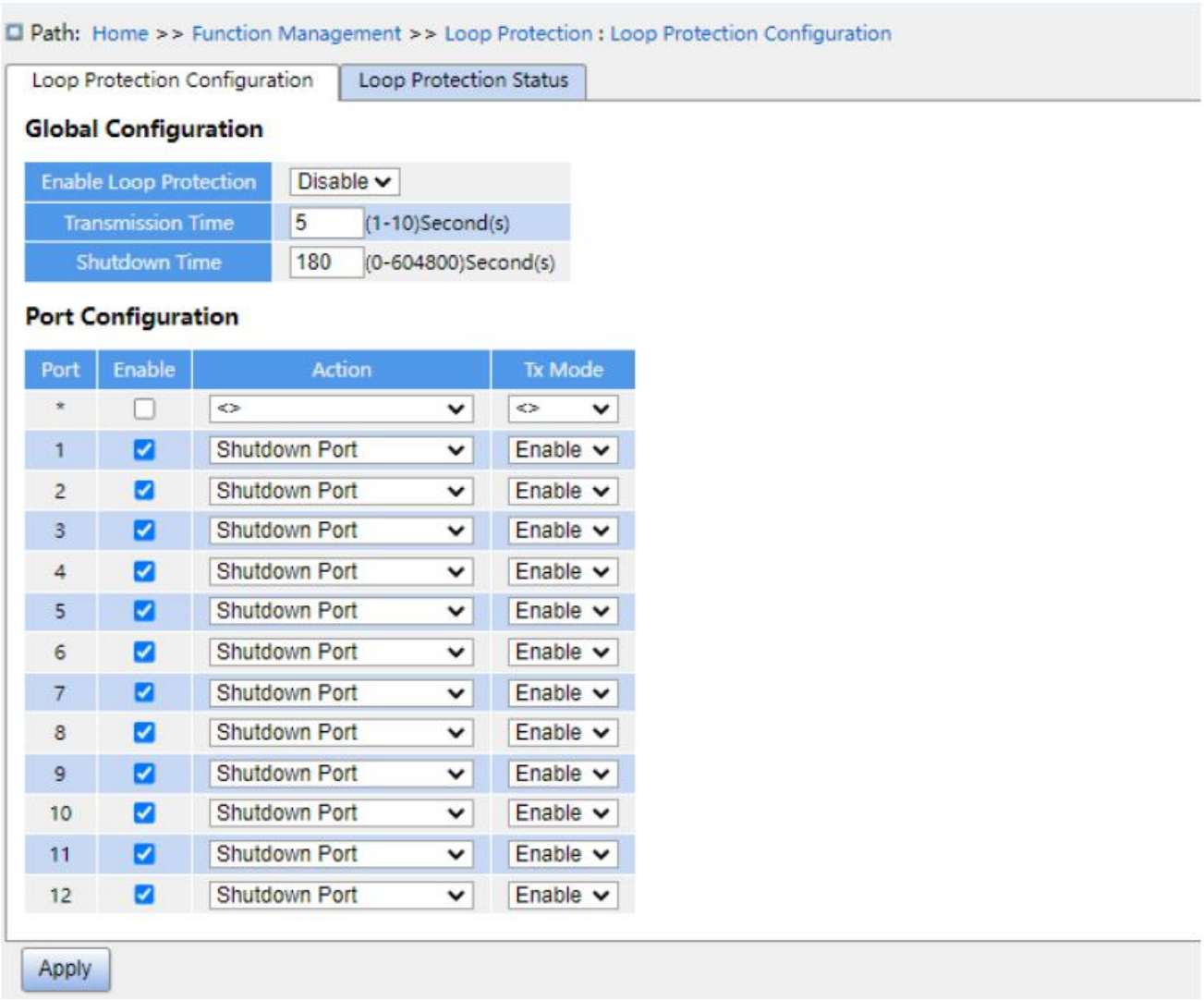


Рис. 216. Функция обнаружения петли порта

Enable Loop Protection

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включите или отключите функцию обнаружения петель для порта.

Transmission Time

Диапазон: 1~10s

Конфигурация по умолчанию: 5s

Функция: Настройте временной интервал для отправки пакетов с обнаружением петель.

Shutdown Time

Диапазон: 0~604800s

Конфигурация по умолчанию: 180s

Функция: Настройте время восстановления порта, 0 означает, что порт не может быть подключен автоматически до перезапуска устройства.

Enable

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Enable

Функция: Включите или отключите функцию обнаружения петли для порта.

Action

Варианты конфигурации: Shutdown Port/Shutdown Port and Log/Log Only

Конфигурация по умолчанию: Shutdown Port

Функция: Укажите действие, которое должно быть выполнено, когда порт обнаруживает, что существует петля.

Tx Mode

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Enable

Функция: Следует ли отправлять пакеты с обнаружением петель или нет.

Порт может точно определить, существует ли петля, только после того, как глобально включена защита от петель, на порту включена защита от петель и режим Tx.

2. Просмотрите состояние защиты от петель, как показано на рисунке далее.

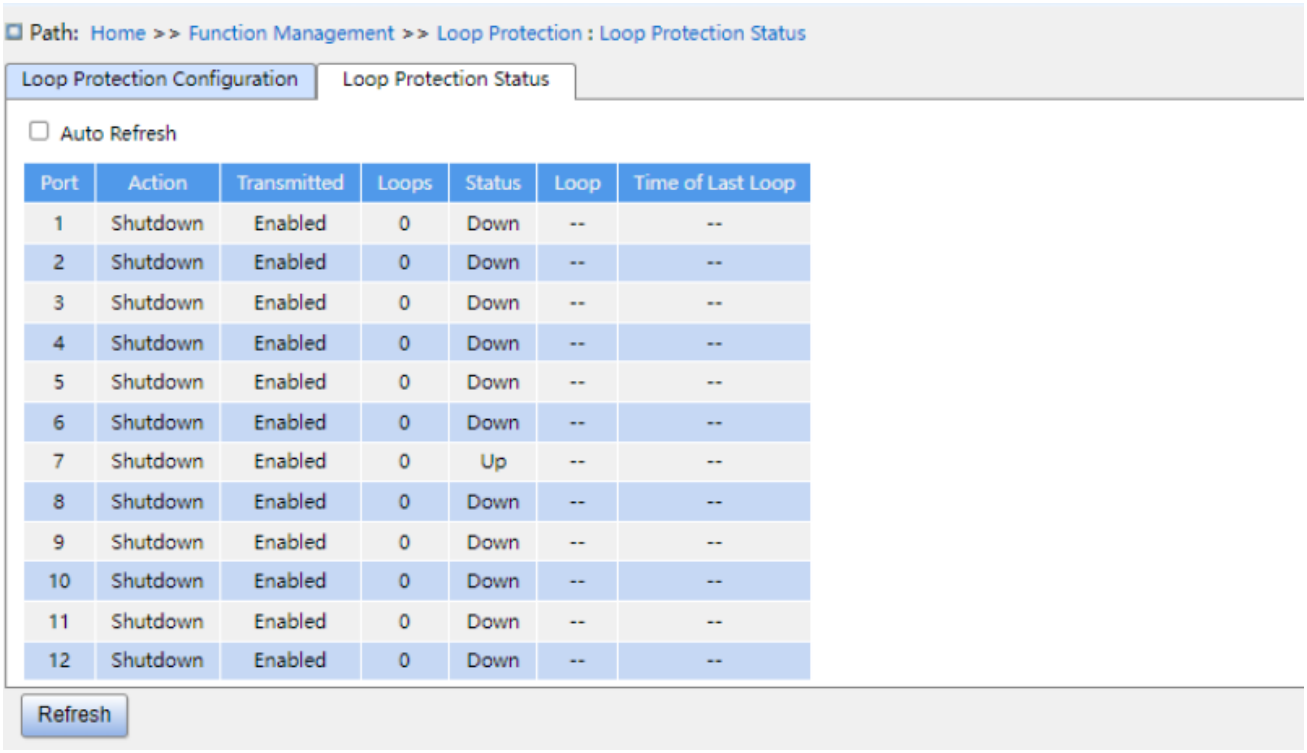


Рис. 217. Состояние защиты от петель

Loop Protection Status

Опции: --/Loop

Функция: Статус обнаружения петли показывает, есть ли петли в сети, когда включена функция обнаружения петли порта. Loop указывает на наличие петель, в то время как -- указывает на отсутствие петли.

8.3 Пример конфигурации

Требования к сети:

Порт 3 коммутатора подключен к внешней сети. Когда в сети появятся петли, то требуется отключить порт 3, как показано на рис. 218.

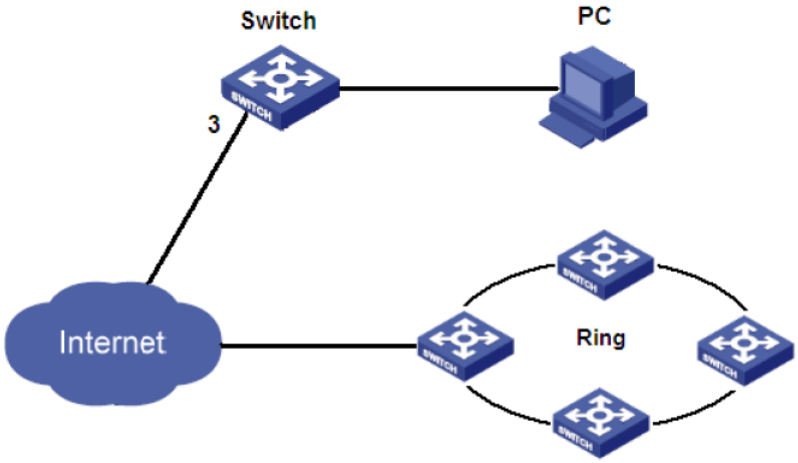


Рис. 218. Пример конфигурации

Конфигурация коммутатора:

Включите обнаружение петель на порту 3, как показано на рис. 216.

9 Диагностика

9.1 Ведение журнала

9.1.1 Введение

Журнал коммутатора содержит информацию о состоянии системы, сбоях, отладке, аномалиях и другую информацию. При соответствующей настройке коммутатор может загружать журналы на сервер, поддерживающий системный журнал Syslog, в режиме реального времени.

Журнал также содержит информацию о тревогах, широковещательном шторме, перезагрузке, памяти и информацию о действиях пользователей.

9.1.2 Web конфигурация

1. Настройка системного журнала (Syslog).

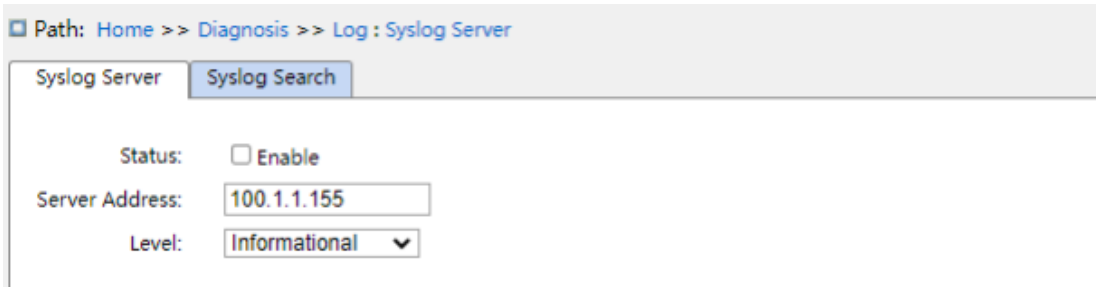


Рис. 219. Настройка сервера Syslog

Status

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включение сервера системного журнала (Syslog).

Server address

Формат: A.B.C.D

Функция: Настройка IP-адреса для сервера Syslog.

Level

Варианты конфигурации: Error/Warning/Notice/ Informational

Конфигурация по умолчанию: Informational

Функция: Выберите уровень отображаемой информации журнала.

Выберите для установки на ПК программное обеспечение, поддерживающее сервер системного журнала, например Tftp32.

Информацию журнала можно просматривать в режиме реального времени на вкладке syslog server.

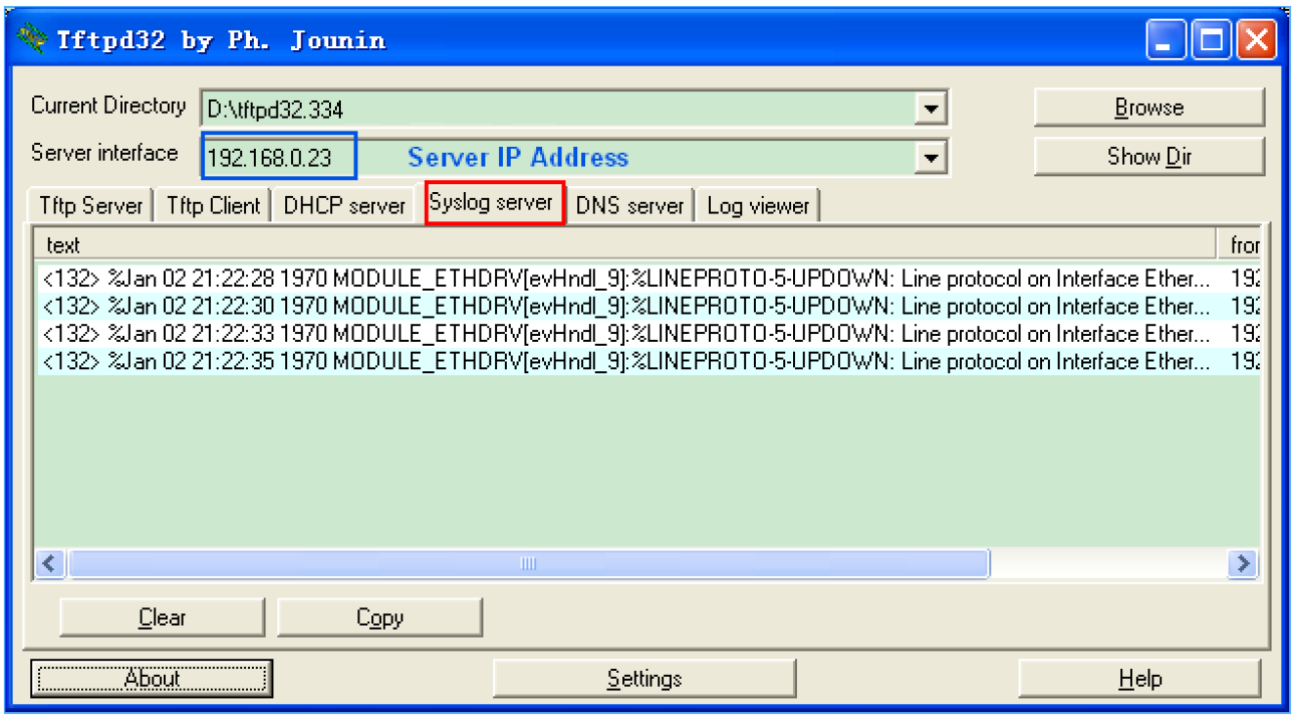


Рис. 220. Настройка сервера Syslog в Tftp32

2. Запрос журнала.

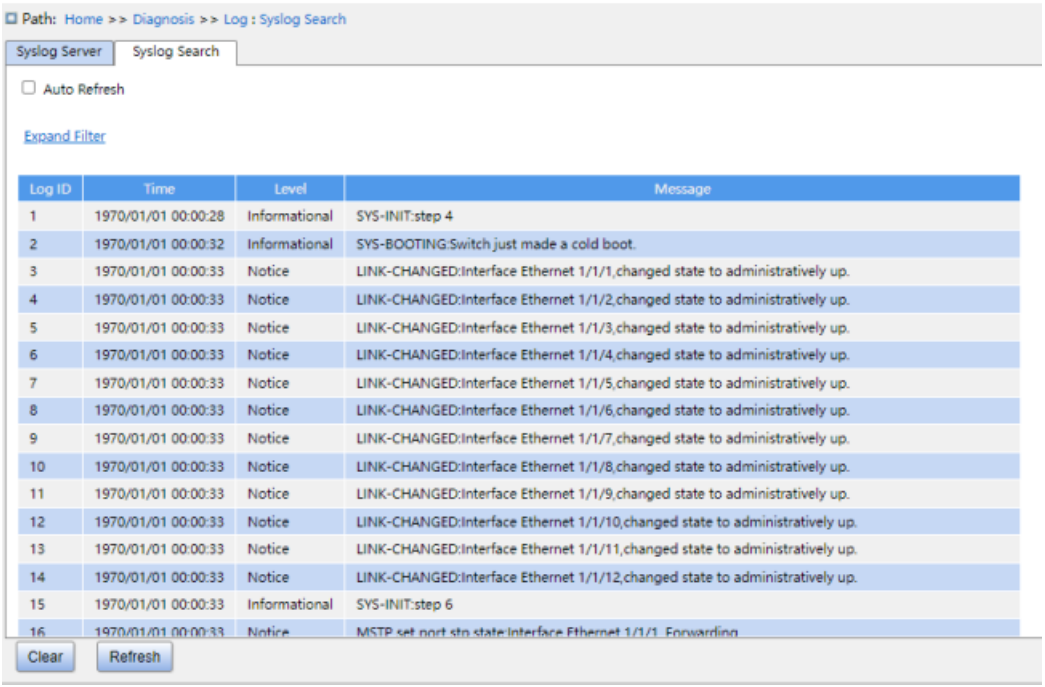


Рис. 221. Настройка поиска в Syslog

Auto Refresh

Варианты конфигурации: Check/uncheck

Конфигурация по умолчанию: uncheck

Функция: Включение функции автоматического обновления.

Log ID

Варианты конфигурации: */>=/<=/select range

Конфигурация по умолчанию: *

Функция: Выберите идентификатор отфильтрованного журнала: «*» - все журналы идентификаторов, «>=» - журналы фильтрации, которые больше или равны идентификатору, «<=» - фильтр меньше или равен идентификатору, «выбрать диапазон» - введите диапазон вручную.

Time

Варианты конфигурации: */Start/end/select range

Конфигурация по умолчанию: *

Функция: Выберите отфильтрованный диапазон времени, «*» - весь журнал времени, «Начало» - время начала журнала, «конец» - время окончания журнала, «выбрать диапазон» - введите диапазон вручную.

Level

Варианты конфигурации: */>=/<=/select range

Конфигурация по умолчанию: *

Функция: Выберите диапазон отфильтрованных уровней, «*» - журнал всех уровней, «>=» - журналы фильтрации больше или равны уровню, «<=» - журналы фильтрации меньше или равны уровню, «выберите диапазон» - введите диапазон уровней вручную, уровни содержат Error，Warning，Notice，Information.

Message

Варианты конфигурации: */include/not include

Конфигурация по умолчанию: *

Функция: Выберите отфильтрованное сообщение, «*» - все журналы, «include» - включить журналы для некоторых полей, «not include» - не включать журналы для некоторых полей.

3. Управление хранилищем журналов.

4. Экспорт журнала. Возможен экспорт журналов из флэш-памяти или оперативной память на локальный компьютер в исходном формате.

9.2 Зеркалирование портов

9.2.1 Введение

С помощью функции зеркалирования порта коммутатор копирует все принятые или переданные кадры данных в выбранном порте (порт зеркального источника) на другой порт (порт зеркального назначения). Порт зеркального назначения возможно подключить к анализатору протоколов или монитору RMON для сетевого мониторинга, управления и диагностики неисправностей.

9.2.2 Принцип работы

Коммутатор поддерживает четыре зеркальных порта назначения, но несколько исходных портов. Несколько исходных портов могут находиться либо в одной VLAN, либо в разных VLAN. Зеркальный порт источника и порт назначения могут находиться в одной VLAN или в разных VLAN. Порт источника и порт назначения не могут быть одним и тем же портом.

Динамическое определение MAC-адреса должно быть отключено на порте назначения.

9.2.3 Web конфигурация

1. Настройка функции зеркалирования портов.

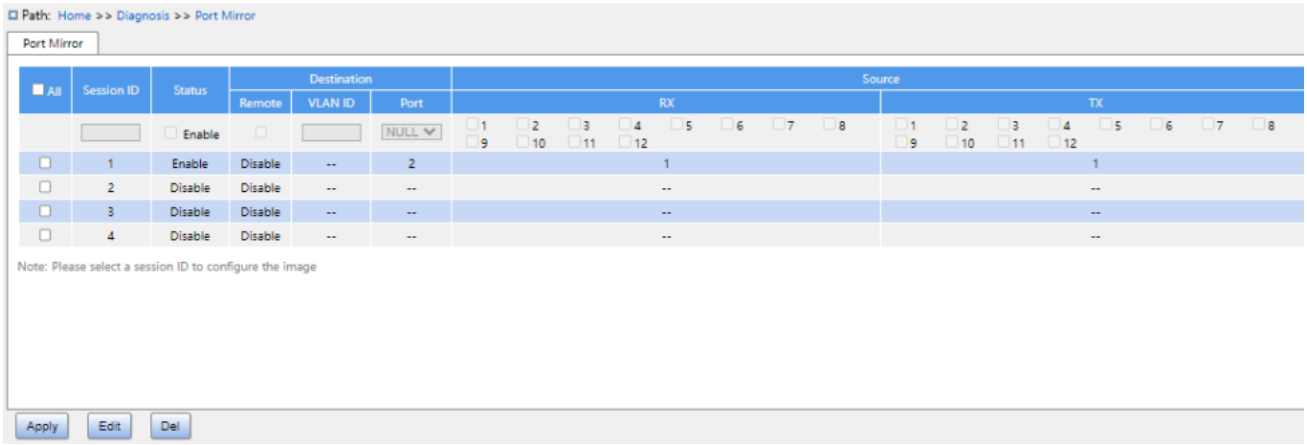


Рис. 222. Настройка функции зеркалирования

ALL

Варианты конфигурации: Check/uncheck

Конфигурация по умолчанию: Uncheck

Функция: Выбор группы зеркалирования для изменения настроек.

Status

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включение зеркалирования на выбранном порте.

Destination Port

Варианты конфигурации: NULL/ номер порта

Конфигурация по умолчанию: NULL

Функция: Выберите порт назначения. Возможно выбрать только один порт.

Rx

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Зеркальное отображение кадров, полученных в указанный порта.

Tx Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Зеркальное отображение кадров, переданных из указанного порта.

2. Настройка удаленного (remote) зеркалирования.

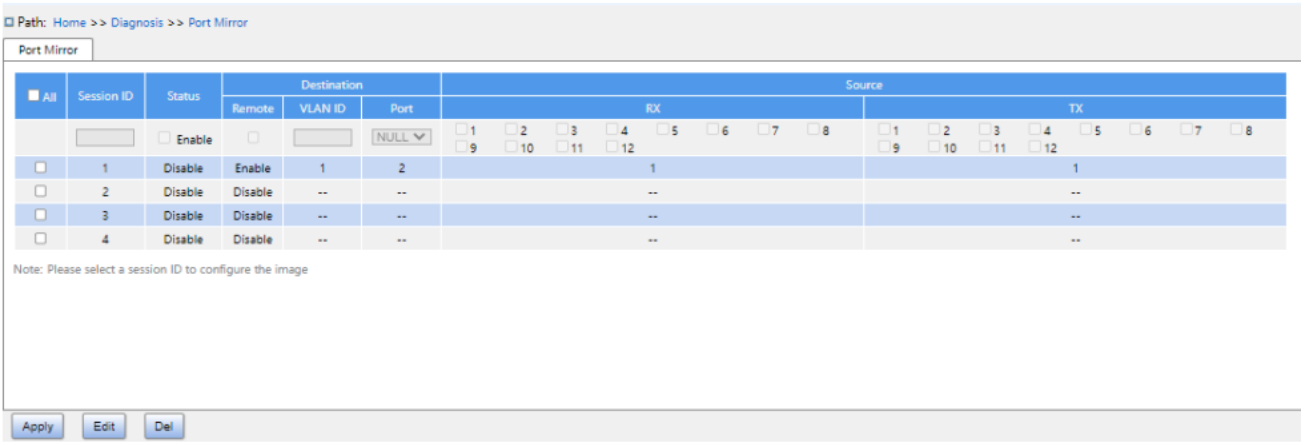


Рис. 223. Настройка функции Remote Mirror

All

Варианты конфигурации: Check/uncheck

Конфигурация по умолчанию: Uncheck

Функция: Выбор группы зеркалирования для изменения настроек.

Status

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включение зеркалирования на выбранном порте.

Destination Remote

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включение функции удаленного (remote) зеркалирования.

Функции desination remote и source remote не могут быть включены одновременно.

Destination VLAN ID

Диапазон: 1~4093

Функция: Настройте Destination VLAN ID для удаленного (remote) зеркалирования.

Destination Port

Варианты конфигурации: NULL/ номер порта

Конфигурация по умолчанию: NULL

Функция: Укажите Destination Port для удаленного (remote) зеркалирования.

Source Port

Варианты конфигурации: Disable/RX/TX

Конфигурация по умолчанию: NULL

Функция: Укажите Source Port для удаленного (remote) зеркалирования.

9.2.4 Пример конфигурации

Зеркальным портом назначения является порт 2, а зеркальным портом источника - порт 1. Как переданные, так и принятые пакеты на порту 1 зеркально отображаются на порт 2.

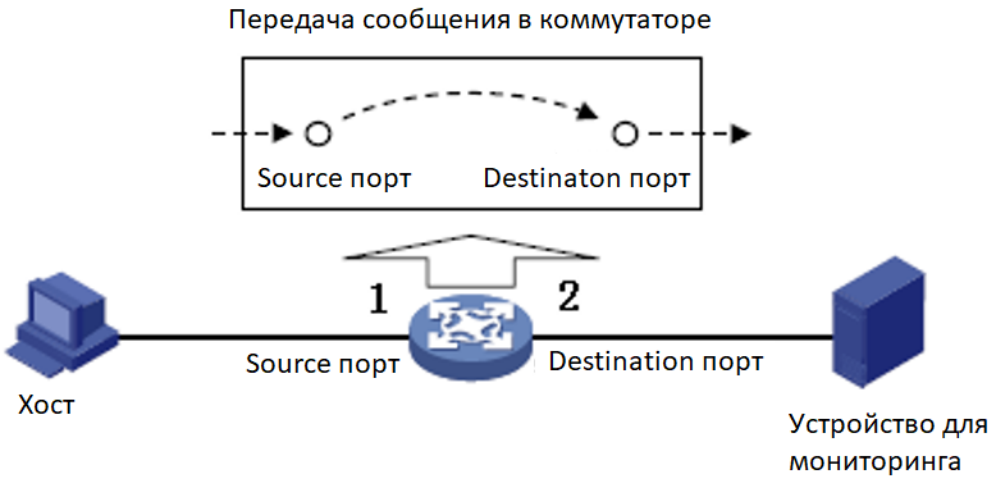


Рис. 224. Пример конфигурации

Настройка коммутатора:

1. Включите функцию зеркального отображения портов, как показано на рис. 222.

2. Установите порт 2 в качестве destination порта , порт 1 в качестве source порта и режим зеркального отображения портов для Rx и Tx, как показано на рис. 222.

9.3 LLDP

9.3.1 Введение

Link Layer Discovery Protocol (LLDP) обеспечивает стандартный механизм обнаружения канального уровня. LLDP инкапсулирует информацию об устройстве, такую как возможности устройства, адрес управления, идентификатор устройства, идентификатор интерфейса в блок данных Link Layer Discovery Protocol Data Unit (LLDPDU) и сообщает LLDPDU своим соседям, подключенным напрямую. После получения LLDPDU соседи сохраняют эту информацию в MIB для запроса и проверки статуса связи службой NMS.

9.3.2 Web конфигурация

1. Конфигурация LLDP.

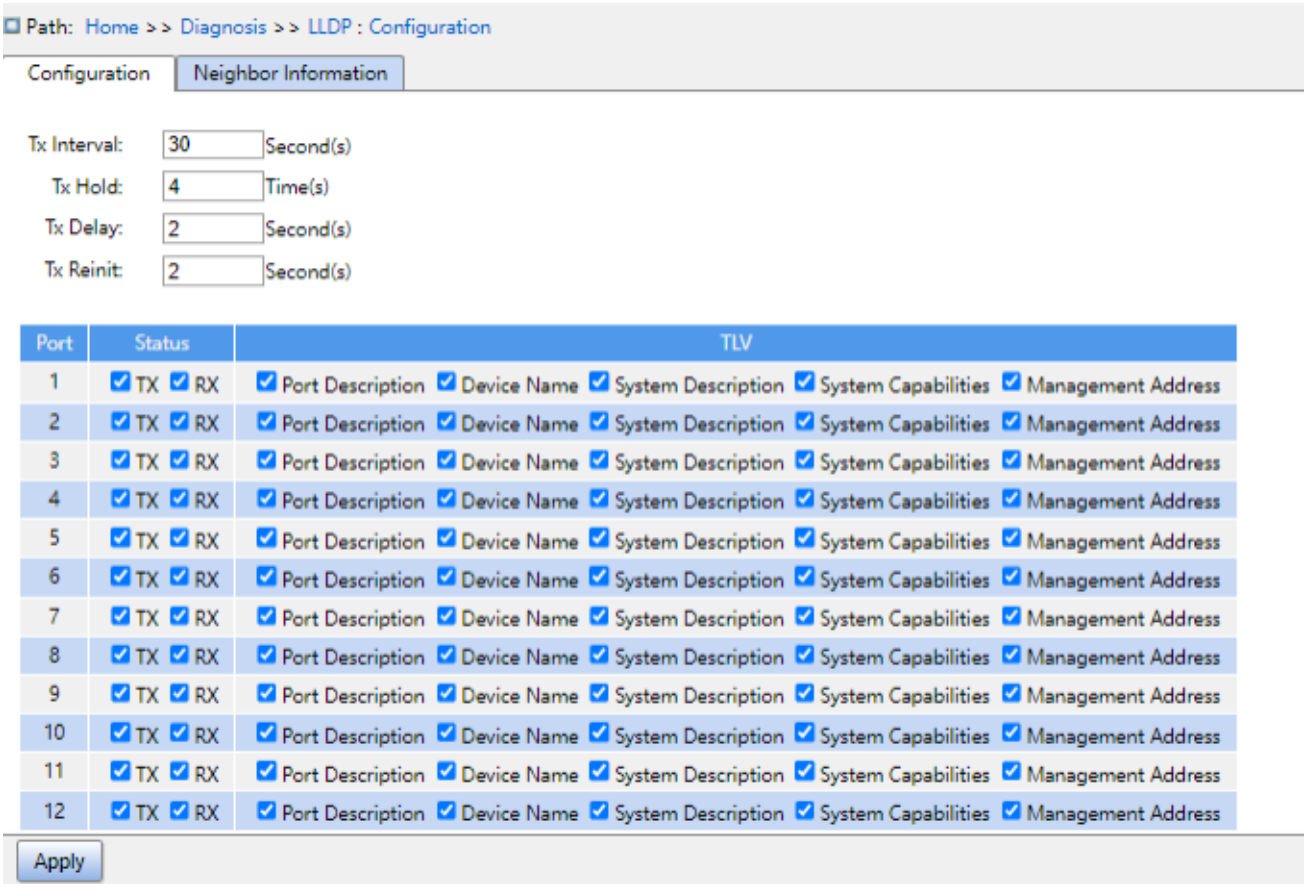


Рис. 225. Конфигурация LLDP

Tx Interval

Диапазон: 5~32768 сек.

Конфигурация по умолчанию: 30 сек.

Функция: Настройка временного интервала для отправки пакетов LLDP.

Tx Hold

Диапазон: 2~10

Конфигурация по умолчанию: 4

Функция: Установите количество периодов Tx holding. Эффективная продолжительность пакета LLDP = Tx Interval * Tx Hold.

Tx Delay

Диапазон: 1~8192 сек.

Конфигурация по умолчанию: 2 сек.

Функция: Установите интервал передачи между новым пакетом LLDP и предыдущим пакетом LLDP при изменения информации о конфигурации. Значение Tx Delay не может превышать 1/4 значения Tx Interval.

Tx Reinit

Диапазон: 1~10 сек.

Конфигурация по умолчанию: 2 сек.

Функция: После отключения LLDP на порту или перезапуска коммутатора коммутатор отправляет кадр завершения работы LLDP соседнему узлу, чтобы объявить, что предыдущий пакет LLDP недействителен. Tx Reinit относится к интервалу времени между отправкой кадра отключения LLDP и повторной инициализацией сообщения LLDP.

Status

Варианты конфигурации: Disable /TX/RX/TX&RX

Конфигурация по умолчанию: TX&RX

Функция: Настройка пакетный режима LLDP. Включение режима TX&RX означает,

что коммутатор отправляет оба пакета LLDP, а также принимает и идентифицирует пакеты LLDP; Disable режим означает, что коммутатор не отправляет пакеты LLDP и не принимает пакеты LLDP; Только режим Rx означает, что коммутатор только принимает и распознает пакеты LLDP и не отправляет пакеты LLDP; Только режим Tx режим означает, что коммутатор отправляет только пакеты LLDP и не принимает пакеты LLDP.

Port Descripition

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Enable

Функция: Enable указывает, что пакеты LLDP будут содержать описание порта.

Device Name

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Enable

Функция: Enable указывает, что пакеты LLDP будут содержать имя системы.

System Descripition

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Enable

Функция: Enable указывает, что пакеты LLDP будут содержать описание системы.

Sys Capability

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Enable

Функция: Enable указывает, что пакеты LLDP будут передавать системные возможности.

Management Address

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Enable

Функция: Enable указывает, что пакеты LLDP будут содержать адрес управления.

2. Просмотр информации о LLDP

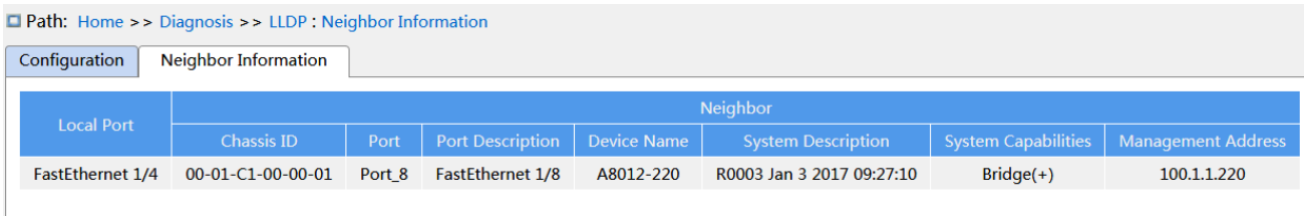


Рис. 226. Просмотр информации по LLDP

Для отображения информации LLDP на двух подключенных устройствах должна быть включена функция LLDP.

9.4 Trace Route

Трассировка маршрута (trace route) позволяет видеть маршрут IP-пакетов данных от одного хоста к другому.

1. Настройка трассировки маршрута.

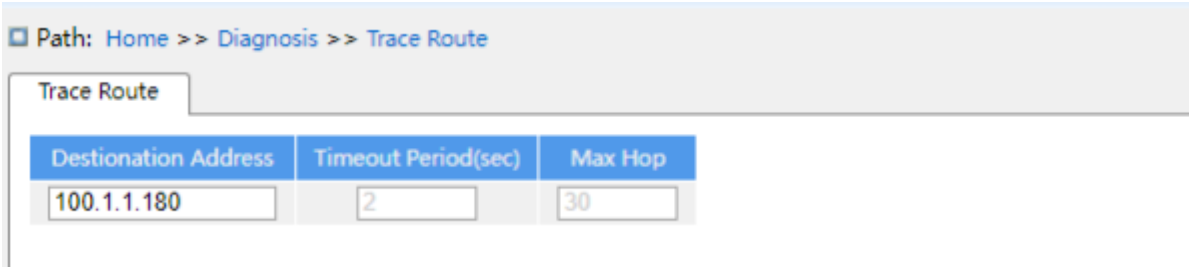


Рис. 227. Настройка Trace route

Destination address

Формат: A.B.C.D

Функция: Настройте IP-адрес конечного устройства.

Timeout Period

Диапазон: 1~10 сек.

Конфигурация по умолчанию: 2 сек.

Функция: Настройка периода ожидания. Если отправляющая сторона не получит ответное сообщение от принимающей стороны в течение этого времени, связь будет

прервана.

Max Hop

Диапазон: 1~255

Конфигурация по умолчанию: 30

Функция: Установите количество шлюзов, через которые проходят пакеты данных от отправляющего устройства к устройству назначения.

2. Просмотр выходных данных команды Trace Route.

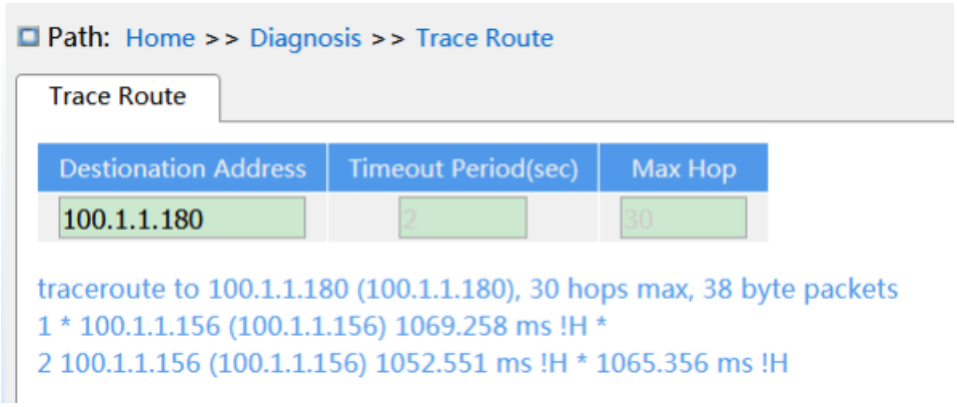


Рис. 228. Просмотр вывода для Trace Route

9.5 Ping

Пользователи могут запустить команду ping, чтобы проверить, доступно ли устройство с указанным адресом и не нарушено ли сетевое подключение во время технического обслуживания системы.

1. Настройка команды ping

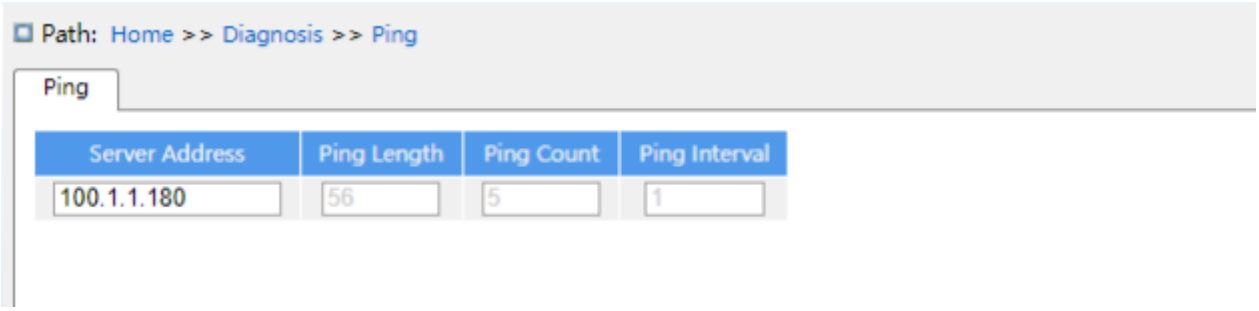


Рис. 229. Настройка команды ping

Server Address

Формат: A.B.C.D

Функция: Введите IP-адрес конечного устройства.

Ping Length

Диапазон: 2~1452 байт

Конфигурация по умолчанию: 56 байт

Функция: Укажите длину ICMP-запроса (исключая IP и заголовок ICMP-пакета).

Ping Count

Диапазон: 1~60

Конфигурация по умолчанию: 5

Функция: Укажите количество раз для отправки ICMP-запроса.

Ping Interval

Диапазон: 0~30 сек.

Конфигурация по умолчанию: 1 сек.

Функция: Укажите интервал для отправки ICMP-запроса.

2. Просмотр выходных данных команды ping.

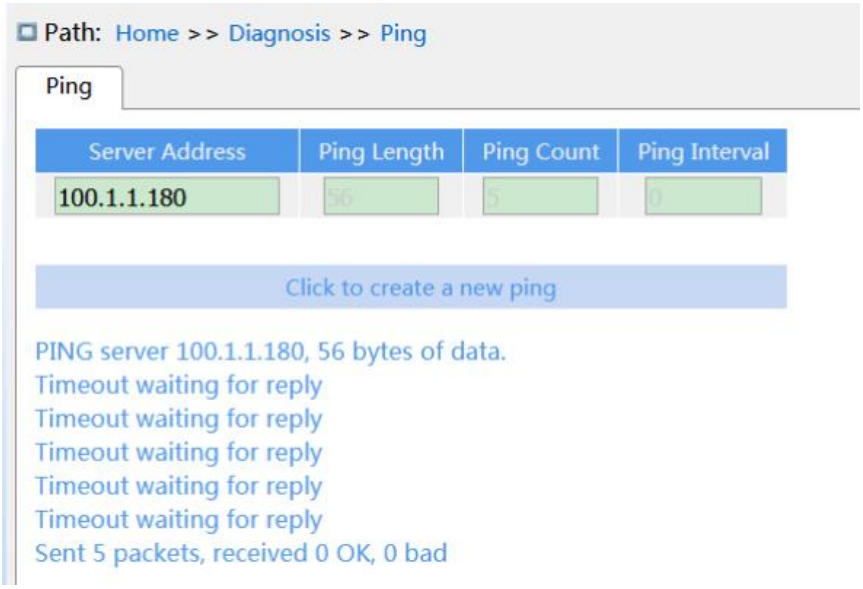


Рис. 230. Просмотр вывода команды ping

Выходные данные команды ping включают ответ устройства назначения на каждый пакет ICMP-запроса и статистику пакетов, собранную во время выполнения команды

ping.

9.6 IP Source Guard

9.6.1 Введение

Благодаря функции IP Source Guard сообщения, пересылаемые портом, могут быть отфильтрованы, чтобы предотвратить прохождение несанкционированнх сообщений через порт, таким образом, это ограничивает несанкционированное использование сетевых ресурсов (например, нелегальный хост выдает себя за IP-адрес разрешенного пользователя).

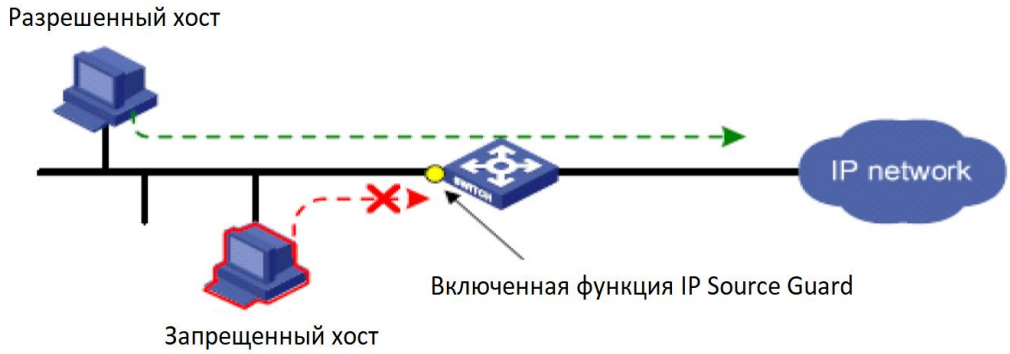


Рис. 231. Пример работы функции IP Source Guard

9.6.2 Принцип работы

Настроенный порт с функцией IP Source Guard выполняет поиск в таблице привязки (binding table) IP Source Guard. После получения сообщения, если элемент функции в сообщении совпадает с записанным элементом функции в таблице привязки, то порт пересылает сообщение, в противном случае сообщение удаляется. Функция привязки предназначена для выбранного порта, и только этот порт будет ограничен, на другие порты привязка не влияет.

Функциональный элемент IP Source Guard включает в себя: IP-адрес источника, MAC-адрес источника и тег VLAN. IP Source Guard поддерживает комбинацию портов со следующими функциональными элементами:

- IP, MAC, IP+MAC
- IP+VLAN, MAC+VLAN, IP+MAC+VLAN

Поддерживаемый тип привязки элементов таблицы к порту связан с типом устройства, в зависимости от фактического состояния устройства.

Функция IP Source Guard делится на статическую привязку (static binding) и динамическую привязку (dynamic binding) в соответствии с режимом генерации элементов таблицы привязки:

- **Static binding:** Ручная настройка элементов таблицы привязки для управления портом подходит для случая, когда количество хостов в локальной сети небольшое или для каждого хоста требуется привязка отдельно;
- **Dynamic binding:** Функция управления портами выполняется путем автоматического получения элементов таблицы привязки DHCP Snooping или DHCP Relay. Принцип заключается в том, что всякий раз, когда DHCP назначает элемент таблицы пользователю, функция динамической привязки добавляет элемент таблицы привязки соответствующим образом, чтобы разрешить пользователю доступ к сети. Если пользователь устанавливает IP-адрес конфиденциально, он не сможет получить доступ к сети, поскольку при этом не запускается элемент таблицы назначения DHCP, а функция динамической привязки не добавляет соответствующее правило разрешения доступа.

8.6.3 Web конфигурация

1. Включение защиты IP Source Guard.

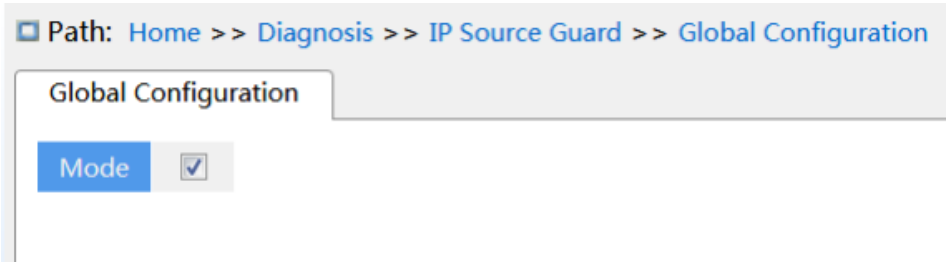


Рис. 232. Включение IP Source Guard

Mode

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включение защиты IP Source Guard на коммутаторе.

2. Настройка защиты IP Source Guard для портов.

Рис. 233. Настройка IP Source Guard для портов

Enable

Варианты конфигурации: Enable / Disable

Конфигурация по умолчанию: Disable

Функция: Включение защиты IP Source Guard для выбранных портов.

3. Настройка таблицы Static Binding

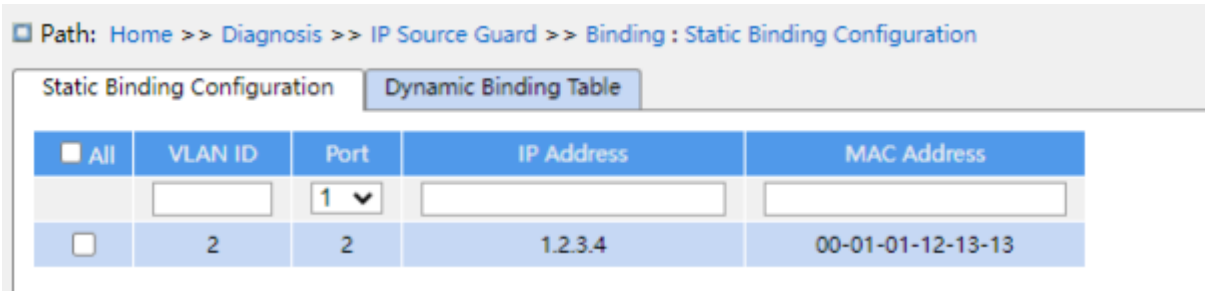


Рис. 234. Настройка Static Binding

VLAN ID

Варианты конфигурации: все доступные VLAN ID

Функция: Настройка VLAN ID для таблицы статической привязки.

Port

Функция: Выберите порт элемента таблицы статической привязки.

IP address

Формат: A.B.C.D

Функция: настройте IP-адрес для элемента таблицы статической привязки.

MAC address

Формат: HH-HH-HH-HH-HH-HH или HH:HH:HH:HH:HH:HH (H - шестнадцатеричное число)

Функция: Настройте MAC-адрес статической таблицы привязки. Настройте только как одноадресный (unicast) MAC-адрес.

4. Просмотр динамической таблицы (Dynamic Binding table)

Рис. 235. Просмотр динамической таблицы

Type

Варианты отображения: Relay/Snooping

Описание: Таблица динамической привязки генерируется устройствами DHCP Relay и DHCP Snooping. Элементы таблицы типа Relay генерируются после включения IP Source Guard, элементы таблицы типа snooping генерируются после включения IP Source Guard и портов, подключающихся по DHCP.

8.6.4 Пример конфигурации

1. Элементы таблицы IP Source Guard типа Relay

Коммутатор A в качестве DHCP-сервера, коммутатор B в качестве DHCP-ретранслятора, коммутатор C в качестве DHCP-клиента. 1 порт коммутатора A подключен к 1 порту коммутатора B, 2 порта коммутатора B подключены ко 2 портам коммутатора C. DHCP-сервер находится не в той же локальной сети, что и DHCP-клиент. После того, как устройство ретрансляции включит IP Source Guard, клиент динамически получает IP-адрес и другие сетевые параметры в режиме DHCP через DHCP relay. Устройство ретрансляции формирует элементы таблицы IP Source Guard.

Рис. 236. Пример конфигурации при работе с DHCP

Конфигурация Коммутатора A:

1. Создайте VLAN1 и настройте IP-адрес: 100.1.1.156;

2. Откройте состояние DHCP-сервера в VLAN 1, см. рис. 168;

3. Создайте пул адресов pool-33, см. рис. 169;

4. Выберите тип пула адресов в качестве Network; IP-адрес: 33.1.1.6; Отметка: 255.0.0.0, см. рис. 170;

Конфигурация Коммутатора B:

1. Создайте VLAN1 и настройте IP-адрес: 100.1.1.180;

2. Создайте VLAN 33 и настройте IP-адрес: 33.1.1.2;

3. Включите DHCP Relay, см. рис. 183:

4. Настройте IP-адрес сервера: 100.1.1.156, см. рис. 183;

5. Включите global IP Source Guard, как показано на рис. 232;

Конфигурация Коммутатора C:

1. Создайте VLAN 33 и включите DHCP-клиент;

2. Коммутатор A назначает адрес 33.0.0.1 коммутатору C;

После того, как коммутатор C получит адрес, таблицу IP Source Guard можно просмотреть на коммутаторе B.

2. Элементы таблицы IP Source Guard типа Snooping

Коммутатор A как DHCP-сервер, коммутатор B как DHCP Snooping устройство, коммутатор C как DHCP-клиент. 1 порт коммутатора A подключен к 1 порту коммутатора B, 2 порта коммутатора B подключены ко 2 портам коммутатора C. DHCP-сервер находится не в той же локальной сети, что и DHCP-клиент. После того, как Snooping устройство включит IP Source Guard, клиент динамически получает IP-адрес и другие сетевые параметры в режиме DHCP посредством DHCP Snooping. Устройство ретрансляции формирует элементы таблицы IP Source Guard.

Рис. 237. Пример конфигурации при работе с DHCP Snooping

Конфигурация Коммутатора A:

1. Создайте VLAN1 и настройте IP-адрес: 100.1.1.156;

2. Откройте состояние DHCP-сервера в VLAN 1, см. рис. 168;

3. Создайте пул адресов pool-1;

4. Выберите тип пула адресов в качестве сети; IP-адрес: 33.1.1.6; Отметка: 255.0.0.0;

Конфигурация Коммутатора B:

1. Создайте VLAN1 и настройте IP-адрес: 100.1.1.180;

2. Включите DHCP Snooping;

3. Настройте 1 порт в качестве trust port, см. рис. 179;

4. Включите IP Source Guard, см. рис. 232

5. Порт 2 включите в IP Source Guard, как показано на рис. 233;

Конфигурация Коммутатора C:

1. Создайте VLAN 1 и включите DHCP-клиент;

2. Коммутатор A назначает адрес 100.0.0.1 коммутатору C;

После того, как коммутатор C получит адрес, таблицу IP Source Guard можно просмотреть на коммутаторе B.

9.7 DDM

9.7.1 Введение

Цифровая диагностика (DDM) является эффективным методом контроля важных рабочих параметров оптических модулей. К параметрам, которые она отслеживает, относятся: передаваемая оптическая мощность, принимаемая оптическая мощность, температура, рабочее напряжение, ток смещения и аварийная информация.

9.7.2 Web конфигурация

1. Основная информация

Просмотр информации об оптическом модуле.

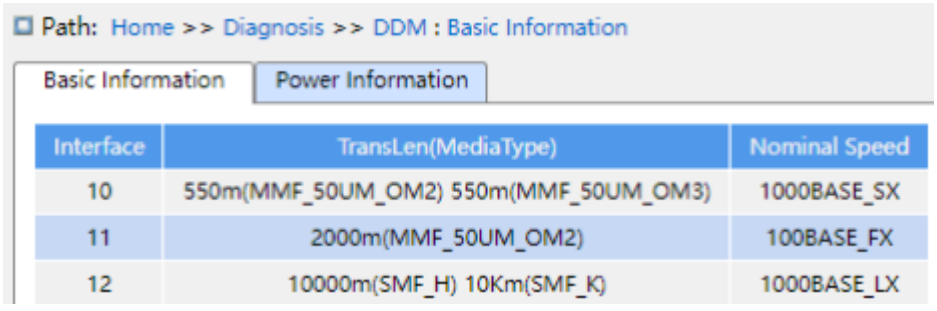


Рис. 238. Основная информация DDM

2. Просмотр информации о мощности сигналов

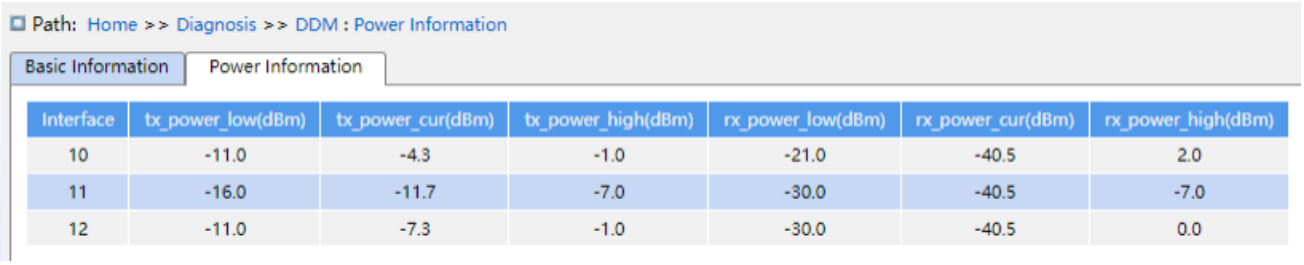


Рис. 239. Информация об оптической мощности

Приложение: принятые сокращения

Сокращение	Полное обозначение	Полное обозначение
ACE	Access Control Entry	Запись для списка контроля доступа
ACL	Access Control List	Список контроля доступа
ARP	Address Resolution Protocol	Протокол разрешения адресов
BootP	Bootstrap Protocol	Протокол получения IP адреса
BPDU	Bridge Protocol Data Unit	Блок данных протокола Spanning Tree
CIST	Common and Internal Spanning Tree	Общее и внутреннее связующее дерево
CLI	Command Line Interface	Интерфейс командной строки
CoS	Class of Service	Класс сервиса
CST	Common Spanning Tree	Общее связующее дерево
DHCP	Dynamic Host Configuration Protocol	Протокол динамического конфигурирования узлов
DHP	Dual Homing Protocol	Протокол двойной обратной связи
DNS	Domain Name System	Система доменных имен
DSCP	Differentiated Services CodePoint	Точка кода дифференцированных сервисов
DST	Daylight Saving Time	Переход на летнее время
EAPOL	Extensible Authentication Protocol over LAN	Протокол пердачи пакетов EAP через локальную сеть
GARP	Generic Attribute Registration Protocol	Протокол регистрации основных атрибутов
GMRP	GARP Multicast Registration Protocol	GARP протокол регистрации многоадресной рассылки
GVRP	GARP VLAN Registration Protocol	GARP ротокол регистрации VLAN
HTTP	Hyper Text Transfer Protocol	Протокол передачи гипертекста
ICMP	Internet Control Message Protocol	Протокол управляющих сообщений в сети
IGMP	Internet Group Management Protocol	Протокол управления групповой (multicast) передачей данных в сетях
IGMP Snooping	Internet Group Management Protocol Snooping	Протокол отслеживания IGMP

IST	Internal Spanning Tree	Внутреннее связующее дерево
LACP	Link Aggregation Control Protocol	Протокол управления агрегацией каналов
LACPDU	Link Aggregation Control Protocol Data Unit	Блок данных LACP
LLDP	Link Layer Discovery Protocol	Протокол обнаружения канального уровня
LLDPDU	Link Layer Discovery Protocol Data Unit	Блок данных LLDP
MIB	Management Information Base	База сведений об управлении
MSTI	Multiple Spanning Tree Instance	Экземпляр (инстанс) множественного связующего дерева
MSTP	Multiple Spanning Tree Protocol	Протокол множественного связующего дерева
NAS	Network Access Server	Сервер сетевого доступа
NetBIOS	Network Basic Input/Output System	Сетевая базовая система Ввода/Вывода
NMS	Network Management Station	Станция управления сетью
NTP	Network Time Protocol	Протокол сетевого времени
OID	Object Identifier	Идентификатор объекта
PCP	Priority Code Point	Код приоритета
PVLAN	Private VLAN	Частная VLAN
QCL	QoS Control List	Список управления QoS
QoS	Quality of Service	Качество обслуживания
RADIUS	Remote Authentication Dial-In User Service	Система аутентификации удаленных пользователей
RMON	Remote Network Monitoring	Дистанционный мониторинг сети
RSTP	Rapid Spanning Tree Protocol	Быстрый протокол связующего дерева
SFTP	Secure File Transfer Protocol	Защищенный протокол передачи файлов на основе SSH
SNMP	Simple Network Management Protocol	Простой протокол сетевого управления
SNTP	Simple Network Time Protocol	Простой протокол синхронизации времени
SP	Strict Priority	Строгий приоритет
SSH	Secure Shell	Протокол защищенной оболочки
SSL	Secure Sockets Layer	Уровень защищенных сокетов, протокол

		шифрования
SSM	Source Specific Multicast	Многоадресная рассылка для конкретных источников
STP	Spanning Tree Protocol	Протокол связующего дерева
TACACS+	Terminal Access Controller Access Control System	Система контроля доступа контроллера для терминалов
TCP	Transmission Control Protocol	Протокол управления передачей
UDP	User Datagram Protocol	Протокол пользовательских датаграмм
USM	User-Based Security Model	Модель безопасности на основе пользователей
VLAN	Virtual Local Area Network	Виртуальная локальная сеть
WINS	Windows Internet Naming Service	служба Internet имен
WRR	Weighted Round Robin	Взвешенный циклический перебор