Промышленный Ethernet коммутатор серии SICOM3000S

Руководство по программной части

Версия 1.0

Сайт: https://kyland-rus.ru/

Эл. почта: sales@kyland-rus.ru
support@kyland-rus.ru

KYLAND

Содержание

Введение

В этом руководстве в основном представлены методы доступа и функции программного обеспечения промышленного Ethernet-коммутатора SICOM3000S, а также подробно описаны методы настройки через веб-интерфейс.

Структура материала

Руководство пользователя содержит следующий материал:

Основное содержание	**Пояснения**
1. Введение	➢ Обзор ➢ Функции программного обеспечения
2. Доступ к коммутатору	➢ Варианты представления ➢ Доступ к коммутатору через консольный порт ➢ Доступ к коммутатору через Telnet ➢ Доступ к коммутатору через веб-интерфейс
3. Пользователи	➢ Управление пользователями ➢ Тип авторизации
4. Система	➢ Основные сведения ➢ Управление конфигурацией ➢ Управление часами ➢ Обновление программного обеспечения（HTTP, FTP,TFTP） ➢ Активация ПО ➢ Обновление языков ➢ Перезапуск ➢ О системе
5. Службы	➢ Настройка SSL ➢ SNMP v1/v2c/v3 ➢ Настройка SSH ➢ Настройка TACACS+ ➢ Настройка RADIUS ➢ DNS

	➢ RMON
6. Аварийная сигнализация	
7. Управление функциями	➢ Настройка порта ➢ VLAN ➢ Настройка IP ➢ Агрегация портов ➢ Резервирование ➢ Настройка ARP ➢ Настройка ACL ➢ Настройка MAC-адреса ➢ POE ➢ IGMP Snooping ➢ Настройка DHCP ➢ Настройка IEEE802.1X ➢ GMRP ➢ Статическая маршрутизация ➢ Настройка QoS
8. Настройка обнаружения петель Loop Detect	➢Настройка обнаружения петель Loop Detect

9. Диагностика	➢ Журнал ➢ Зеркалирование портов ➢ LLDP ➢ Трассировка ➢ Ping ➢ IP Source Guard ➢ DDM

Условные обозначения в руководстве

1. Условные обозначения в тексте

Формат	**Пояснения**
< >	Текст в угловых скобках < > – это название кнопки. Например, щелкните кнопку <Apply>.
[ ]	Текст в квадратных скобках [ ] – это название окна или меню. Например, щелкните пункт меню [File].
{ }	Текст в фигурных скобках { } – это сгруппированные элементы. Например, {IP-адрес, MAC-адрес} означает, что IP-адрес и MAC-адрес объединены в группу, и их можно настраивать и отображать совместно.
→	Элементы многоуровневых меню разделяются знаком “→”. Например, Start → All Programs → Accessories. Щелкните меню [Start], щелкните подменю [All programs], затем щелкните подменю [Accessories].
/	Выбор одного из двух или нескольких вариантов, разделенных знаком “/”. “Добавление/вычитание” означает добавление или вычитание.
~	Обозначает диапазон. Например, «1~255» означает диапазон от 1 до 255.

2. Условные обозначения в командной строке

Формат	**Описание**
Полужирный	Команды и ключевые слова, например, **show version**, выделяются **полужирным** шрифтом.
Курсив	Параметры, для которых нужно задать значение, выделяются *курсивом*. Например, в команде **Show vlan** *vlan id* нужно задать фактическое значение *vlan id*.

3. Символы

Символ	**Пояснения**

 **Предостережение**	На эти моменты следует обратить внимание при эксплуатации и настройке, они дополняют описание действий.
 **Примечание**	Необходимые пояснения к описанию действий.
 **Внимание**	Требует особого внимания. Некорректные действия могут привести к потере данных или повреждению оборудования.

Документация по изделию

Документация к промышленному коммутатору SICOM3000S включает в себя:

Наименование документа	**Содержание**
Промышленный коммутатор Ethernet серии SICOM3000S	Описана конструкция оборудования, технические
Руководство по монтажу оборудования Hardware Installation Manual_V1.0.pdf	характеристики, способы монтажа и демонтажа.
Руководство пользователя по веб-интерфейсу промышленного коммутатора SICOM3000S Руководство пользователя по веб-интерфейсу	Описаны функции ПО, способы настройки через веб-интерфейс и все функции.

Получение документации

Документацию по изделию можно получить:

➢На сайте Kyland: www.kyland.com

1 Введение

1.1 Обзор

SICOM3000S – это серия высокопроизводительных управляемых промышленных Ethernet-коммутаторов, применяемых в отрасли железнодорожного транспорта. Устройства серии соответствуют EN50155, EN50121 и другим промышленным стандартам. Коммутатор поддерживает протоколы резервирования MSTP/RSTP и IEC62439-6, гарантируя надежную работу системы.

1.2 Функции программного обеспечения

SICOM3000S предоставляет обширный набор функций программного обеспечения, удовлетворяющих различные потребности заказчиков.

- Протоколы резервирования: DRP, STP/RSTP и MSTP.
- Многоадресные протоколы: IGMP Snooping, GMRP
- Протоколы фильтрации: VLAN, GVRP, QoS и ARP
- Управление пропускной способностью: статическая агрегация портов, LACP.
- Безопасность: управление пользователями, управление доступом, SSH, SSL, TACACS+, RADIUS, IEEE802.1X, ACL, IP Source Guard.
- Протоколы синхронизации времени: SNTP, NTP.
- Управление устройством: обновление программного обеспечения, загрузка/выгрузка файла конфигурации, запись и выгрузка журнала.
- Диагностика устройства: зеркалирование портов, LLDP.
- Функция аварийной сигнализации: аварийная сигнализация по электропитанию, аварийная сигнализация по порту, аварийная сигнализация по кольцу.
- Интерфейсы управления: командная строка, Telnet, веб-интрефейс и ПО Kyvision, DHCP и SNMP v1/v2c/v3.

2 Доступ к коммутатору

Доступ к коммутатору осуществляется через:

- Консольный порт

- Telnet/SSH
- Веб-браузер
- Программное обеспечение Kyvision

Программное обеспечение для управления сетью Kyvision разработано компанией Kyland. Подробная информация содержится в руководстве пользователя.

2.1 Варианты представления

При входе в интерфейс командной строки (CLI) через консольный порт или Telnet можно входить в различные режимы и переключаться между ними с помощью следующих команд.

Таблица 1 Режимы

Приглашение	**Режим**	**Функция**	**Команда для переключения представления**
SWITCH #	Привилегированный режим	Просмотр недавно использованных команд. Просмотр версии программного обеспечения. Просмотр информации об ответе на операцию ping. Выгрузка/загрузка файла конфигурации. Восстановление конфигурации по умолчанию. Перезагрузка коммутатора. Сохранение текущей конфигурации. Отображение текущей конфигурации. Обновление программного обеспечения.	Введите **configure terminal** для переключения из привилегированного режима в режим настройки. Введите **exit** для возврата в общий режим.
SWITCH（config）#	Режим настройки	Настройка всех функций коммутатора.	Введите "**exit**" или "**end**" для возврата в привилегированный режим.

При настройке коммутатора через интерфейс командной строки для получения справки по командам можно использовать "?". В справочной информации используются

различные форматы описания параметров. Например, <1, 255> означает числовой диапазон; <xx:xx:xx:xx:xx:xx> означает MAC-адрес; <word31> означает диапазон строк 1~31. Кроме того, символы ↑ и ↓ могут использоваться для просмотра недавно использованных команд.

2.2 Доступ к коммутатору через консольный порт

Доступ к коммутатору можно получить через его консольный порт и гипертерминал операционной системы Windows или другое программное обеспечение, поддерживающее подключение через последовательный порт, например, HTT3.3. В следующем примере показано, как использовать HyperTerminal для доступа к коммутатору через консольный порт.

1. Подключите последовательный порт ПК к консольному порту коммутатора с помощью кабеля DB9-RJ45.
2. Запустите HyperTerminal на рабочем столе Windows. Щелкните [Start] → [All Programs] → [Accessories] → [Communications] → [Hyper Terminal], как показано на рисунке 1.

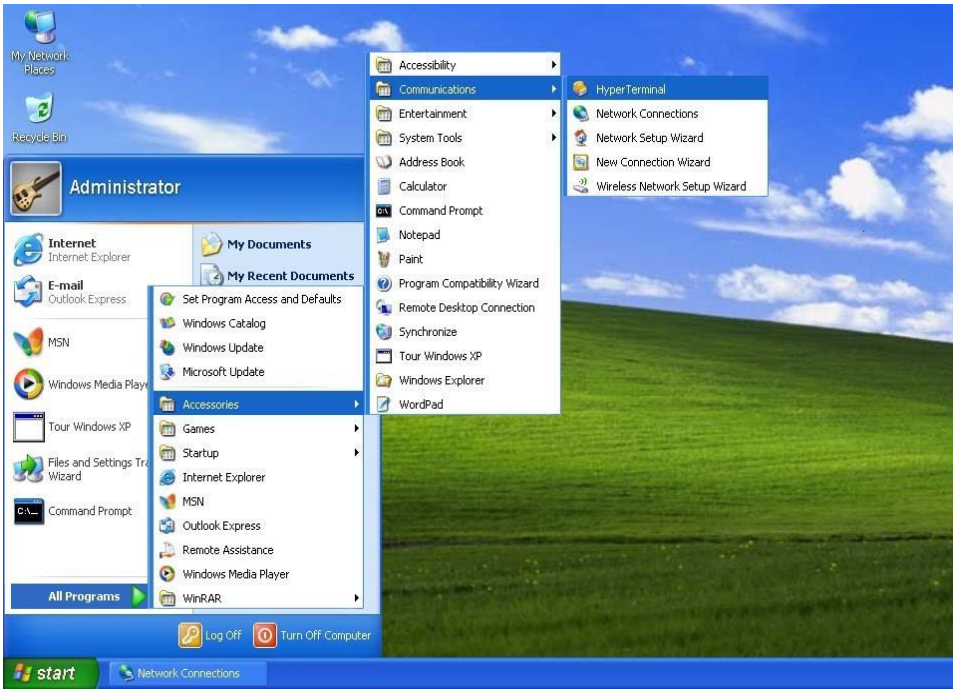


Рисунок 1 Запуск Hyper Terminal

3. Создайте новой подключение "Switch", как показано на рисунке 2.

Рисунок 2 Создание нового подключения

4. Выберите порт для подключения, как показано на рисунке 3.

Рисунок 3 Выбор порта для подключения

Примечание:
Чтобы убедиться, что порт выбран верно, щелкните правой кнопкой [My Computer] и щелкните [Property] → [Hardware] → [Device Manager] → [Port].

5. Настройте параметры порта (Bits per second: 115200, Data bits: 8, Parity: None, Stop bits: 1, Flow control: None), как показано на рисунке 4.

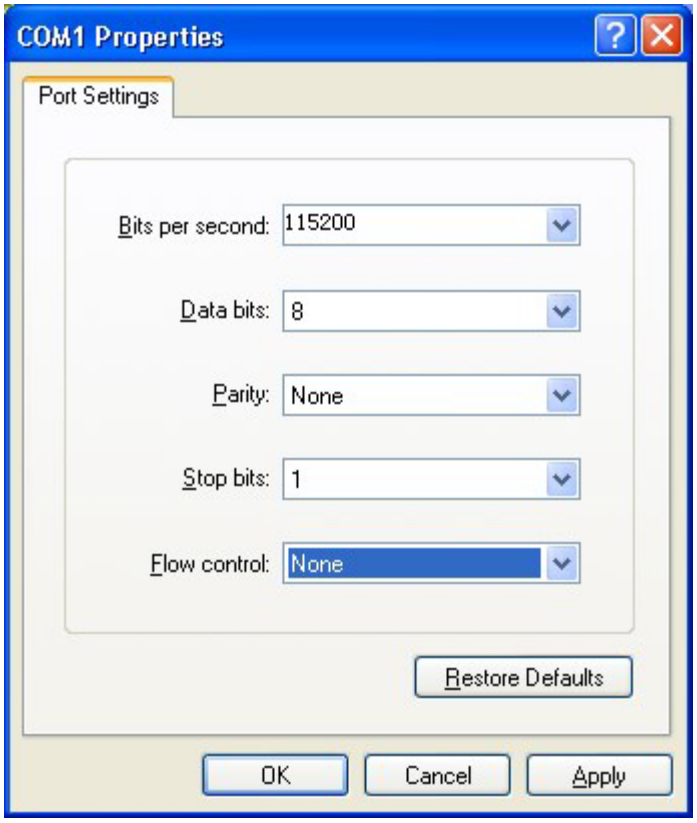


Рисунок 4 Настройка параметров порта

6. Щелкните кнопку <OK>, чтобы войти в интерфейс командной строки коммутатора. Введите имя пользователя по умолчанию "admin" и пароль "123" для входа в привилегированный режим. Можно также ввести другие созданные имя пользователя и пароль, как показано на рисунке 5.

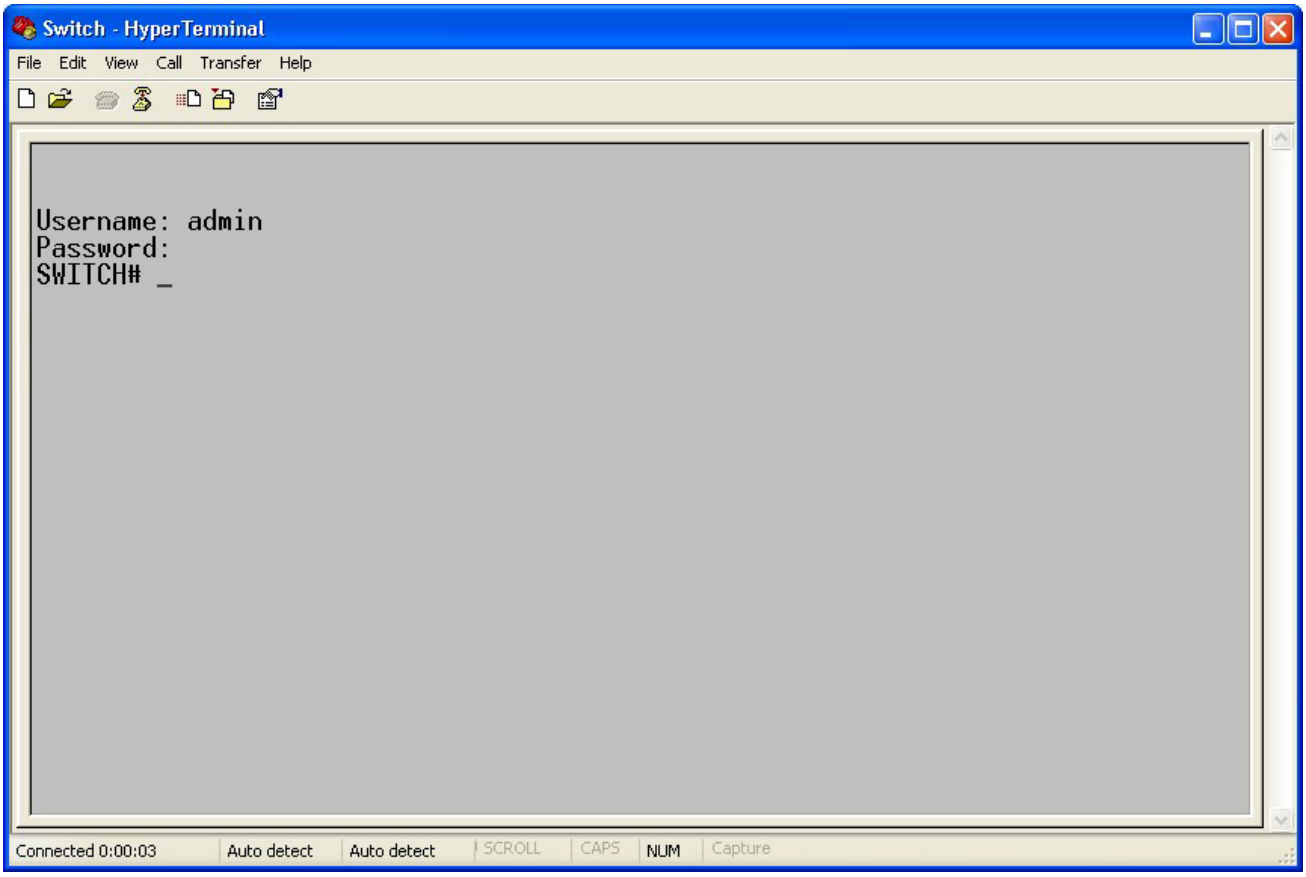


Рисунок 5 Интерфейс командной строки

2.3 Доступ к коммутатору через Telnet

Предварительным условием доступа к коммутатору по протоколу Telnet является нормальная связь между ПК и коммутатором.

1. Введите **telnet** *IP address* в диалоговом окне Run, как показано на рисунке 6. IP-адрес коммутатора Kyland по умолчанию 192.168.0.2.

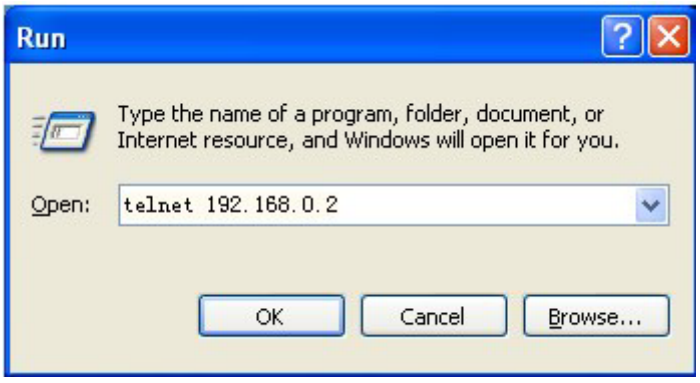


Рисунок 6 Доступ по Telnet

Примечание:
Для подтверждения IP-адреса обратитесь к разделу 7.3 Настройка IP, чтобы узнать, как получить IP-адрес.

2. В интерфейсе Telnet введите имя пользователя admin и пароль 123 для подключения к коммутатору. Можно также ввести другие созданные имя пользователя и пароль, как показано на рисунке 7.

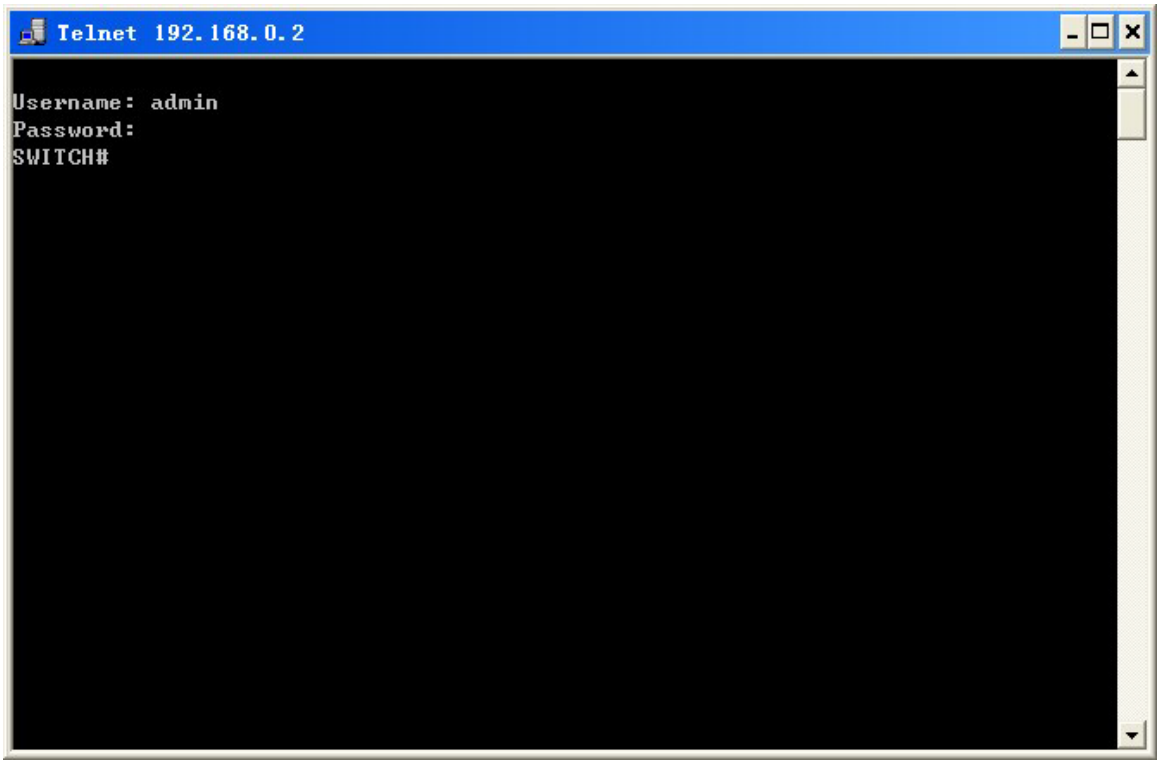


Рисунок 7 Интерфейс Telnet

2.4 Доступ к коммутатору через веб-интерфейс

Предварительным условием доступа к коммутатору через веб-интерфейс является нормальная связь между ПК и коммутатором.

Примечание:

Для наилучшего отображения доступа через веб-интерфейс рекомендуется использовать IE8.0 или более позднюю версию.

1. Введите *IP-адрес* в адресной строке браузера. Отображается интерфейс для входа, как показано на рисунке 8. Введите имя пользователя по умолчанию admin,

пароль 123 и проверочные символы в поле Verification. Щелкните <Login>. Можно также ввести другие созданные имя пользователя и пароль.

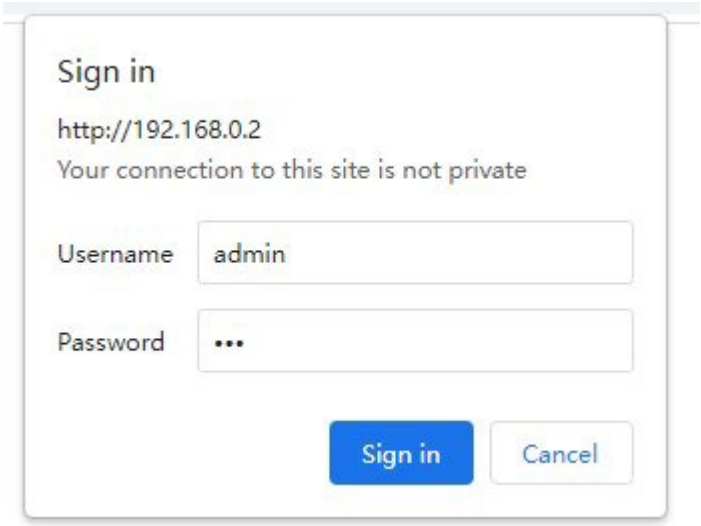


Рисунок 8 Вход через веб-интерфейс

Войдите на главную страницу интерфейса. В правом верхнем углу можно выбрать английский или китайский интерфейс. По умолчанию отображается английский интерфейс.

Примечание:

Для подтверждения IP-адреса обратитесь к разделу 7.3 Настройка IP, чтобы узнать, как получить IP-адрес.

2. После успешного входа слева в окне интерфейса появится дерево навигации, как показано на рисунке 9.

Рисунок 9 Веб-интерфейс

Щелкнув меню в дереве навигации, можно развернуть или свернуть дерево навигации. Можно щелкнуть Home для перехода в вид, показанный на рисунке 9, , а для выхода из веб-интерфейса можно щелкнуть  .

3 Пользователи

3.1 Управление пользователями

3.1.1 Введение

Чтобы решить проблему безопасности, вызванную незаконным доступом пользователей, коммутатор обеспечивает функцию иерархического управления пользователями, основанную на различных идентификационных данных пользователей, обеспечивающую различные уровни разрешений для пользователей.

3.1.2 Настройка через веб-интерфейс

1. Создайте нового пользователя, как показано ниже.

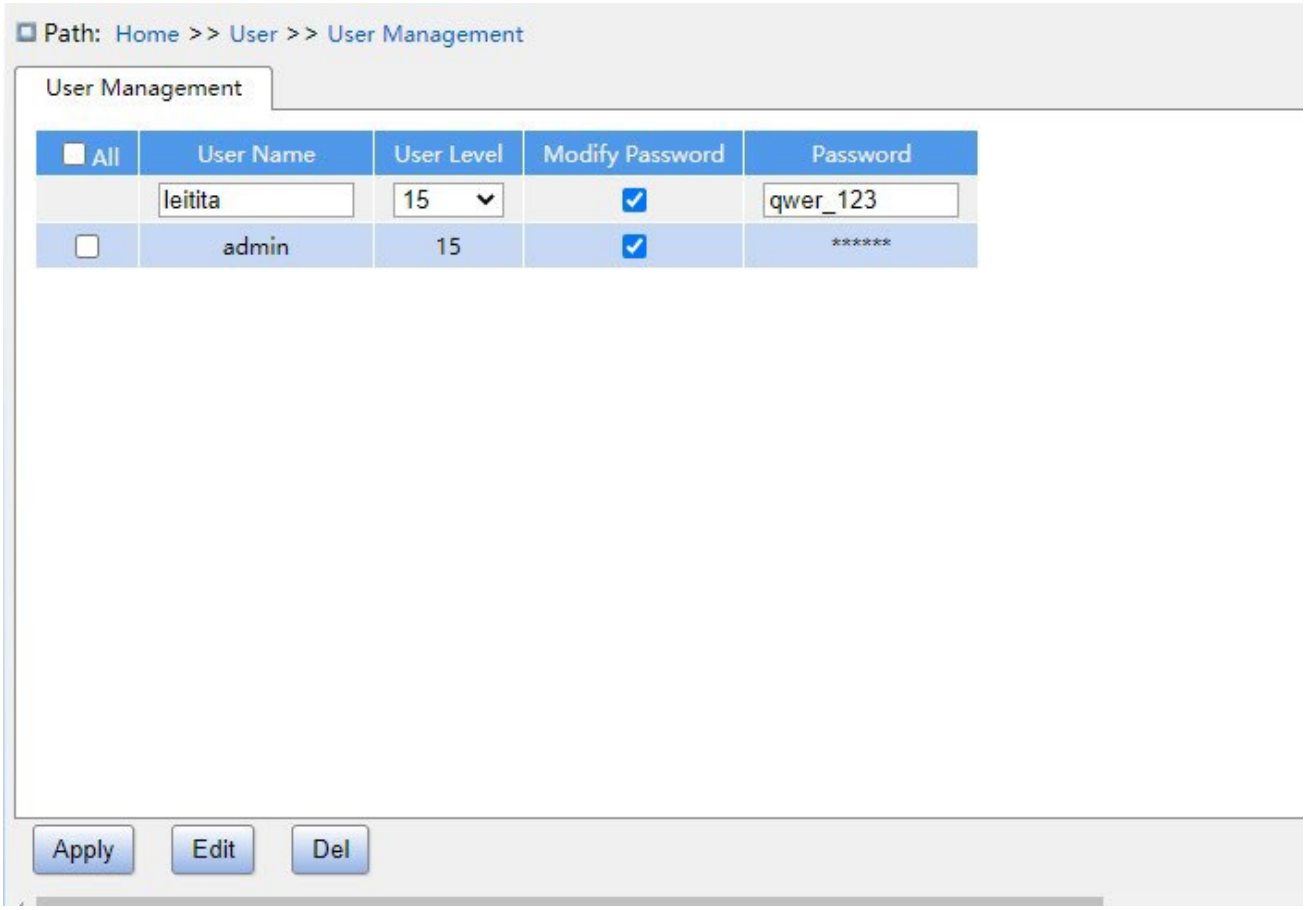


Рисунок 10 Создание нового пользователя

Добавьте нового пользователя в поле имени пользователя, настройте различные уровни пользователя. Можно создать максимум 20 пользователей.

User Name

Диапазон настройки: 1~31 символ Функция: настройка имени пользователя.

User level

Диапазон настройки: 0~15

Функция: настройка уровня разрешений пользователя. Пользователи с разными уровнями разрешений имеют разные разрешения на доступ.

Password

Диапазон настройки: 1~31 символ

Функция: настройка пароля пользователя

2. Отредактируйте настройки пользователя, как показано ниже.

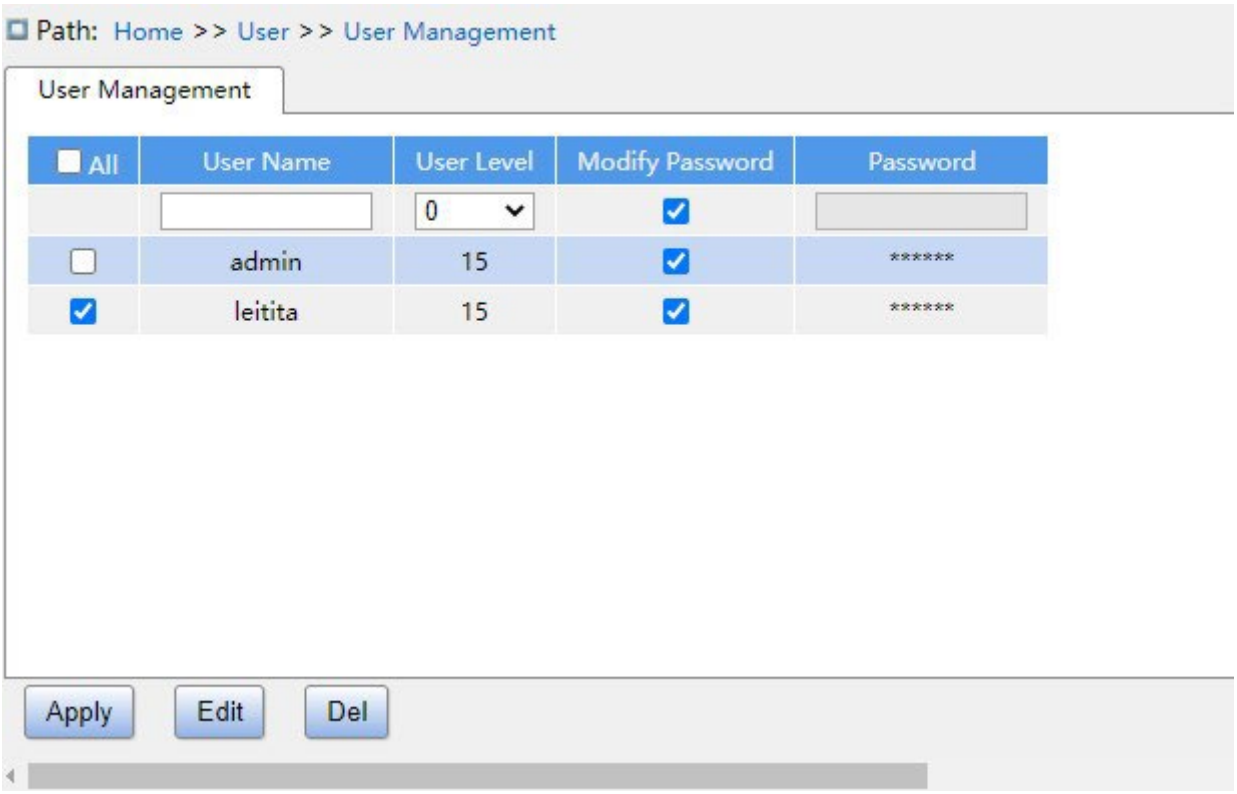


Рисунок 11 Редактирование настроек пользователей

Отметьте пользователя, параметры которого необходимо отредактировать, щелкните нажмите кнопку <Edit>, чтобы изменить пароль и уровни разрешений пользователя.

Щелкните кнопку <Del>, чтобы удалить текущего пользователя.

Примечание:

☐Пользователя по умолчанию admin удалить нельзя.

3. Настройте уровень привилегий групп, как показано ниже.

Рисунок 12 Настройка уровня привилегий групп

Group Name

Варианты конфигурации: Все группы функций

Функция: Выбор группы функций для работы

Read Level

Варианты конфигурации: 0-15

Конфигурация по умолчанию: 5

Функция: Настройка уровня, на котором пользователь видит текущую группу функций. Различные уровни групп функций имеют разные требования к уровню разрешений для просмотра пользователем.

Config Level

Варианты конфигурации: 0-15

Конфигурация по умолчанию: 10

Функция: Настройка уровня, на котором пользователь может использовать текущую группу функций. Различные уровни групп функций имеют разные требования к уровню разрешений для действий пользователя.

Примечание:

> Когда уровень привилегий пользователя такой же или выше, чем уровень привилегий группы, пользователь может получить доступ к группе или настроить ее. Право доступа или настройки зависит от уровня привилегий пользователя.

3.2 Тип авторизации

Настройте режим доступа к коммутатору, режим аутентификации и порядок аутентификации, как показано ниже.

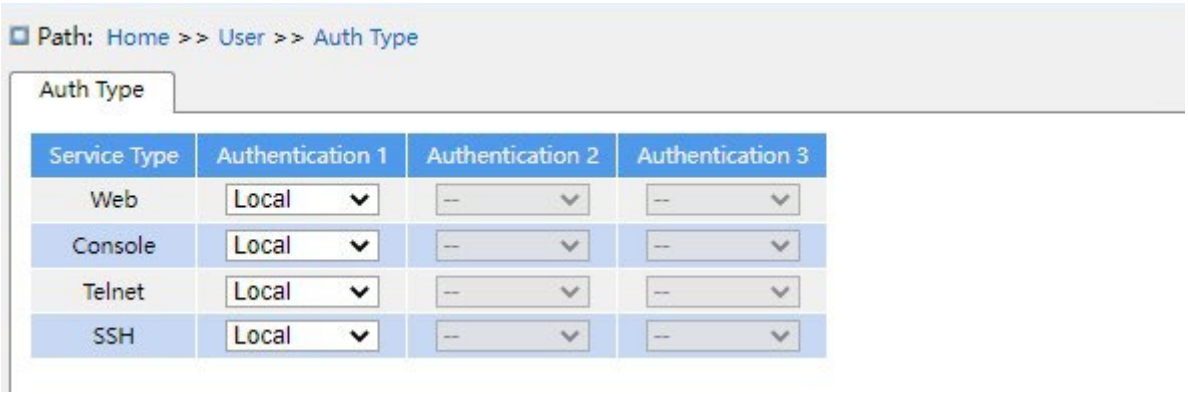


Рисунок 13 Настройка аутентификации при входе

Service Type

Варианты конфигурации: Web/Console/Telnet/SSH

Функция: Выбор режима доступа к коммутатору.

Authentication1/ Authentication2/ Authentication3

Варианты конфигурации: --/local/tacacs/radius

Конфигурация по умолчанию: local

Функция: Методы слева направо Authentication1, Authentication2 и Authentication3. Выбор порядка аутентификации. Сначала выполняется метод аутентификации 1. Если аутентификация не удалась, применяется метод аутентификации 2. Если и метод аутентификации 1, и метод аутентификации 2 неудачны, выполняется метод аутентификации 3.

Описание: -- означает, что аутентификация отключена и вход в систему невозможен. **local** означает использование имени пользователя и пароля, установленных в локальном компьютере, для выполнения аутентификации. **tacacs** означает использование имени пользователя и пароля, установленных на сервере TACACS+ для аутентификации. **radius** означает использование имени пользователя и пароля, установленных на сервере RADIUS для аутентификации.

Предупреждение:

Если для Authentication1 и Authentication 2 выбрано значение tacacs/radius, рекомендуется для Authentication3 выбрать значение local. Это позволит клиенту управления войти в систему как локальному пользователю, если ни один из настроенных удаленных серверов аутентификации не активен.

4 Система

4.1 Основные сведения

Информация о системе включает в себя тип устройства, имя устройства, MAC-адрес, версию оборудования, версию логики, версию программного обеспечения, дату кода, используемый процессор, используемую память, системную дату, время работы системы, контактные данные и местоположение, как показано ниже.

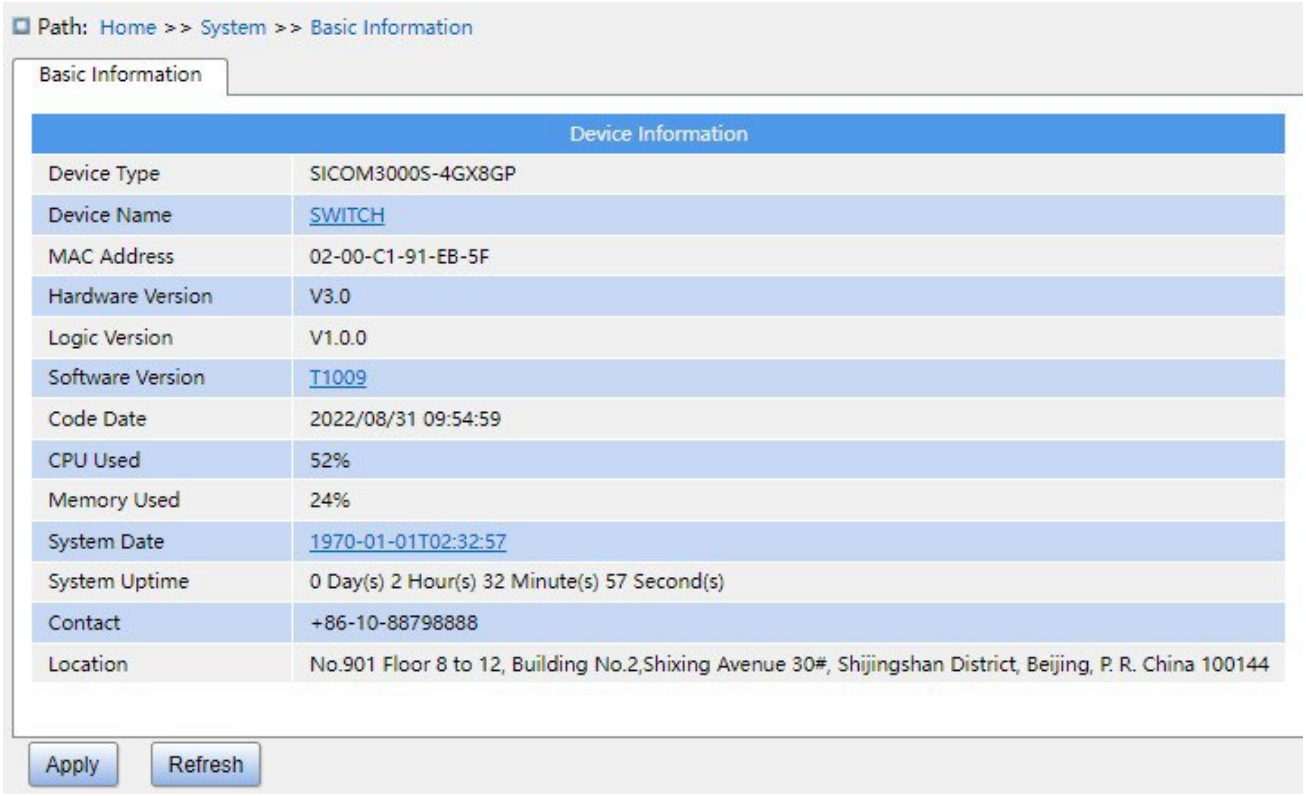


Рисунок 14 Основные сведения

4.2 Управление конфигурацией

1. Сохраните текущую конфигурацию, как показано на следующем рисунке.

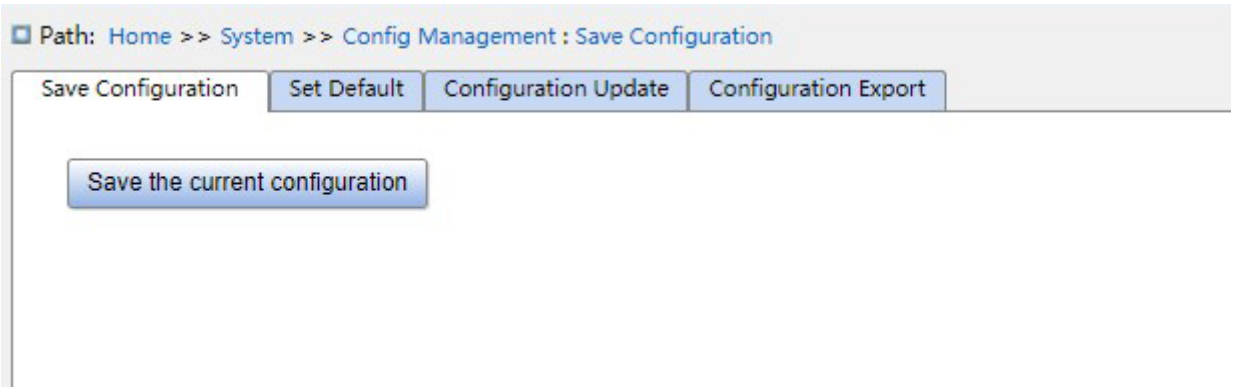


Рисунок 15 Сохранение текущей конфигурации

2. Восстановите заводскую конфигурацию, как показано ниже.

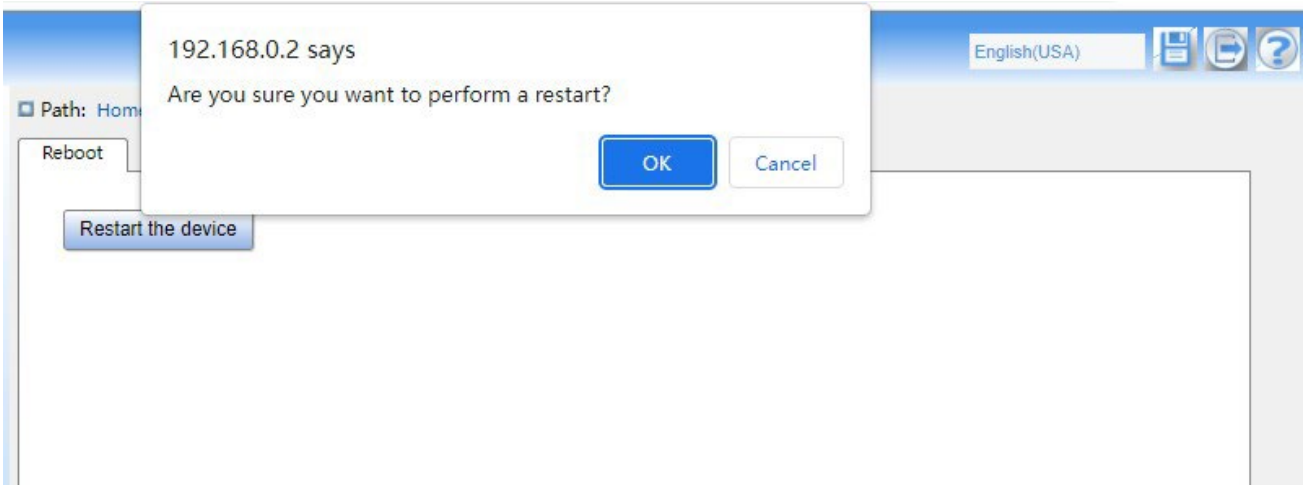


Рисунок 16 Восстановление заводской конфигурации

3. Экспорт конфигурации Выгрузите файл с коммутатора на локальный компьютер/сервер, как показано на рисунках 17 – 19.

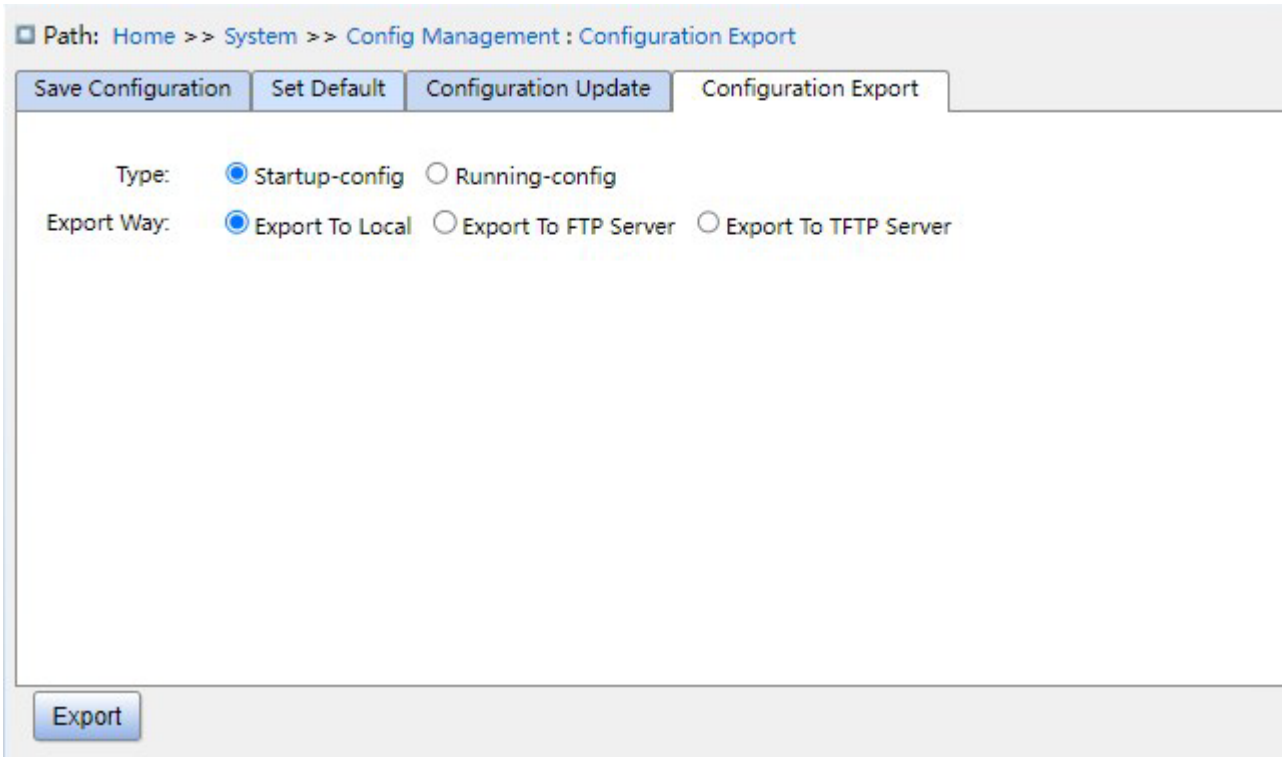


Рисунок 17 Экспорт файла конфигурации - HTTP

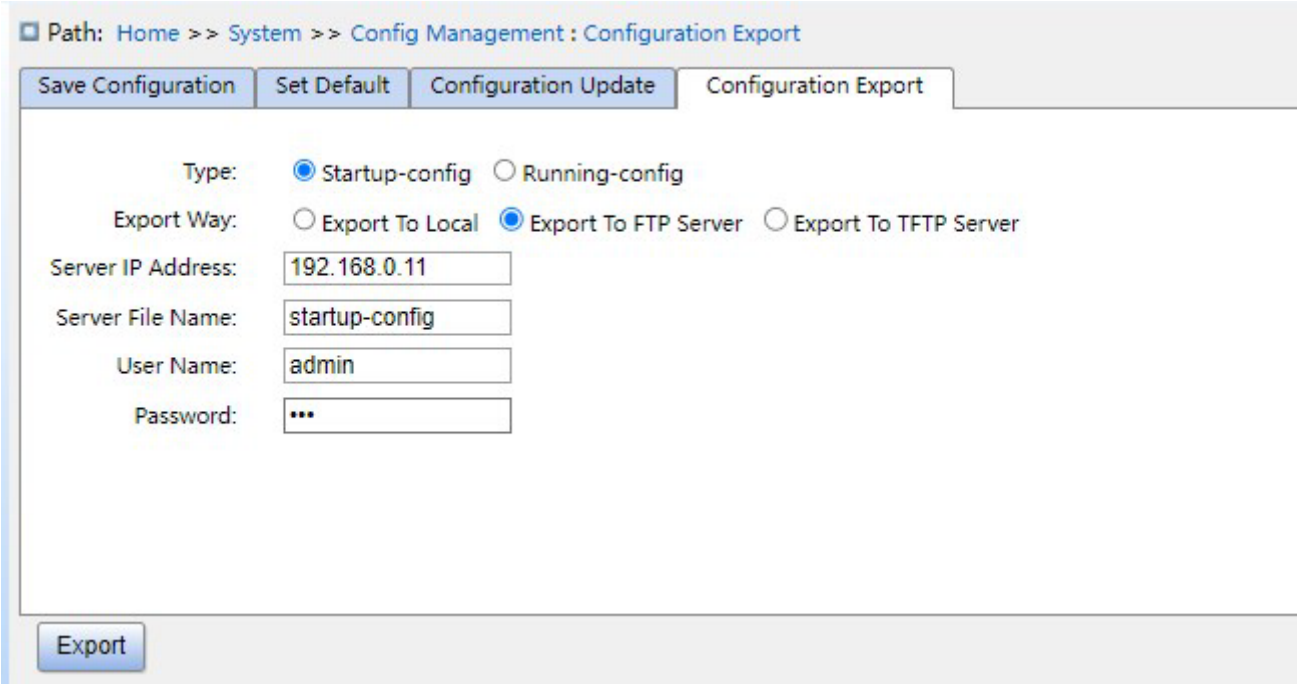


Рисунок 18 Экспорт файла конфигурации - FTP

Server IP address

Формат: A.B.C.D

Описание: Настройка IP-адреса сервера FTP.

Server file name

Диапазон настройки: 1~63 символа

Описание: Укажите имя сохраненного на сервере FTP файла конфигурации.

{ User name, Password }

Диапазон настройки: {1~63 символа, 1~63 символа}

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

Предупреждение:

- При передаче файлов по FTP необходимо настроить имя пользователя FTP, пароль и IP-адрес сервера FTP.
- При передаче файла сервер FTP должен находиться в рабочем состоянии.

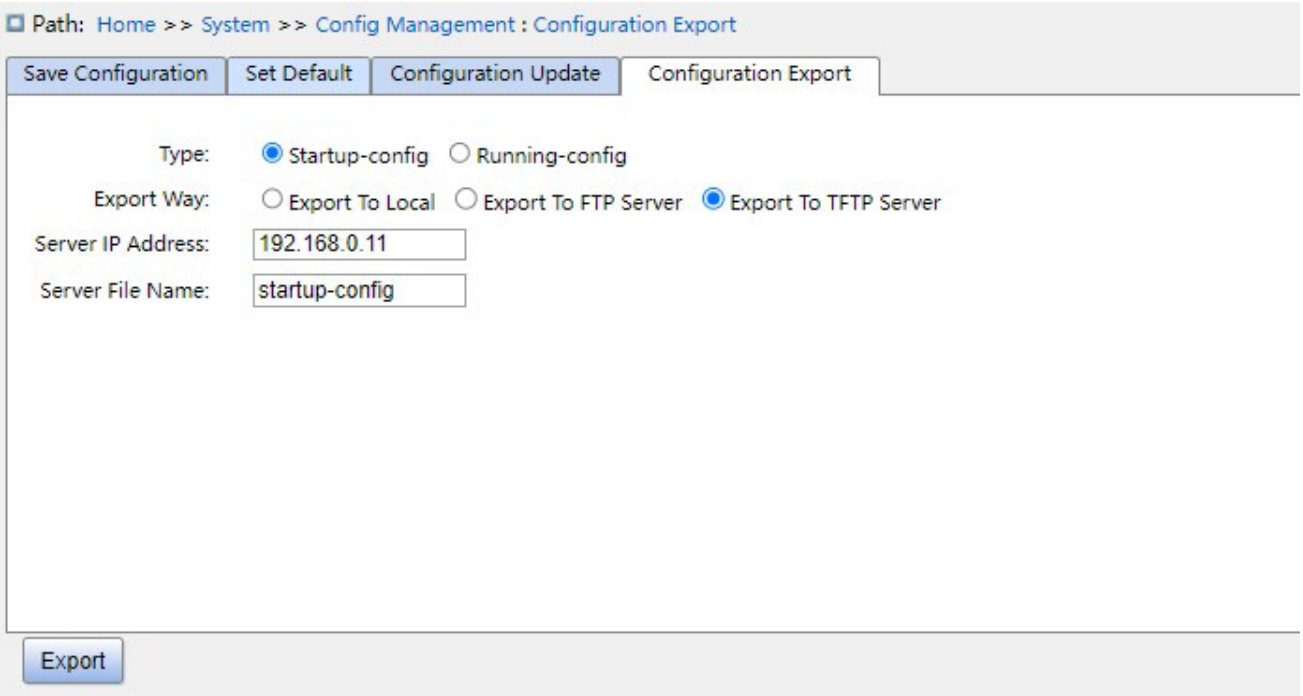


Рисунок 19 Экспорт файла конфигурации - TFTP

Файл коммутатора можно сохранить на локальном компьютере/сервере. **running-config –** это файл текущей конфигурации коммутатора, а **startup-config** – файл запуска коммутатора. Выберите файл и щелкните <Export>, чтобы сохранить файл на локальном компьютере/сервере.

4. Обновление конфигурации Загрузите файл конфигурации с локального компьютера/сервера в качестве нового файла запуска коммутатора, как показано на рисунках 20 – 22.

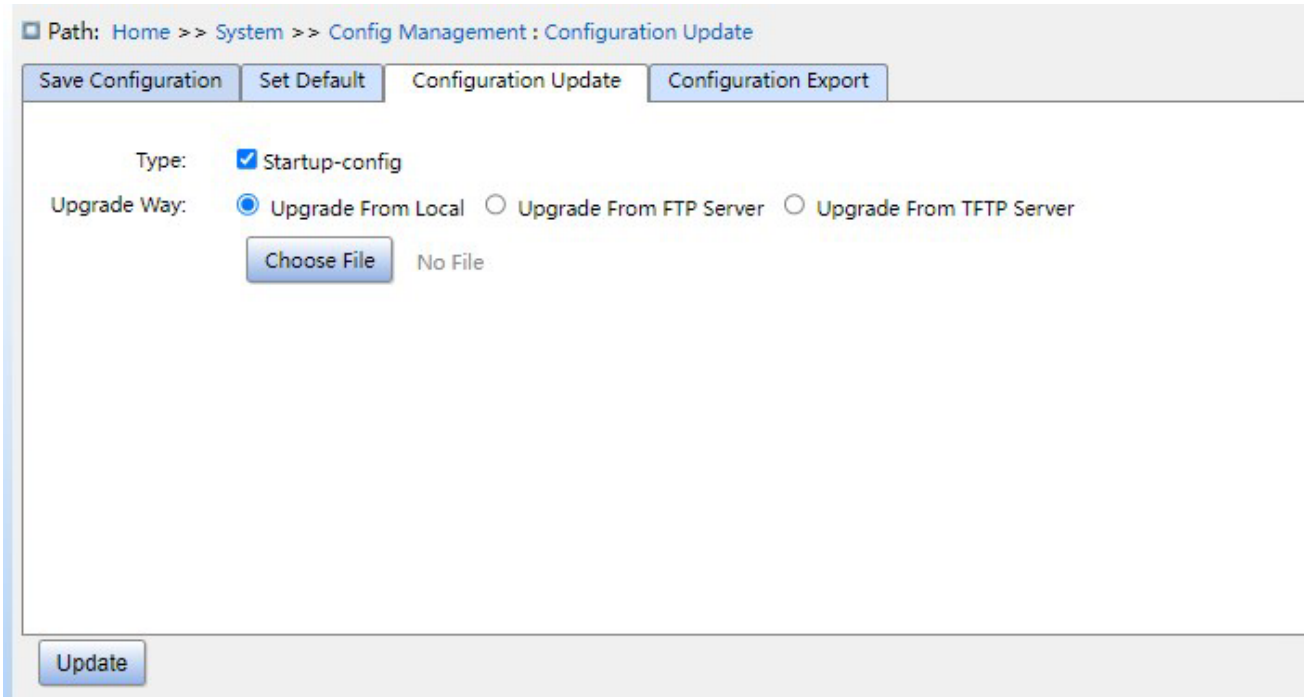


Рисунок 20 Загрузка файла конфигурации - HTTP

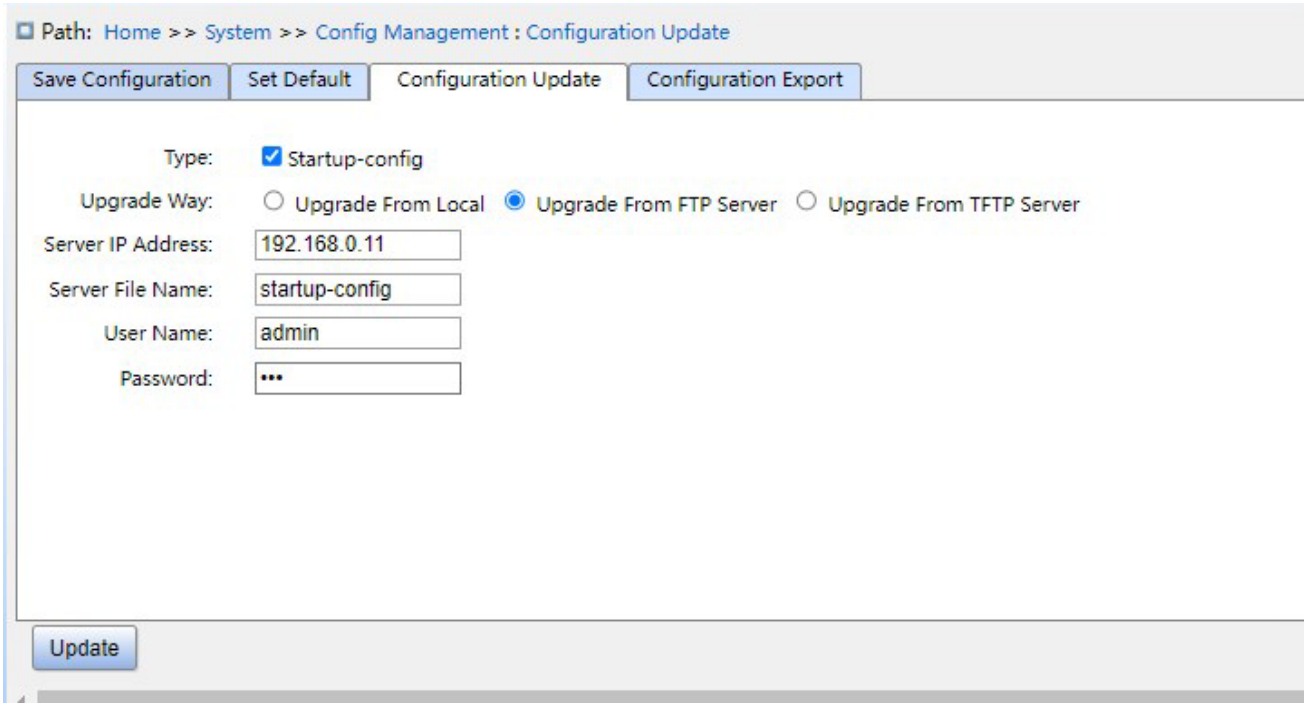


Рисунок 21 Загрузка файла конфигурации - FTP

Server IP address

Формат: A.B.C.D

Описание: Настройка IP-адреса сервера FTP.

Server file name

Диапазон настройки: 1~63 символа

Описание: Указание имени сохраненного на сервере FTP файла обновления прошивки.

{ User name, Password }

Диапазон настройки: {1~63 символа, 1~63 символа}

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

Предупреждение:

➢При передаче файлов по FTP необходимо указать имя пользователя FTP, пароль, IP-адрес сервера FTP и имя файла.

➢При передаче файла сервер FTP должен находиться в рабочем состоянии.

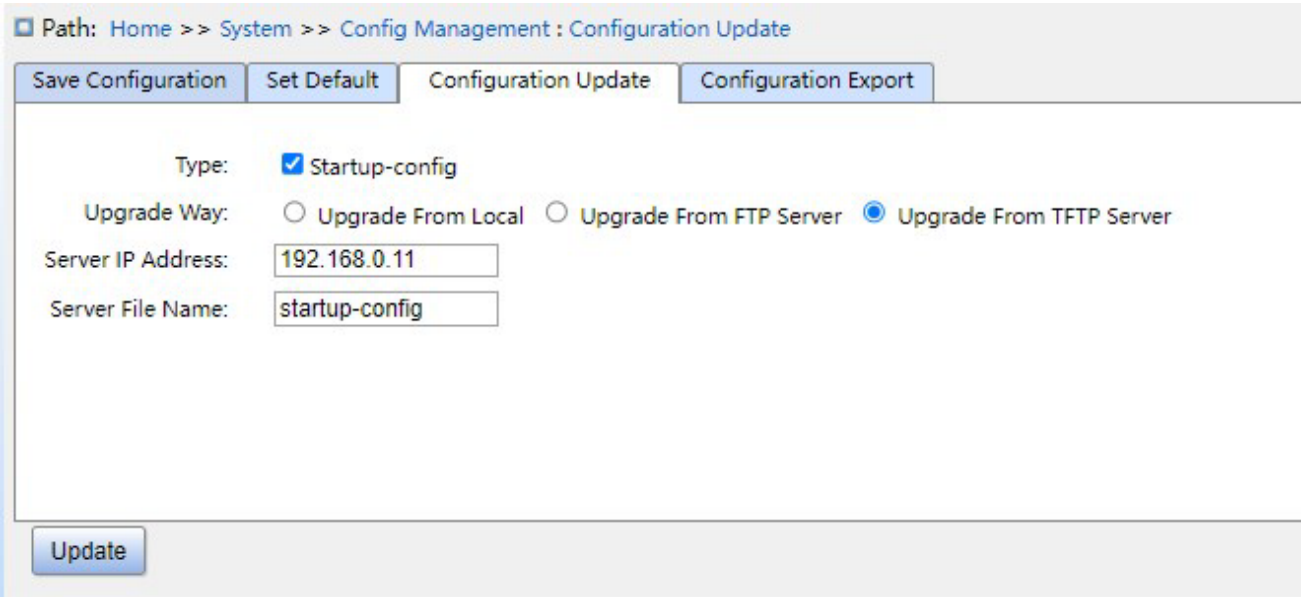


Рисунок 22 Загрузка файла конфигурации - TFTP

Можно загрузить в коммутатор файл конфигурации с локального компьютера/сервера в качестве нового файла запуска. Новый файл заменит исходный файл **startup-config**. Щелкните <Update>, чтобы загрузить в коммутатор файл конфигурации с локального компьютера/сервера.

4.3 Управление часами

1. Установите DST, как показано ниже.

Чтобы в полной мере использовать дневной свет и экономить энергию летом, можно использовать DST (DST: летнее время). Настройка DST включает в себя повторяющуюся и неповторяющуюся настройку.

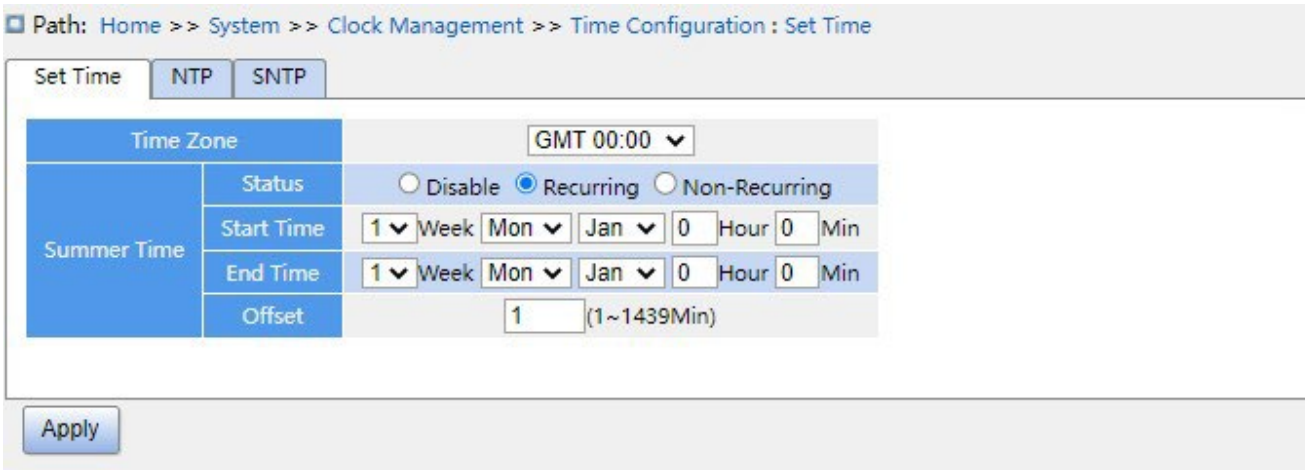


Рисунок 23 Повторяющаяся настройка

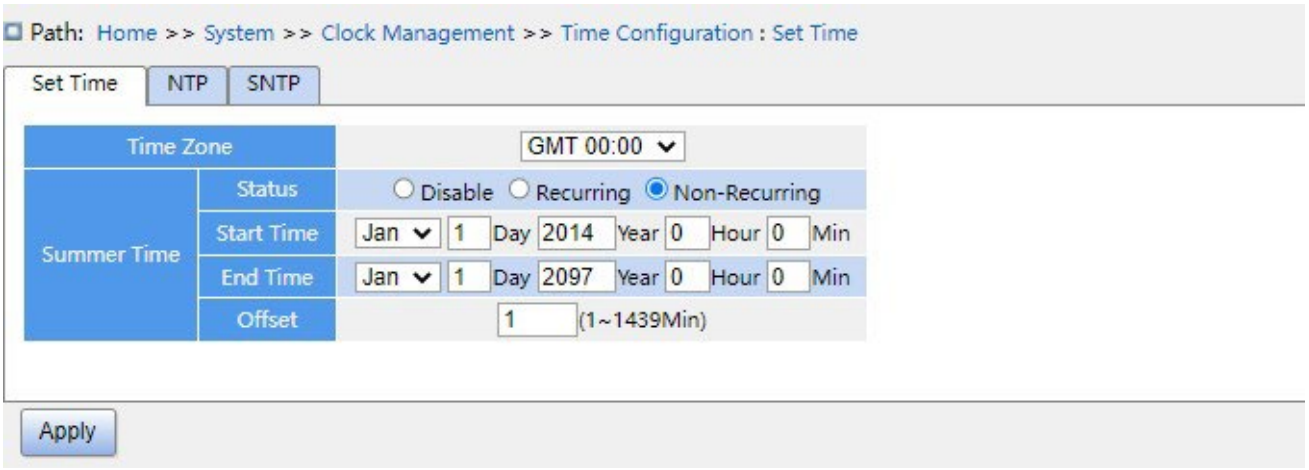


Рисунок 24 Неповторяющаяся настройка

Time Zone

Функция: выбор местного часового пояса

Состояние DST

Варианты конфигурации：disable/recurring/non-recurring

Конфигурация по умолчанию: disable

Функция： включение летнего времени, выбор режима летнего времени после включения, задание повторяющегося режима по годам.

Start time/end time

Функция: Задание диапазона DST после включения летнего времени. В неповторяющемся режиме настройте год, месяц, день, час и минуту, чтобы назначить рабочий диапазон летнего времени, как показано на рисунке 24. Установите летнее время между 00:00 1 января 2014 года и 23:59 1 июля 2097 года. В повторяющемся

режиме настройте месяц, неделю, дату, час и минуту, чтобы назначить рабочий диапазон летнего времени в году, как показано на рис. 23, установите летнее время между 00:00 в первый понедельник января и 23:59 в первый понедельник июля каждого года.

Offset

Диапазон：1~1439 мин.

Настройка по умолчанию: 1 мин.

Функция: настройка смещения DST, т.е. времени начала и завершения DST

Предупреждение:

- Время начала должно отличаться от времени окончания.
- Время начала задается по зимнему времени, время окончания – по летнему времени.

Пример: период летнего времени с 10:00:00 1 апреля до 9:00:00 1 октября, поэтому смещение летнего времени составляет 60 минут.

Зимнее время продолжается до 10: 00: 00 1 апреля и перескакивает на 11: 00: 00 летнего времени, чтобы начать период летнего времени. Когда летнее время доходит до 8: 00: 00 1 октября, время возвращается на 8: 00: 00 зимнего времени.

2、Настройка NTP

Протокол NTP (протокол сетевого времени) используется для синхронизации времени между сервером распределенного времени и клиентом. NTP может синхронизировать часы всех устройств с часами в сети, чтобы часы всех устройств в сети работали одинаково. Так что устройство может предоставлять различные функции в одно и то же время. Локальная система, использующая NTP, может получать синхронизацию от других источников синхронизации или синхронизировать другие часы в качестве источника синхронизации.

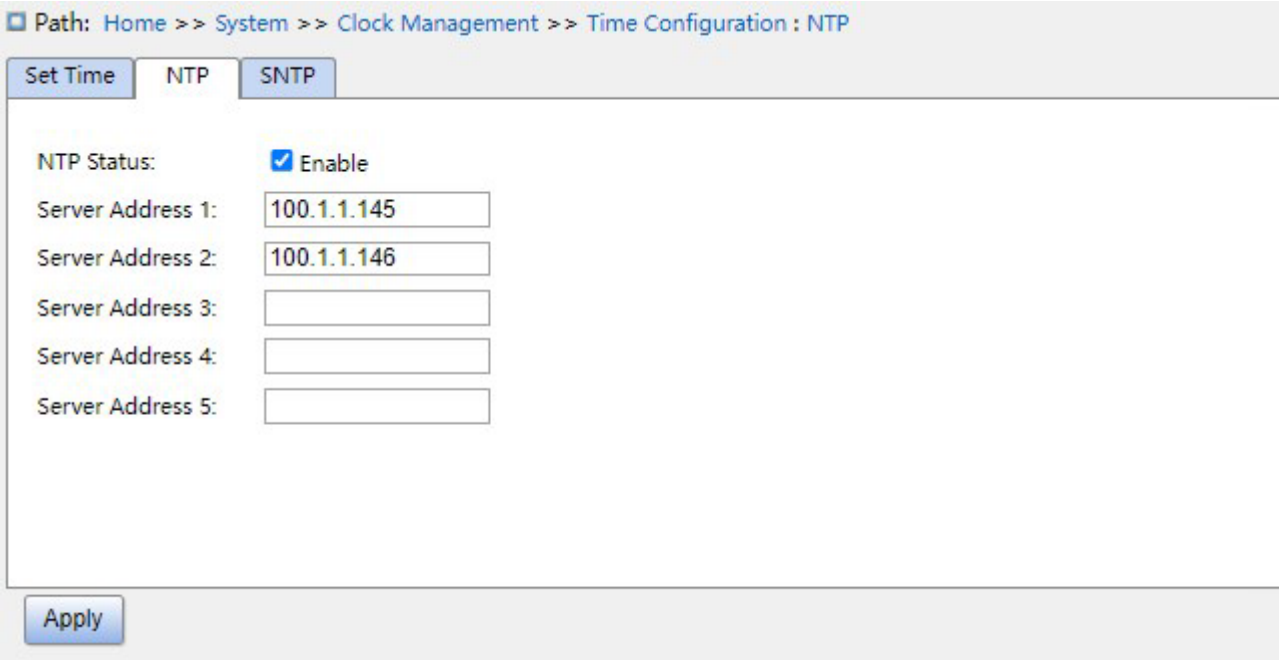


Рисунок 25 Настройка NTP

Состояние NTP

Варианты настройки: enable/disable

Конфигурация по умолчанию: disable

Функция：Включение глобальных служб NTP.

CAUTION

_ :

- Протоколы NTP и SNTP взаимоисключающие. Поскольку NTP и SNTP используют один и тот же портUDP,

  их нельзя включить одновременно.

- Когда службы NTP отключены, службы NTP можно настроить и сохранить, то есть

  включение или отключение служб NTP не влияет на конфигурацию служб NTP.

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

Формат: A.B.C.D

Функция: Настройка IP-адреса сервера NTP. Калибровка времени клиента будет осуществляться по сообщениям сервера NTP.

3、Настройка SNTP

Протокол SNTP (простой сетевой протокол времени) калибрует время, используя запрос и ответ между сервером и клиентом. Коммутатор в качестве клиента калибрует время в соответствии с сообщением сервера.

Предупреждение:

- Когда на коммутаторе включается SNTP, сервер SNTP должен быть активен.
- Вся информация о времени, передаваемая в протоколе SNTP, является стандартной информацией о времени часового пояса 0.

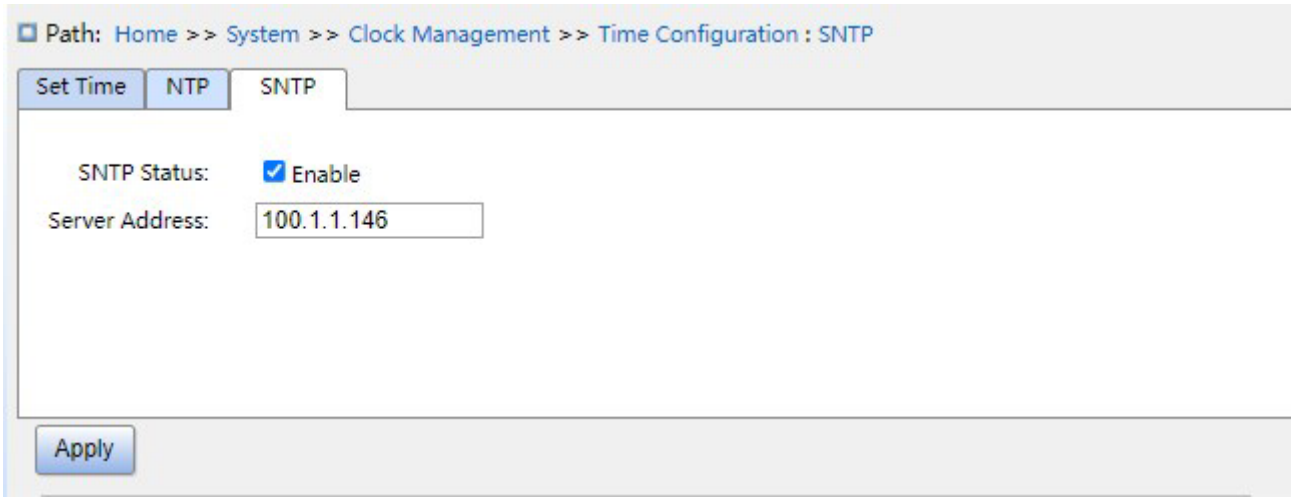


Рисунок 26 Настройка SNTP

Состояние SNTP

Варианты настройки: enable/disable

Конфигурация по умолчанию: disable

Функция：Включение SNTP.

Server Address

Формат: A.B.C.D

Функция: Настройка IP-адреса сервера SNTP. Калибровка времени клиента будет осуществляться по сообщениям службы.

4. Проверьте, что время коммутатора синхронизировано со временем сервера.

Щелкните в дереве навигации [system] → [basic information], чтобы просмотреть информацию о системном времени, как показано ниже.

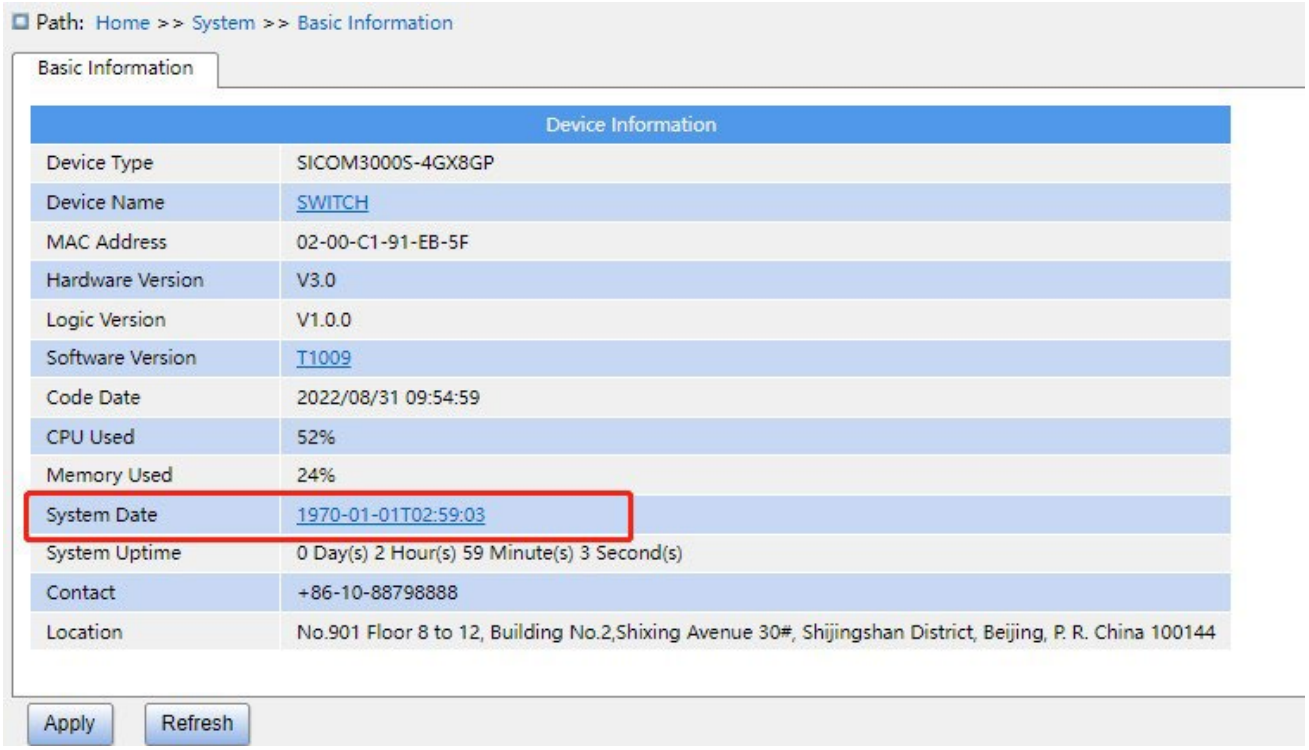


Рисунок 27 Просмотр информации о часах

Просмотрите информацию о времени коммутатора в соответствии со временем сервера, часовым поясом и настройками летнего времени.

4.4 Обновление программного обеспечения

Производительность коммутаторов можно повысить за счет обновления версии программного обеспечения. Для коммутаторов этой серии обновление прошивки включает обновление версии загрузчика и обновление версии системного программного обеспечения: сначала обновляется версия загрузчика, затем обновляется версия программного обеспечения; если версия загрузчика остается прежней, обновляется только версия программного обеспечения. Версию программного обеспечения можно обновить с локального компьютера или по протоколу FTP/TFTP.

4.4.1 Локальное обновление

1. Обновите ПО локально, как показано ниже.

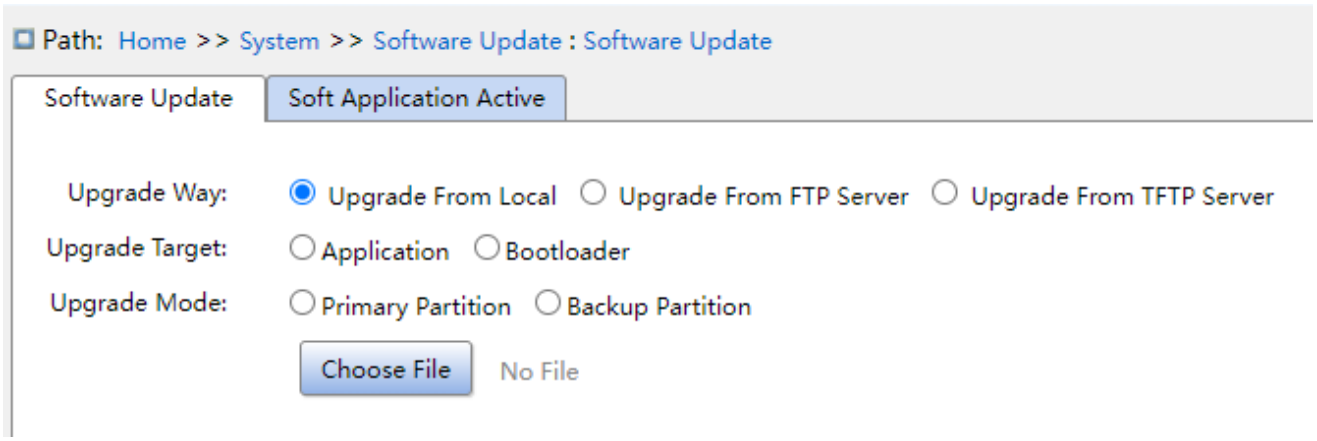


Рисунок 28 Обновление ПО – локальный компьютер

Upgrade way

Варианты настройки：upgrade from local/upgrade from FTP server/ Upgrade From TFTP Server.

Функция: выбор режима обновления.

Upgrade target

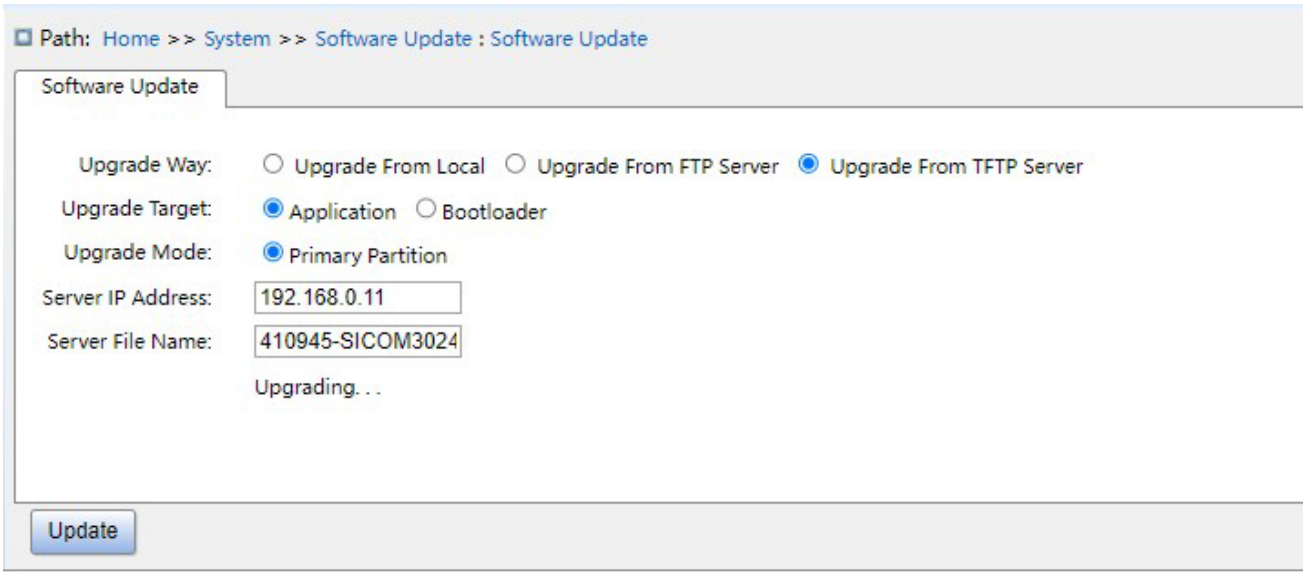
Варианты настройки：software version/Boot version Функция: выбор цели обновления.

Upgrade mode

Варианты настройки：primary partition/backup partition

Описание: Можно загрузить две версии ПО, одинаковые или разные.

2. После успешного обновления, как показано на рисунке 28, активируйте версию программного обеспечения и перезагрузите устройство, затем в разделе информации о системе проверьте, является ли версия программного обеспечения обновленной версией.



WARNING

➢ После успешного обновления программного обеспечения необходимо активировать версию программного обеспечения и перезагрузить устройство, прежде чем версия программного обеспечения вступит в силу;

➢ Невозможно перезапустить коммутатор после сбоя обновления. Избегайте потери файла версии – устройство не сможет нормально запуститься.

4.4.2 Обновление по FTP

Установите FTP-сервер. Ниже в качестве примера используется программное обеспечение WFTPD для ознакомления с конфигурацией FTP-сервера и обновлением программного обеспечения.

1. Щелкните [Security] → [Users/Rights]. Появится диалоговое окно Users/Rights Security Dialog. Щелкните <New User>, чтобы создать нового пользователя, как показано на рисунке 30. Создайте имя пользователя и пароль, например, имя пользователя admin и пароль 123. Щелкните <OK>.

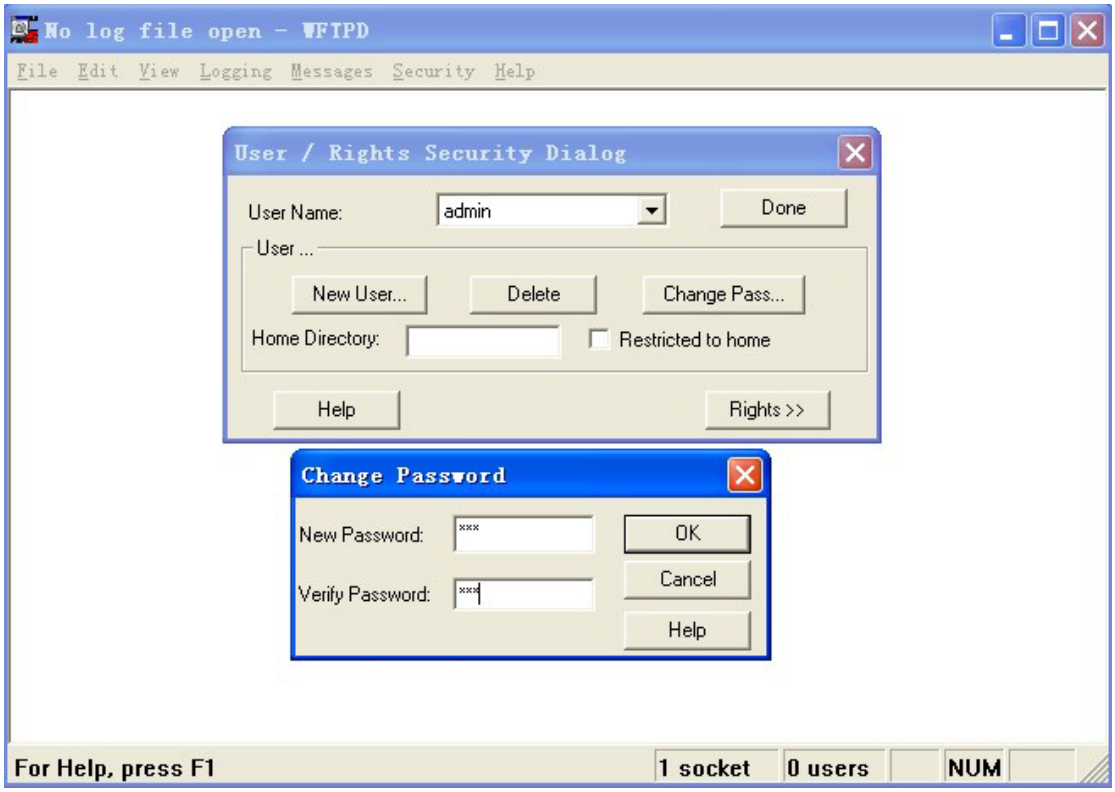


Рисунок 30 Создание нового пользователя FTP

2. Введите путь хранения файла обновления в Home Directory, как показано на рисунке 31. Щелкните <Done>.

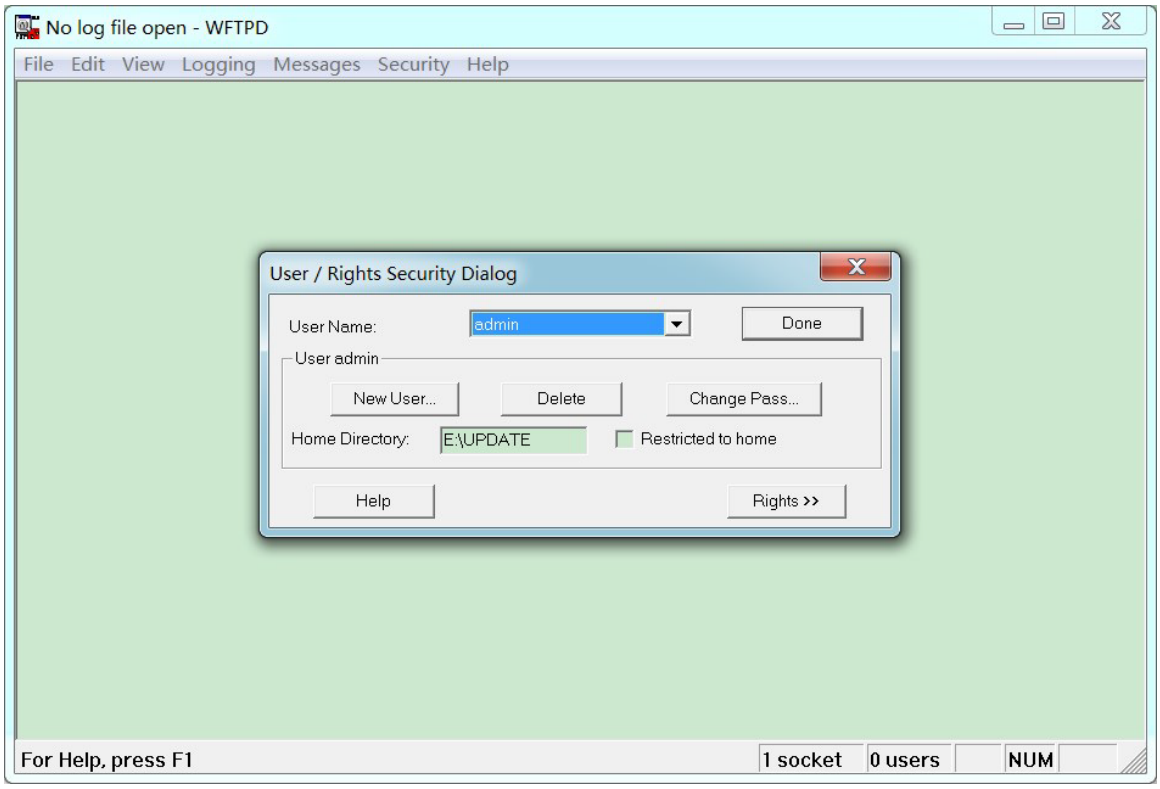


Рисунок 31 Местоположение файла

3. Щелкните [System] → [Software Update] в дереве навигации, чтобы перейти на страницу обновления ПО, как показано на рисунке 32. Введите IP-адрес FTP-сервера, имя пользователя FTP, пароль и имя файла на сервере. Щелкните <Update>.

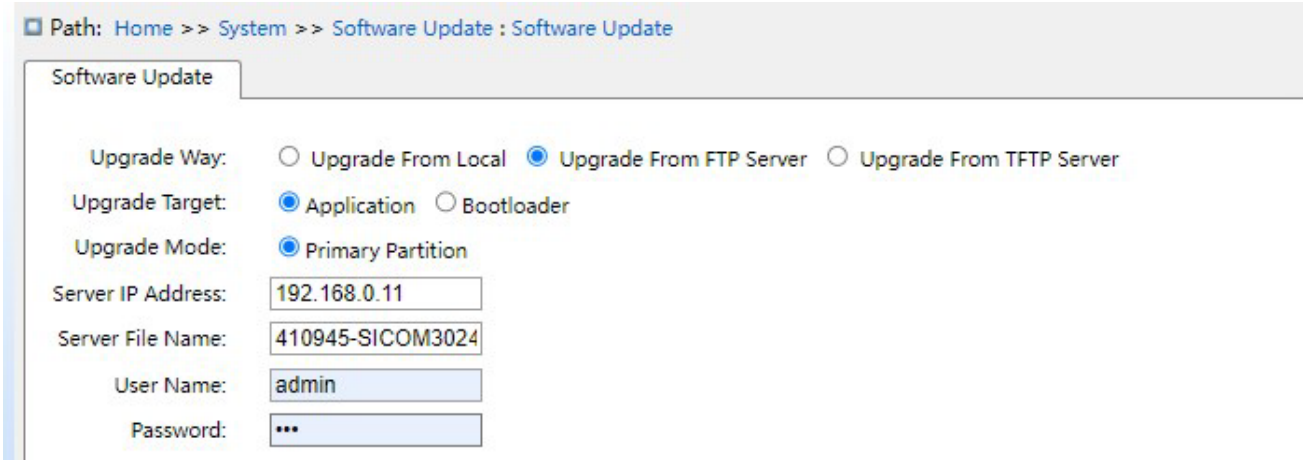


Рисунок 32 Обновление программного обеспечения по FTP

Upgrade way

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

Пояснение: Выбор режима обновления.

Upgrade Target

Варианты конфигурации: Application/Bootloader

Функция: Выбор цели обновления.

Режим обновления

Варианты конфигурации: Primary Partition/Backup Partition

Описание: В коммутатор можно загрузить две версии ПО, одинаковые или разные.

Внимание:

Имя файла должно содержать расширение. В противном случае обновление может пройти неудачно.

4. Убедитесь в наличии нормальной связи между FTP-сервером и коммутатором, как показано ниже.

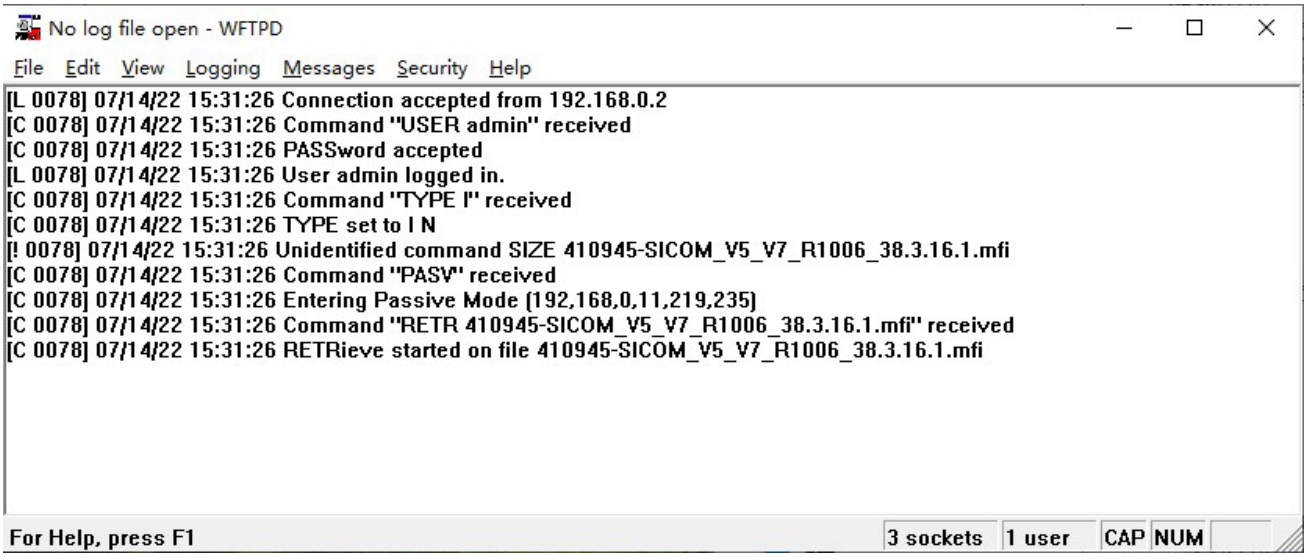


Рисунок 33 Нормальная связь между FTP-сервером и коммутатором

Предупреждение:
Чтобы отобразить информацию журнала обновлений, как показано на рисунке 33, нужно щелкнуть [Logging] → [LogOptions] in WFTPD в WFTPD и выбрать Enable Logging и информацию журнала для отображения.

5. Дождитесь завершения обновления, как показано на рисунке 34.

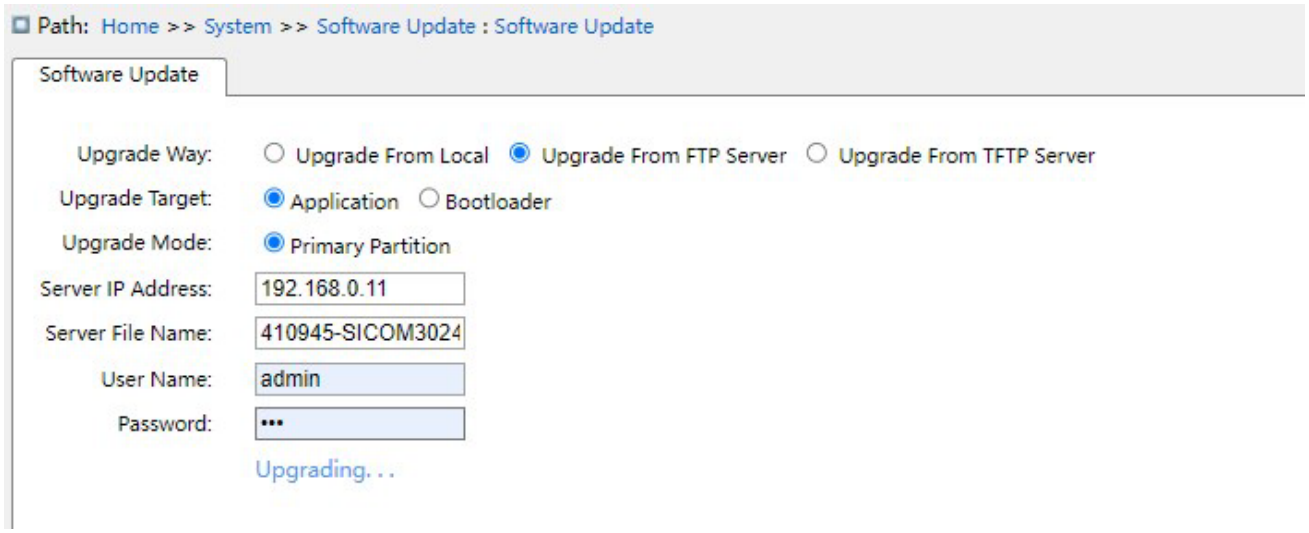


Рисунок 34 Ожидание завершения обновления

6. Когда обновление будет завершено, перезагрузите устройство и откройте страницу Switch Basic Information, чтобы проверить, успешно ли выполнено обновление и активна ли новая версия.

Внимание

- По завершении обновления перезагрузите устройство для активации новой версии.
- Если обновление не удалось, не перезагружайте устройство, чтобы избежать потери файла программного обеспечения и запуска с ошибкой.

4.4.3 Обновление по TFTP

Установите TFTP-сервер. Ниже в качестве примера используется программное обеспечение TFTPD для ознакомления с конфигурацией TFTP-сервера.

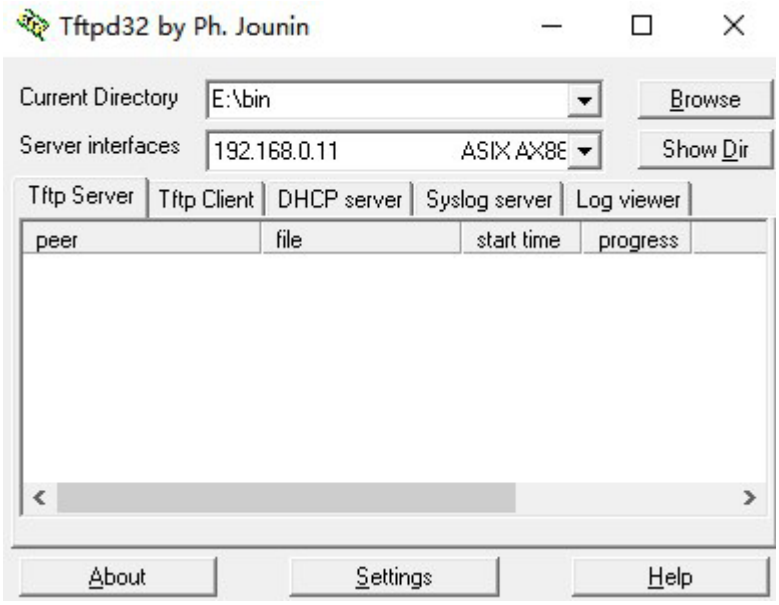


Рисунок 35 Конфигурация TFTP-сервера

1. В поле Current Directory выберите путь хранения файла обновления на сервере. Введите IP-адрес сервера в поле Server interface.
2. Щелкните [System] → [Software Update] в дереве навигации, чтобы перейти на страницу обновления ПО, как показано ниже. Введите IP-адрес FTP-сервера, имя пользователя FTP и имя файла на сервере.

Щелкните <Update> и дождитесь завершения обновления.

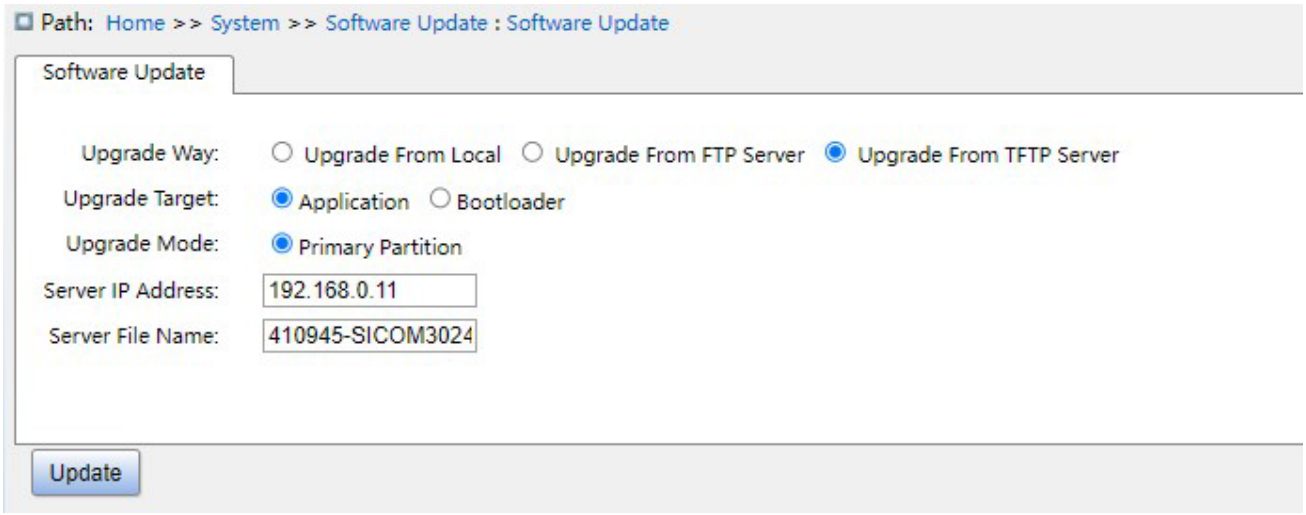


Рисунок 36 Обновление программного обеспечения по TFTP

3. Убедитесь в наличии нормальной связи между TFTP-сервером и коммутатором, как показано ниже.

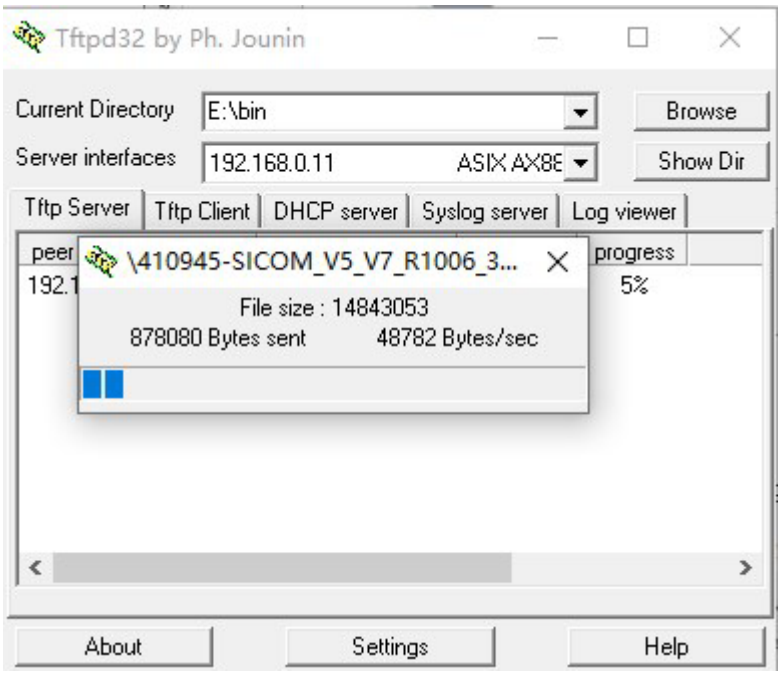


Рисунок 37 Нормальная связь между TFTP-сервером и коммутатором

4. Дождитесь завершения обновления, как показано ниже.

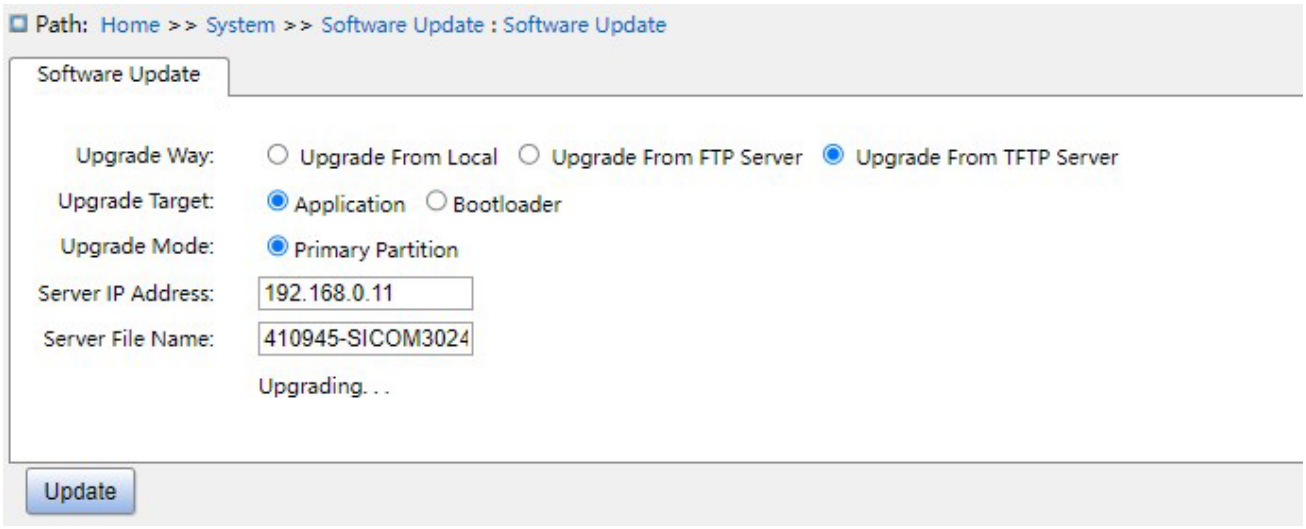


Рисунок 38 Ожидание завершения обновления

5. Когда обновление будет завершено, перезагрузите устройство и откройте страницу Switch Basic Information, чтобы проверить, успешно ли выполнено обновление и активна ли новая версия.

Внимание

- Во время обновления прошивки не выключайте TFTP-сервер.
- По завершении обновления перезагрузите устройство для активации новой версии.
- Если обновление не удалось, не перезагружайте устройство, чтобы избежать потери файла программного обеспечения и запуска с ошибкой.

4.5 Перезапуск

Перезапустите устройство, как показано ниже.

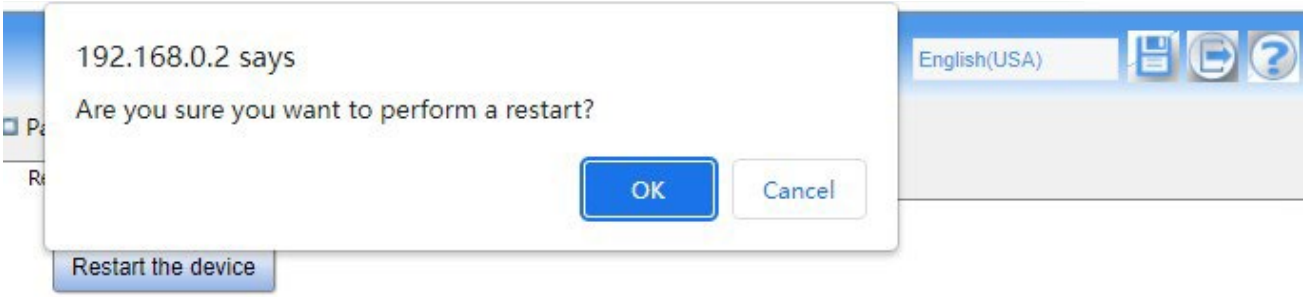


Рисунок 39 Перезапуск устройства

Перед перезапуском устройства подтвердите, что текущая конфигурация сохранена. При отсутствии сохраненной конфигурации после перезапуска конфигурация коммутатора будет возвращена к заводским параметрам по умолчанию.

4.6 О системе

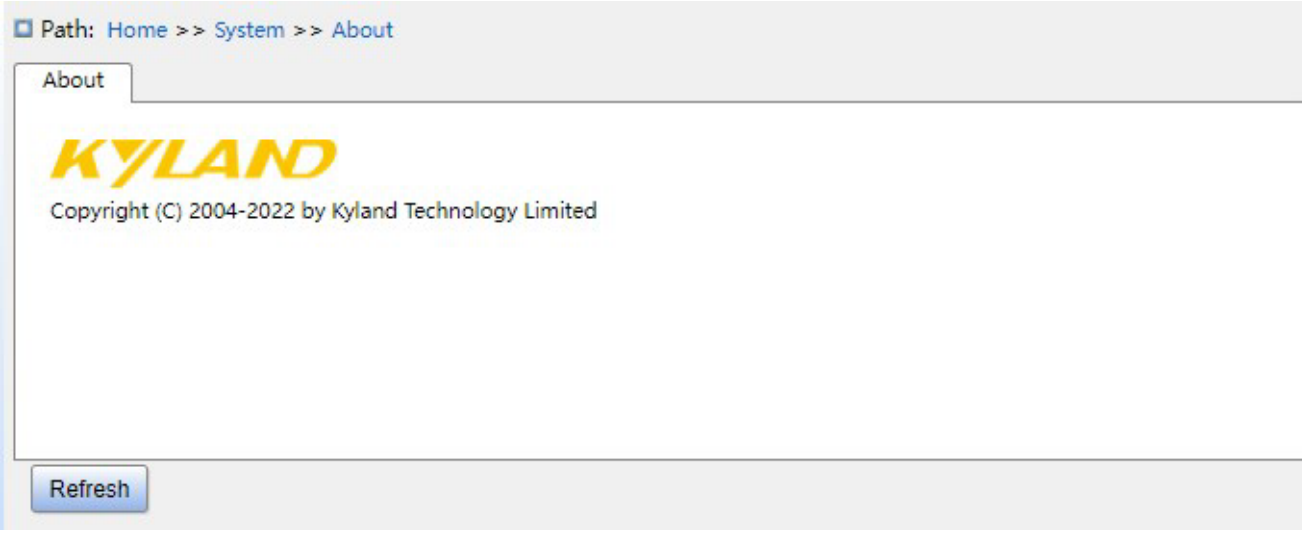


Рисунок 40 Информация о системе

5 Службы

5.1 Настройка SSL

5.1.1 Введение

SSL (Secure Socket Layer) — это протокол безопасности, обеспечивающий безопасный канал 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, для получения и отправки электронной почты, сетевого факса, связи в реальном времени и т. д., обеспечивая протокол шифрования для безопасной передачи данных в сети.

5.1.2 Настройка через веб-интерфейс

1. Включите HTTPS, как показано ниже.

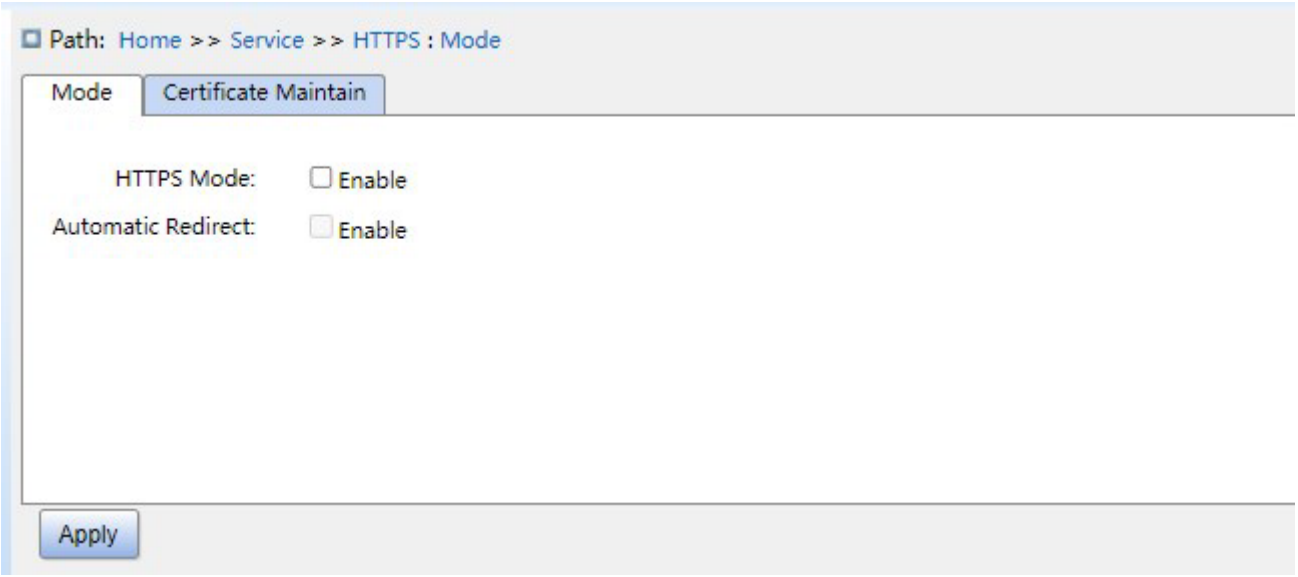


Рисунок 41 Включение HTTPS

HTTPS Mode

Варианты конфигурации: Enable /Disable

Конфигурация по умолчанию: Disable

Функция： включение или выключение HTTPS, при включении можно войти в веб-интерфейс коммутатора через http://*ip address* и безопасную ссылку https://*ip address*.

Automatic Redirect

Варианты настройки: enable/disable

Конфигурация по умолчанию: Disable

Функция: если режим включен, для доступа к веб-страницам коммутатора разрешена только безопасная ссылка https://*ip address.* Если режим выключен, для входа на веб-страницы можно использовать http и https. Параметр автоматической переадресации можно настроить только при включенном https.

2. Управляйте сертификатом, как показано ниже.

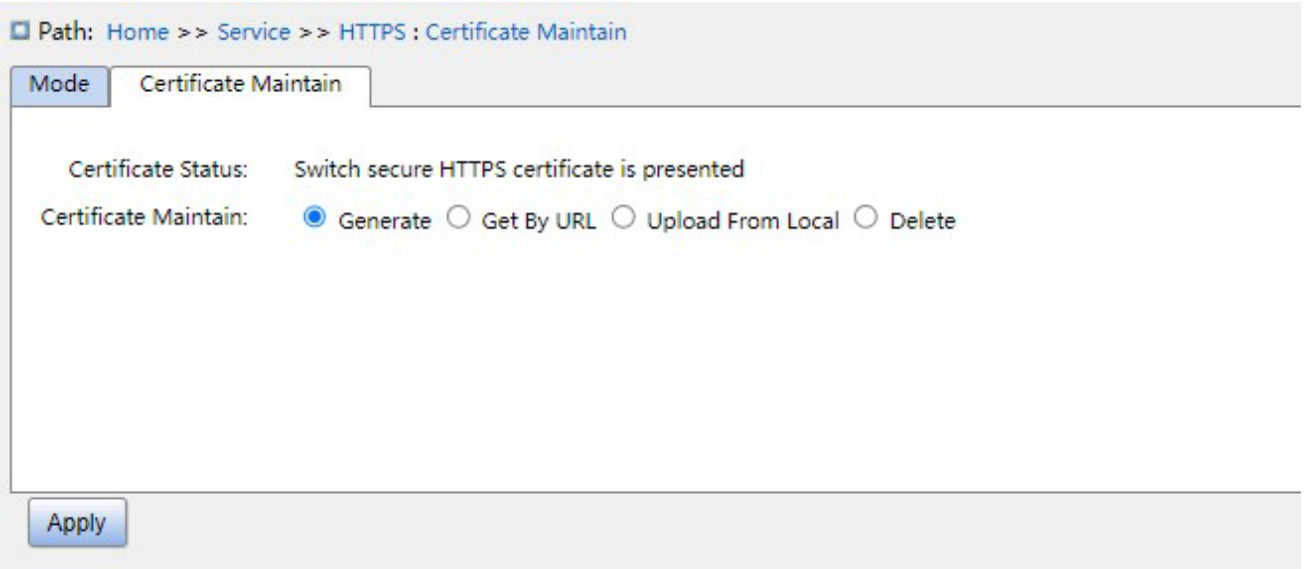


Рисунок 42 Создание сертификата

Certificate Maintain

Варианты настройки：Generate/Get by URL/Upload from local/Delete

Функция: выбор режима выгрузки сертификата.

Получить сертификат по URL

URL

Функция：задать путь как https://10.10.10.10:80/new_image_path/new_image.dat

Выгрузка с локального компьютера

Выбрать файл

Функция: выбор сертификатов HTTPS на локальном компьютере.

5.2 SNMP v1/SNMP v2c

5.2.1 Введение

Simple Network Management Protocol (SNMP) — это структура, использующая TCP/IP для управления сетевыми устройствами. С помощью SNMP администратор может запрашивать информацию об устройстве, изменять настройки параметров, отслеживать состояние устройства и обнаруживать сбои в сети.

5.2.2 Реализация:

SNMP использует режим станции управления/агента. Таким образом, SNMP включает в себя два типа сетевых элементов: NMS и агент.

Станция управления сетью (NMS) — это станция, на которой работает программный клиент управления сетью с поддержкой SNMP. Это ядро для управления сетью 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 средством управления сетью SNMP, а агент управляется сетью 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 пакеты Get-Request, Get-Next-Request и Set-Request агентам для запроса, настройки и управления переменными. После получения этих запросов агенты отвечают пакетами Get-Response. Когда возникает тревога, агент упреждающе сообщает об этом в NMS с помощью пакета Trap.

5.2.3 Пояснения

Коммутаторы этой серии поддерживают SNMP v2c.. SNMP v2c совместим с SNMPv1. SNMP v1 использует для аутентификации имя сообщества. Имя сообщества действует как пароль, ограничивая доступ NMS к агентам. Если имя сообщества, переносимое пакетом SNMP, не подтверждается коммутатором, запрос завершается неудачно и возвращается сообщение об ошибке.

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

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

5.2.4 Знакомство с MIB

Любой управляемый ресурс называется управляемым объектом. Management Information Base (MIB) хранит управляемые объекты. Она определяет иерархические отношения управляемых объектов и атрибутов объектов, таких как имена, разрешения на доступ и типы данных. У каждого Агента есть своя MIB. NMS может читать/записывать MIB на основе разрешений. На рисунке 43 показаны взаимоотношения между NMS, агентом и MIB.

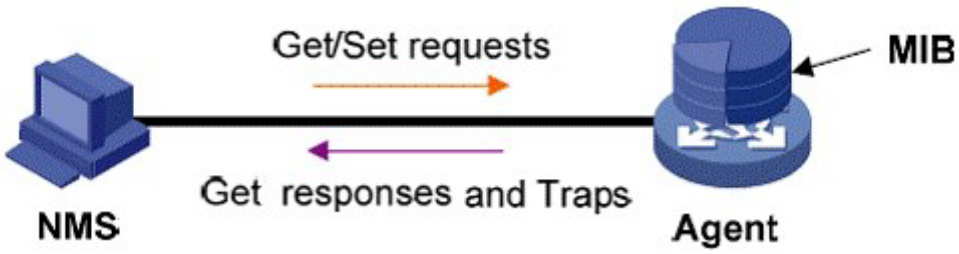


Рисунок 43 Взаимоотношения между NMS, агентом и MIB

MIB определяет древовидную структуру. Узлы дерева являются управляемыми объектами. Каждый узел имеет уникальный идентификатор Object Identifier (OID), который указывает расположение узла в структуре MIB. Как показано на рисунке 44, OID объекта A – 1.2.1.1.

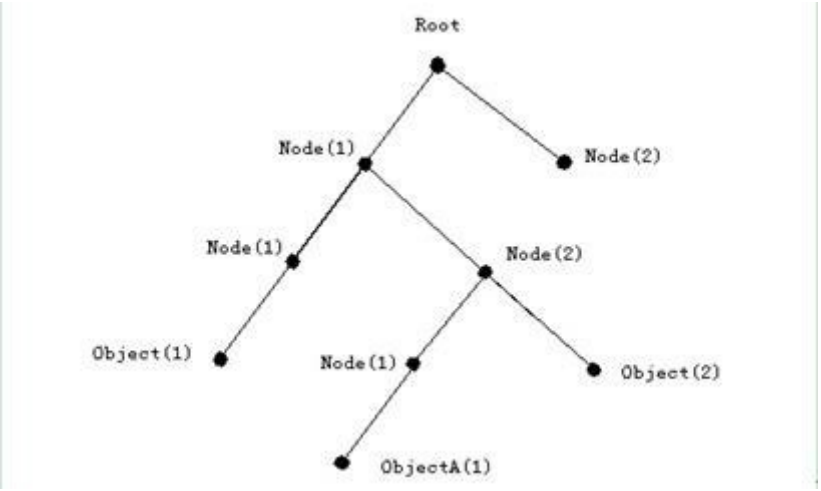


Рисунок 44 Структура MIB

5.2.5 Настройка через веб-интерфейс

1. Включите SNMP, как показано ниже.

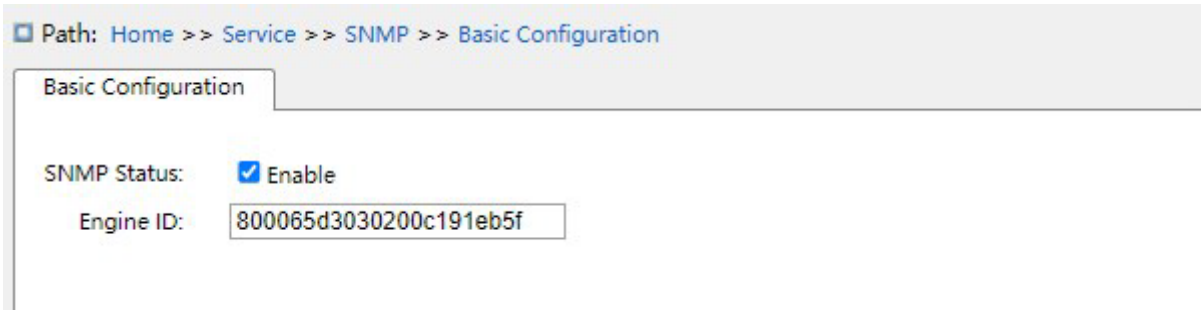


Рисунок 45 Включение SNMP

SNMP status

Варианты настройки: enable/disable

Конфигурация по умолчанию: Enable

Функция: включение или отключение SNMP.

Engine ID

Диапазон значений: четное шестнадцатеричное число, не может состоять только из 0 или F, диапазон значений четного числа составляет 10~64.

Функция: Настройка engine ID SNMP v3. При изменении Engine ID пользователи, соответствующие идентификаторам устройств в таблице пользователей, удаляются.

2. Настройте сообщество, как показано ниже.

Рисунок 46 Настройка сообщества

Community

Диапазон настройки: 1~32 символа

Функция: настройка сообщества коммутатора.

Описание: Доступ к информации библиотеки MIB коммутатора возможен только в том случае, если имя сообщества в сообщении SNMP соответствует строке сообщества.

Примечание: можно настроить до 16 строк сообщества.

Access Priority

Варианты конфигурации: Read Only/Read And Write

По умолчанию: Read Only.

Функция: настройка приоритета доступа для библиотеки MIB.

Описание: информация библиотеки MIB может быть доступна только с разрешениями только на чтение; информацию библиотеки MIB можно читать с разрешениями на чтение и запись.

3. Настройте Trap, как показано ниже.

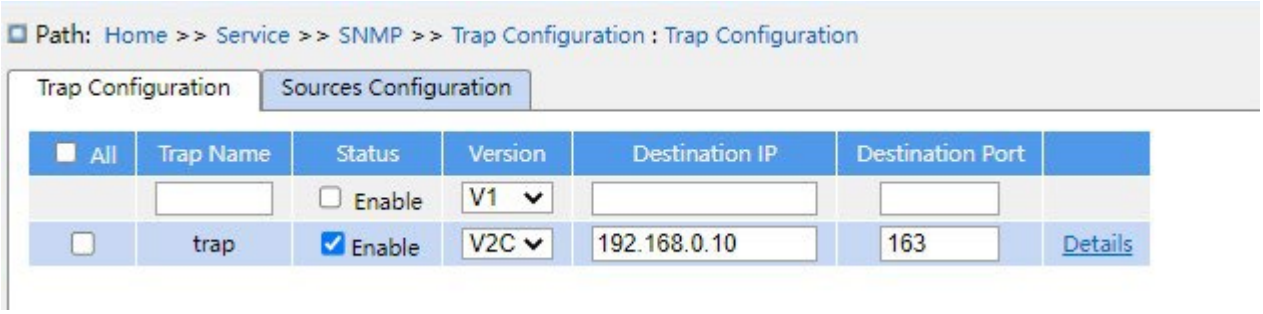


Рисунок 47 Настройка Trap

Trap name

Диапазон настройки: 1~32 символа

Функция: настройка имени Trap/.

status

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: включение или отключение trap, при включении коммутатор отправляет на сервер соответствующие сообщения trap.

Version

Варианты конфигурации: SNMP v1/SNMP v2c/SNMP v3

Конфигурация по умолчанию: SNMP v1

Функция: настройка номера версии сообщения trap, которое коммутатор отправляет на сервер.

Destination IP

Формат: A.B.C.D

Функция: Настройка адреса сервера для получения сообщения trap.

Destination Port

Диапазон настройки: 1~65535

Конфигурация по умолчанию: 162

Функция: Настройка номера порта, который отправляет сообщение trap.

4. Щелкните вкладку настроек trap, чтобы просмотреть подробную информацию, как показано ниже.

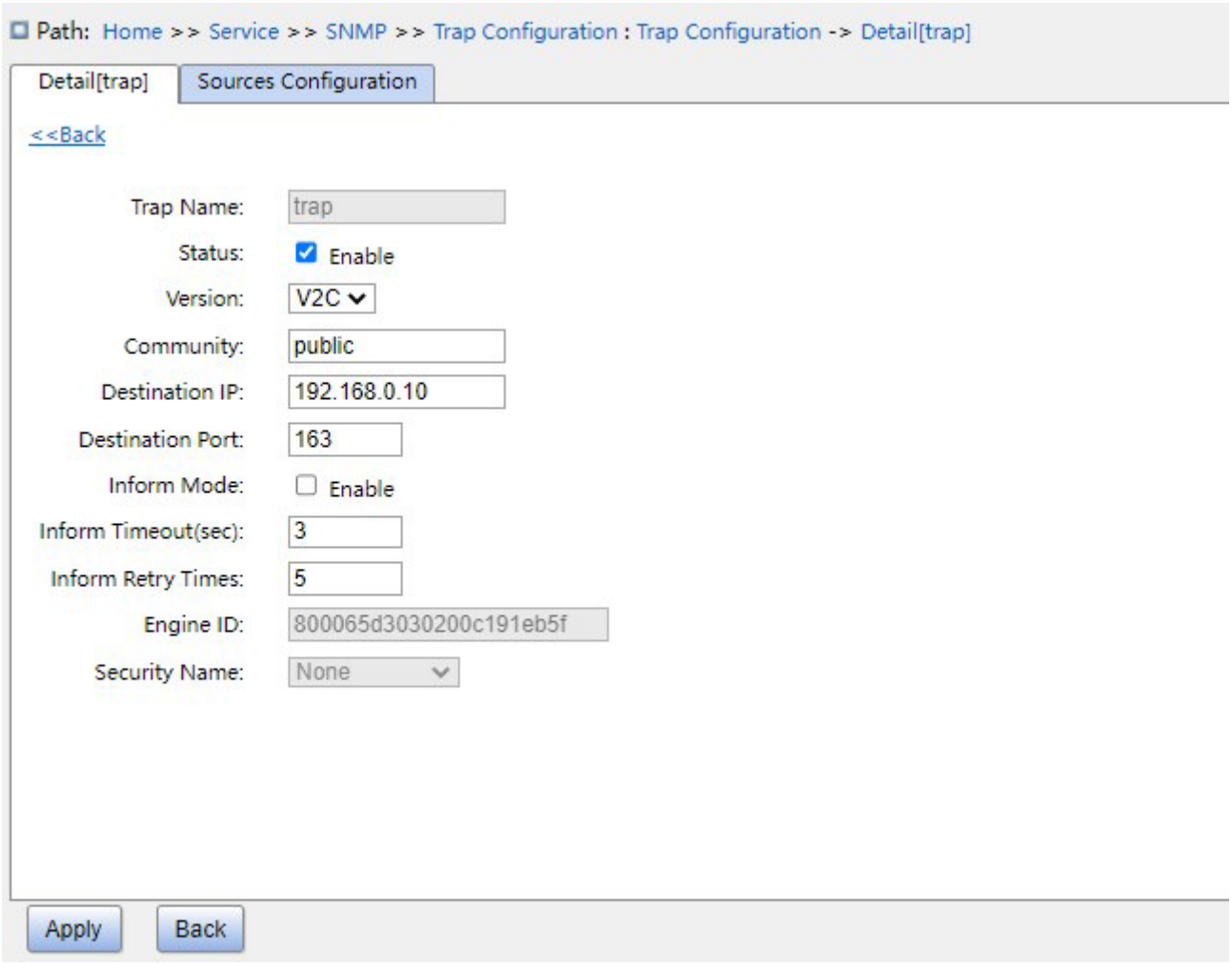


Рисунок 48 подробная информация trap

Community

Диапазон настройки: 1~255 символов

Конфигурация по умолчанию: public

Функция: Настройка имени сообщества, которое передается в сообщении trap.

Inform Mode

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: Включение/выключение отправки сервером ответного сообщения коммутатору после получения сообщения trap.

Inform Timeout

Диапазон настройки: 0~2147 с

Конфигурация по умолчанию: 3 с

Функция: Настройка таймаута отправки сообщений trap; при отсутствии ответа от сервера в течение этого времени после отправки сообщения trap сообщение будет отправлено повторно.

Inform retry Times

Диапазон настройки: 0~255

Конфигурация по умолчанию: 5

Функция: Настройка числа попыток отправки сообщений Trap по таймауту. Если совокупное количество раз отправки превышает значение настройки, а сервер все равно не отвечает, то отправка считается неудачной.

5. Настройте событие Trap, как показано ниже.

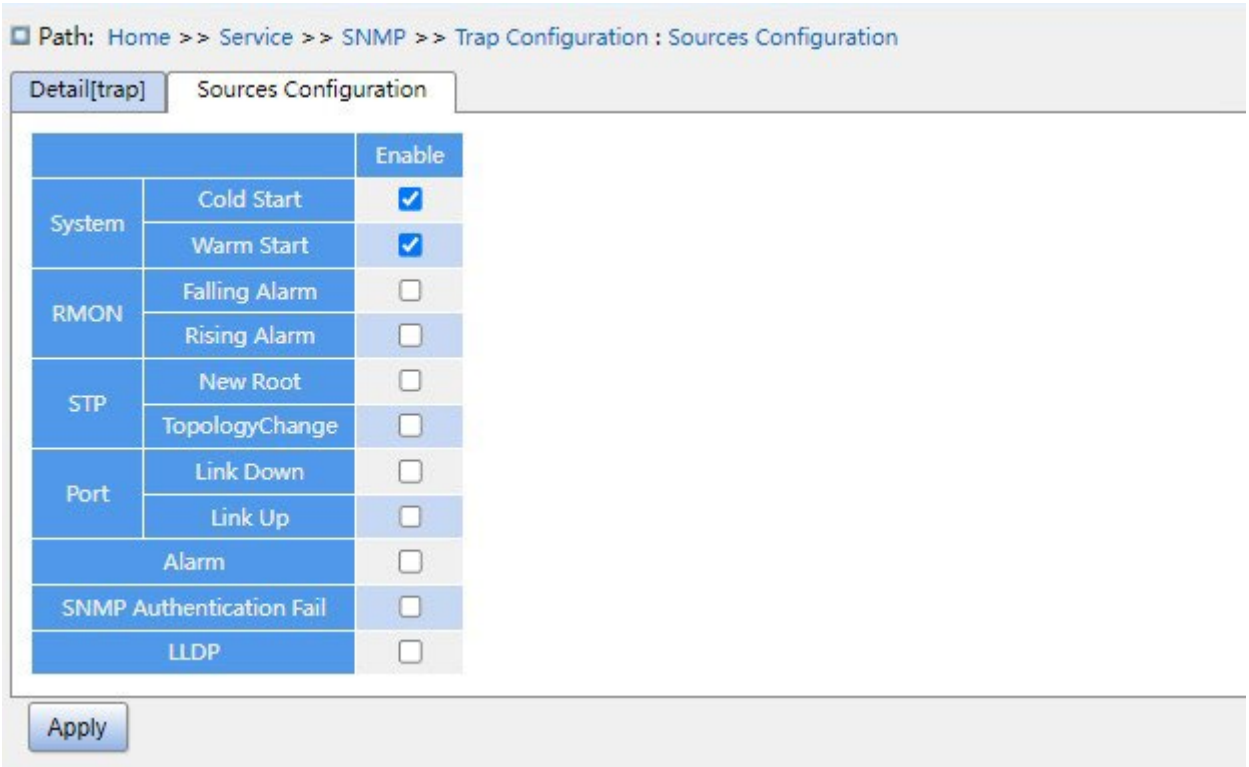


Рисунок 49 Настройка источника trap

System warm start/cold start

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: Включение/выключение отправки сообщения trap при «теплом»/»холодном» запуске системы.

RMON falling alarm/rising alarm

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: Включение/выключение отправки сообщения trap, когда RMON генерирует сигнал тревоги по отказу/повышению значения.

STP new root/ topology change

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: Включение/выключение отправки сообщения trap при изменении состояния STP.

Port link up/down

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: Включение/выключение отправки сообщения trap при изменении статуса порта.

Оповещение

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: Настройка отправки сообщений Trap при наличии информации о тревоге.

SNMP authentication fail

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: Настройка отправки сообщений Trap при ошибке аутентификации SNMP.

LLDP

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: Настройка отправки сообщений Trap LLDP при изменении статуса соседа.

5.2.6 Пример типовой конфигурации

Управляющий сервер SNMP подключается к коммутатору через Ethernet. IP-адрес управляющего сервера 192.168.0.23, а IP-адрес коммутатора 192.168.0.2. NMS отслеживает и управляет агентом через SNMP v2c, а также считывает и записывает информацию узла MIB агента. Когда агент неисправен, он упреждающе отправляет пакеты Trap в NMS, как показано на рисунке 50.

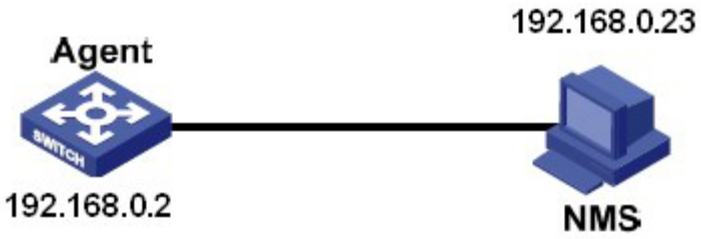


Рисунок 50 Пример конфигурации SNMP v2c

Настройка агента:

1. Включите состояние SNMP и v2c; настройте права доступа сообщества Read only – public и сообщества Read and write – private, как показано на рисунках 45 и 46.
2. Настройте глобальный режим Trap, как показано на рисунке 47.
3. Создайте запись Trap 111, включите режим Trap; установите версию trap SNMP v2c, IP-адрес назначения 192.168.0.23. Выберите систему, интерфейс, аутентификацию и все сообщения Trap для коммутатора, а также установите настройки по умолчанию для других параметров, как показано на рисунках 48 и 49. При необходимости отслеживание и управление агентами запустите соответствующее программное обеспечение для управления в NMS, например, Kyvision, разработанное Kyland.

Подробные сведения о работе Kyvision приведены в *Руководстве пользователя Kyvision*.

5.3 SNMPv3

5.3.1 Введение

SNMP v3 обеспечивает механизм аутентификации модели безопасности на основе пользователей (USM). Можно настроить функции аутентификации и шифрования.

Аутентификация используется для проверки подлинности отправителя пакета, предотвращая доступ незаконных пользователей. Шифрование используется для шифрования пакетов, передаваемых между NMS и агентом, во избежание перехвата. Функции аутентификации и шифрования могут повысить безопасность связи между SNMP NMS и SNMP-агентом.

Чтобы обеспечить связь между NMS и агентом, их версии SNMP должны совпадать. Для агента 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.

Можно создать несколько пользователей в таблице пользователей. Каждый пользователь использует разные политики безопасности для аутентификации и шифрования.

Таблица групп — это совокупность нескольких пользователей. В таблице групп права доступа определяются на основе групп пользователей. Все пользователи группы имеют права группы. Таблица просмотра относится к информации просмотра MIB, которая указывает информацию MIB, к которой могут обращаться пользователи. Представление MIB может содержать все узлы определенного поддерева MIB (то есть пользователям разрешен доступ ко всем узлам поддерева MIB) или не содержать ни одного из узлов определенного поддерева MIB (то есть пользователям не разрешен доступ ни к одному из узлов поддерева MIB).

Можно определить права доступа MIB в таблице доступа по имени группы, модели безопасности и уровню безопасности.

5.3.3 Настройка через веб-интерфейс

1. Включите SNMP, как показано ниже.

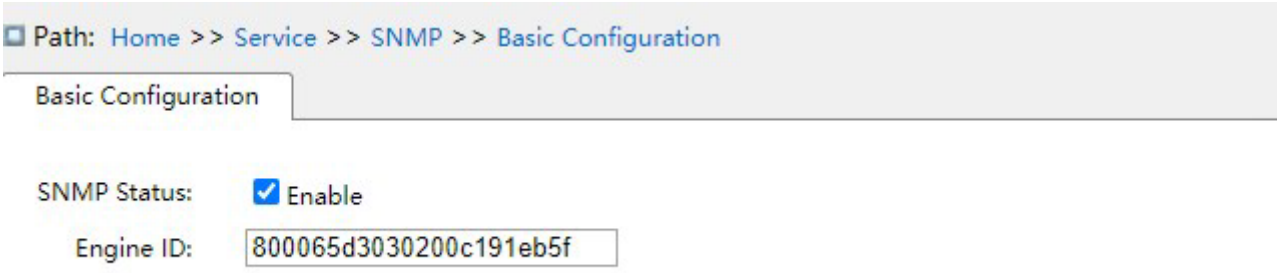


Рисунок 51 Включение SNMP

SNMP status

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: включение или отключение SNMP.

Engine ID

Диапазон значений: четное шестнадцатеричное число, не может состоять только из 0 или F, диапазон значений четного числа составляет 10~64.

Функция: Настройка engine ID SNMP v3. При изменении Engine ID пользователи, соответствующие идентификаторам устройств в таблице пользователей, удаляются.

2. Настройте Trap, как показано ниже.

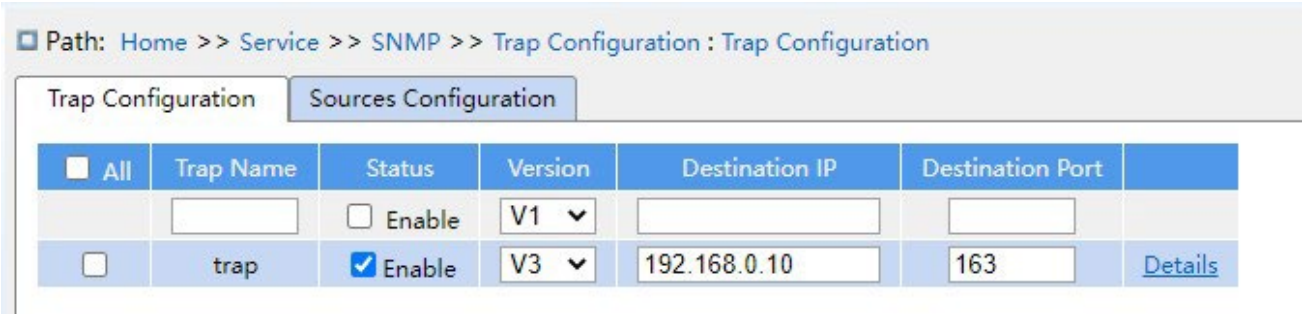


Рисунок 52 Настройка Trap

Trap name

Диапазон настройки: 1~32 символа Функция:

настройка имени Trap.

Status

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: включение или отключение trap, при включении коммутатор отправляет на сервер соответствующие сообщения trap.

Version

Варианты конфигурации: SNMP v1/SNMP v2c/SNMP v3

Конфигурация по умолчанию: SNMP v1

Функция: настройка номера версии сообщения trap, которое коммутатор отправляет на сервер.

Destination IP

Формат: A.B.C.D

Функция: Настройка адреса сервера для получения сообщения trap.

Destination port

Диапазон настройки: 1~65535

Конфигурация по умолчанию: 162

Функция: Настройка номера порта, который отправляет сообщение trap.

3. Щелкните вкладку настроек trap, чтобы просмотреть подробную информацию, как показано ниже.

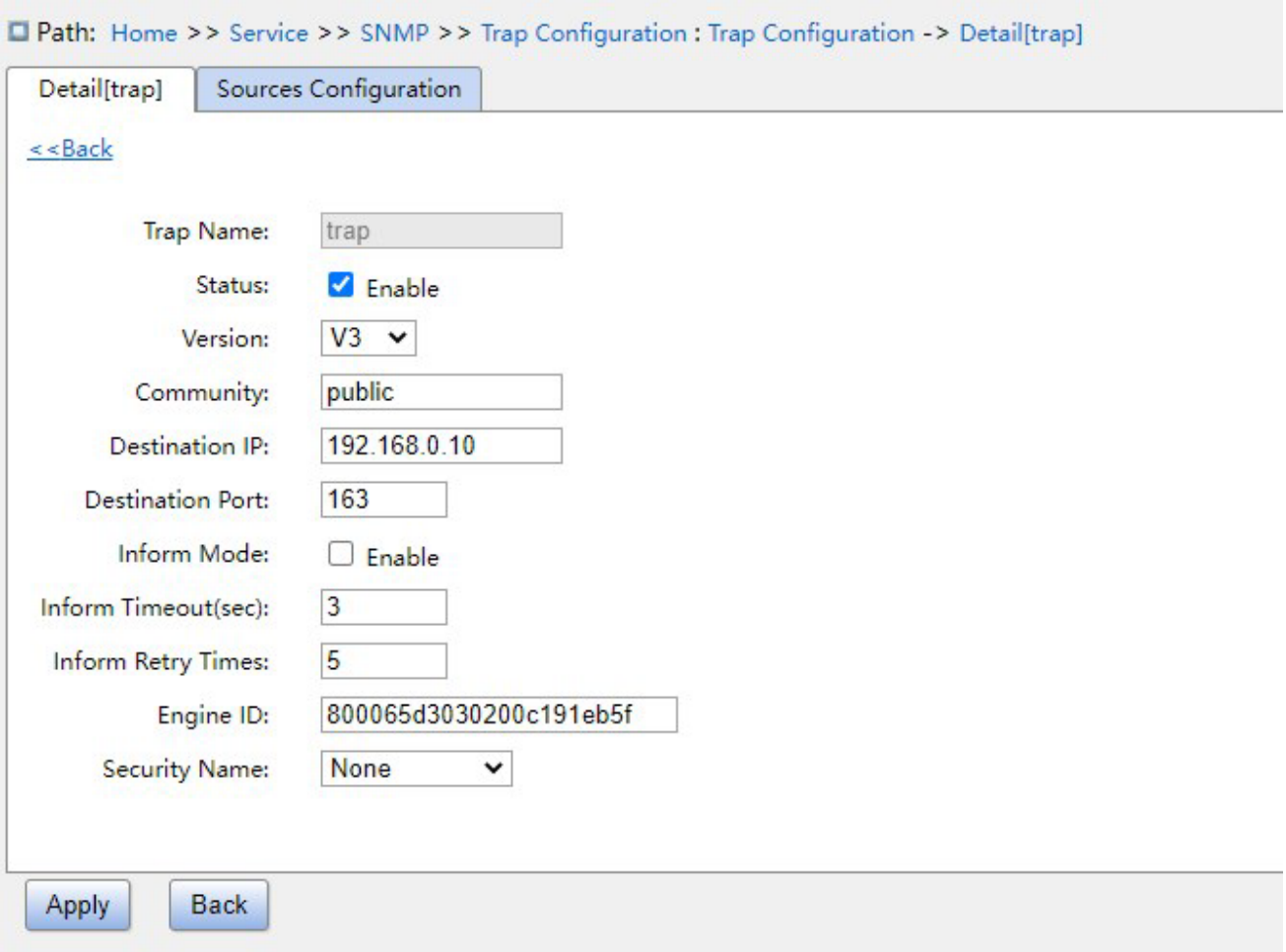


Рисунок 53 Подробная информация trap

Trap name

Диапазон настройки: 1~32 символа

Конфигурация по умолчанию: public

Функция: Настройка имени сообщества, которое передается в сообщении trap.

Inform Mode

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: Включение/выключение отправки сервером ответного сообщения коммутатору после получения сообщения trap.

Inform Timeout

Диапазон настройки: 0~2147 с

Конфигурация по умолчанию: 3 с

Функция: Настройка таймаута отправки сообщений trap; при отсутствии ответа от сервера в течение этого времени после отправки сообщения trap сообщение будет отправлено повторно.

Inform Retry Times

Диапазон настройки: 0~255

Конфигурация по умолчанию: 5

Функция: Настройка числа попыток отправки сообщений Trap по таймауту. Если совокупное количество раз отправки превышает значение настройки, а сервер все равно не отвечает, то отправка считается неудачной.

Engine ID

Диапазон значений: четное шестнадцатеричное число, не может состоять только из 0 или F, диапазон значений четного числа составляет 10~64.

Функция: Настройка идентификатора механизма безопасности, передаваемого в сообщениях Trap SNMP v3.

Security Name

Конфигурация по умолчанию: None

Функция: При использовании Trap SNMP V3 необходимо выполнить привязку к имени пользователя V3.

4. Настройте событие Trap, как показано ниже.

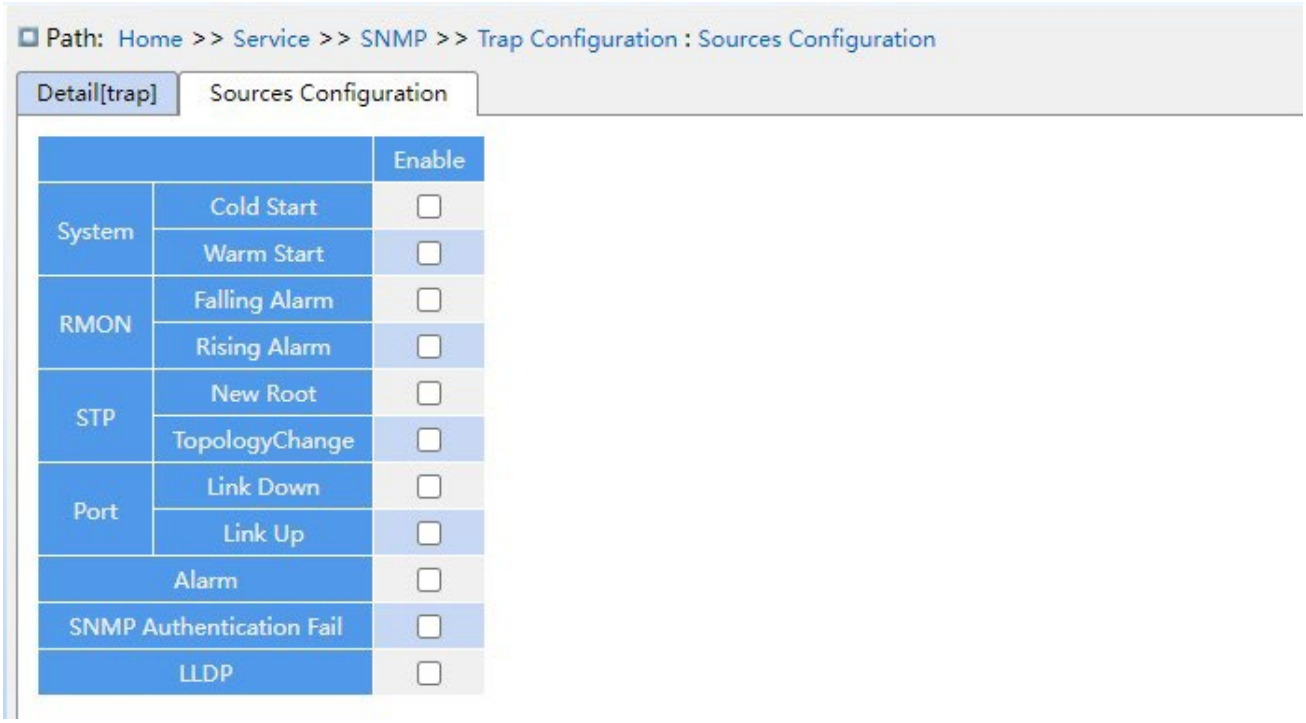


Рисунок 54 Настройка источника trap

System warm start/cold start

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: Включение/выключение отправки сообщения trap при «теплом»/«холодном» запуске системы.

RMON falling alarm/rising alarm

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: Включение/выключение отправки сообщения trap, когда RMON генерирует сигнал тревоги по отказу/повышению значения.

STP new root/ topology change

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: Включение/выключение отправки сообщения trap при изменении состояния STP.

Port link up/down

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: Включение/выключение отправки сообщения trap при изменении статуса порта.

Оповещение

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: Настройка отправки сообщений Trap при наличии информации о тревоге.

SNMP authentication fail

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: Настройка отправки сообщений Trap при ошибке аутентификации SNMP.

LLDP

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: Настройка отправки сообщений Trap LLDP при изменении статуса соседа.

5. Настройте таблицу имен пользователей, как показано ниже.

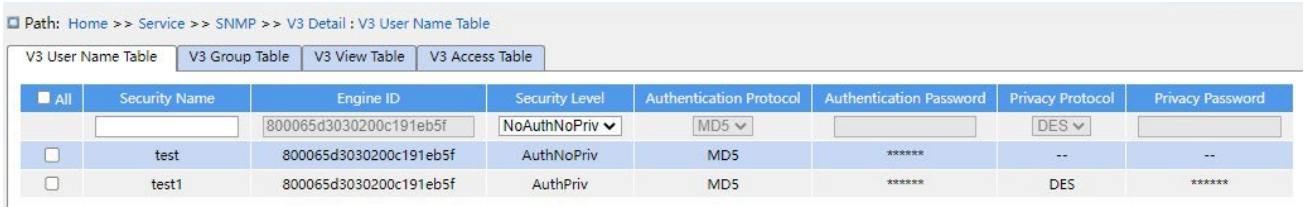


Рисунок 55 Настройка таблицы имен пользователей SNMPv3

Security Name

Диапазон настройки: 1~32 символа Функция:

Создание имени пользователя.

Engine ID

Диапазон значений: четное шестнадцатеричное число, не может состоять только из 0 или F, диапазон значений четного числа составляет 10~64.

Функция: Настройка идентификатора механизма безопасности, передаваемого в сообщениях Trap SNMP v3.

Security Level

Варианты конфигурации: No Auth No Priv/Auth No Priv/Auth Priv

Функция: Настройка уровня безопасности текущего пользователя.

Описание: No Auth No Priv не требуется ни аутентификации, ни шифрования, Auth No Priv требуется аутентификация, не требуется шифрование, Auth Priv требуется и аутентификация, и шифрование.

Authentication Protocol

Варианты конфигурации: MD5/SHA

Функция: Выбор протокола аутентификации. При выборе уровня безопасности no priv/auth priv необходимо настроить протокол и пароль аутентификации.

Authentication Password

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

Функция: Создание пароля аутентификации.

Privacy Protocol

Варианты конфигурации: DES/AES

Функция: Выбор протокола конфиденциальности. Протокол конфиденциальности и пароль конфиденциальности должны быть установлены, когда уровень безопасности установлен на Auth, Priv.

Privacy Password

Диапазон настройки: 8~32 символа Функция:

Создание пароля конфиденциальности.

Можно настроить до 16 пользователей.

5. Настройте таблицу групп, как показано ниже.

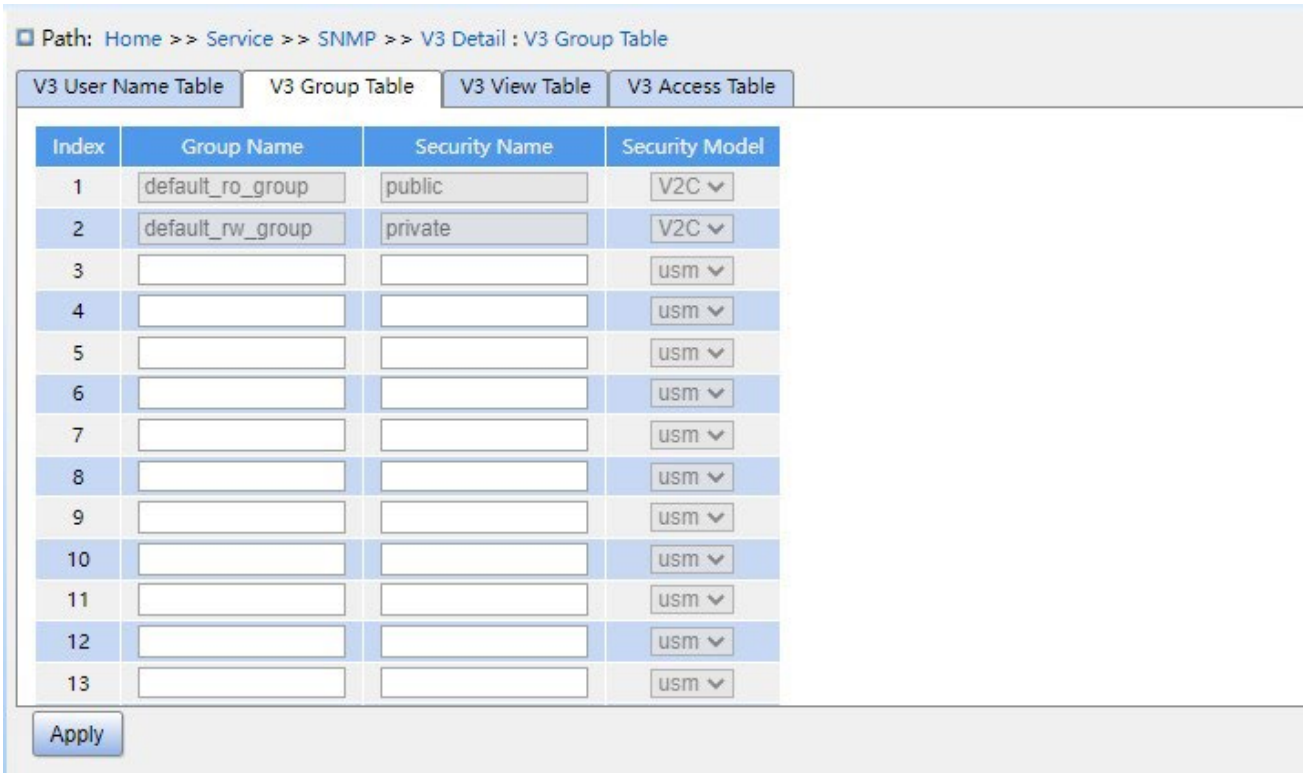


Рисунок 56 Настройка таблицы групп SNMPv3

Group Name

Диапазон настройки: 1~32 символа

Функция: Настройка имени таблицы групп. Пользователи с одинаковым именем группы принадлежат к одной группе.

Security Model

Конфигурация по умолчанию: SNMP v3

Функция: Выбор модели безопасности текущей группы (версия SNMP).

SNMPv3 использует технологию USM (модель безопасности, основанную на пользователе). В настоящее время эта опция применяется к модели SNMP V3.

Security name

Диапазон настройки: Созданное имя пользователя, 1~32 символа

Функция: Настройка доверенного имени, доверенное имя должно совпадать с именем пользователя в таблице пользователей. Пользователи с одинаковым именем группы принадлежат к одной группе.

Можно настроить до 32 таблиц групп.

6. Настройте таблицу представлений, как показано ниже.

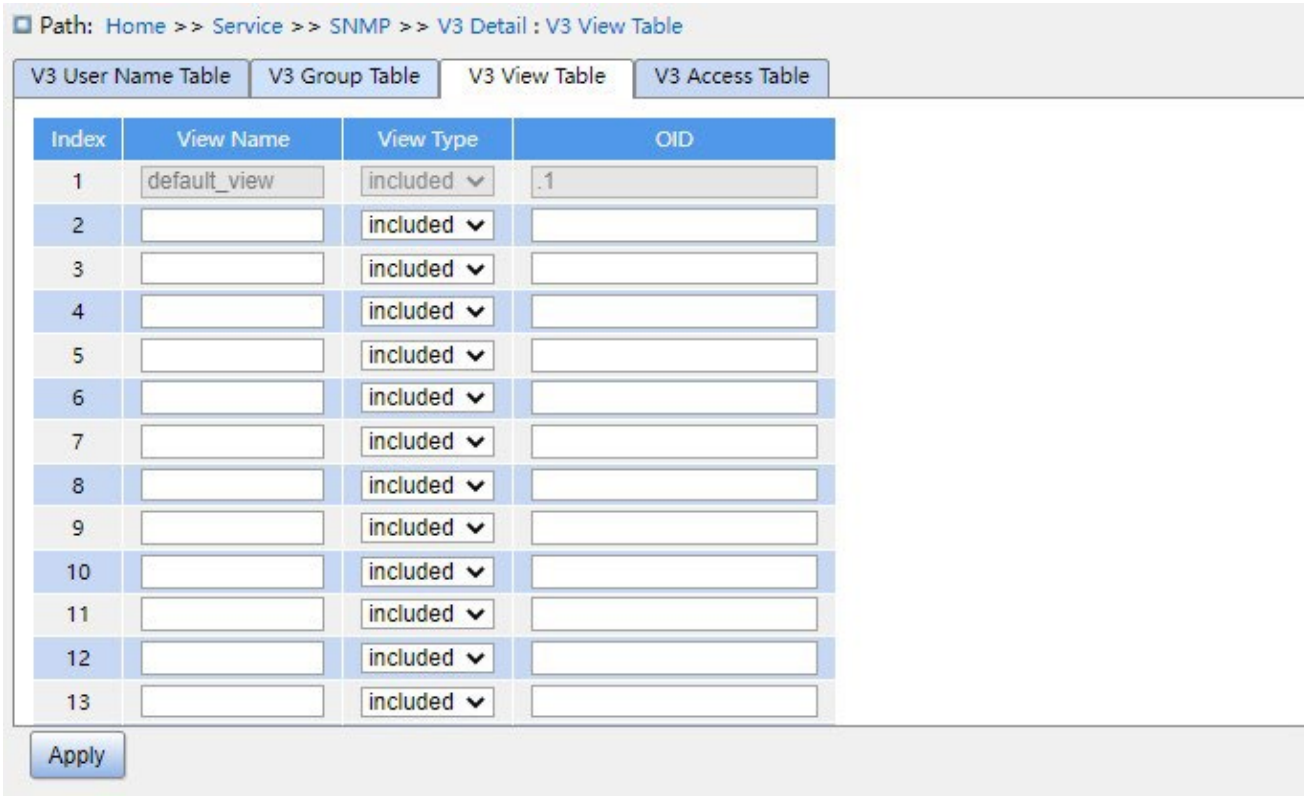


Рисунок 57 Настройка таблицы представлений SNMPv3

View Name

Диапазон настройки: 1~32 символа Функция:

Настройка имени представления.

Вариант представления

Варианты: included/excluded

Функция: Included указывает, что текущее представление включает все узлы поддерева MIB, excluded указывает, что текущее представление не включает узлы поддерева MIB.

OID sub node

Функция: Настройка поддерева MIB, указанного OID корневого узла поддерева.

Можно настроить до 16 таблиц представления.

Примечание:

Таблица представлений по умолчанию включает в себя все узлы поддерева.

7. Настройте таблицу доступа, как показано ниже.

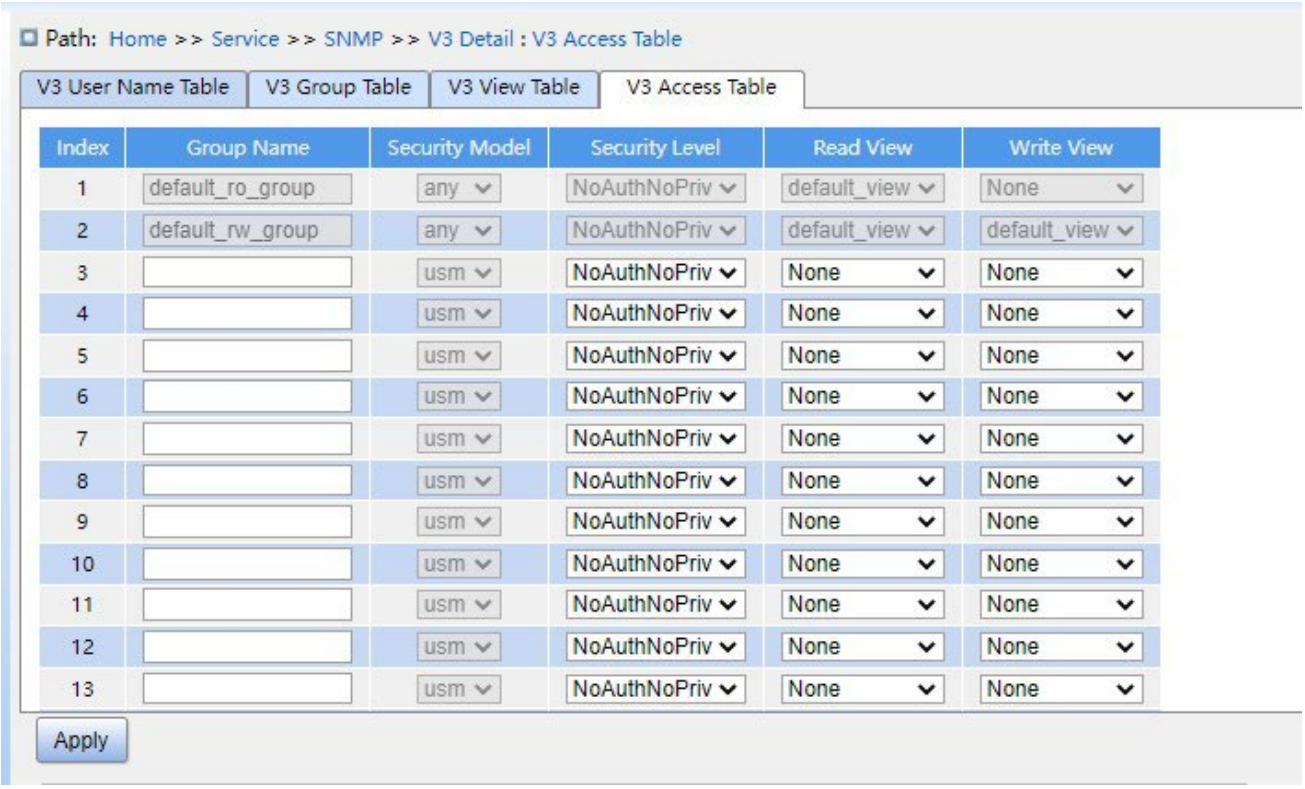


Рисунок 58 Настройка таблицы доступа SNMPv3

Group Name

Диапазон настройки: Созданное имя группы, 1~32 символа

Описание: Пользователи в группе имеют одинаковые права доступа.

Security Model

Конфигурация по умолчанию: any /use

Функция: Выбор модели безопасности текущей группы (версия SNMP). SNMPv3 использует технологию USM (модель безопасности, основанную на пользователе). Any означает использование любой модели безопасности. Имя группы и значение Security Model должны совпадать с именем группы и моделью безопасности в таблице групп.

Security Level

Варианты конфигурации: No Auth No Priv/Auth No Priv/Auth Priv

Функция: Настройка уровня безопасности текущей группы.

Описание: No Auth No Priv не требуется ни аутентификации, ни шифрования, Auth No Priv требуется аутентификация, не требуется шифрование, Auth Priv требуется и аутентификация, и шифрование. Когда требуется шифрование, протокол аутентификации/шифрования, пароль аутентификации/шифрования на стороне NMS

должны соответствовать конфигурации таблицы пользователей, тогда можно будет успешно получить доступ к информации узла коммутатора.

Уровни безопасности No Auth No Priv, Auth No Priv, Auth Priv нарастают, низкий уровень безопасности позволяет получить доступ к нему с высоким уровнем безопасности. Если в группе настроен уровень безопасности Auth No Priv, пользователи с уровнем безопасности Auth No Priv и Auth Priv в этой группе могут успешно получить доступ к коммутатору, если и протокол аутентификации/шифрования, и пароль аутентификации/шифрования верны, но пользователи с уровнем безопасности No Auth No Priv не могут получить доступ к коммутатору.

Read View

Варианты конфигурации: default_view/None/Created view name

Функция: Выбор имени представления read only.

Write View

Варианты конфигурации: default_view/None/Created view name

Функция: Выбор имени представления read and write.

Можно настроить до 16 таблиц доступа.

Примечание:
Таблицы доступа по умолчанию {default_ro_group, any, No Auth, No Priv, default_view, None}, {default_rw_group, any, No Auth, No Priv, default_view, default_view}.

5.3.4 Пример типовой конфигурации

Управляющий сервер SNMP подключается к коммутатору через Ethernet. IP-адрес управляющего сервера 192.168.0.23, а IP-адрес коммутатора 192.168.0.2. Пользователь 1111 и пользователь 2222 управляют Агентом через SNMP v3. Уровень безопасности установлен на Auth No Priv, и коммутатор может выполнять операцию только для чтения со всей информацией об узле Агента. При возникновении тревоги агент заранее отправляет сообщения trap v3 в NMS, как показано на рисунке 59.

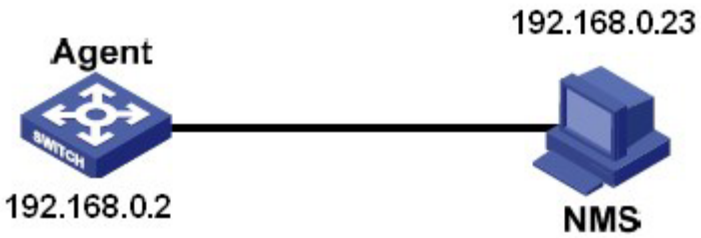


Рисунок 59 Пример конфигурации SNMP v3

Настройка агента:

1. Включите протокол SNMP v3, как показано на рисунке 51.
2. Настройте таблицу пользователей SNMP v3.

Задайте имя пользователя 1111, уровень безопасности Auth, Priv, протокол аутентификации MD5, пароль аутентификации aaaaaaaa, протокол конфиденциальности DES и пароль конфиденциальности xxxxxxxx.

Задайте имя другого пользователя 2222, уровень безопасности Auth, Priv, протокол аутентификации SHA, пароль аутентификации bbbbbbbb, протокол конфиденциальности AES и пароль конфиденциальности yyyyyyyy, как показано на рисунке 55.

3. Создайте группу, установите модель безопасности usm и добавьте пользователей 1111 и 2222 в группу, как показано на рисунке 56.
4. Настройте таблицу доступа SNMP v3.

Задайте имя группы group, модель безопасности usm, уровень безопасности Auth, NoPriv, значение default_view для параметра read view, значение None для параметра write view, как показано на рисунке 58.

5. Включите глобальный режим Trap, как показано на рисунке 52.
6. Создайте запись trap 222, включите режим trap; установите версию trap SNMP v3, IP-адрес назначения 192.168.0.23. Выберите систему, интерфейс, аутентификацию и все сообщения Trap для коммутатора, а также установите настройки по умолчанию для других параметров, как показано на рисунке 117.

При необходимости отслеживание и управление агентами запустите соответствующее программное обеспечение для управления в NMS.

5.4 Настройка SSH

5.4.1 Введение

SSH (Secure Shell) — это сетевой протокол для безопасного удаленного входа в систему. Он шифрует все передаваемые данные, чтобы предотвратить раскрытие информации. Когда данные шифруются SSH, пользователи могут использовать только командную строку для настройки коммутаторов.

Коммутатор поддерживает функцию SSH-сервера и позволяет подключаться нескольким пользователям SSH, которые удаленно входят в коммутатор через SSH.

5.4.2 Реализация

Чтобы осуществить безопасное SSH подключение, сервер и клиент должны пройти следующие пять этапов:

Этап согласования версий: в настоящее время SSH состоит из двух версий: SSH1 и SSH2. Обе стороны должны согласовать версию для использования.

Этап согласования ключей и алгоритмов. SSH поддерживает несколько типов алгоритмов шифрования. Обе стороны должны согласовать, какой алгоритм будет использоваться.

Этап аутентификации: клиент SSH отправляет на сервер запрос на аутентификацию, после чего сервер должен аутентифицировать клиента.

Этап запроса сеанса: после прохождения аутентификации клиент отправляет запрос на сеанс к серверу.

Этап сеанса: после передачи запроса на сеанс клиент и сервер начинают обмен данными.

5.4.3 Настройка через веб-интерфейс

1. Включите SSH Протокол, как показано ниже.

Рисунок 60 Включение протокола SSH

SSH Status

Варианты конфигурации: Enabled/Disabled

Конфигурация по умолчанию: Enabled

Функция: Включение/отключение протокола SSH Если протокол включен, коммутатор работает как сервер SSH.

5.4.4 Пример типовой конфигурации

Хост работает как SSH-клиент для установления локального соединения с коммутатором, как показано на рисунке 61.

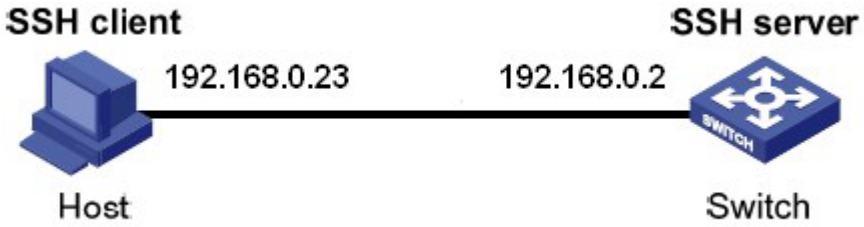


Рисунок 61 Пример настройки SSH

1. Включите протокол SSH, как показано на рисунке 60.
2. Установите соединение с сервером SSH. Сначала запустите программу PuTTY.exe, как показано на рисунке 62; введите IP-адрес SSH-сервера 192.168.0.2 в поле Host Name (or IP address).

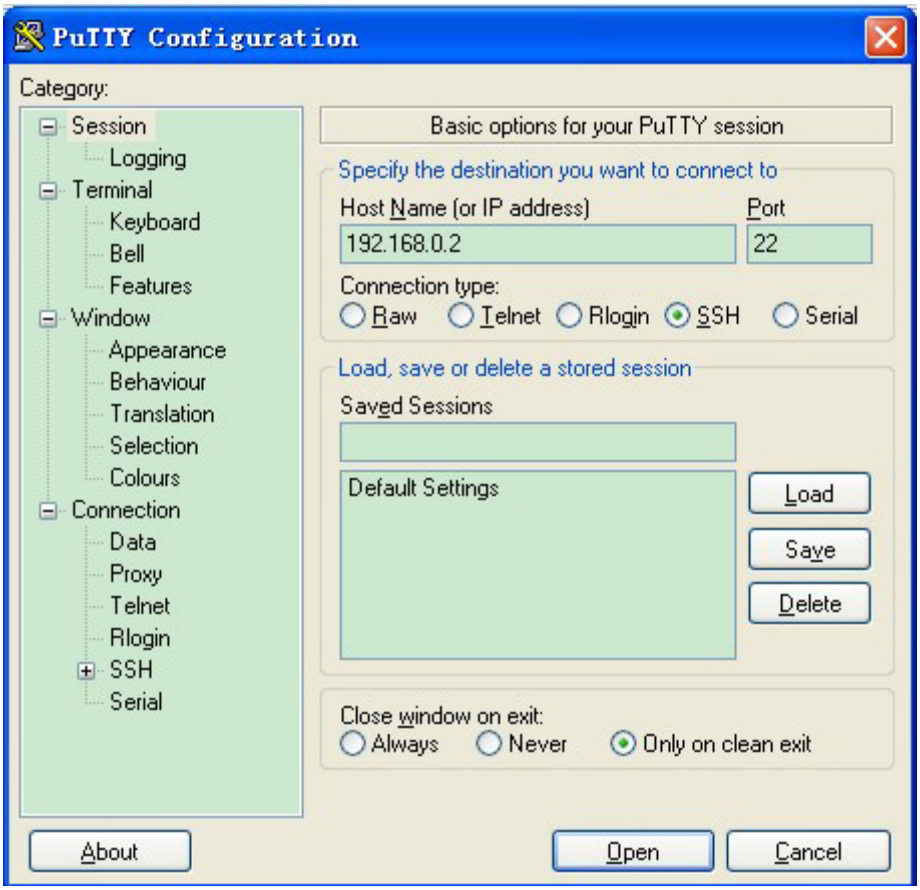


Рисунок 62 Настройка клиента SSH

3. Щелкните кнопку <Open>, появится предупреждающее сообщение, показанное на рисунке 63, щелкните кнопку <Yes(Y)>.

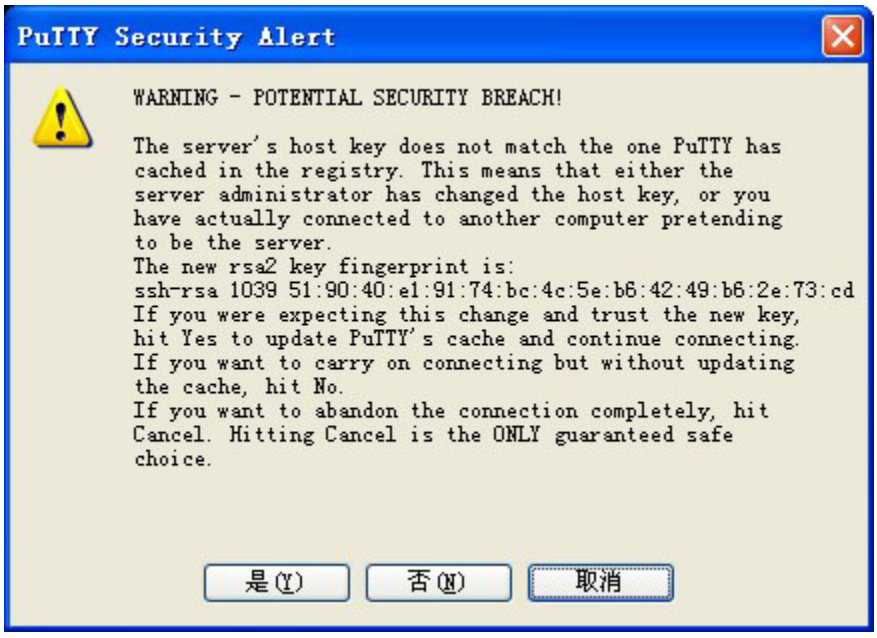


Рисунок 63 Предупреждающее сообщение

4. Введите имя пользователя admin и пароль 123, чтобы войти в интерфейс настройки коммутатора, как показано на рисунке 64.

Рисунок 64 Интерфейс входа в SSH-аутентификацию

5.5 Настройка TACACS+

5.5.1 Введение

TACACS+ (Terminal Access Controller Access Control System) представляет собой приложение на основе TCP.

Оно использует режим клиент/сервер для реализации связи между сервером доступа к сети (NAS) и сервером TACACS+. Клиент работает на NAS, а информация о пользователях управляется централизованно на сервере. NAS — это сервер для пользователей, но клиент для сервера.

На рисунке 65 показана структура.

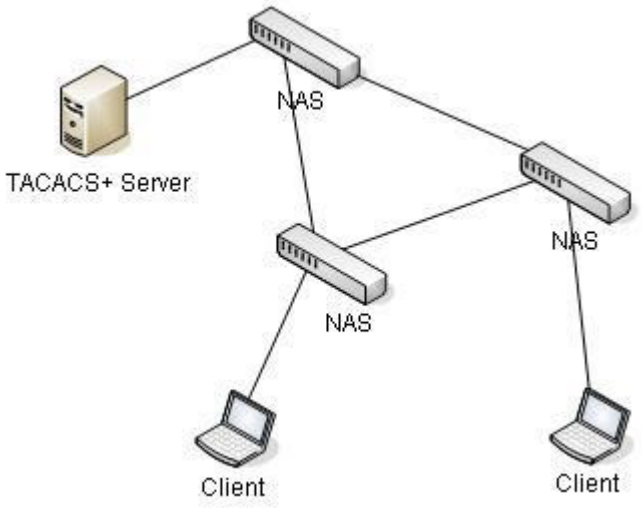


Рисунок 65 Структура TACACS+

Протокол аутентифицирует, авторизует и учитывает пользователей терминалов, которым необходимо войти на устройство для выполнения операций. Устройство служит клиентом 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 на устройство для выполнения операций.

5.5.2 Настройка через веб-интерфейс

1. Настройте сервер TACACS+, как показано ниже.

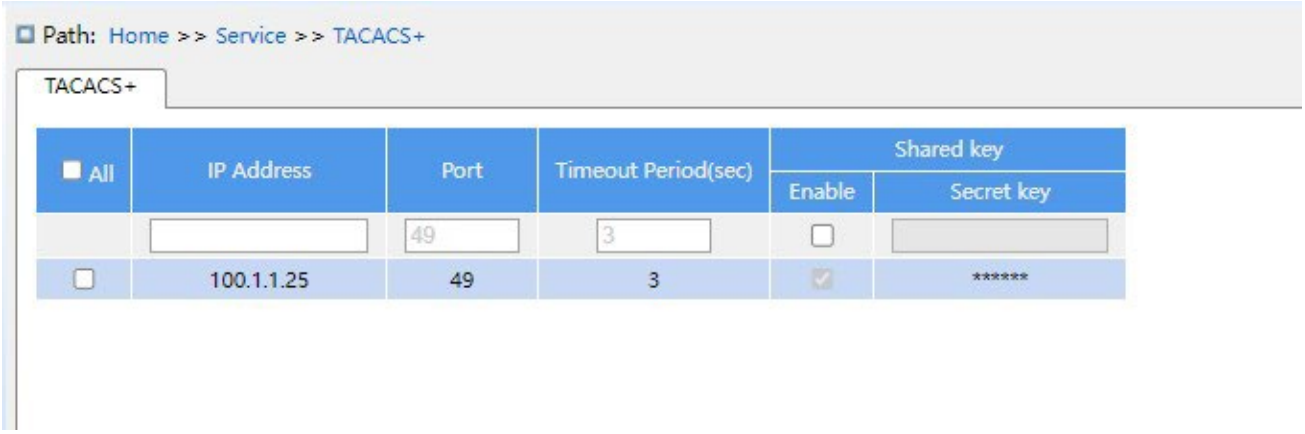


Рисунок 66 Конфигурация сервера TACACS+

IP Address

Функция: Настройка IP-адреса или имени хоста сервера TACACS+. Можно настроить не более 5 серверов TACACS+.

Port

Диапазон настройки: 0~65535

Конфигурация по умолчанию: 49

Функция: Назначение порта TCP сервера TACACS+ для аутентификации.

Timeout Period(sec)

Диапазон настройки: 1~1000 с

Функция: Настройка времени для получения отклика от сервера TACACS+. Если после отправки пакета запроса TACACS+ устройство не получает ответа от сервера TACACS+ по истечении указанного времени, аутентификация завершается неудачно, и устройство считает сервер TACACS+ недействительным.

Share Key

Диапазон настройки: 1~63 символа

Функция: Задание ключа для повышения безопасности связи между клиентом и сервером TACACS+. Две стороны совместно используют ключ для проверки легитимности пакетов. Обе стороны могут получать пакеты друг от друга только тогда, когда ключи совпадают. Поэтому нужно, чтобы настроенный ключ совпадал с ключом на сервере TACACS+.

5.5.3 Пример типовой конфигурации

Как показано на рисунке 67, сервер TACACS+ может выполнять аутентификацию и авторизацию пользователей с помощью коммутатора. IP-адрес сервера — 192.168.0.23, а общий ключ, используемый при обмене пакетами между коммутатором и сервером, — aaa.

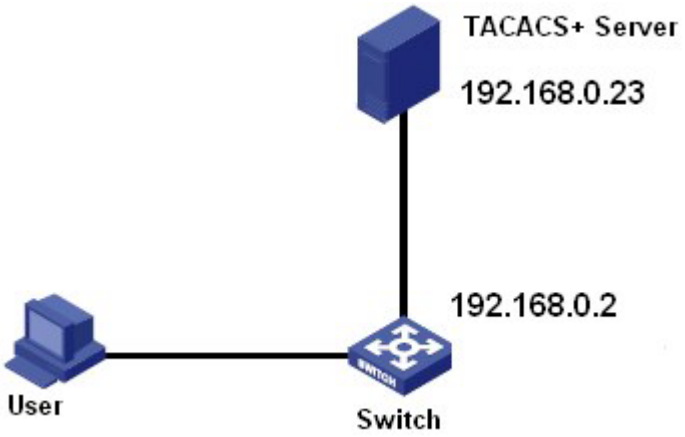


Рисунок 67 Пример аутентификации TACACS+

1. Настройка сервера TACACS+. Задайте IP-адрес сервера 192.168.0.23 и значение ключа aaa, как показано на рисунке 66.
2. При входе в коммутатор через веб-интерфейс выберите Local, при входе в коммутатор через telnet выберите Tacacs+, как показано на рисунке 13.
3. Настройте имя пользователя и пароль bbb, зашифруйте ключ aaa на сервере TACACS+.
4. При входе в коммутатор через веб-интерфейс введите имя пользователя admin и пароль 123, чтобы пройти локальную аутентификацию.
5. При входе в коммутатор через Telnet введите имя пользователя и пароль bbb, чтобы пройти аутентификацию TACACS+.

5.6 Настройка RADIUS

5.6.1 Введение

RADIUS (Remote Authentication Dial-In User Service) — это распределенный протокол 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 (сервером доступа к сети) и сервером RADIUS. Клиент RADIUS работает на NAS. Сервер RADIUS обеспечивает централизованное управление пользовательской

информацией. NAS — это сервер для пользователей, но клиент для сервера RADIUS. На рисунке 68 показана структура.

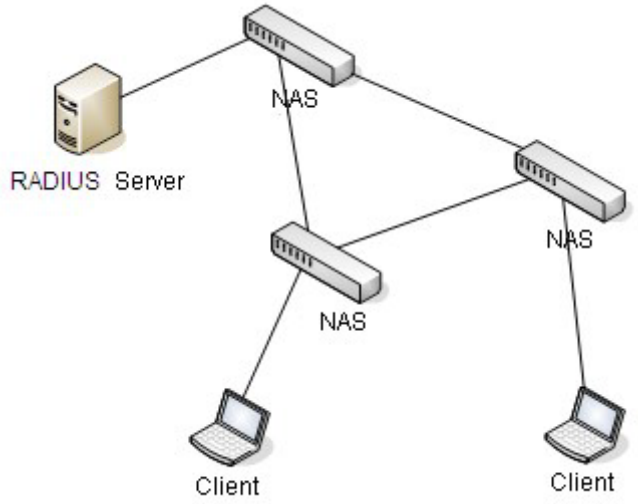


Рисунок 68 Структура RADIUS

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

5.6.2 Настройка через веб-интерфейс

1. Настройте сервер RADIUS, как показано ниже.

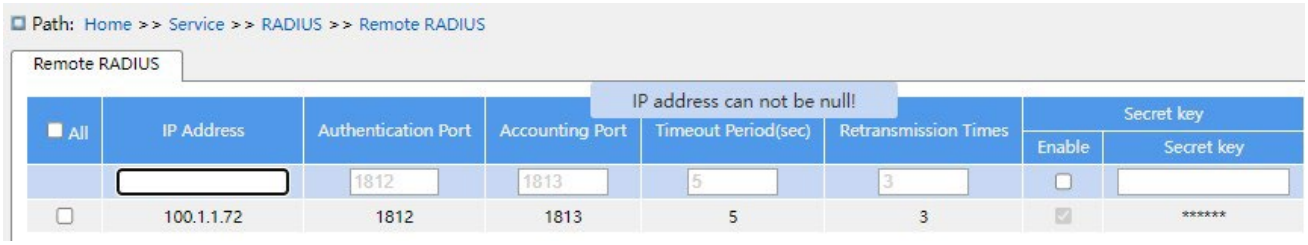


Рисунок 69 Настройка сервера RADIUS

IP Address

Функция: Настройка IP-адреса или имени хоста сервера RADIUS. Можно настроить не более 5 серверов RADIUS.

Authentication Port

Диапазон настройки: 0~65535

Конфигурация по умолчанию: 1812

Функция: Задание порта UDP сервера RADIUS для аутентификации.

Accounting Port

Диапазон настройки: 0~65535

Конфигурация по умолчанию: 1813

Функция: Задание порта UDP сервера RADIUS для учета. Поскольку RADIUS использует разные порты UDP для получения и отправки сообщений аутентификации и учета, необходимо настроить разные номера портов для аутентификации и учета.

Timeout Period(sec)

Диапазон настройки: 1~1000 с

Функция: Настройка времени для получения отклика от сервера RADIUS. После отправки пакета запроса RADIUS устройство повторит передачу пакета запроса RADIUS, если оно по-прежнему не получит ответа от сервера RADIUS по истечении указанного времени.

Retransmission Times

Диапазон настройки: 1~1000

Функция: Задание максимального количества попыток повторной передачи для пакетов запросов RADIUS. Если устройство по-прежнему не получает ответные пакеты от сервера RADIUS после максимального числа попыток повторной передачи, аутентификация завершается ошибкой, и устройство считает, что сервер RADIUS недействителен.

Secret Key

Диапазон настройки: 1~63 символа

Функция: Задание ключа для повышения безопасности связи между клиентом и сервером RADIUS. Две стороны совместно используют ключ для проверки легитимности пакетов. Обе стороны могут получать пакеты друг от друга только тогда, когда ключи совпадают. Поэтому нужно, чтобы настроенный ключ совпадал с ключом на сервере RADIUS.

Примечание:
Приоритет параметров Timeout Period, Retransmission Times и Secret Key в конфигурации сервера RADIUS выше, чем в глобальной конфигурации.

2. Глобальные настройки RADIUS показаны ниже.

Рисунок 70 Вкладка Global Configuration

RADIUS Enable

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включить использование локального RADIUS другими устройствами в качестве серверов RADIUS. 3. Конфигурация клиента RADIUS показана ниже.

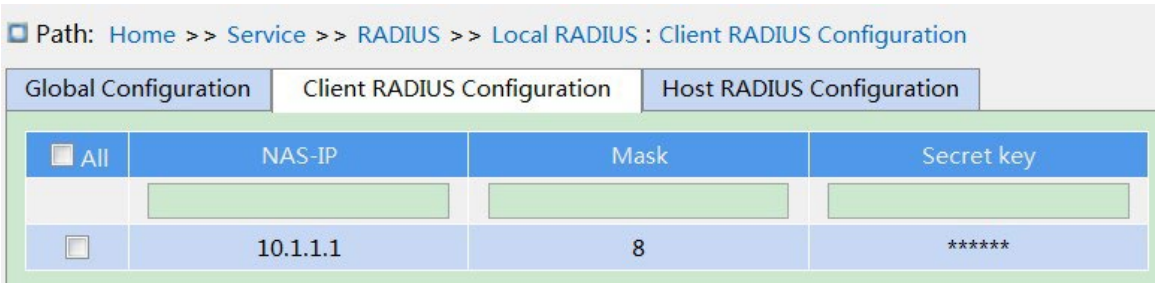


Рисунок 71 Конфигурация клиента RADIUS

NAS-IP

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

Mask

Диапазон настройки: 1-32

Функция: Настройка сегмента сети клиента RADIUS, IP-адрес сегмента той же сети настраивает только один сегмент.

Secret Key

Диапазон настройки: 1~63 символа

Функция: Настройка общего ключа устройства и клиента RADIUS для проверки достоверности сообщения. Сообщения принимаются и ответы посылаются только в том случае, когда ключ один и тот же, поэтому общий ключ, настроенный на устройстве, должен совпадать со значением ключа на клиенте RADIUS.

4. Конфигурация хоста RADIUS показана ниже.

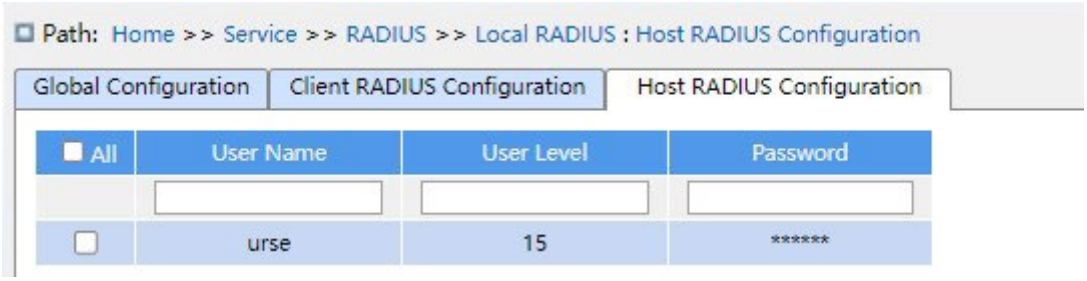


Рисунок 72 Конфигурация хоста RADIUS

User Name

Диапазон настройки: 1~31 символ

Функция: Настрой имени пользователя RADIUS.

Уровень пользователей

Диапазон настройки: 1~15

Функция: Настройка уровня полномочий пользователей Пользователи с разными уровнями полномочий имеют разные разрешения на доступ.

Password

Диапазон настройки: 1~31 символ

Функция: Настройка пароля пользователя для входа.

5.6.3 Пример типовой конфигурации

Как показано на рисунке 73, IEEE802.1X включен на порту 1 коммутатора. Пользователи могут войти в коммутатор через порт 1 после прохождения аутентификации на сервере RADIUS. IP-адрес сервера 192.168.0.23. Ключ для обмена пакетами между коммутатором и сервером — aaa.

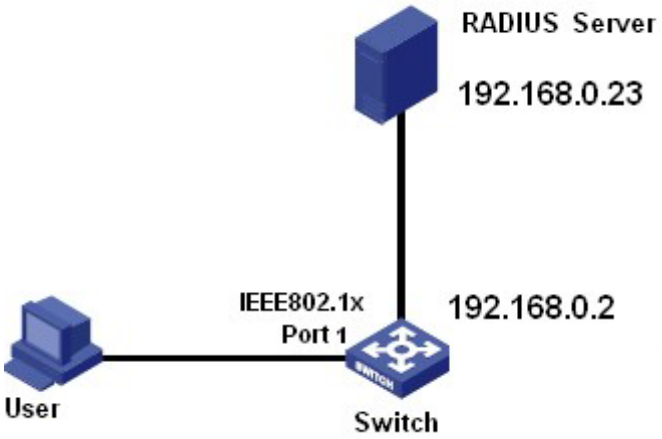


Рисунок 73 Пример аутентификации RADIUS

1. Задайте IP-адрес сервера аутентификации 192.168.0.23 и пароль aaa, как показано на рисунке 69.

2. Настройки IEEE802.1x: включить IEEE802.1X глобально. Установите тип аутентификации radius, состояние администратора порта 1 802.1X на основе порта, оставьте настройки по умолчанию для других параметров. 3. Установите для имени пользователя и пароля на сервере RADIUS значение ccc, для ключа шифрования — aaa.

4. Установите и запустите клиентское ПО 802.1x на ПК. Введите ccc в качестве имени пользователя и пароля.

Затем пользователь может пройти аутентификацию и получить доступ к коммутатору через порт 1.

5.7 RMON

5.7.1 Введение

Основанный на архитектуре SNMP, удаленный мониторинг сети (RMON) позволяет устройствам управления сетью осуществлять упреждающий мониторинг и управление управляемыми устройствами. Сеть RMON обычно включает в себя станцию управления сетью и агенты. NMS управляет агентами, а агенты могут собирать статистику по различным типам трафика на этих портах. RMON в основном обеспечивает статистику и функции сигнализации. С помощью функции статистики

Агенты могут периодически собирать статистику по различным типам трафика на этих портах, например, количество пакетов, полученных из определенного сегмента сети за определенный период. Функция тревоги заключается в том, что агенты могут отслеживать значения указанных переменных MIB. Когда значение достигает порога тревоги (например, количество пакетов достигает указанного значения), агент может автоматически записывать события тревоги в журнал RMON или отправлять сообщение Trap на управляющее устройство.

5.7.2 Группы RMON

RMON (RFC2819) определяет несколько групп RMON. Устройства серии поддерживают группу статистики, группу истории, группу событий и группу сигналов тревоги в общедоступной MIB.

- Группа статистики

С помощью группы статистики система собирает статистику по всем типам трафика на портах и сохраняет статистику в таблице статистики Ethernet для дальнейшего запроса управляющим устройством. Статистика включает в себя количество сетевых коллизий, пакетов с ошибками CRC, пакетов меньшего или большего размера, широковещательных и многоадресных пакетов, полученных байтов и полученных пакетов. После успешного создания записи статистики на указанном порту группа статистики подсчитывает количество пакетов на порту, и статистика представляет собой постоянно накапливаемое значение.

- Группа истории

Группа истории требует, чтобы система периодически отбирала все виды трафика на портах и сохраняла значения выборки в таблице записей истории для дальнейшего запроса устройством управления. Группа истории подсчитывает статистические значения всех видов данных в интервале выборки.

- Группа событий

Группа событий используется для определения индексов событий и методов обработки событий. События, определенные в группе событий, используются в элементе конфигурации группы тревог. Событие запускается, когда контролируемое

устройство соответствует условию тревоги. События обрабатываются следующими способами:

Log: регистрирует события и соответствующую информацию в таблице журнала событий.

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

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

None: указывает на отсутствие действий.

- Группа тревоги

Управление сигналами тревоги RMON может отслеживать указанные переменные аварийных сигналов тревоги. После того, как записи сигналов тревоги определены, система получит значения контролируемых переменных сигналов тревоги за определенный период. Когда значение переменной тревоги больше или равно верхнему пределу, инициируется событие роста значения. Когда значение переменной тревоги меньше или равно нижнему пределу, инициируется событие падения значения. Сигналы тревоги будут обрабатываться в соответствии с определением события.

Предупре

Если выбранное значение переменной тревоги превышает пороговое значение несколько раз в одном и том же направлении, то событие тревоги срабатывает только в первый раз. Таким образом, сигналы повышения и падения значения генерируются попеременно.

5.7.3 Настройка через веб-интерфейс

1. Настройте таблицу статистики, как показано ниже.

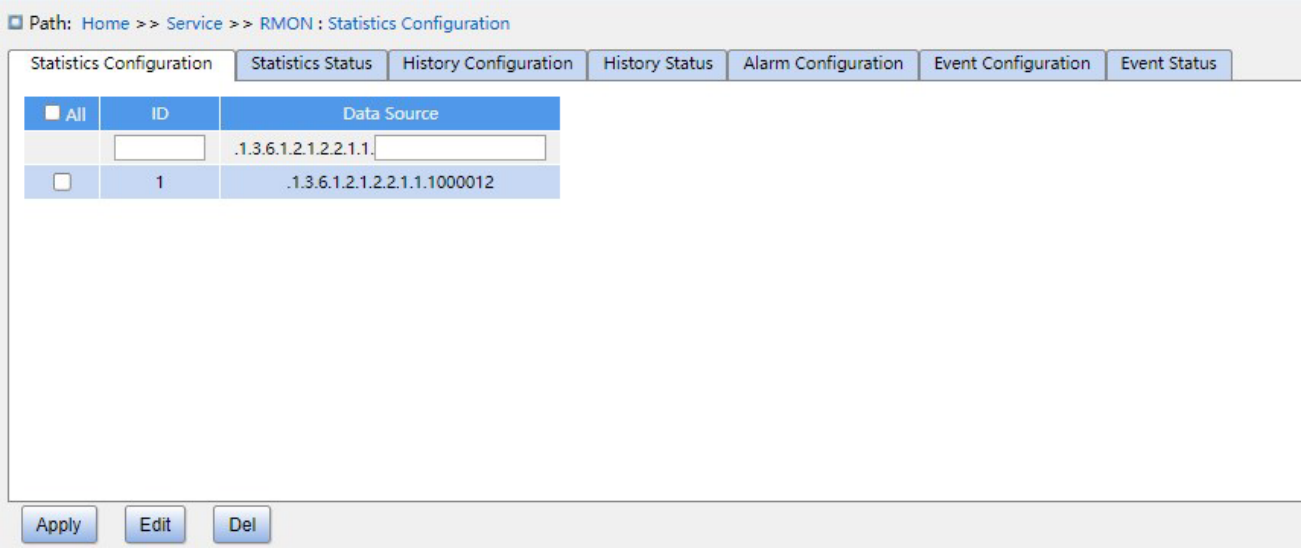


Рисунок 74 Настройка таблицы статистики RMON

ID

Диапазон настройки: 1~65535

Функция: Настройка номера записи статистики. Группа статистики поддерживает до 128 записей.

Data Source

Диапазон настройки: 10000portid

Функция: Выбор порта для сбора статистики.

2. Просмотрите статус группы статистики, как показано ниже.

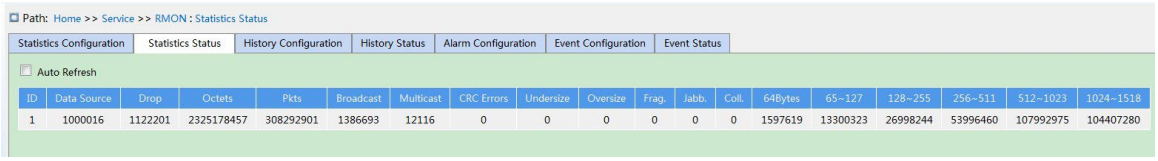


Рисунок 75 Статус группы статистики Drop:

количество пакетов, отброшенных портом.

Octets: количество байтов, полученных портом.

Pkts: количество пакетов, полученных портом.

Broadcast: количество широковещательных пакетов, полученных портом.

Multicast: количество многоадресных пакетов, полученных портом.

CRC Errors: количество пакетов с ошибками 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 ошибками CRC размером менее 64 байт, полученных портом.

Jabb.: количество пакетов ошибок 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.

Примечание:
Значение oversize зависит от параметра Maximum Frame Size в настройке порта, как показано в 7.1 Настройка порта. В примере выше значение oversize 9600 байт.

3. Настройте таблицу истории, как показано ниже.

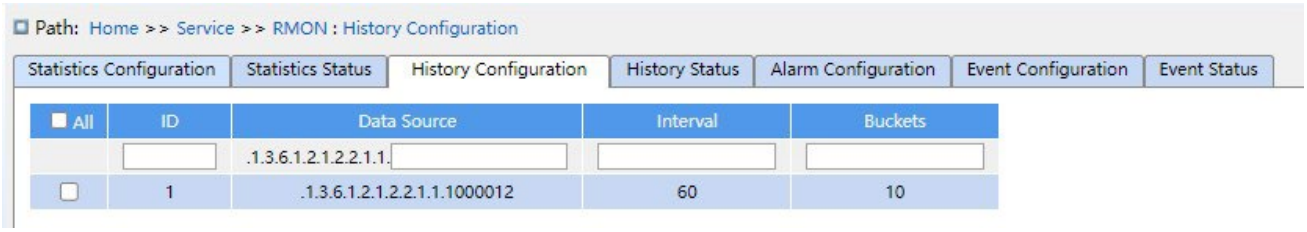


Рисунок 76 Настройка таблицы истории

ID

Диапазон настройки: 1~65535

Функция: Настройка номера записи истории. Группа истории поддерживает до 256 записей.

Data Source

Формат: 100000portid

Функция: Выбор порта для сбора информации.

Interval

Диапазон настройки: 1~3600 с

Функция: Настройка периода выборки для порта.

Buckets

Диапазон настройки: 1~65535

Конфигурация по умолчанию: 50

Функция: Настройка количества последних значений выборки информации о порте, хранящейся в RMON.

4. Просмотрите статус группы истории, как показано ниже.

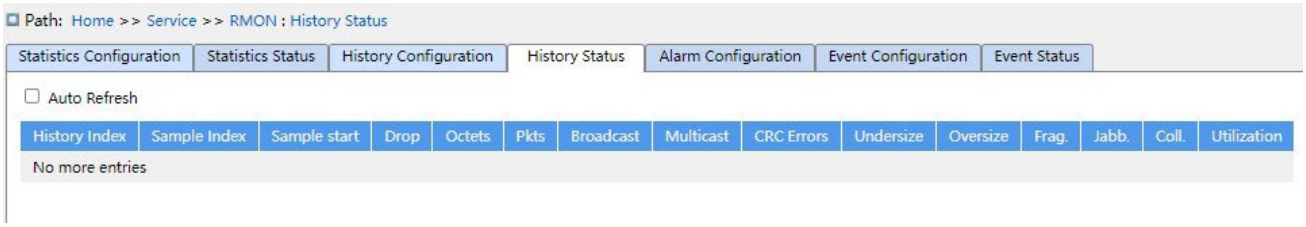


Рисунок 77 Просмотр статуса группы истории

5. Настройте таблицу событий, как показано ниже.

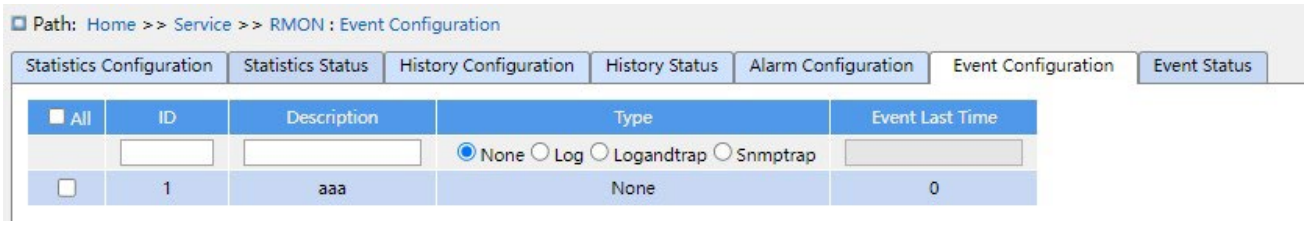


Рисунок 78 Настройка таблицы событий

ID

Диапазон настройки: 1~65535

Функция: Настройка порядкового номера записи событий. Группа событий поддерживает до 128 записей.

Описание

Диапазон настройки: 1~127 символов

Функция: Описание события.

Type

Варианты конфигурации: none/log/snmptrap/logandtrap

Конфигурация по умолчанию: none

Функция: Настройка типа события для сигналов тревоги, то есть режима обработки сигналов тревоги.

Event Last Time

Функция: Отображает значение sysUpTime, когда событие использовалось в последний раз.

6. Просмотрите статус группы событий, как показано ниже.

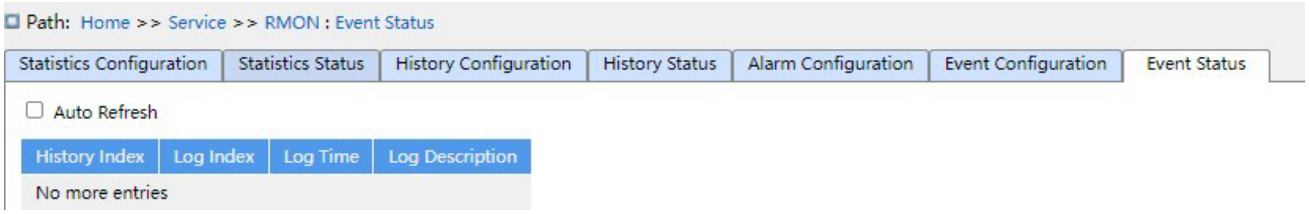


Рисунок 79 Просмотр статуса группы событий

7. Настройте таблицу сигналов тревоги, как показано ниже.

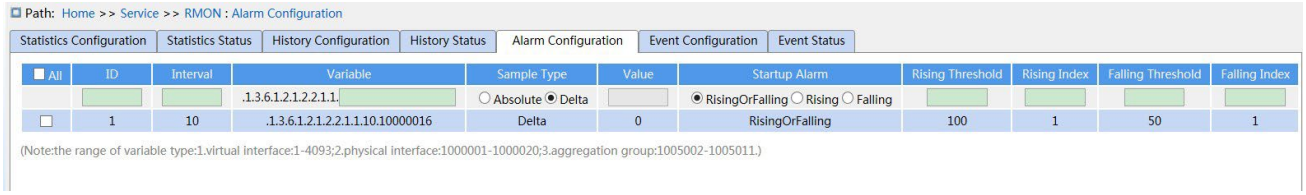


Рисунок 80 Настройка таблицы сигналов тревоги

ID

Диапазон настройки: 1~65535

Функция: Настройка номера записи сигнала тревоги. Группа сигналов тревоги поддерживает до 256 записей.

Interval

Диапазон настройки: 1~2147483647 с

Функция: Настройка периода выборки.

Variable

Формат: A.10000portid

Диапазон настройки: A：10~21

Функция: Выбор информации MIB порта для мониторинга.

InOctets: A=10, количество байтов, 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 с ошибками, полученных портом.

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

OutOctets: A=16, количество байтов, 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 с ошибками, отправленных портом.

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

Sample Type

Варианты конфигурации: Absolute/Delta

Конфигурация по умолчанию: Delta

Функция: выбор метода сравнения значения выборки и порога.

Описание: Absolute: прямое сравнение каждого значения выборки с пороговым значением; Delta: значение выборки минус предыдущее значение выборки, затем разница используется для сравнения с порогом.

Startup Alarm

Варианты конфигурации: Rising/Falling/Rising or Falling

Конфигурация по умолчанию: Rising or Falling

Функция: выбор типа сигнала тревоги.

Rising Threshold

Диапазон настройки: 1~2147483647

Функция: Задание порога повышения. Когда значение выборки превышает порог повышения и типом тревоги является Rising Alarm или RisOrFallAlarm, срабатывает тревога и активируется индекс событий повышения.

Rising Index

Диапазон настройки: 1~65535

Функция: Задание индекса события повышения. Это способ обработки сигнала тревоги при повышении значения.

Falling Threshold

Диапазон настройки: 1~2147483647

Функция: Задание порога понижения. Когда значение выборки ниже порога понижения и типом тревоги является Falling Alarm или RisOrFallAlarm, срабатывает тревога и активируется индекс событий понижения.

Falling Index

Диапазон настройки: 1~65535

Функция: Задание индекса события понижения. Это способ обработки сигнала тревоги при понижении значения.

6 Аварийная сигнализация

6.1 Введение

Коммутаторы этой серии поддерживают следующие типы аварийной сигнализации:

- Аварийная сигнализация по электропитанию: Если функция включена, то для отдельного источника питания будет генерироваться аварийный сигнал.
- Аварийная сигнализация по конфликту IP/MAC Если функция включена, то будет генерироваться аварийный сигнал при возникновении конфликта IP/MAC-адресов.
- Аварийная сигнализация по использованию памяти/ЦП. Если эта функция включена, аварийный сигнал генерируется, когда использование ЦП/памяти превышает указанный порог.
- Аварийная сигнализация по порту: Если эта функция включена, аварийный сигнал генерируется, когда порт находится в состоянии Link Down.
- Аварийная сигнализация по трафику порта: Если эта функция включена, аварийный сигнал генерируется, когда скорость входящего/исходящего трафика порта превышает указанный порог.

6.2 Настройка через веб-интерфейс

1. Основные аварийные сигналы показаны ниже.

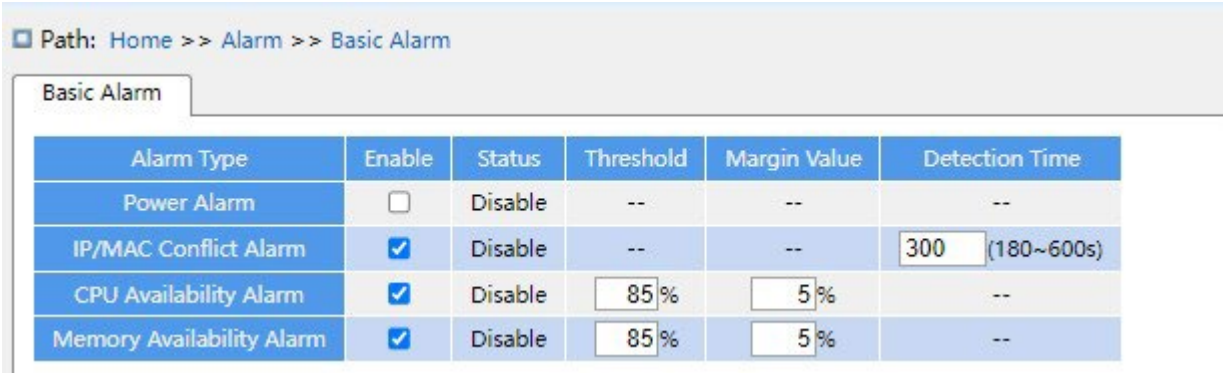


Рисунок 81 Основные аварийные сигналы

Power Alarm

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение/выключение аварийной сигнализации по питанию.

Status

Варианты конфигурации: Normal/Alarm

Функция: Просмотр состояния аварийной сигнализации по питанию.

Alarm: Для изделий с резервным питанием: один из модулей питания выходит из строя или работает ненормально, срабатывает аварийный сигнал.

Normal: Для изделий с одним источником питания: модуль питания работает нормально; для изделий с резервным питанием: два модуля питания работают нормально.

IP, MAC Conflict

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Enable

Функция: Включение/выключение аварийной сигнализации по конфликту IP/MAC.

Status

Варианты конфигурации: Conflict / No Conflict

Описание: Когда возникает конфликт IP/MAC, отображается Conflicts; в противном случае отображается No Conflicts.

Check Time

Диапазон настройки: 180~600 с

Конфигурация по умолчанию: 300 с

Функция: Настройка интервала времени для обнаружения конфликтов IP/MAC.

CPU/Memory Availability Alarm

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Enable

Функция: Включение/выключение сигнализации по доступности процессора/памяти

Threshold (%)

Диапазон настройки: 50~100

Конфигурация по умолчанию: 85

Функция: Задание порога использования памяти/ЦП. Когда использование ЦП/памяти коммутатора превышает пороговое значение, генерируется аварийный сигнал.

Margin Value (%)

Диапазон настройки: 1~20

Конфигурация по умолчанию: 5

Функция: Задание порога использования ЦП/памяти.

Описание: Если использование ЦП/памяти колеблется около порогового значения, аварийные сигналы могут генерироваться и сбрасываться неоднократно. Чтобы предотвратить это явление, можно указать значение допуска (по умолчанию 5 %). Аварийный сигнал будет сброшен только в том случае, если использование ЦП/памяти ниже порогового значения на величину допуска или более. Например, пороговое значение использования памяти равно 60 %, а значение допуска равно 5 %. Если использование памяти коммутатора меньше или равно 60 %, аварийный сигнал не генерируется. Если использование памяти превышает 60%, будет сгенерирован сигнал тревоги. Аварийный сигнал будет сброшен только в том случае, если использование памяти равно или ниже 55%.

2. Настройте и отобразите аварийную сигнализацию по порту, как показано ниже.

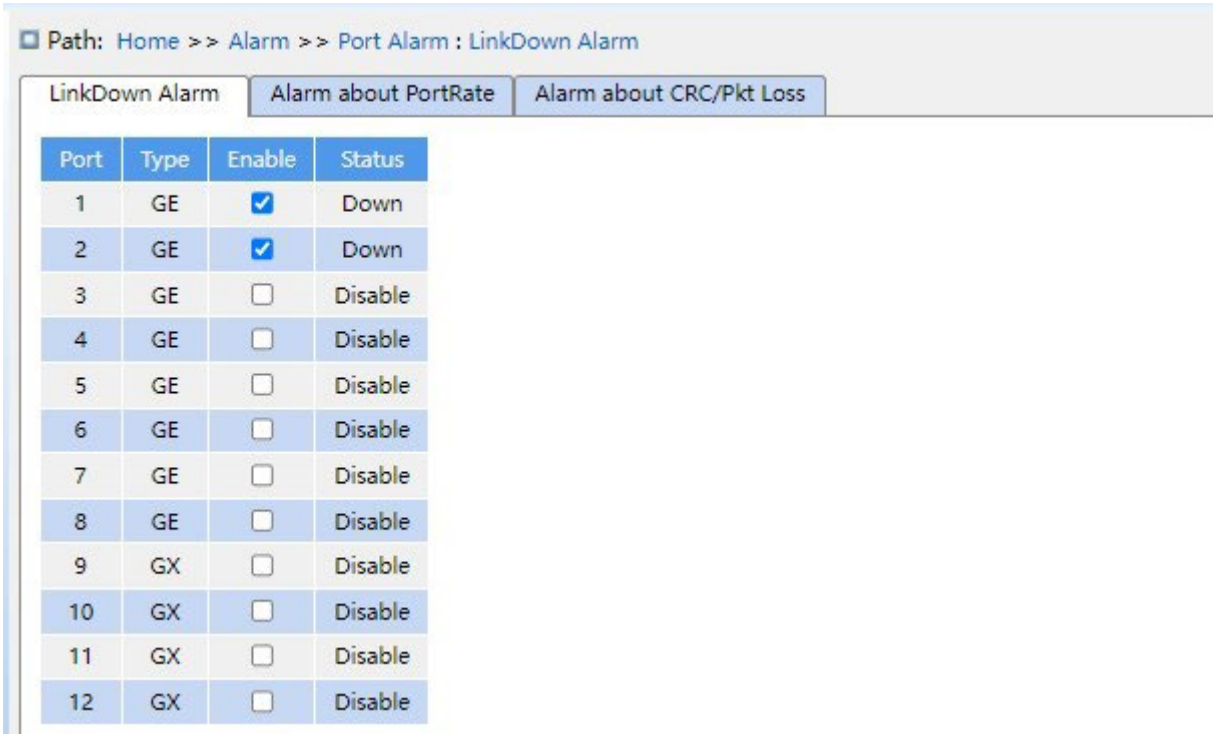


Рисунок 82 Аварийная сигнализация по порту

Настройки аварийной сигнализации по порту

Варианты конфигурации: Disable/Enable

Конфигурация по умолчанию: Disable

Функция: Включение/выключение аварийной сигнализации по порту.

Status

Варианты конфигурации: Link up/ Link down

Описание: Link Up означает, что порт находится в состоянии подключения и поддерживает нормальный обмен данными. Link Down означает, что порт отключен или находится в ненормальном состоянии (сбой обмена данными).

3. Настройте и отобразите аварийную сигнализацию по трафику порта, как показано ниже.

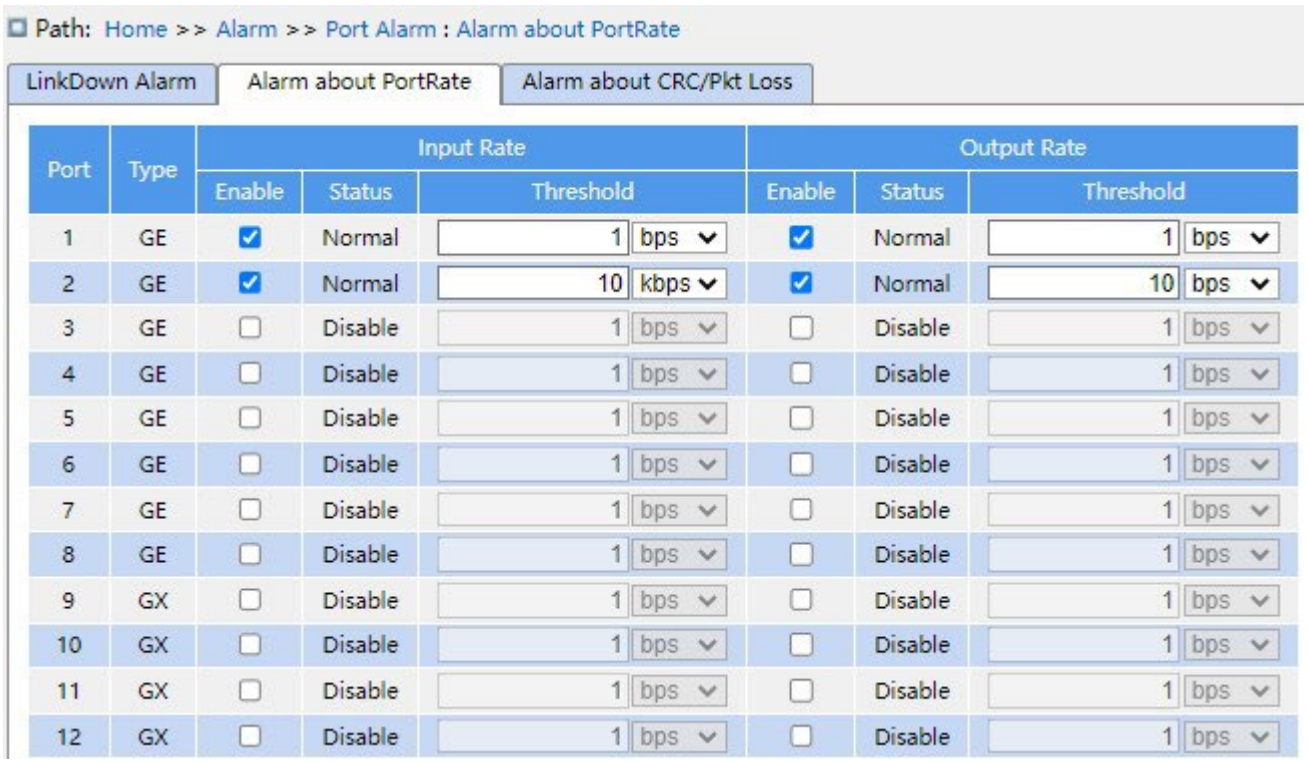


Рисунок 83 Настройка аварийной сигнализация по трафику порта

input rate alarm/output rate alarm

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение/выключение аварийной сигнализации по трафику порта.

Threshold

Диапазон настройки: от 1 до 1000000000 bps или от 1 до 1000000 kbps.

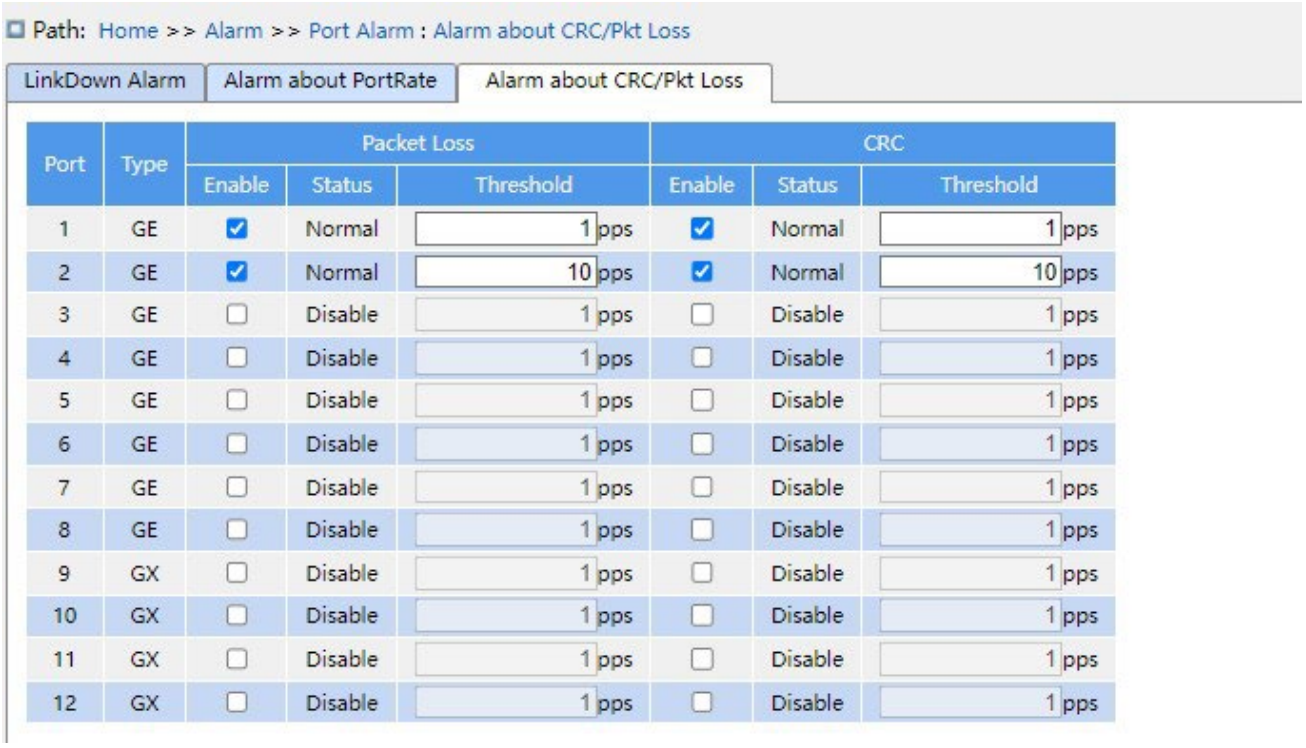
Функция: Задание порогового значения для трафика порта.

Alarm Status

Варианты конфигурации: Disable/Alarm/ Normal

Функция: Просмотр состояния трафика порта. Alarm означает, что входящий/исходящий трафик превышает пороговое значение и вызывает сигнал тревоги.

4. Настройте и отобразите аварийную сигнализацию по CRC и потере пакетов, как показано ниже.



Port	Type	Packet Loss			CRC		
		Enable	Status	Threshold	Enable	Status	Threshold
1	GE	☑	Normal	1 pps	☑	Normal	1 pps
2	GE	☑	Normal	10 pps	☑	Normal	10 pps
3	GE	☐	Disable	1 pps	☐	Disable	1 pps
4	GE	☐	Disable	1 pps	☐	Disable	1 pps
5	GE	☐	Disable	1 pps	☐	Disable	1 pps
6	GE	☐	Disable	1 pps	☐	Disable	1 pps
7	GE	☐	Disable	1 pps	☐	Disable	1 pps
8	GE	☐	Disable	1 pps	☐	Disable	1 pps
9	GX	☐	Disable	1 pps	☐	Disable	1 pps
10	GX	☐	Disable	1 pps	☐	Disable	1 pps
11	GX	☐	Disable	1 pps	☐	Disable	1 pps
12	GX	☐	Disable	1 pps	☐	Disable	1 pps

Рисунок 84 Настройка аварийной сигнализации по CRC и потере пакетов

Аварийная сигнализация по CRC/потере пакетов

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение/выключение аварийной сигнализации по CRC и потере пакетов.

Threshold

Диапазон настройки: от 1 до 1000000 pps.

Функция: Задание порогового значения для аварийной сигнализации по CRC и потере пакетов для порта.

Alarm Status

Варианты конфигурации: Disable/Alarm/ Normal

Функция: Просмотр состояния аварийной сигнализации по CRC и потере пакетов для порта. Alarm означает, что CRC/потеря пакетов для порта превышает пороговое значение и вызывает сигнал тревоги.

6. Настройте и отобразите аварийную сигнализацию по кольцу, как показано ниже.

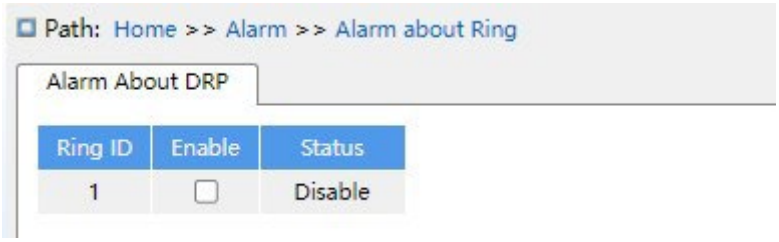


Рисунок 85 Настройка аварийной сигнализация по кольцу

Alarm About DRP

Варианты конфигурации: Disable/Enable

Конфигурация по умолчанию: Disable

Функция: Включение/выключение аварийной сигнализации DRP.

Alarm Status

Варианты конфигурации: Disable/Alarm/---

Функция: Просмотр состояния DRP. --- означает замыкание DRP. Alarm означает, что DRP разомкнуто или находится в ненормальном состоянии.

7. Настройте и отобразите аварийную сигнализацию по мощности RX порта SFP, как показано ниже.

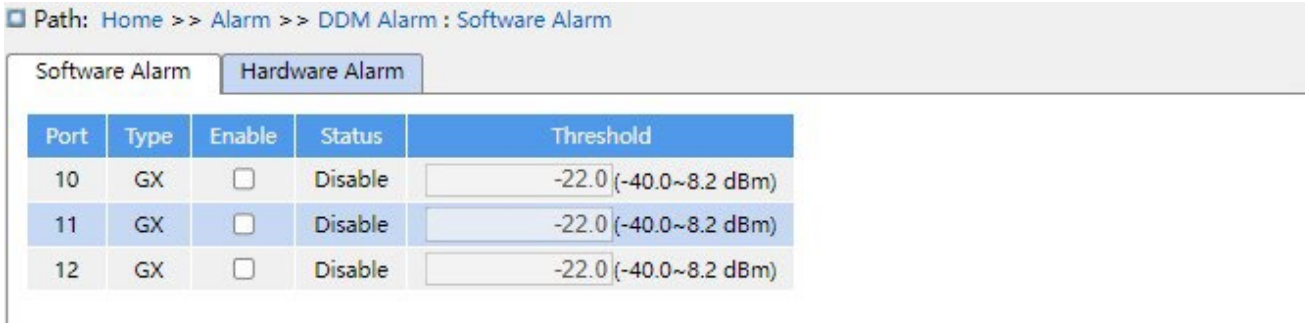


Рисунок 86 Аварийная сигнализация по мощности RX порта SFP

Software Alarm

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение аварийной сигнализации по мощности RX SFP.

Threshold

Диапазон: -40~8,2 (ед. изм: dBm)

По умолчанию: -22,0 dBm

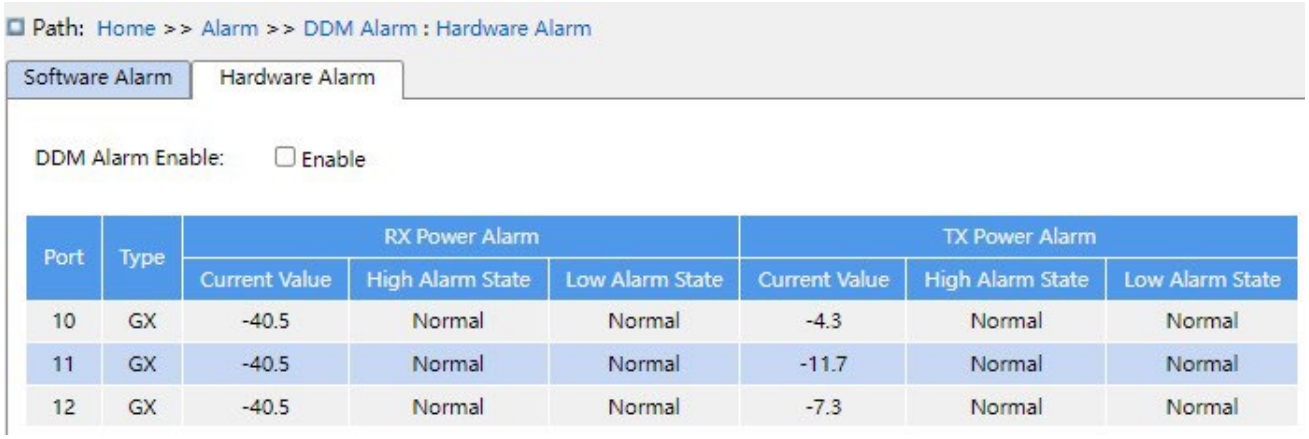
Функция: Настройка порогового значения для аварийной сигнализации по мощности порта RX SFP.

Alarm Status

Варианты: Normal/Alarm

Описание: После того, как функция включена, Alarm означает, что мощность Rx для порта SFP меньше указанного порога и вызывает тревогу.

8. Настройте и отобразите аварийную сигнализацию приемопередатчика, как показано ниже.



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

Рисунок 87 Настройка аварийной сигнализации приемопередатчика

DDM Alarm Enable

Варианты: Enable /Disable

По умолчанию: Disable

Функция: Включение/выключение аварийной сигнализации приемопередатчика. Аварийный сигнал о низком уровне оптической мощности генерируется, когда отслеживаемое значение оптической мощности на порту SFP меньше нижнего порога аварийного сигнала; тревога высокой оптической мощности генерируется, когда отслеживаемое значение оптической мощности на порту SFP превышает верхнее пороговое значение.

Предупреждение:
Нижний и верхний порог оптической мощности зависят от оборудования и не могут быть настроены программно.

7 Управление функциями

7.1 Настройка портов

1. Настройте состояние порта, скорость порта, управление потоком и другую информацию, как показано ниже.

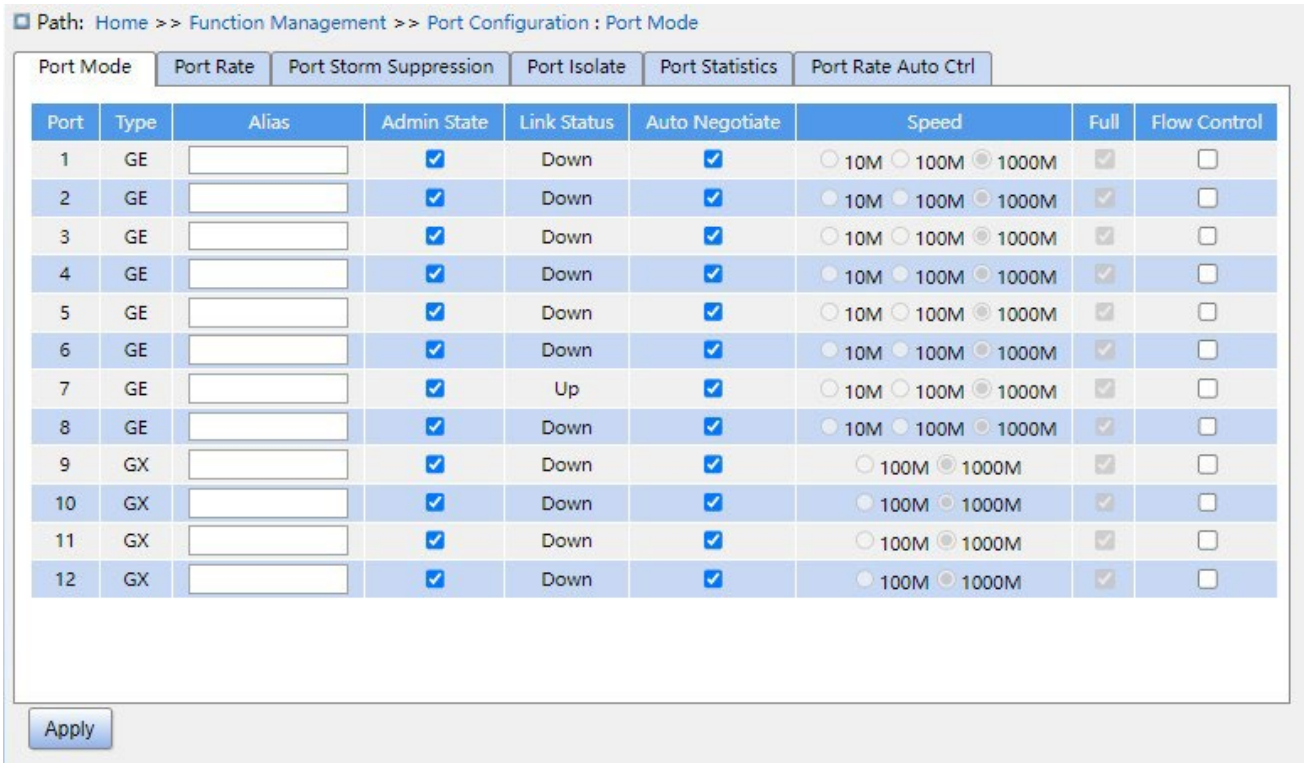


Рисунок 88 Настройка режима порта

Administration Status

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Enable

Функция: Разрешение передачи данных для порта.

Описание: Для значения enable порт открыт, для значения disable порт закрыт и данные не передаются. Эта опция напрямую влияет на аппаратное состояние порта и запускает аварийные сигналы порта.

Link Status

Просмотр состояния подключения порта.

Up означает, что порт находится в состоянии LinkUp и связь нормальная.

Down означает, что порт находится в состоянии LinkDown и связь нарушена.

Auto Negotiate

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Enable

Описание: Настройка скорости и дуплексного режима порта. Скорость и дуплексный режим порта могут согласовываться автоматически или принудительно. Скорость и дуплексный режим порта автоматически согласовываются в соответствии с состоянием соединения обоих портов, если настроен режим автоматического согласования. Пользователям рекомендуется настроить автоматическое согласование скорости и дуплексного режима порта, чтобы, насколько это возможно, избежать проблем с подключением, вызванных несоответствием конфигурации портов. Если пользователь принудительно настраивает для порта скорость и дуплексный режим, убедитесь, что настройки скорости соединения/дуплексного режима на обоих концах одинаковы.

Предупреждение:

- Для электрического порта 100M можно настроить автоматическое согласование, полный дуплекс 10M, полудуплекс 10M, полный дуплекс 100M, полудуплекс 100M.
- Для гигабитного электрического порта можно настроить автоматическое согласование, полный дуплекс 10M, полудуплекс 10M, полный дуплекс 100M и 1000M.

Speed

Варианты конфигурации: 10M/100M или 10M/100M/1000M

Функция: Настройка автосогласования скорости порта.

Описание: При настройке режима порта на автоматическое согласование скорость порта по умолчанию определяется посредством автосогласования с противоположным концом. Согласованная скорость может быть любой в пределах диапазона скоростей порта. Настраивая скорость, порт может согласовывать только частичную скорость, таким образом контролируя согласование скорости.

Предупреждение:
Конфигурацию дуплекса и скорости можно настроить только при отключенном режиме автосогласования.

Full

Варианты конфигурации: Enable/Disable

Функция: Настройка дуплексного режима автосогласования.

Описание: полнодуплексный режим означает, что порт может получать данные во время отправки данных; полудуплексный порт может только либо отправлять, либо получать данные в любой момент времени. Когда для режима порта установлено автосогласование, дуплексный режим порта по умолчанию определяется путем согласования со сквозным соединением. Согласованный дуплексный режим может быть либо полнодуплексным, либо полудуплексным. При настройке дуплекса порт может согласовывать только один дуплексный режим, тем самым контролируя согласование дуплексного режима.

Flow Control

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение или выключение управления потоком.

Описание: после включения управления потоком порта, в случае, когда порт получает больше трафика, чем максимальное значение, которое может храниться в кэше порта, порт сообщит отправляющей стороне о снижении скорости отправки, чтобы предотвратить потерю пакетов в соответствии с алгоритмом или протоколом. Для полудуплексного и полнодуплексного режимов управление потоком осуществляется по-разному. В полнодуплексном режиме принимающая сторона информирует передающую сторону о прекращении отправки сообщения, отправляя специальный кадр данных (pause frame), после получения кадра паузы отправляющая сторона прекращает отправку сообщения в соответствии со временем ожидания в кадре. Полудуплексный режим поддерживает управление потоком противодавления, и принимающая сторона может намеренно создать коллизию или сигнал несущей. Когда

передающая сторона обнаружит коллизию или сигнал несущей, она использует алгоритм задержки передачи данных.

2. Настройте скорость порта, как показано ниже.

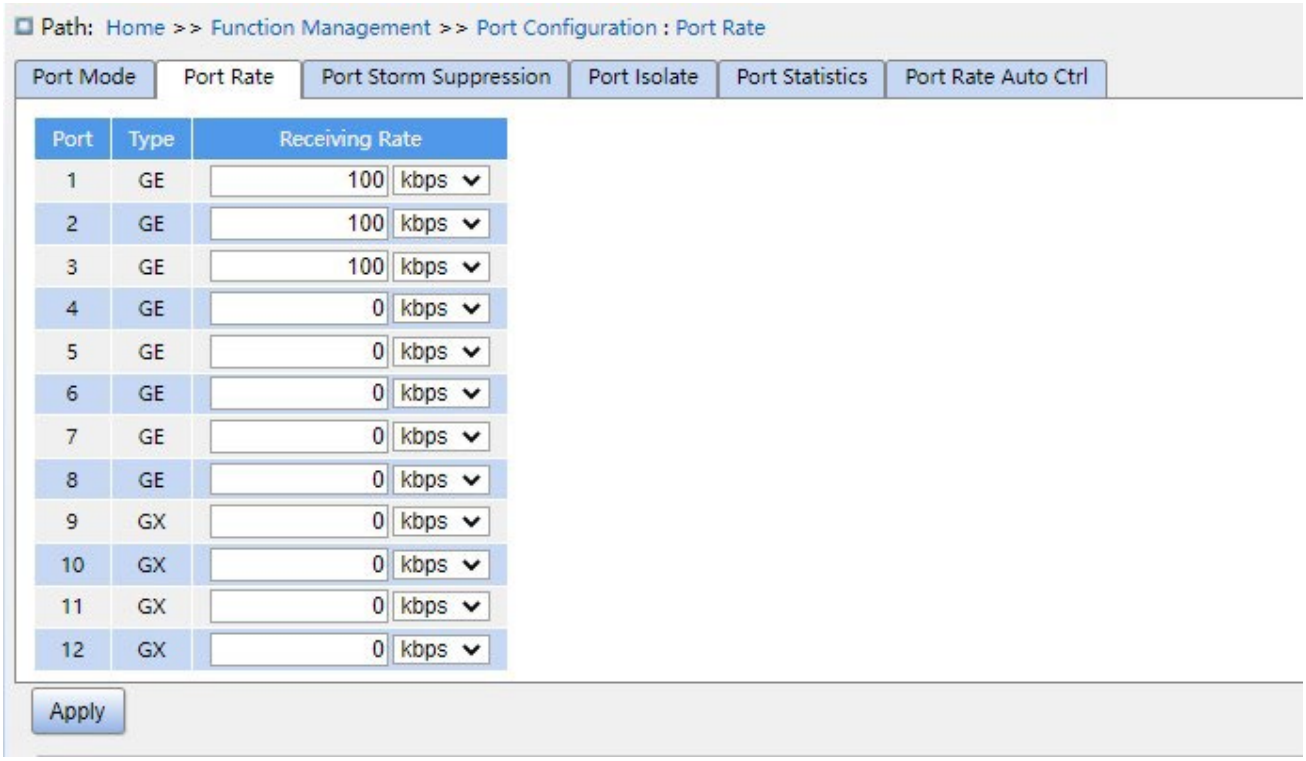


Рисунок 89 Скорость порта

Receiving Rate

Варианты настройки: 0/16~1000000 кбит/с / 1~1000 Мбит/с

Конфигурация по умолчанию: 0, Значение 0 означает отключение ограничения скорости.

Функция: настройка порогового значения скорости порта. Данные сообщения, превышающие пороговое значение, будут отброшены.

3. Настройка подавления штормов показана ниже.

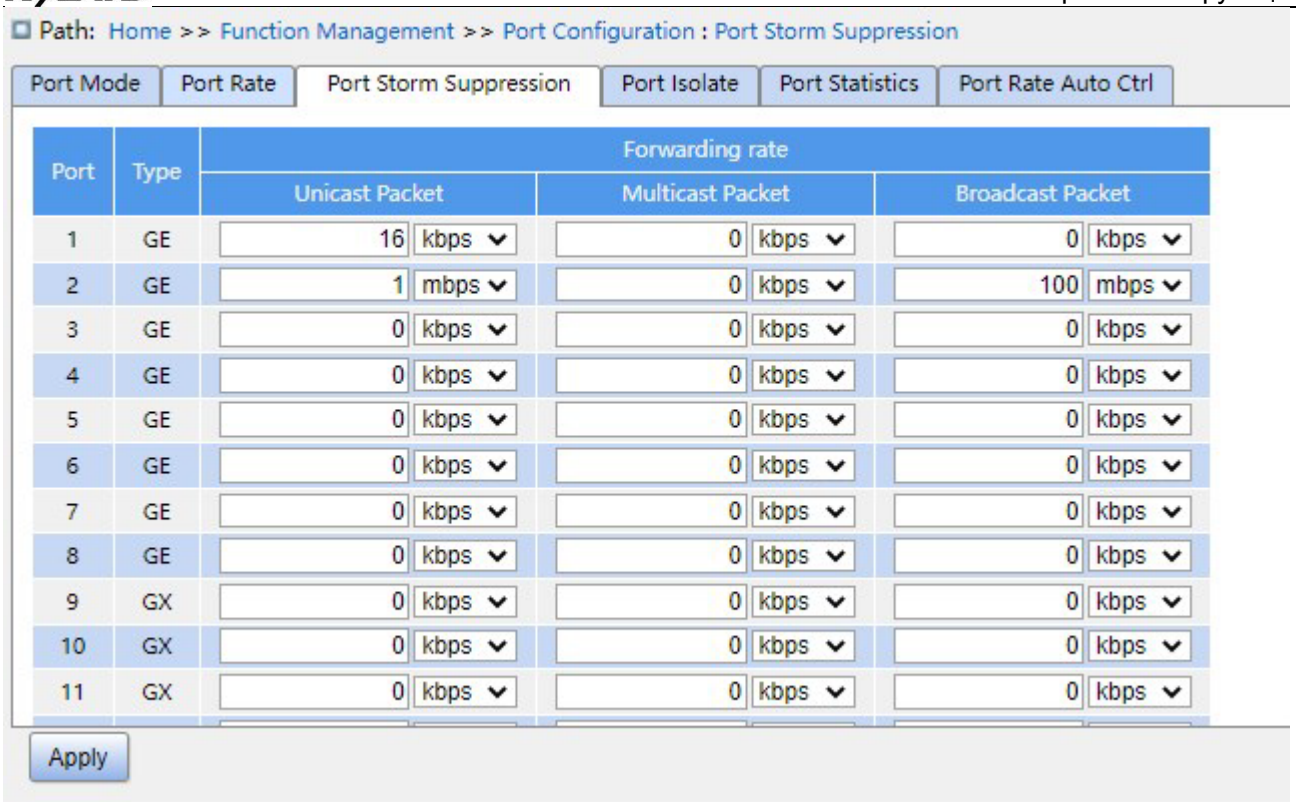


Рисунок 90 Подавление штормов

Forwarding Rate

Варианты конфигурации: Unicast Packet/Multicast Packet/Broadcast Packet

Диапазон настройки: 0/16~1000000 кбит/с / 1~1000 Мбит/с

Конфигурация по умолчанию: 0 (Подавление штормов отключено)

Функция: Настройка порога скорости переадресации портов, пакетные данные этого типа, превышающие пороговое значение, будут отброшены.

4. Настройка изоляции портов показана ниже.

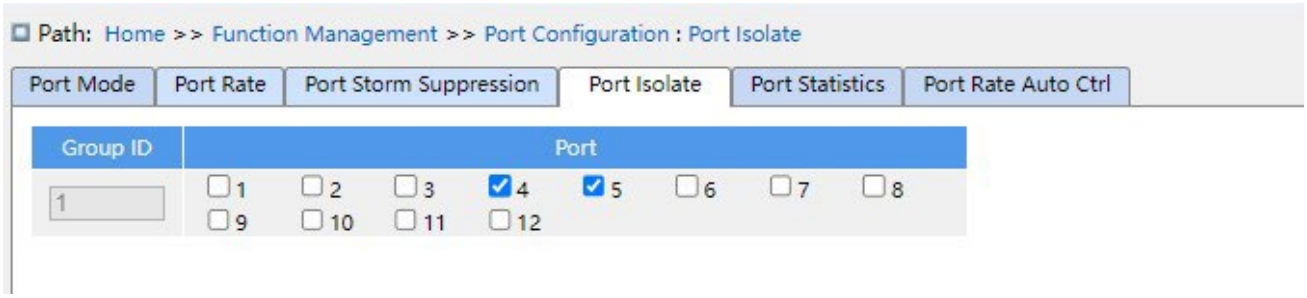


Рисунок 91 Изоляция портов

Enable Port Isolate

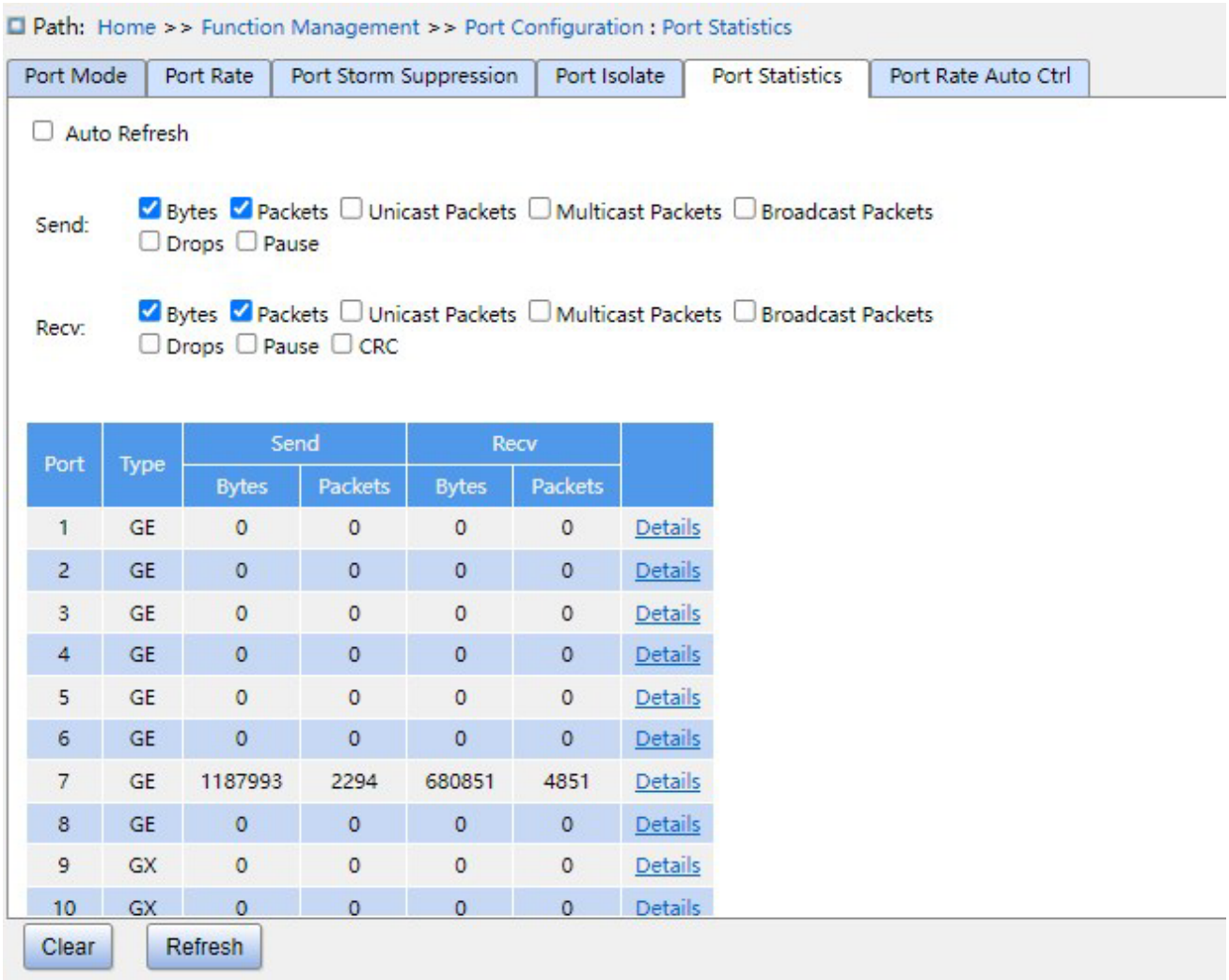
Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение или выключение изоляции портов.

Примечание: Есть только одна группа изоляции портов.

5. Статистика порта показана ниже.



Port	Type	Send		Recv		
		Bytes	Packets	Bytes	Packets	
1	GE	0	0	0	0	Details
2	GE	0	0	0	0	Details
3	GE	0	0	0	0	Details
4	GE	0	0	0	0	Details
5	GE	0	0	0	0	Details
6	GE	0	0	0	0	Details
7	GE	1187993	2294	680851	4851	Details
8	GE	0	0	0	0	Details
9	GX	0	0	0	0	Details
10	GX	0	0	0	0	Details

Рисунок 92 Статистика порта

Bytes

Подсчет количества полученных/отправленных байтов.

Packets

Подсчет количества полученных/отправленных пакетов.

Unicast Packets

Подсчет количества полученных/отправленных одноадресных пакетов.

Multicast Packets

Подсчет количества полученных/отправленных многоадресных пакетов.

Broadcast Packets

Подсчет количества полученных/отправленных широковещательных пакетов.

Drops

Подсчет количества сообщений, отброшенных из-за конфликтов приема/отправки.

Pause

Подсчет количества полученных/отправленных фреймов паузы.

CRC

Подсчет количества полученных/отправленных сообщений CRC.

Щелкните соответствующий номер порта, чтобы войти в интерфейс подробной статистики соответствующего порта.

6. Подробная статистика порта показана ниже.

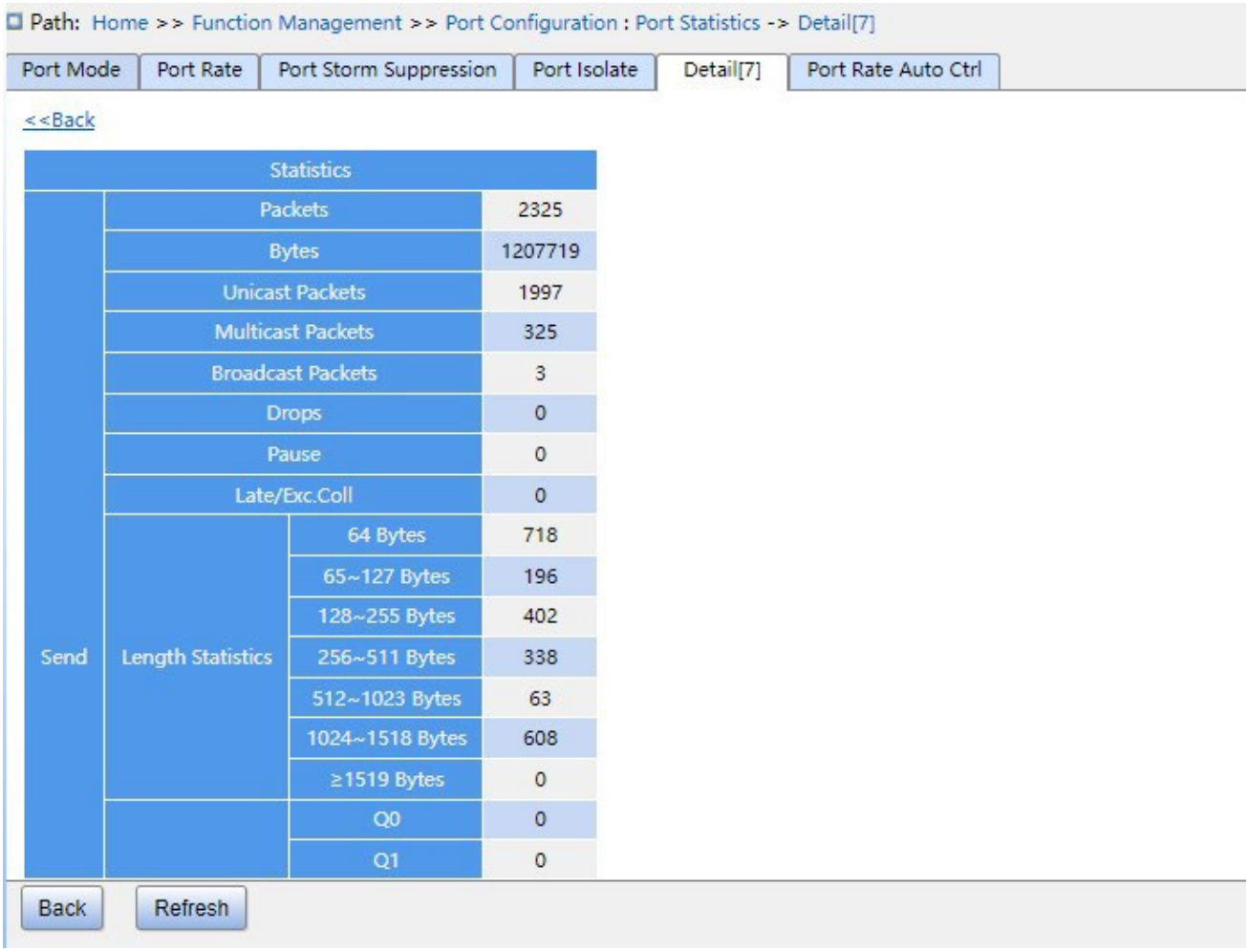


Рисунок 93 Подробная статистика порта

7. Автоматическое ограничение скорости порта показано ниже.

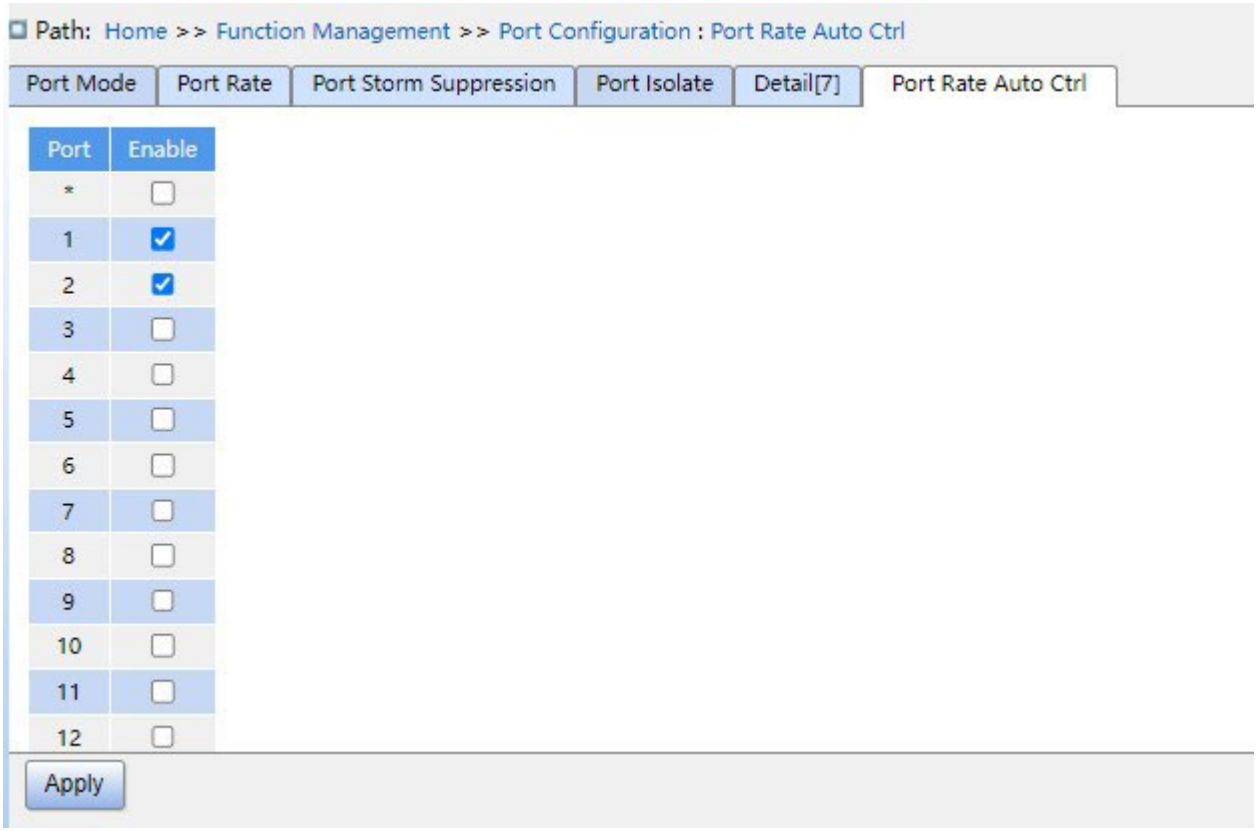


Рисунок 94 Автоматическое ограничение скорости порта

Port

Область действия настройки: все порты коммутатора.

Enable

Варианты конфигурации: enable/disable

Функция: Включение или выключение автоограничения скорости портов.

7.2 VLAN

7.2.1 Настройка VLAN

7.2.1.1 Введение

Одна локальная сеть может быть разделена на несколько логических виртуальных локальных сетей (VLAN). Устройство может обмениваться данными только с устройствами в той же VLAN. В результате широковещательные пакеты ограничиваются VLAN, что повышает безопасность LAN.

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

7.2.1.2 Принцип работы

Чтобы сетевые устройства могли различать пакеты из разных VLAN, в пакеты необходимо добавить поля для идентификации VLAN. В настоящее время для идентификации VLAN чаще всего используется протокол IEEE802.1Q. В таблице 2 показана структура кадра 802.1Q. Таблица 2 Структура кадра 802.1Q

DA	SA	Заголовок 802.1Q				Длина/тип	Данные	FCS
		TPID	PRI	CFI	VID			

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

TPID: 16 бит. Используется для идентификации кадра данных, несущего тег VLAN. Значение равно 0x8100.

Значение TPID, указанное в протоколе 802.1Q, равно 0x8100.

PRI: три бита, определяющие приоритет пакета 802.1p.

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

VID: 12 бит, обозначающих номер VLAN. Диапазон значений от 1 до 4093. 0, 4094 и 4095 являются зарезервированными значениями.

Прим

- VLAN 1 является VLAN по умолчанию, и ее нельзя создать или удалить вручную.
- Зарезервированные VLAN зарезервированы для реализации системой определенных функций и их нельзя создать или удалить вручную.

Пакет, содержащий заголовок 802.1Q, является тегированным пакетом; пакет без заголовка 802.1Q является нетегированным пакетом. Все пакеты, передаваемые коммутатором, содержат тег 802.1Q.

7.2.1.3 VLAN на основе порта

Раздел VLAN может быть либо на основе порта, либо на основе MAC-адреса. Коммутаторы этой серии поддерживают разделы VLAN на основе порта. Участники VLAN могут быть определены на основе портов коммутатора.

После добавления порта в указанную VLAN порт может пересылать пакеты с тегом для VLAN.

1. Режим порта

Порты делятся на два типа в зависимости от того, как они обрабатывают теги VLAN при пересылке пакетов. Access: В режиме Access порт можно добавить только в одну VLAN. По умолчанию все порты коммутатора являются портами в режиме Access и принадлежат VLAN1. Пакеты, пересылаемые портом в режиме Access, не имеют тегов VLAN. Порты в режиме Access обычно используются для подключения к терминалам, не поддерживающим 802.1Q.

Trunk：В режиме Trunk порт можно добавить в несколько VLAN. При отправке пакетов PVID для порта в режиме Trunk можно указать, следует ли передавать тег. Он передает тег при отправке других пакетов. Порты в режиме Trunk обычно используются для подключения сетевых передающих устройств. Hybrid：В режиме Hybrid порт можно добавить в несколько VLAN. Можно указать тип пакетов, которые должны быть получены портом в режиме Hybrid, и указать, передается ли тег, когда порт в режиме Hybrid отправляет пакеты. Порт в режиме Hybrid можно использовать для подключения сетевых устройств и пользовательских устройств. Разница между портом в режиме Hybrid и портом в режиме Trunk заключается в следующем: Порт в режиме Hybrid не передает тег при отправке пакетов из нескольких VLAN, а порт в режиме Trunk не передает 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.

Предупреждение:

- При настройке PVID порта выберите один из идентификаторов VLAN, разрешенных для порта; в противном случае порт может не пересылать пакеты.
- Когда тег PVID добавляется к нетегированным пакетам, можно обратиться к настройкам PCP и DEI на рисунке 214 для значений PRI и CFI по умолчанию для порта.

Таблица 3 показывает, 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>Нетегированные пакеты</th><th>Тегированные пакеты</th><th>Режим порта</th><th>Обработка пакетов</th></tr>
<tr><td rowspan="2">Добавить теги PVID в пакеты:
➢ Если PVID находится в списке разрешенных VLAN, принять пакет.
➢ Если PVID не находится в списке разрешенных VLAN, отклонить пакет.</td><td rowspan="2">➢ Если VLAN ID в пакете находится в списке разрешенных VLAN, принять пакет.
➢ Если VLAN ID в пакете не находится в списке разрешенных VLAN, отклонить пакет.</td><td>Access</td><td>Переслать пакет после удаления тега.</td></tr>
<tr><td>Trunk</td><td>Переслать пакет в соответствии с конфигурацией Egress Tagging:
➢ Untag порт VLAN: Если VLAN ID в пакете совпадает с PVID и находится в списке разрешенных VLAN, перенаправить пакет после удаления тега. Если VLAN ID в пакете отличается от PVID и в списке разрешенных VLAN, сохранить тег и перенаправить пакет.
➢ Tag All: Если VLAN ID в пакете находится в списке разрешенных VLAN, сохранить тег и перенаправить пакет.</td></tr>
</table>

		Hybrid	Переслать пакет в соответствии с конфигурацией Egress Tagging: ➢ Untag Port VLAN: как указано выше. ➢ Tag All: как указано выше. ➢ Untag All: Если VLAN ID в пакете находится в списке разрешенных VLAN, переслать пакет после удаления тега.

7.2.1.4 Настройка через веб-интерфейс

1. Настройте для порта режим обработки пакетов, как показано ниже

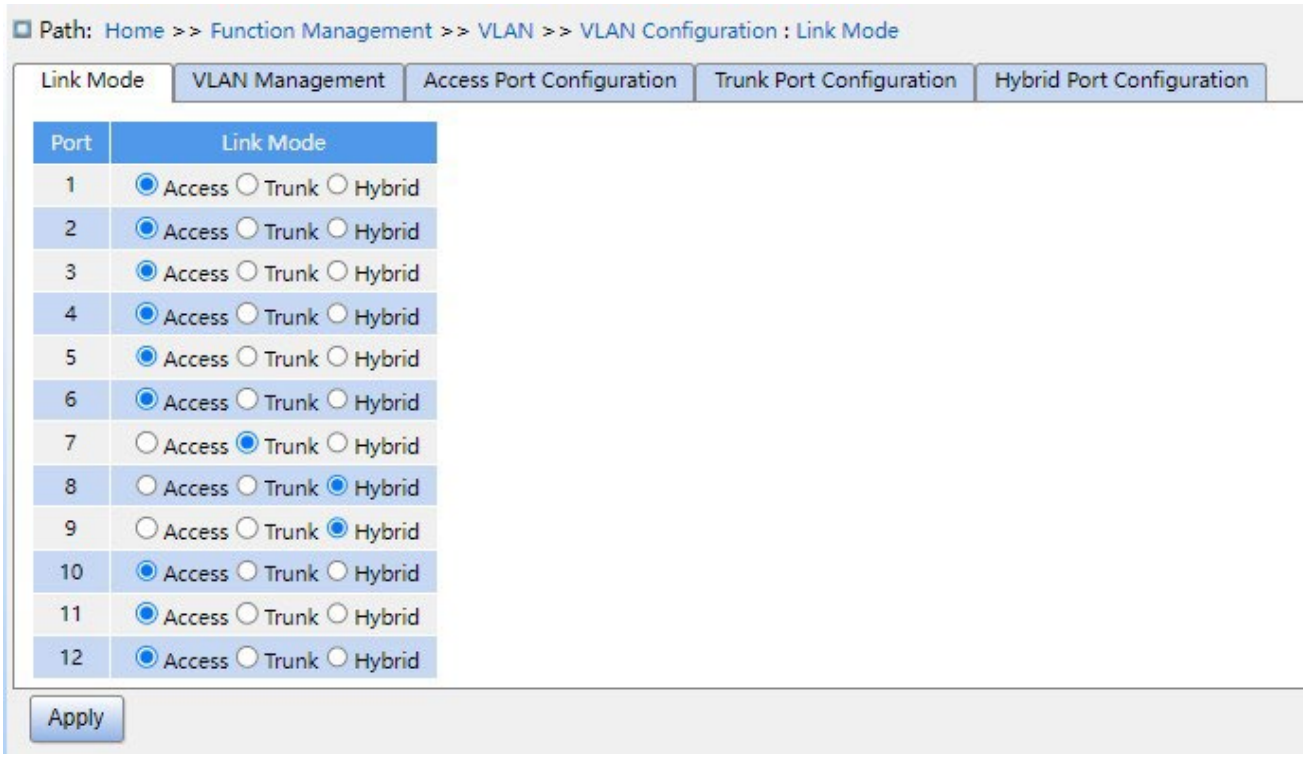


Рисунок 95 Настройка режима обработки пакетов для порта

Link Mode

Варианты конфигурации: Access / Trunk / Hybrid

Конфигурация по умолчанию: Access

Функция: Настройка режима обработки пакетов для указанного порта.

2. Управление VLAN показано ниже.

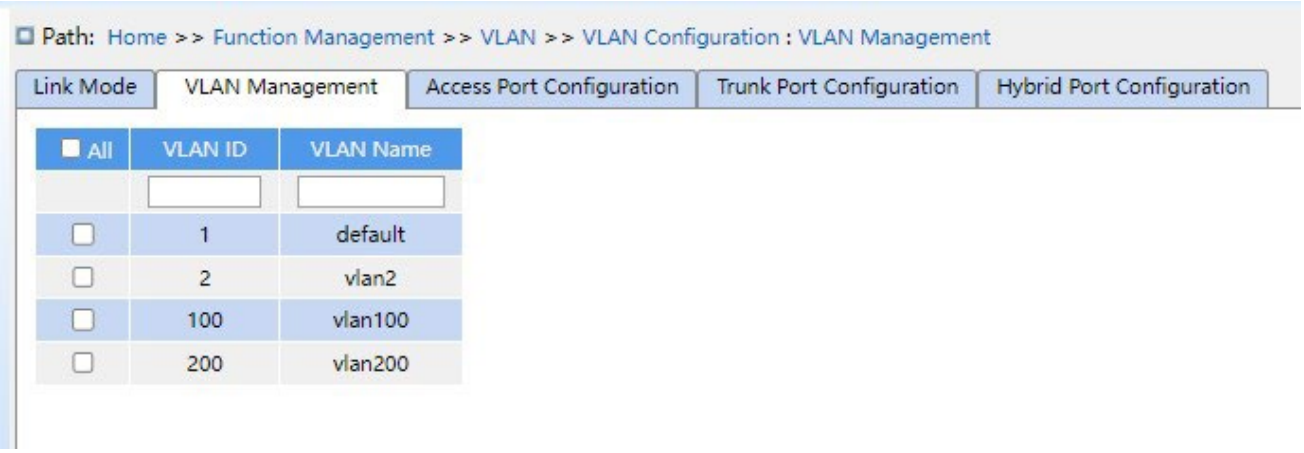


Рисунок 96 Управление VLAN

VLAN ID

Диапазон настройки: 1-4094

Конфигурация по умолчанию: 1

Функция: Создание VLAN.

VLAN Name

Диапазон настройки: 1-32 символа, включая заглавные буквы, строчные буквы, цифры и знак подчеркивания.

Функция: Настройка имени VLAN

3. Настройка порта доступа показана ниже.

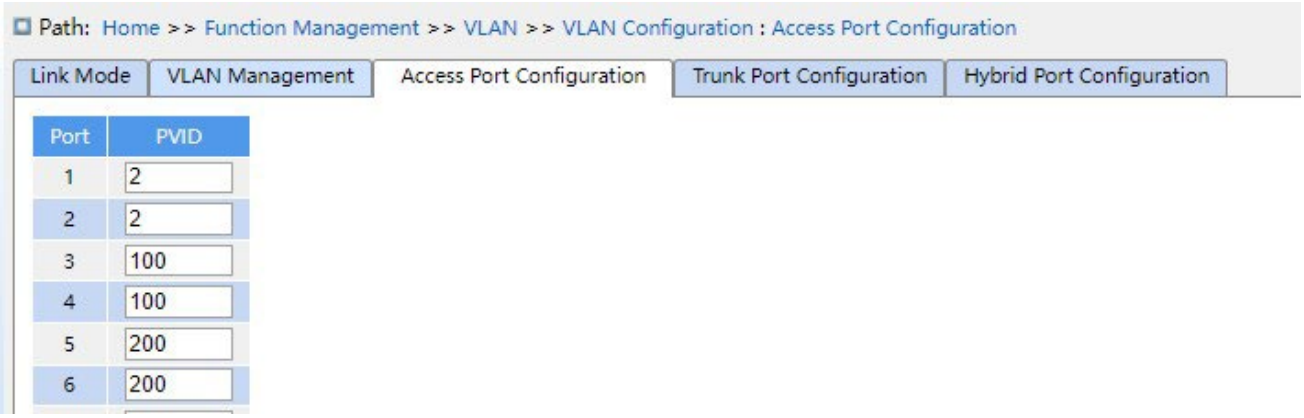


Рисунок 97 Настройка порта доступа

PVID

Диапазон настройки: 1-4094

Конфигурация по умолчанию: 1

Функция: Настройка VLAN по умолчанию для порта доступа.

Предупреждение:

VLAN необходимо создать перед настройкой идентификатора VLAN порта доступа, магистральный и гибридный порт аналогичны.

4. Конфигурация порта Trunk показана ниже.

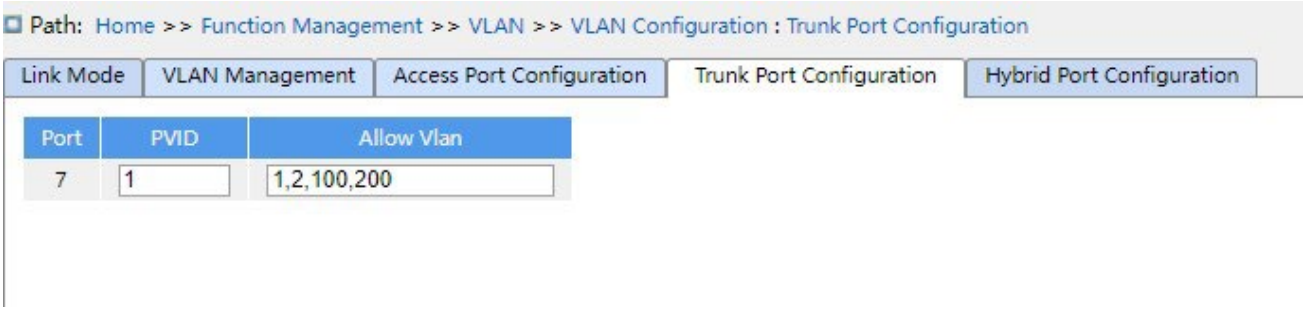


Figure 98 Настройка порта Trunk

PVID

Диапазон настройки: 1-4094

Конфигурация по умолчанию: 1

Функция: Настройка VLAN по умолчанию порта Trunk.

Allowed VLAN

Диапазон настройки: 1-4094, разделенные запятой (ASCII) ',' и дефисом '-“ (M-N，M должно быть меньше N), например: 2, 33, 34-77.

Конфигурация по умолчанию: 1

Функция: Настройка разрешенной VLAN порта Trunk.

5. Конфигурация гибридного порта показана ниже.

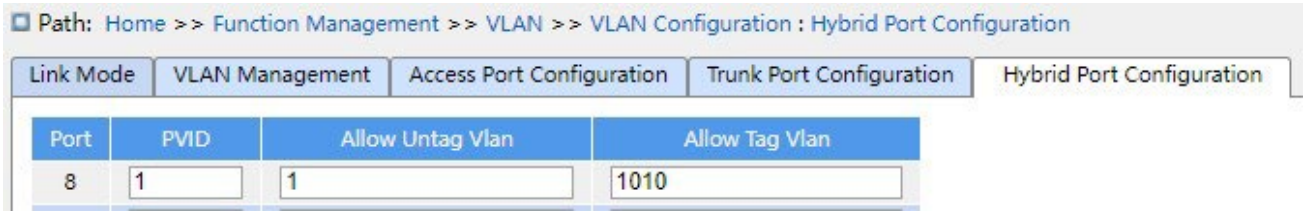


Рисунок 99 Настройка гибридного порта

PVID

Диапазон настройки: 1-4094

Конфигурация по умолчанию: 1

Функция: Настройка VLAN по умолчанию гибридного порта.

Allowed Untag VLAN

Диапазон настройки: 1-4094, разделенные запятой (ASCII) ',' и дефисом '-“ (M-N，M должно быть меньше N), например: 2,33,34-77.

Конфигурация по умолчанию: 1

Функция: Настройка разрешенного нетегированной VLAN гибридного порта.

Allowed Tag VLAN

Диапазон настройки: 1-4094, разделенные запятой (ASCII) ',' и дефисом '-“ (M-N，M должно быть меньше N), например: 2,33,34-77.

Конфигурация по умолчанию: None

Функция: Настройка разрешенного тегированной VLAN гибридного порта.

7.2.1.5 Пример типовой конфигурации

Как показано на рисунке 100, сеть разделена на 3 VLAN: VLAN2, VLAN100 и VLAN200. Требуется, чтобы устройства в одной VLAN могли осуществлять обмен данными друг с другом, но разные VLAN были изолированы. Терминальные ПК не могут различать тегированные пакеты, поэтому порты, соединяющие коммутатор A и коммутатор B с ПК, настроены на порт Access. Пакеты VLAN2, VLAN100 и VLAN200 должны передаваться между коммутатором A и коммутатором B, поэтому порты, соединяющие коммутатор A и коммутатор B, должны быть настроены на порт Trunk, что позволит пропускать пакеты VLAN 2, VLAN 100 и VLAN 200. В таблице 4 показана конкретная конфигурация.

Таблица 4 Конфигурация VLAN

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

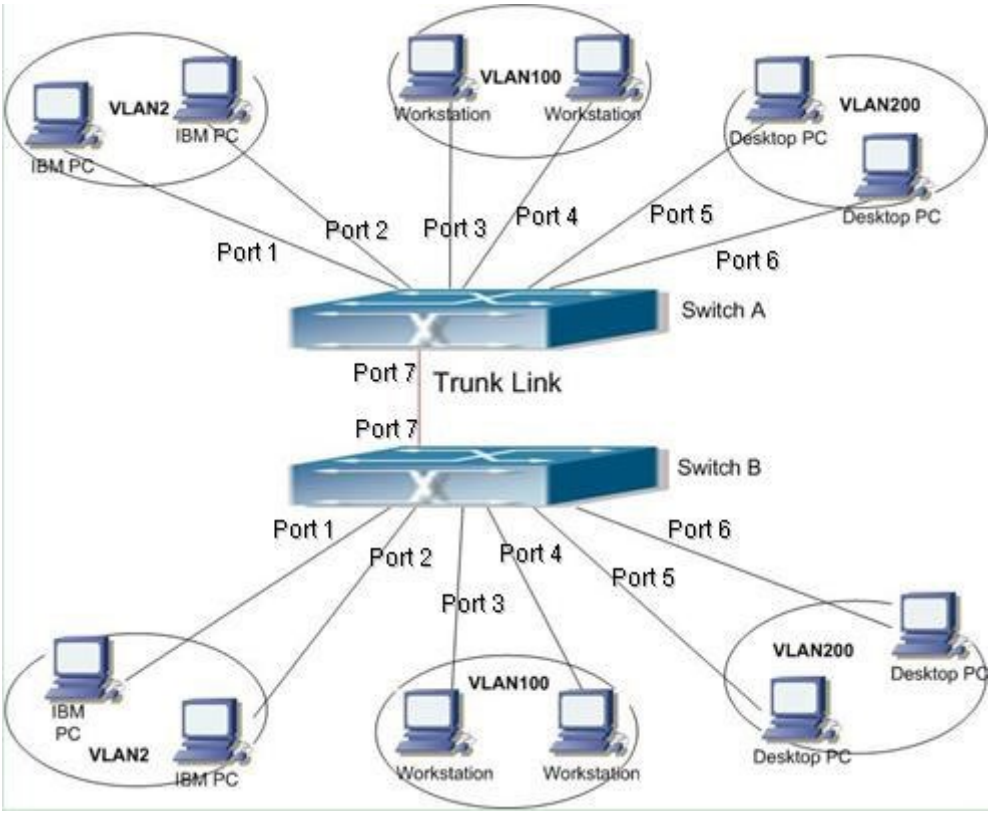


Рисунок 100 Использование VLAN

Конфигурация коммутатора A и коммутатора B:

1. Настройте VLAN с разрешенным доступом 1,2,100,200, как показано на рисунке 97.
2. Настройте порты 1, 2 как порты Access, порт VLAN как 2. Настройте порты 3, 4 как порты Access, порт VLAN как 100. Настройте порты 5, 6 как порты Access, порт VLAN как 200. Настройте порт 7 как порт Trunk, порт VLAN как 1, разрешенные VLAN как 1,2,100,200, как показано на рисунке 98.
3. Оставьте все остальные параметры со значениями по умолчанию.

7.2.2 GVRP

7.2.2.1 Введение

Протокол GARP (Generic Attribute Registration Protocol) используется для распространения, регистрации и отмены определенной информации (VLAN, адрес многоадресной рассылки) между коммутаторами в одной сети.

При использовании GARP информация о конфигурации участника GARP будет распространяться по всей сети коммутатора. Устройства, поддерживающие GARP,

передают друг другу инструкции о регистрации или отмене тех или иных настроек путём отправки соответствующих сообщений join/leave. Участник также регистрирует или отменяет информацию о конфигурации других участников на основе сообщений join/leave, отправленных другими участниками.

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

Когда прикладной объект GARP хочет зарегистрировать свою собственную информацию на других коммутаторах, объект отправляет сообщение Join. Сообщения Join делятся на два типа: JoinEmpty и JoinIn. Сообщение JoinIn отправляется для объявления зарегистрированного атрибута, а сообщение JoinEmpty отправляется для объявления еще не зарегистрированного атрибута.

Когда прикладной объект GARP хочет удалить свою собственную информацию на других коммутаторах, объект отправляет сообщение Leave.

После запуска объекта GARP он запускает таймер LeaveAll. Когда период таймера истекает, объект отправляет сообщение LeaveAll.

Примечание:

Объект указывает порт с поддержкой GARP.

Таймеры GARP – это таймер Hold, таймер Join, таймер Leave и таймер LeaveAll.

Таймер Hold: когда коммутатор с поддержкой GARP получает сообщение о регистрации, он запускает таймер Hold, а не сразу отправляет сообщение Join. По истечении времени ожидания таймера Hold вся регистрационная информация, полученная за это время, будет помещена в одно и то же сообщение Join и отправлена, что уменьшит количество сообщений для стабильности сети.

Таймер Join: для того, чтобы гарантировать, что сообщение Join может быть надежно передано другим коммутаторам, коммутатор с поддержкой GARP будет ждать в течение временного интервала таймера Join после отправки первого сообщения Join. Если коммутатор не получит сообщение Join в течение этого времени, он снова отправит сообщение Join, в противном случае он не отправит второе сообщение.

Таймер Leave: когда коммутатор с поддержкой GARP желает, чтобы другие коммутаторы аннулировали его атрибутивную информацию, он отправляет сообщение

Leave. Другие коммутаторы с поддержкой GARP, получившие это сообщение, включат таймер Leave. Если они не получат сообщение Join до истечения времени таймера, они аннулируют эту атрибутивную информацию.

Таймер LeaveAll: 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 атрибутах, а затем перезапустит таймер LeaveAll, чтобы начать новый цикл.

7.2.2.2 Введение

GVRP (протокол регистрации GARP VLAN) — это приложение GARP, основанное на рабочем механизме GARP для поддержки динамической регистрационной информации VLAN устройства и распространения этой информации на другие устройства.

Устройство с поддержкой GVRP может получать регистрационную информацию VLAN от других устройств и динамически обновлять регистрационную информацию локальной VLAN, а также устройство может распространять регистрационную информацию локальной VLAN на другие устройства, достигая согласованности информации VLAN на всех устройствах в одной и той же локальной сети. Регистрационная информация VLAN, распространяемая GVRP, содержит не только локальную статическую регистрационную информацию, сконфигурированную вручную, но также динамическую регистрационную информацию от других устройств.

Предупреждение:

Канал портов и порт GVRP являются взаимоисключающими. Порт в канале портов нельзя настроить как порт GVRP, а порт GVRP нельзя добавить в канал портов.

7.2.2.3 Настройка через веб-интерфейс

1. Включите протокол GVRP и настройте таймер, как показано ниже.

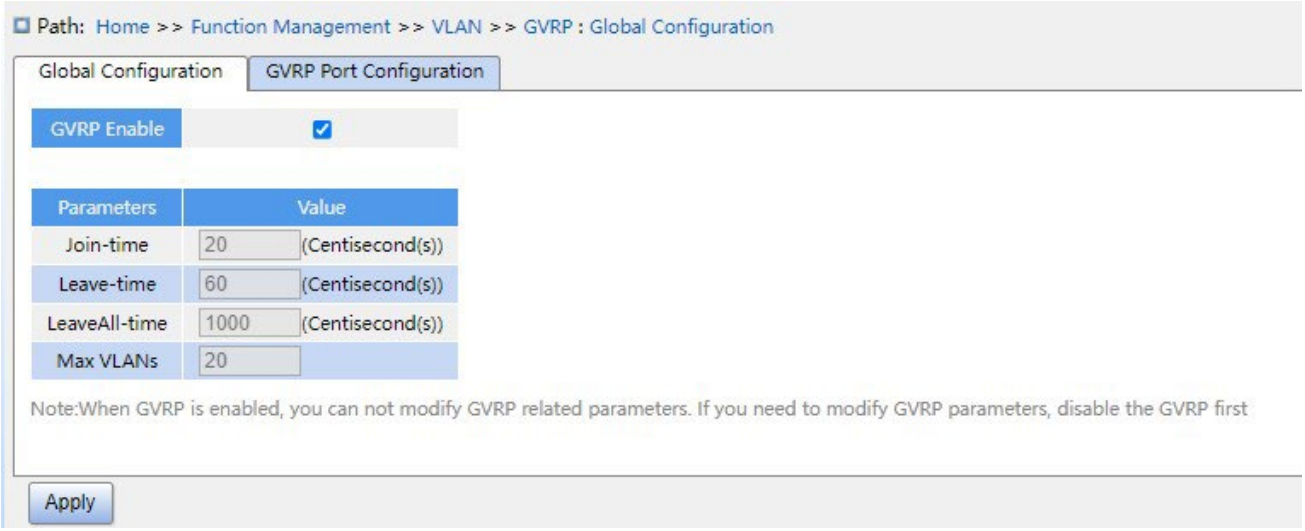


Рисунок 101 Глобальная настройка GMRP

GVRP enable

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение или выключение GVRP

Join Timer

Варианты конфигурации: 1-20 (сантисекунд)

Конфигурация по умолчанию: 20 (сантисекунд)

Функция: Настройка значения таймера Join.

Leave Timer

Варианты конфигурации: 60-300 (сантисекунд)

Конфигурация по умолчанию: 60 (сантисекунд)

Функция: Настройка значения таймера Leave.

LeaveAll timer

Варианты конфигурации: 1000-5000 (сантисекунд)

Конфигурация по умолчанию: 1000 (сантисекунд)

Функция: Настройка значения таймера LeaveAll.

Описание: если время таймера LeaveAll для разных устройств истекает одновременно, одновременно отправляется несколько сообщений LeaveAll, что увеличивает количество ненужных сообщений. Чтобы избежать одновременного истечения таймера LeaveAll на разных устройствах, фактическое значение параметра LeaveAll — это

случайное значение, которое больше значения таймера LeaveAll и меньше, чем 1,5 значения таймера LeaveAll.

Max VLANs

Диапазон настройки: 1~4094

Конфигурация по умолчанию: 20

Функция: Настройка максимального числа динамически зарегистрированных VLAN порта GVRP.

Предупреждение:

Отключите GVRP перед настройкой таймера GVRP и параметра Max VLANs.

2. Конфигурация порта GVRP показана ниже.

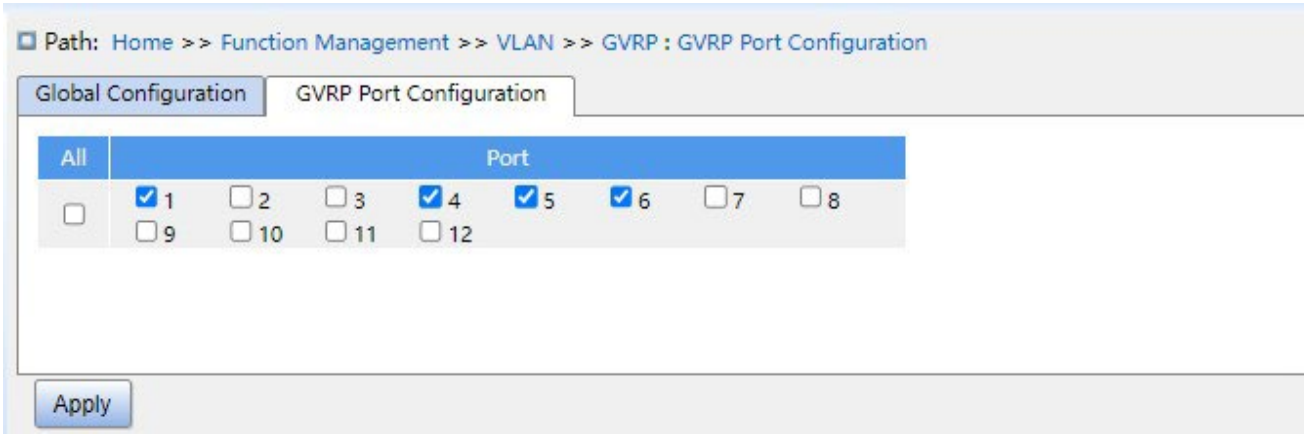


Рисунок 102 Настройка порта GVRP

Port

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение или выключение GVRP для порта.

Предупреждение:

- Порт GVRP должен быть сконфигурирован как порт Trunk.
- Порт GVRP распределяет свойства VLAN других портов GVRP со статусом UP.

7.2.2.4 Пример типовой конфигурации

Как показано на рисунке 103, на устройствах необходимо включить GVRP, чтобы информация VLAN динамически регистрировалась и обновлялась между устройством A и устройством B.

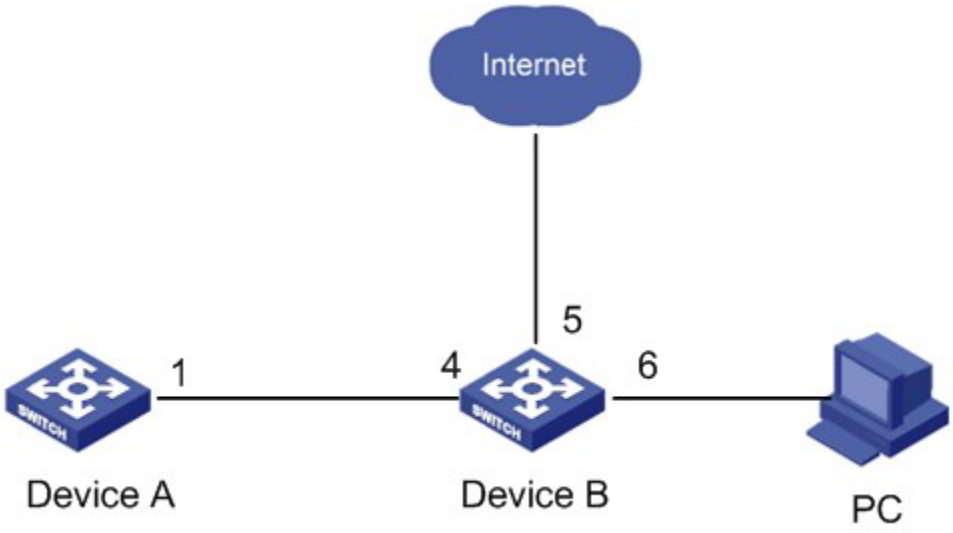


Рисунок 103 Пример настроек GVRP

Настройки устройства A:

1. Настройте порт 1 как порт Trunk, разрешенные VLAN на 1.
2. Включите глобальный GVRP, как показано на рисунке 101.
3. Включите GVRP на порту 1, как показано на рисунке 102.

Настройки устройства B:

1. Настройте порт 4 как порт Trunk, разрешенные VLAN на 1; настройте порт 5 как порт Access, разрешенные VLAN на 5; настройте порт 6 как порт Trunk, разрешенные VLAN на 1, 6.
2. Включите глобальный GVRP, как показано на рисунке 101.
3. Включите GVRP на порту 4, 5, 6, как показано на рисунке 102.

Порт 1 коммутатора A может регистрировать ту же информацию о VLAN, что и порт 5 и 6 коммутатора

B.

7.2.3 СОСТОЯНИЕ VLAN

Проверьте состояние VLAN, как показано ниже.

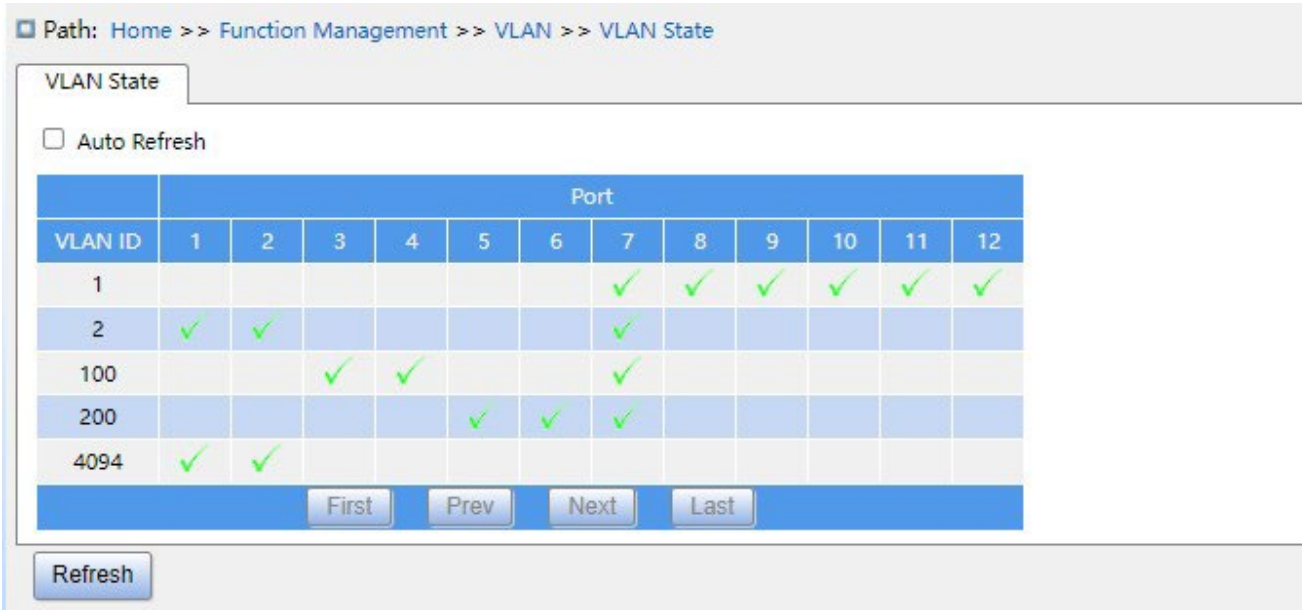


Рисунок 104 Состояние VLAN порта

7.3 Настройка IP

7.3.1 Настройка IP-адреса

1. Просмотр IP-адреса коммутатора через консольный порт.

Войдите в интерфейс командной строки коммутатора через консольный порт. В режиме привилегированного пользователя выполните команду **show interface vlan 1**, чтобы увидеть IP-адрес коммутатора.

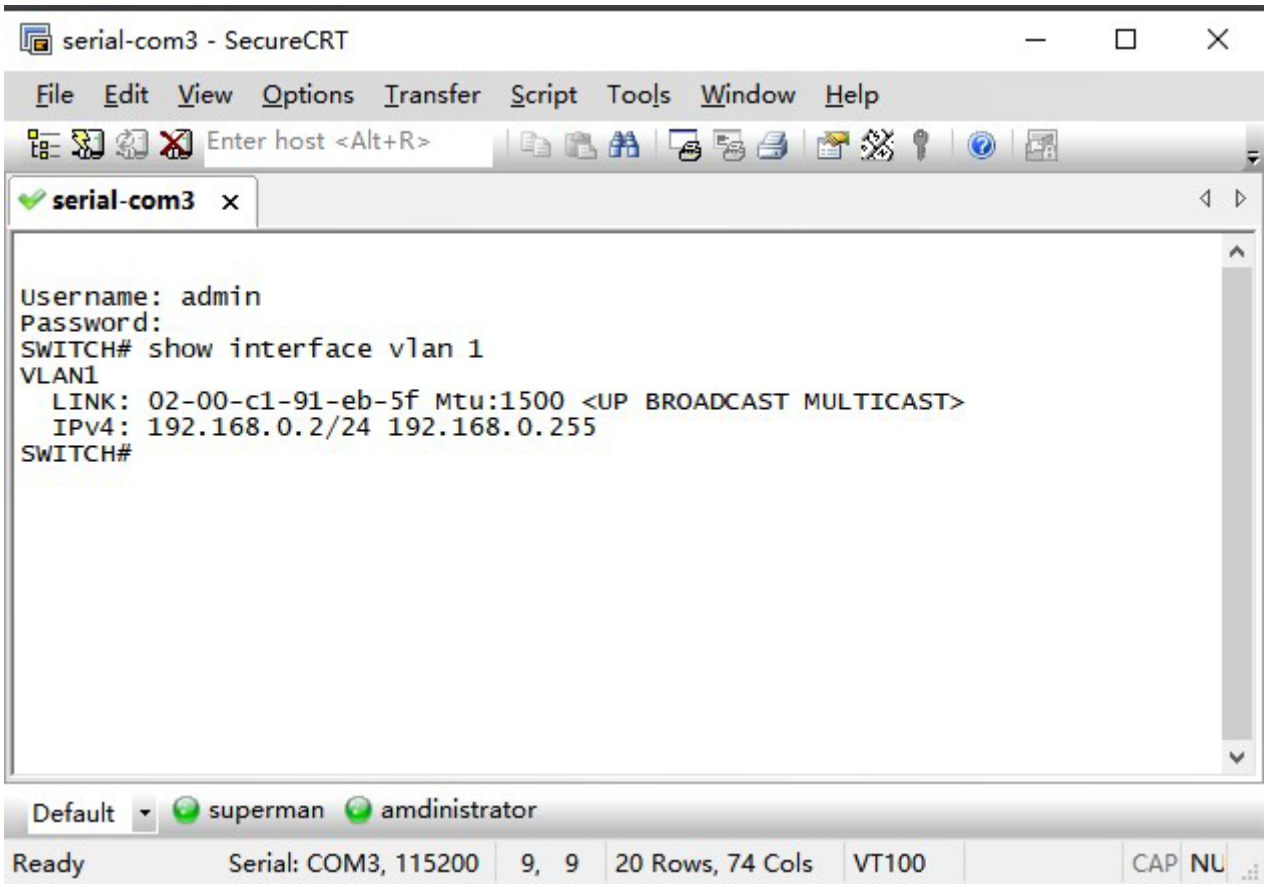


Рисунок 105 Отображение IP-адреса

2. Создание интерфейса IP.

Хосты в разных VLAN не могут связываться друг с другом. Их коммуникационные пакеты должны пересылаться маршрутизатором или коммутатором уровня 3 через IP-интерфейс.

Коммутаторы данной серии поддерживают IP-интерфейсы, которые представляют собой виртуальные интерфейсы уровня 3, используемые для связи между VLAN. Для каждой VLAN можно создать один IP-интерфейс. Интерфейс используется для пересылки пакетов уровня 3 в VLAN.

3. Настройте основной IP-адрес.

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

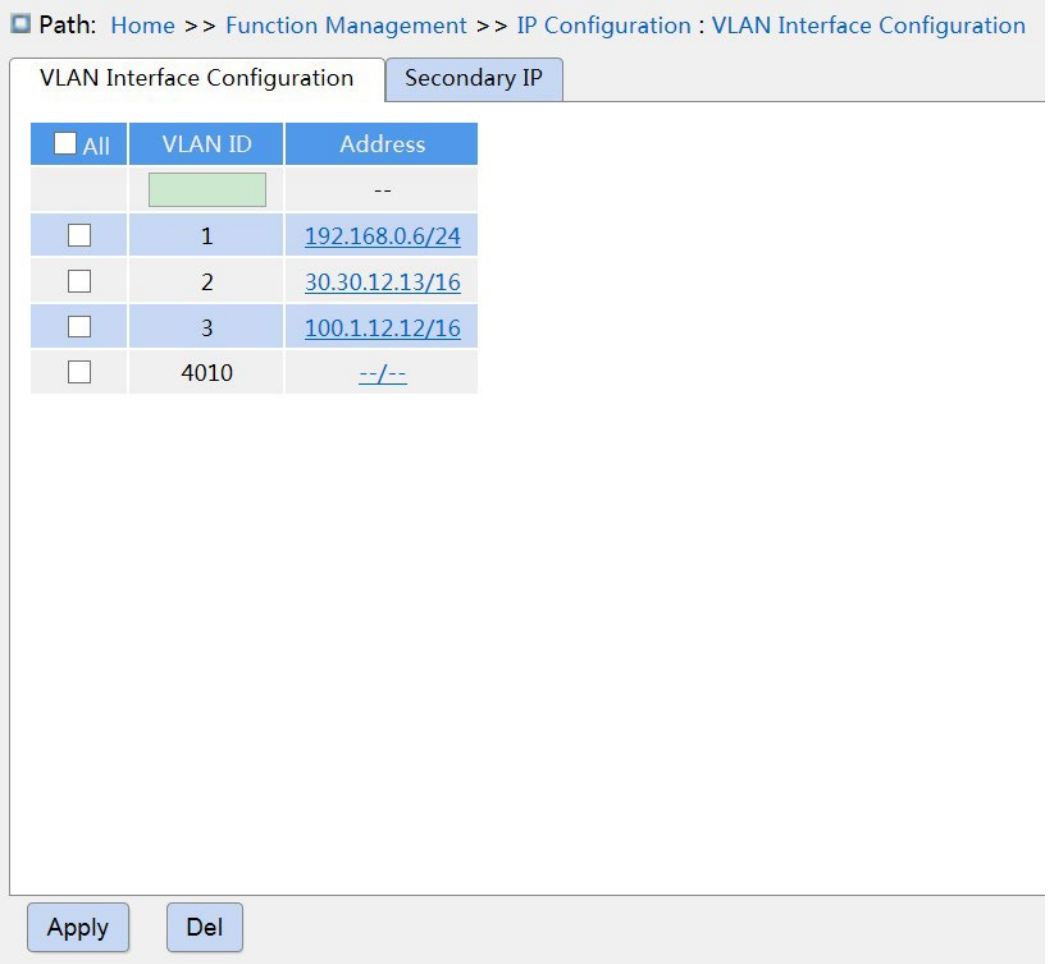


Рисунок 106 Настройка интерфейса VLAN

VLAN ID

Функция: Настройка свойств VLAN IP-интерфейса. Только порт-участник VLAN сможет получить доступ к текущему IP-интерфейсу.

Address

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

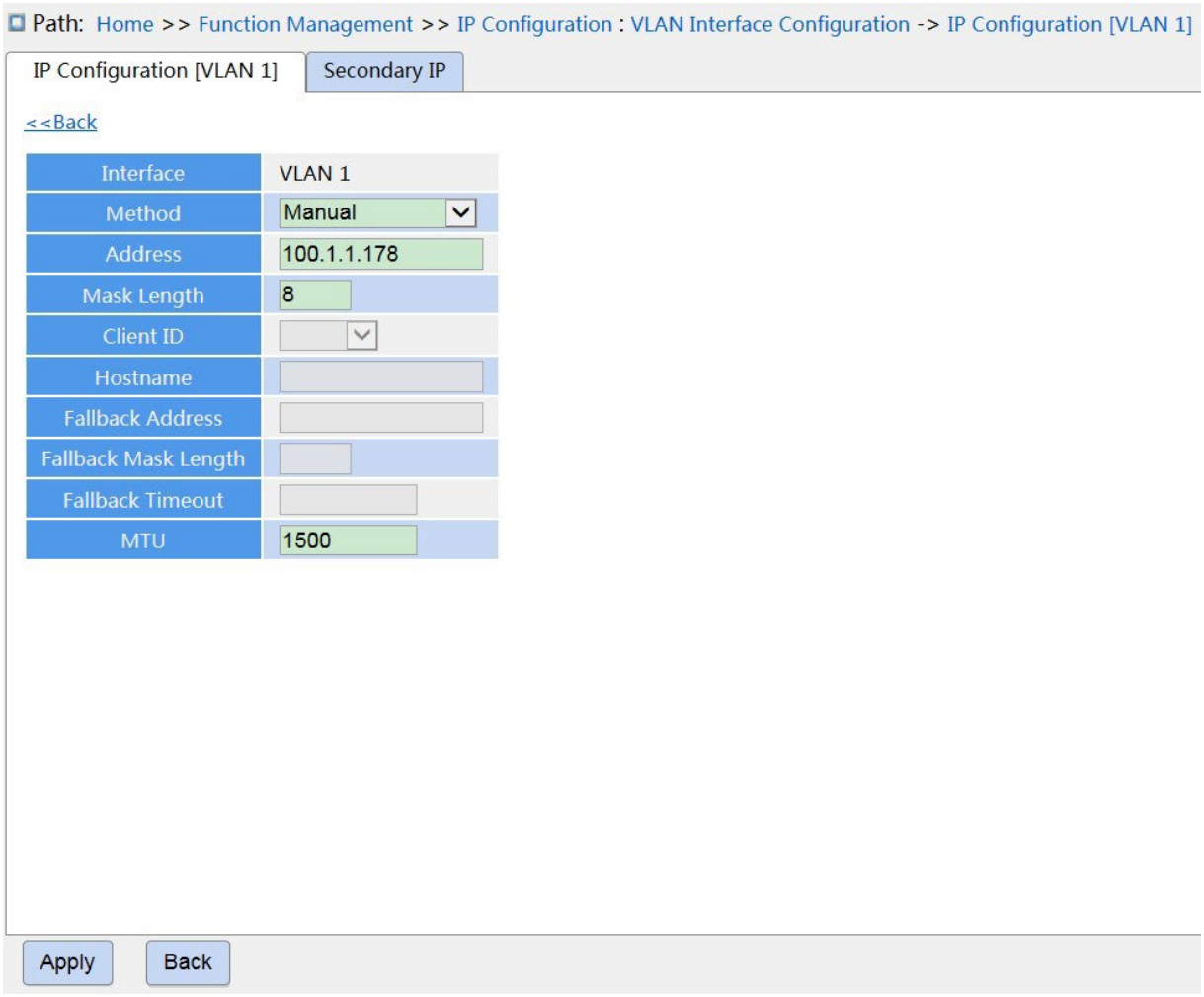


Рисунок 107 Настройка IP-адреса

Method

Варианты конфигурации: None/DHCP/Manual

Функция: Manual – необходимо вручную настроить IP-адрес и маску подсети.

Коммутатор автоматически получает IP-адрес через протокол DHCP в качестве клиента DHCP, если включен 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-разрядное число, состоящее из последовательности 1 и последовательности

0. «1» соответствует полям номера сети и полям номера подсети, а «0» соответствует полям номера хоста. Длина маски — это количество 1 в маске подсети.

Client ID

Варианты конфигурации: Hex/ASCII/Port

Функция: Подробная информация о переносимом параметре option61 сохраняется, когда указанный IP-адрес отправляет требование DHCP. Hex относится к заполнению option61 01+mac-адрес. ASCII относится к заполнению option61 00+строка. Port относится к заполнению option61 MAC соответствующего интерфейса.

Hostname

Диапазон настройки: 1~63 символа

Функция: Настройка имени хоста интерфейса VLAN.

Fallback Address

Формат: A.B.C.D

Функция: После того, как интерфейс VLAN получит тайм-аут IP-адреса через протокол DHCP, адрес устанавливается на резервный IP-адрес.

Fallback Mask Length

Функция: Маска подсети – это 32-разрядное число, состоящее из последовательности 1 и последовательности 0. «1» соответствует полям номера сети и полям номера подсети, а «0» соответствует полям номера хоста. Длина маски — это количество 1 в маске подсети.

Fallback Timeout

Диапазон настройки: 0~4294967295 с

Функция: если значение не равно нулю, коммутатор получает время попытки IP-адреса через протокол DHCP, в это время необходимо настроить IP-адрес вручную, после истечения времени попытки IP-адрес, настроенный вручную, вступает в силу. Если значение равно нулю, коммутатор будет пытаться снова и снова, пока IP-адрес не будет получен по протоколу DHCP. Нет необходимости настраивать IP-адрес вручную.

MTU

Диапазон настройки: 68~9600

Настройка по умолчанию: 1500

Функция: Настройка максимальной длины пакета, который может пройти на уровне IP.

4. Настройка вторичного IP

Вручную настройте дополнительный IP-адрес IP-интерфейса коммутатора, как показано ниже.

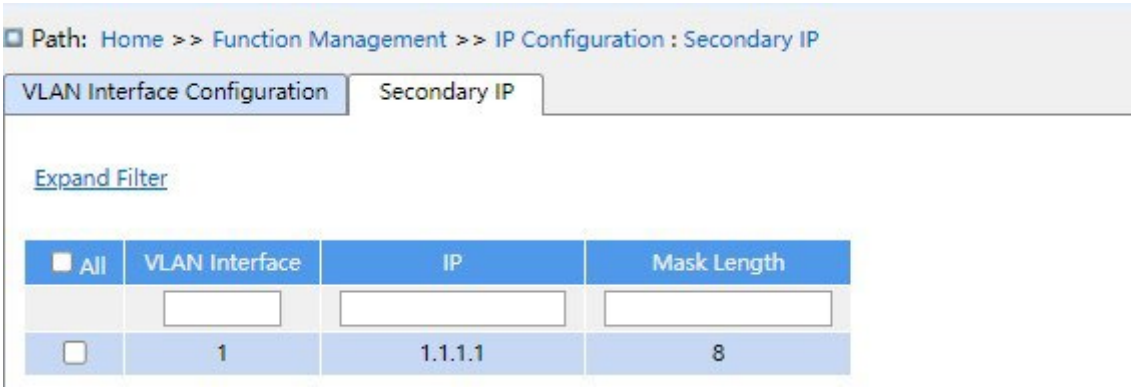


Рисунок 108 Настройка вторичного IP

Интерфейс VLAN

Функция: Настройка свойств VLAN IP-интерфейса. Только порт-участник VLAN сможет получить доступ к текущему IP-интерфейсу.

IP

Формат: A.B.C.D

Функция: Задание IP-адреса вручную.

Mask Length

Функция: Маска подсети – это 32-разрядное число, состоящее из последовательности 1 и последовательности 0. «1» соответствует полям номера сети и полям номера подсети, а «0» соответствует полям номера хоста. Длина маски — это количество 1 в маске подсети.

Предупреждение:

- Каждый IP интерфейс соответствует основному IP-адресу и может соответствовать нескольким

  вторичным IP-адресам.

- Различные IP-интерфейсы должны быть настроены с первичными и вторичными IP-адресами для

  разных сегментов сети.

7.4 Агрегация портов

7.4.1 Статическая агрегация

7.4.1.1 Введение

Канал порта предназначен для привязки группы физических портов с одинаковой конфигурацией к логическому порту для увеличения пропускной способности и повышения скорости передачи. Порты-участники одной группы совместно используют трафик и служат друг для друга динамическими резервными копиями, повышая надежность соединения.

Группа портов — это группа физических портов на уровне конфигурации. Только физические порты, входящие в группу портов, могут участвовать в агрегации каналов и становиться участниками канала портов. Когда физические порты в группе портов соответствуют определенным условиям, они могут выполнять агрегацию портов, формировать агрегированный канал и становиться независимым логическим портом, тем самым увеличивая пропускную способность сети и обеспечивая резервирование канала.

7.4.1.2 Реализация

Как показано на рисунке 109, три порта на коммутаторах A и B объединяются, образуя канал портов. Пропускная способность канала портов — это общая пропускная способность этих трех портов.

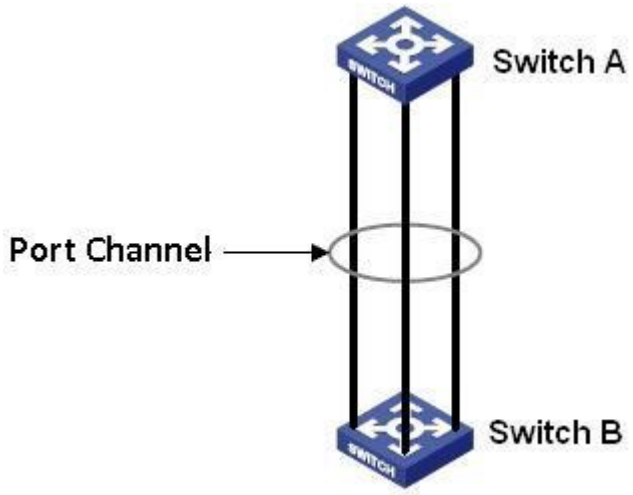


Рисунок 109 Канал портов

Если коммутатор A отправляет пакеты коммутатору B через канал портов, коммутатор A определяет порт-участник для передачи трафика на основе результатов расчета распределения нагрузки. Если один порт-участник канала порта выходит из строя, трафик, передаваемый через порт, передается другому работоспособному порту на основе алгоритма распределения нагрузки.

Предупреждение:

- Порт можно добавить только в одну группу портов.
- Только полнодуплексные порты могут присоединиться к агрегации.
- Для порта в канале портов нельзя включить LACP, а порт с включенным LACP нельзя добавить в канал портов.
- Канал портов и резервный порт являются взаимоисключающими. Порт в канале портов нельзя настроить как

резервный порт, а резервный порт нельзя добавить в канал портов. ➢Термин «резервный порт» в этом документе относится к кольцевому порту кольцевому порту DRP, резервному порту DRP, порту RSTP и

порту MSTP.

7.4.1.3 Настройка через веб-интерфейс

1. Статическая агрегация показана ниже.

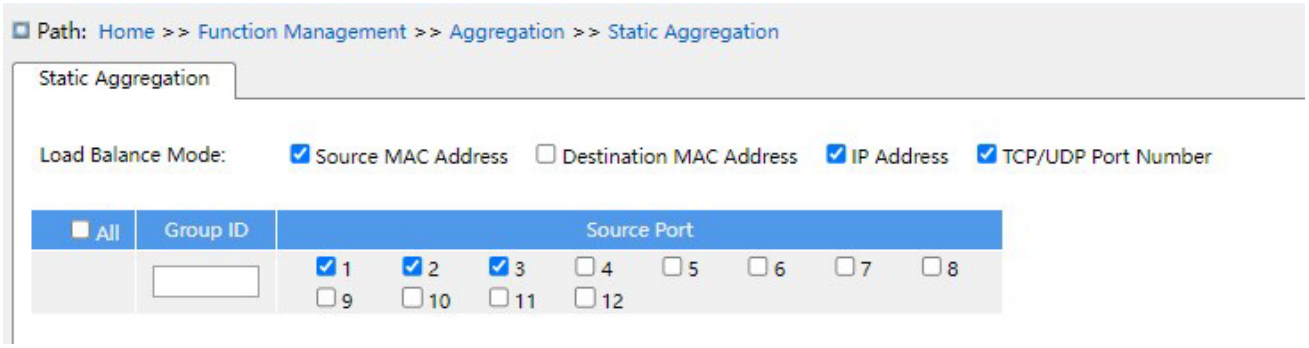


Рисунок 110 Настройка статической агрегации

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 балансировки нагрузки группы агрегации.

Описание: Source MAC address балансирует трафик согласно MAC-адресу источника; destination MAC балансирует трафик в соответствии с MAC-адресом назначения; IP address балансирует трафик в соответствии с IP-адресом; TCP/UDP port number балансирует трафик в соответствии с номером порта TCP/UDP.

Group ID

Диапазон настройки: 1-10

Функция: Настройка ID группы.

Описание: Все порты в одной группе агрегации имеют одинаковые свойства. Количество групп агрегации зависит от порта устройства, каждая группа агрегации поддерживает до 8 портов-участников.

Source Port

Варианты конфигурации: Enable/Disable

Функция: Выбор порта для присоединения к указанной группе агрегации.

7.4.1.4 Пример типовой конфигурации

Как показано на рисунке 109, добавьте три порта (порты 1, 2 и 3) коммутатора A в группу портов 1 и три порта (порты 1, 2 и 3) коммутатора B в группу портов 1. Используйте сетевые кабели, чтобы соединить эти порты, чтобы сформировать канал

портов, реализуя распределение нагрузки между портами. (Предполагается, что три порта на коммутаторах A и B имеют одинаковые атрибуты соответственно).

Настройка на коммутаторах:

1. Добавьте порты 1, 2 и 3 коммутатора A в группу портов 1, как показано на рисунке 110.
2. Добавьте порты 1, 2 и 3 коммутатора B в группу портов 1, как показано на рисунке 110.

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 блок данных протокола управления агрегацией каналов (LACPDU), чтобы выбрать порт-участник в группе динамического агрегирования.

7.4.2.2 Реализация

Порт с поддержкой LACP информирует одноранговый порт о своем приоритете LACP локального оборудования, MAC-адресе оборудования, приоритете LACP порта, номере порта и значении ключа, отправляя сообщение LACPDU. Одноранговый порт согласовывает с локальным портом после получения сообщения LACPDU:

1. Сравнивает идентификаторы оборудования на обоих концах (идентификатор оборудования = приоритет оборудования LACP + MAC-адрес оборудования). Сначала сравниваются приоритеты LACP. Если приоритеты LACP совпадают, сравниваются MAC-адреса. В качестве основного (master) выбирается оборудование с наименьшим идентификатором.
2. Сравниваются идентификаторы портов оборудования master (идентификатор порта = приоритет порта LACP + номер порта). Сначала сравниваются приоритеты LACP. Если приоритеты LACP совпадают, сравниваются номера портов. Порт с меньшим идентификатором выбирается в качестве ссылочного порта.

3. Если этот порт и ссылочный порт имеют одинаковые значения ключей и одинаковые конфигурации атрибутов порта в состоянии Up, а одноранговые порты этого порта и ссылочного порта имеют одинаковые значения ключей и конфигурации атрибутов порта, этот порт может стать портом-участником группы динамической агрегации.

7.4.2.3 Настройка через веб-интерфейс

1. Настройте приоритет LACP, как показано ниже.

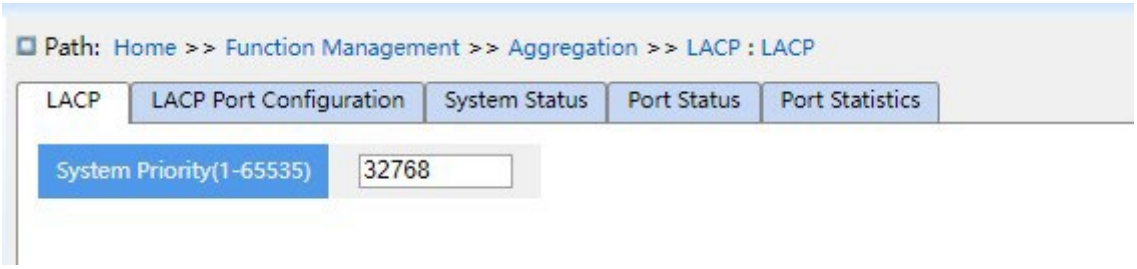


Рисунок 111 Настройка приоритета LACP

LACP

Диапазон настройки: 1-65535

Конфигурация по умолчанию: 32768

Функция: Настройка приоритета LACP, используемого для выбора основного устройства при согласовании LACP.

2. Конфигурация порта LACP показана ниже.

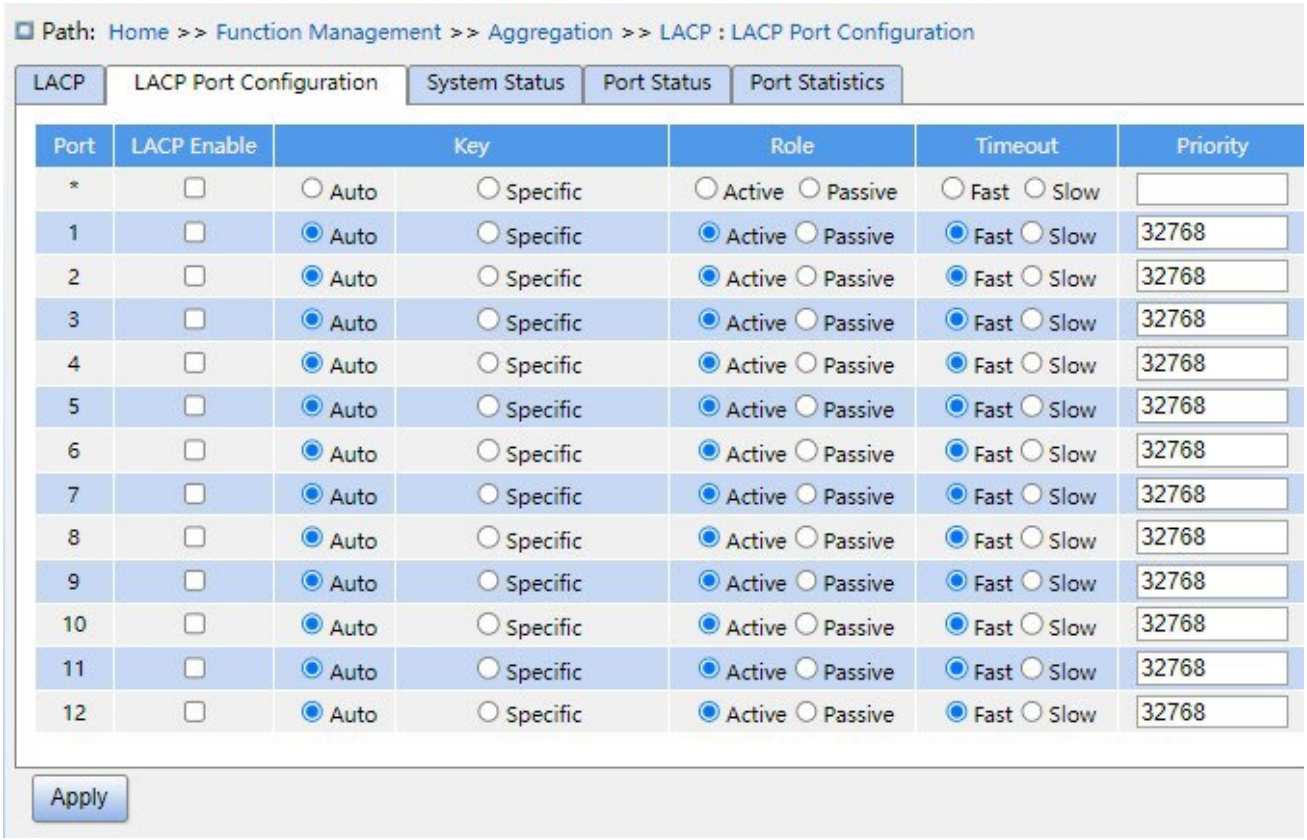


Рисунок 112 Настройка порта GVRP

LACP Enable

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: включение LACP для порта.

Key

Варианты конфигурации: Auto/specific（1~65535）

Конфигурация по умолчанию: Auto

Функция: Настройка значения ключа порта. Значение ключа определяется скоростью порта, если выбрано значение «Авто», key=1 (10Mb); key=2 (100Mb); key=3 (1000Mb). Порты с разными значениями ключей не могут быть добавлены в группу динамической агрегации.

Role

Варианты конфигурации: Active/ passive

Конфигурация по умолчанию: Active

Функция: выбор роли LACP. Активный порт будет активно отправлять сообщение LACPDU на конечный порт; пассивный порт получает сообщение LACPDU на противоположный конец и отправляет сообщение LACPDU на конечный порт.

Предупреждение:
По крайней мере один из двух подключенных портов должен быть активен, иначе два конца не смогут обмениваться информацией.

Timeout

Варианты конфигурации: Fast/slow

Конфигурация по умолчанию: Fast

Функция: Настраивает для активного порта интервал для отправки сообщений LACPDU. Fast относится к интервалу времени, равному 1 с, а Slow относится к интервалу времени, равному 30 с.

Priority

Диапазон настройки: 1~65535

Конфигурация по умолчанию: 32768

Функция: Настройка приоритет порта LACP, используется для выбора ссылочных портов. Порты с низким приоритетом на основном устройстве выбираются в качестве ссылочных портов.

3. Просмотрите статус LACP системы, как показано ниже.

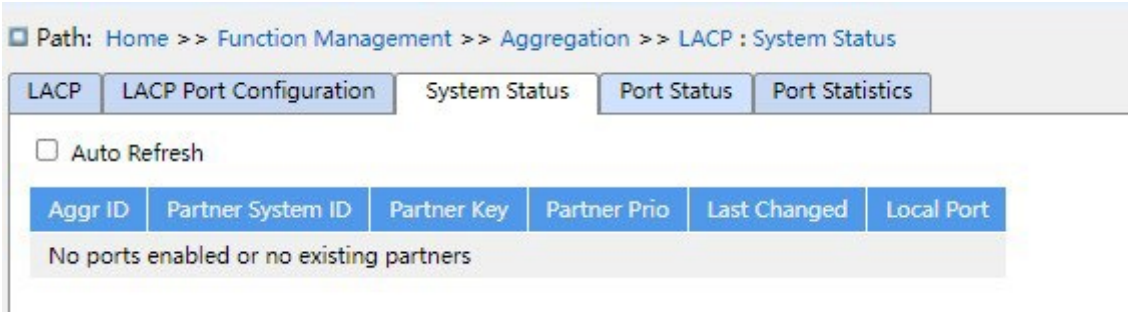


Рисунок 113 Просмотр статуса LACP системы

Aggr ID

Функция: Используется для указания ID группы агрегации.

Partner System ID

Функция: Используется MAC-адрес, указывающий ID устройства на противоположном конце.

Partner Key

Функция: Отображение значения ключа порта однорангового устройства.

Partner Prio

Функция: Указание приоритета системы на противоположном конце.

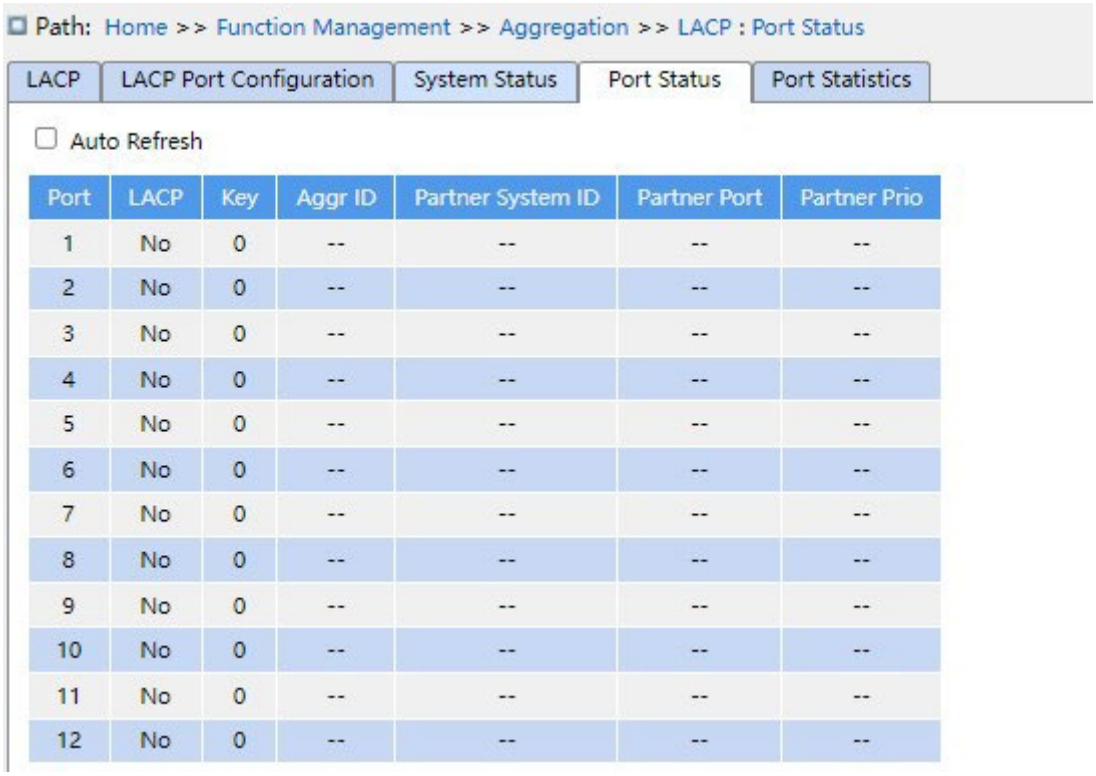
Last Changed

Функция: Указание на переключение LACP до текущего интервала отображения.

Local Port

Функция: Включение номера локального порта LACP.

4. Просмотрите статус LACP порта, как показано ниже.



Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	No	0	--	--	--	--
2	No	0	--	--	--	--
3	No	0	--	--	--	--
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	--	--	--	--

Рисунок 114 Просмотр статуса LACP порта

LACP Status

Варианты отображения: Yes/No

Функция: Отображение статуса LACP для порта. Yes означает, что LACP включен и порт включен.

No означает, что LACP выключен и порт выключен.

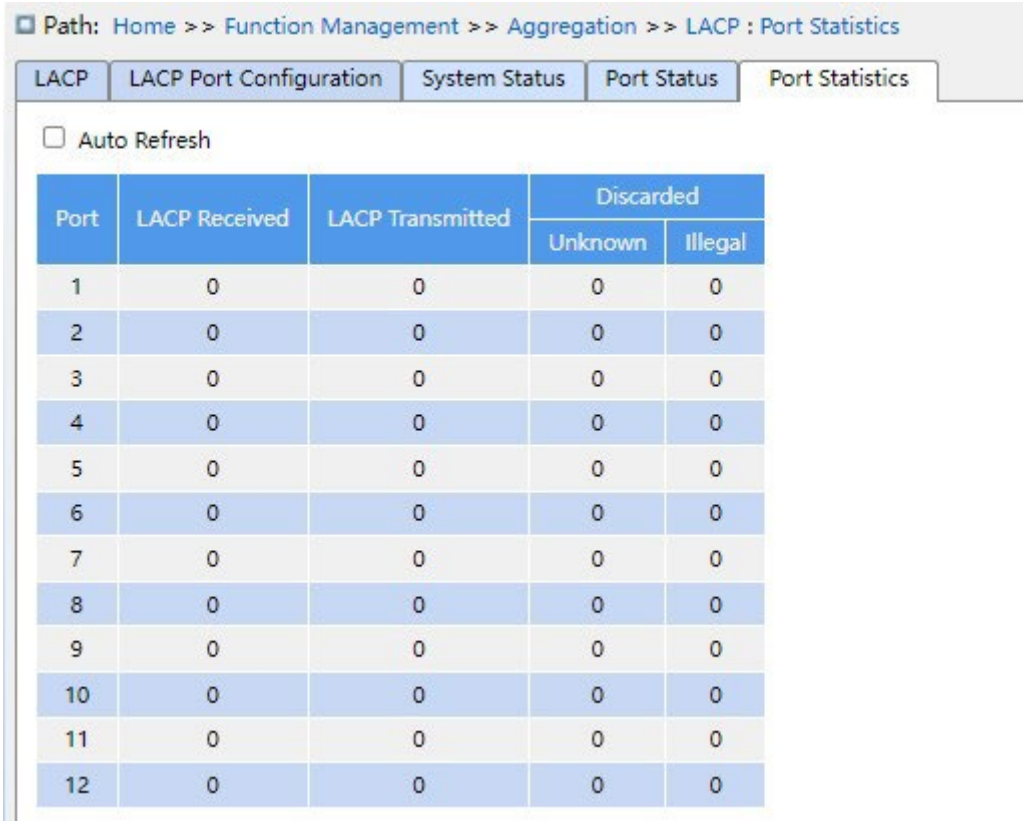
Key

Функция: Отображение значения ключа порта локального устройства.

Partner Prio

Функция: Отображение приоритета порта однорангового устройства.

5. Просмотрите статистику LACP порта, как показано ниже.



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

Рисунок 115 Просмотр статистики LACP порта

Port

Область действия настройки: все порты коммутатора.

LACP Received

Функция: Количество сообщений LACP, полученных данным портом.

LACP Transmitted

Функция: Количество сообщений LACP, отправленных данным портом.

Discarded

Функция: Unknown, отбрасывание неизвестных сообщений LACP. Illegal, отбрасывание недопустимых сообщений LACP.

7.4.2.4 Пример типовой конфигурации

Как показано на рисунке 109, добавьте три порта (порты 1, 2 и 3) коммутатора A в группу портов 1 и три порта (порты 1, 2 и 3) коммутатора B в группу портов 1.

Используйте сетевые кабели, чтобы соединить эти порты, чтобы сформировать канал портов, реализуя распределение нагрузки между портами. (Предполагается, что три порта на коммутаторах A и B имеют одинаковые атрибуты соответственно).

Настройка на коммутаторах:

1. Включите LACP на портах 1, 2 и 3 коммутатора A, как показано на рисунке 112.
2. Включите LACP на портах 1, 2 и 3 коммутатора B, как показано на рисунке 112.

7.5 Резервирование

7.5.1 DT-Ring

7.5.1.1 Введение

DT-Ring и DT-Ring+ — это собственные протоколы резервирования компании Kyland. Они позволяют сети восстанавливаться в течение 50 мс при сбое канала, обеспечивая стабильную и надежную связь.

Кольца DT делятся на два типа: на основе портов (DT-Ring-Port) и на основе VLAN (DT-Ring-VLAN).

DT-Ring-Port: указывает порт для пересылки или блокировки пакетов.

DT-Ring-VLAN: указывает порт для пересылки или блокировки пакетов определенной VLAN. Это позволяет использовать несколько VLAN на общем порту, то есть один порт является частью разных резервных колец, основанных на разных VLAN.

DT-Ring-Port и DT-Ring-VLAN нельзя использовать вместе.

7.5.1.2 Основные понятия

Master: Одно кольцо может иметь только один узел в статусе Master. Узел в статусе Master отправляет пакеты протокола DT-Ring и определяет состояние кольца. Когда кольцо замкнуто, из двух портов, которые включены в кольцо, один находится в состоянии пересылки, а другой в состоянии блокировки, соответственно.

Примечание:
Первый порт, статус связи которого меняется на up при замыкании кольца, находится в состоянии пересылки. Остальные кольцевые порты находятся в состоянии блокировки.

Slave: Кольцо может включать в себя несколько устройств Slave. Устройства Slave прослушивают и пересылают пакеты протокола DT-Ring и сообщают информацию об ошибках устройству Master.

Резервный порт: Порт для связи между кольцами DT называется резервным портом.

Резервный порт Master: Когда кольцо имеет несколько резервных портов, резервный порт с большим MAC-адресом является резервным портом Master. Он находится в состоянии пересылки.

Резервный порт Slave: Когда кольцо имеет несколько резервных портов, все резервные порты, кроме резервного порта Master, являются резервными портами Slave. Они находятся в состоянии блокировки.

Состояние пересылки: Если порт находится в состоянии пересылки, порт может и принимать, и отправлять данные. Состояние блокировки: Если порт находится в состоянии блокировки, он может принимать и пересылать только пакеты протокола DT-Ring.

7.5.1.3 Реализация

Реализация DT-Ring-Port

Порт пересылки на устройстве Master периодически отправляет пакеты протокола DT-Ring для определения состояния кольца. Если блокирующий порт устройства Master получает пакеты, кольцо замкнуто; в противном случае кольцо разомкнуто.

Рабочий процесс коммутатора A, коммутатора B, коммутатора C и коммутатора D:

1. Настройте коммутатор A как Master, а остальные коммутаторы — как Slave.
2. Кольцевой порт 1 на Master находится в состоянии пересылки, а кольцевой порт 2 находится в состоянии блокировки. Оба порта на Slave находятся в состоянии пересылки.
3. Если линия связи CD неисправна, как показано ниже.

a) Когда линия связи CD неисправна, порт 6 и порт 7 на устройстве Slave находятся в состоянии блокировки. Порт 2 устройства Master переходит в состояние пересылки, обеспечивая работающую линию связи.

b) Когда неисправность устранена, порт 6 и порт 7 устройства Slave находятся в состоянии пересылки. Порт 2 устройства Master переходит в состояние блокировки. Происходит переключение каналов, и каналы восстанавливаются до состояния, предшествующего отказу линии CD.

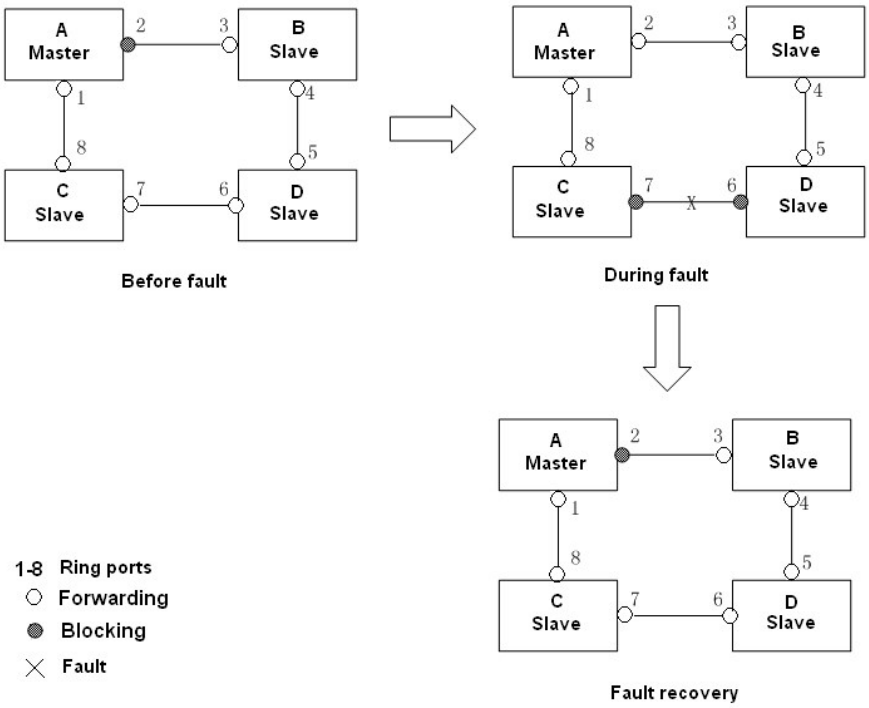


Figure 116 Отказ линии CD

4. Если линия связи AC неисправна, как показано ниже.

a) Если линия связи AC неисправна, порт 1 находится в состоянии блокировки, а порт 2 переходит в состояние пересылки, обеспечивая работающую линию связи.

b) Когда неисправность устранена, порт 1 по-прежнему находится в состоянии блокировки, а порт 8 находится в состоянии пересылки. Переключение не происходит.

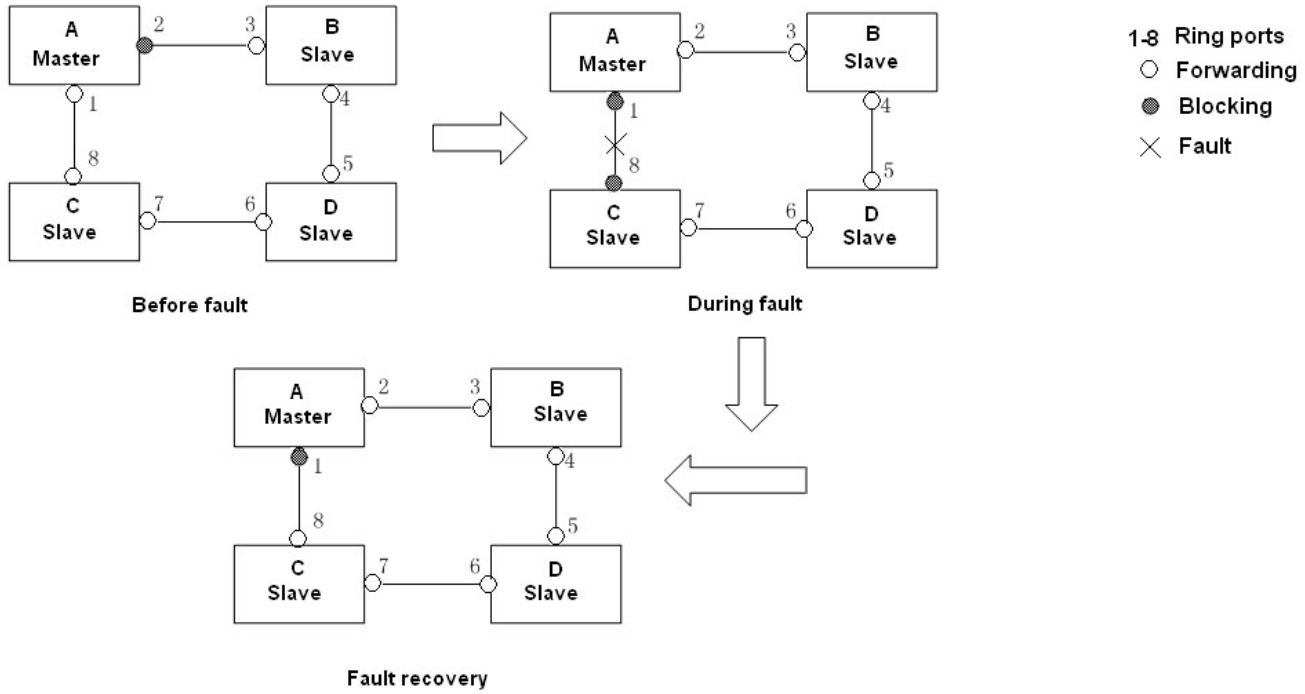


Рисунок 117 Отказ линии DT-Ring

Предупреждение:
Изменение статуса соединения влияет на статус кольцевых портов.

Реализация DT-Ring-VLAN

DT-Ring-VLAN позволяет пересылать пакеты из разных VLAN по разным путям. Каждый путь пересылки для VLAN образует DT-Ring-VLAN. Различные DT-VLAN-Rings могут иметь разные устройства Master. Как показано на рисунке 118, настроено 2 DT-Ring-VLAN.

Линии связи DT-Ring-VLAN 10: AB-BC-CD-DE-EA.

Линии связи DT-Ring-VLAN 20: FB-BC-CD-DE-EF.

Два кольца соприкасаются линиями связи BC, CD и DE. Коммутатор C и коммутатор D используют одни и те же порты в двух кольцах, но используют разные логические каналы на основе VLAN.

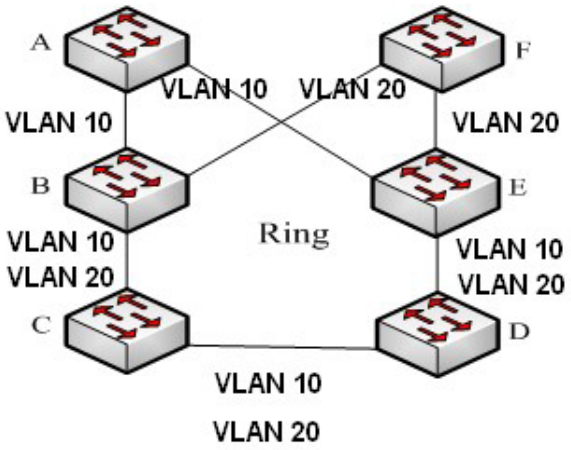


Рисунок 118 DT-Ring-VLAN

Примечание:
В каждом логическом кольце DT-Ring-VLAN реализация идентична таковой для DT-Ring-Port.

Реализация DT-Ring+

DT-Ring+ обеспечивает резервирование для двух колец DT, как показано ниже. Один резервный порт настроен соответственно на коммутаторе C и коммутаторе D. Какой порт является резервным портом Master, зависит от MAC-адресов двух портов. Если резервный порт Master или его канал выходят из строя, резервный порт Slave будет пересылать пакеты, предотвращая образование петель и обеспечивая нормальную связь между резервными кольцами.

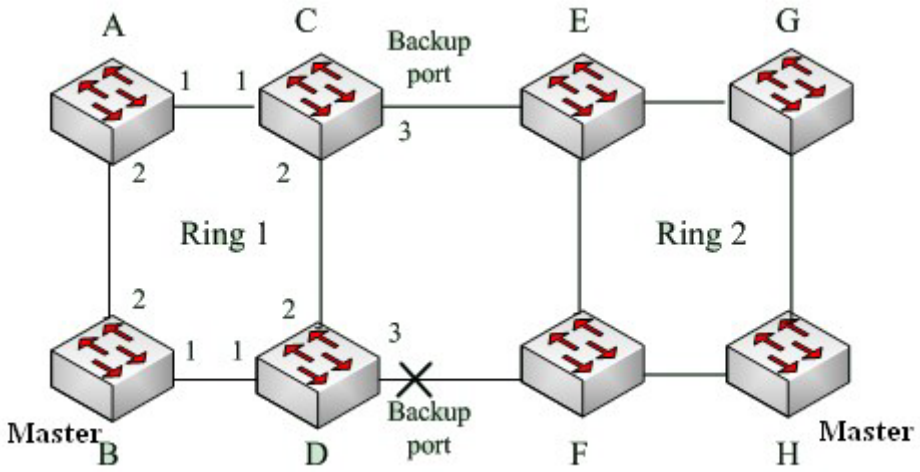


Рисунок 119 Топология DT-Ring+

Предупреждение:
Изменение статуса соединения влияет на статус резервных портов.

7.5.1.4 Пояснения

Конфигурация DT-Ring должны удовлетворять следующим условиям:

- Все коммутаторы в одном кольце должны иметь одинаковый номер домена.
- В каждом кольце может быть только один Master и несколько Slave.
- На каждом коммутаторе можно настроить только два порта для кольца.
- Для двух объединенных колец резервные порты можно настроить только в одном кольце.
- В одном кольце можно настроить не более двух резервных портов.
- На коммутаторе в одном кольце может быть настроен только один резервный порт.
- DT-Ring-Port и DT-Ring-VLAN нельзя настроить на одном коммутаторе одновременно.

7.5.1.5 Настройка через веб-интерфейс

1. Настройте режим резервирования DT-Ring, как показано на рисунке 120.

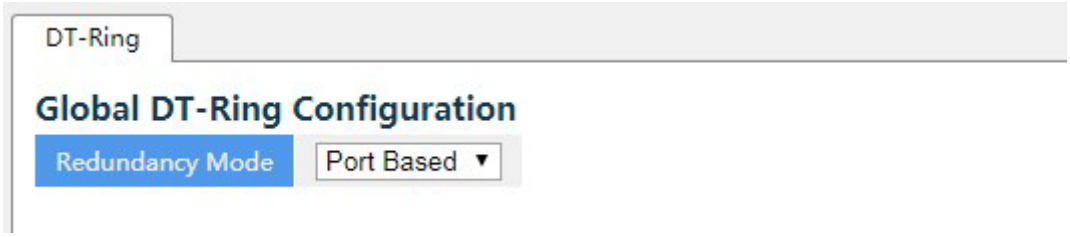


Рисунок 120 Настройка режима резервного кольца

Режим резервирования

Варианты: Port Based/Vlan Based

По умолчанию: Port Based

Функция: Выбор режима резервирования DT-Ring

Предупреждение:

- К кольцевым протоколам на основе портов относятся RSTP, DT-Ring-Port и DRP-Port, а к протоколам на основе VLAN – MSTP, DT-Ring-VLAN и DRP-VLAN.
- Кольцевые протоколы на основе VLAN являются взаимоисключающими, и для одного устройства можно настроить только 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. Настройте DT-Ring-Port и DT-Ring-VLAN, как показано на рисунке 212 и рисунке 122.

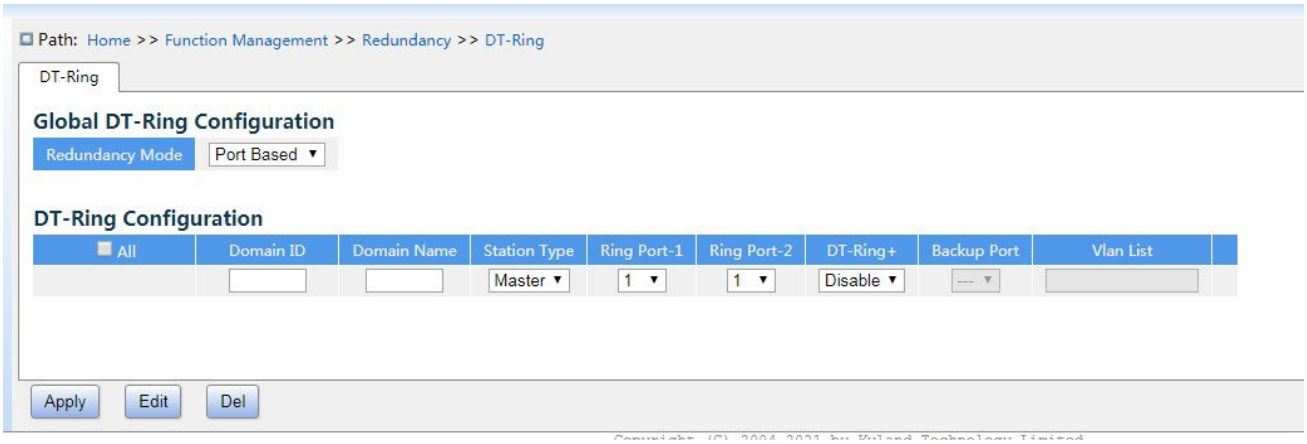


Рисунок 121 Настройка DT-Ring-Port

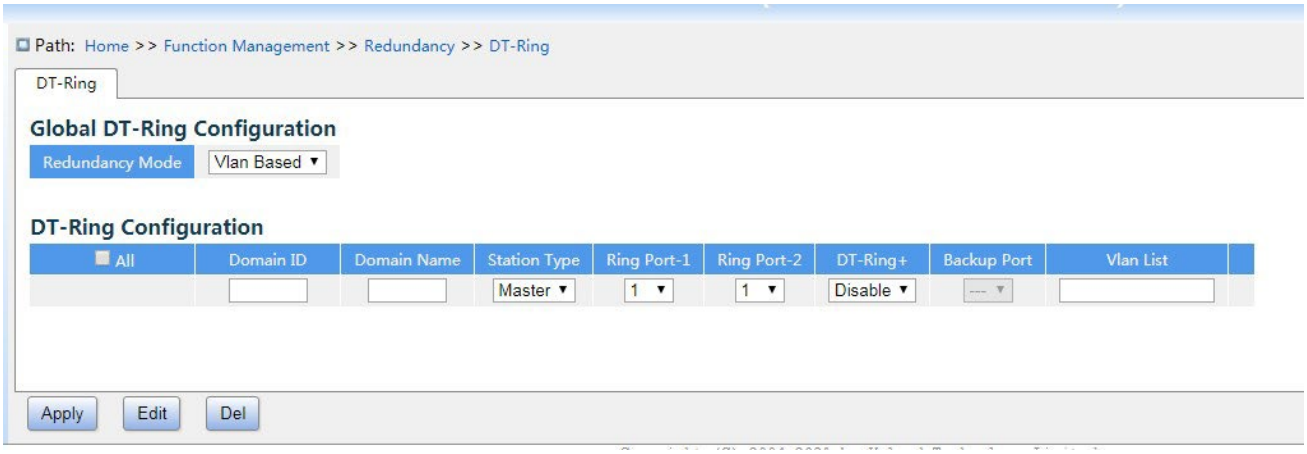


Рисунок 122 Настройка DT-Ring-VLAN

Domain ID

Диапазон: 1~32

Функция: Идентификатор домена используется, чтобы различать разные кольца. Один коммутатор поддерживает максимум 16 колец на основе VLAN, количество колец на основе портов зависит от количества портов коммутатора.

Domain Name

Диапазон: 1~31 символ

Функция: Задание доменного имени.

Station Type

Варианты: Master/Slave

По умолчанию: Master

Функция: Выбор роли коммутатора в кольце.

Ring Port-1/Ring Port-2

Варианты: все порты коммутатора.

Функция: Выбор двух кольцевых портов.

Предупреждение:

- Кольцевой порт DT-Ring или резервный порт и канал портов являются взаимоисключающими. Кольцевой порт DT-Ring или резервный порт не могут быть добавлены к каналу портов; порт в канале портов не может быть настроен в качестве кольцевого порта DT-Ring или резервного порта.
- Кольцевые порты между кольцевыми протоколами на основе портов RSTP, DT-Ring-Port и DRP-Port являются взаимоисключающими, то есть кольцевой порт и резервный порт DT-Ring-Port не могут быть настроены как порт RSTP, DRP-Port. кольцевой порт или резервный порт DRP-Port. Порт RSTP, кольцевой порт DRP-Port и резервный порт DRP-Port нельзя настроить как кольцевой порт DT-Ring-Port или резервный порт.

- Не рекомендуется одновременно настраивать порты в изолированной группе как порты DT-Ring и резервные порты, а порты DT-Ring и резервные порты нельзя добавлять в изолированную группу.

DT-Ring+

Варианты: Enable/Disable По умолчанию: Disable

Функция: Включение/выключение DT-Ring+.

Резервный порт

Варианты: все порты коммутатора.

Функция: Настройка порта как резервного.

Пояснение: Включите DT-Ring+ прежде чем настраивать резервный порт.

Предупреждение:

Не следует настраивать кольцевой порт в качестве резервного.

VLAN List

Варианты: все созданные VLAN

Функция: Выбор VLAN для кольцевого порта. При наличии нескольких VLAN их можно разделить запятой (,) и дефисом (-), где дефис используется для разделения двух последовательных идентификаторов VLAN, а запятая — для разделения двух непоследовательных идентификаторов VLAN.

3. Просмотрите и измените конфигурацию DT-Ring, как показано на рисунке 123.

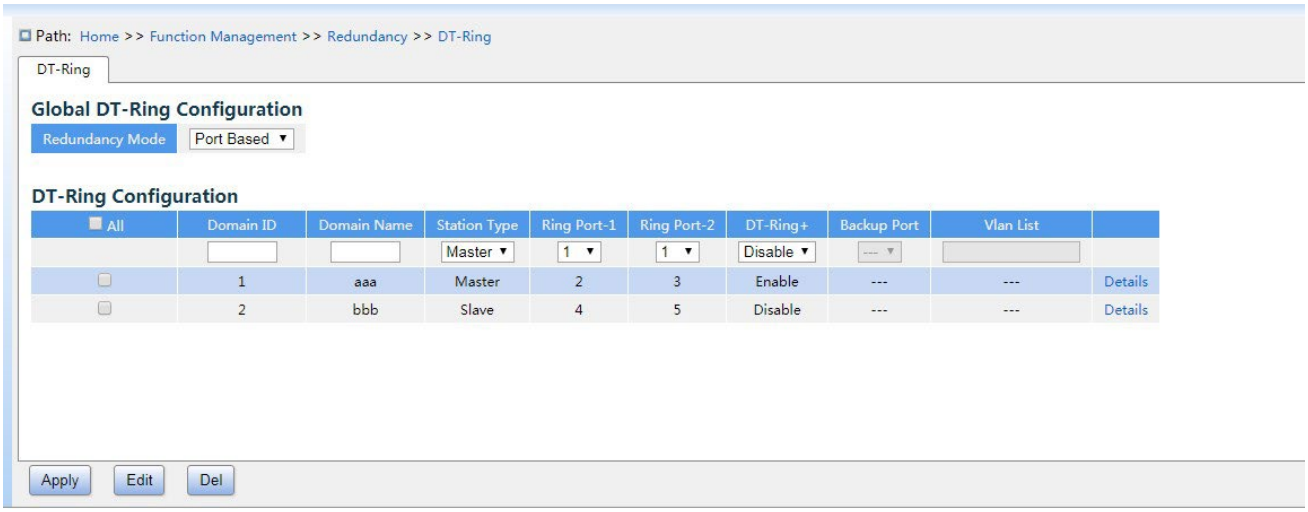


Рисунок 123 Конфигурация DT-Ring

Выберите запись DT-Ring, щелкните <Modify>, чтобы редактировать конфигурацию DT-Ring; щелкните <Delete>, чтобы удалить выбранную запись DT-Ring.

4. Щелкните запись DT-Ring на рисунке 123, чтобы отобразить состояние DT-Ring и порта, как показано на рисунке 124.

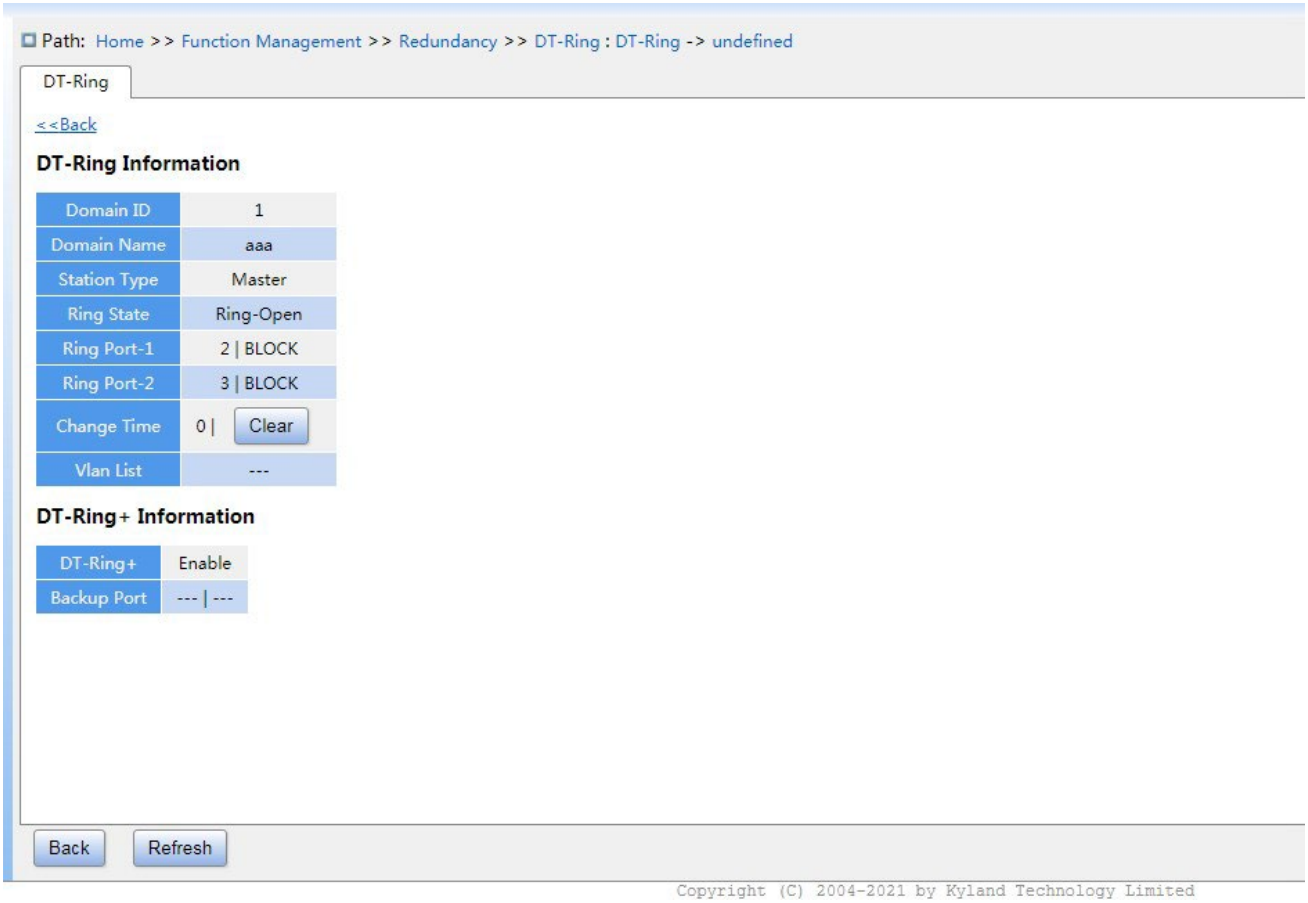


Рисунок 124 Состояние DT-Ring

7.5.1.6 Пример типовой конфигурации

Как показано на рисунке 119, коммутаторы A, B, C и D образуют кольцо 1; коммутаторы E, F, G и H образуют кольцо 2.

Каналы CE и DF являются резервными каналами между кольцом 1 и кольцом 2.

Конфигурация коммутатора A:

1. Настройте Domain ID 1, имя домена a, кольцевые порты 1, 2, тип узла Slave, DT-Ring+ Disable, резервный порт не установлен, как показано на рисунке 121.

Конфигурация коммутатора B:

2. Настройте Domain ID 1, имя домена a, кольцевые порты 1, 2, тип узла Master, DT-Ring+ Disable, резервный порт не установлен, как показано на рисунке 121;

Конфигурация коммутатора C и коммутатора D:

3. Настройте Domain ID 1, имя домена a, кольцевые порты 1, 2, тип узла Slave, DT-Ring+ Enable, резервный порт 3, как показано на рисунке 121.

Конфигурация коммутатора E, коммутатора F и коммутатора G:

4. Настройте Domain ID 2, имя домена b, кольцевые порты 1, 2, тип узла Slave, DT-Ring+ Disable, резервный порт не установлен, как показано на рисунке 121;

Конфигурация коммутатора H:

5. Настройте Domain ID 2, имя домена b, кольцевые порты 1, 2, тип узла Master, DT-Ring+ Disable, резервный порт не установлен, как показано на рисунке 121.

7.5.2 DRP

7.5.2.1 Обзор

Компания Kyland разрабатывает протокол распределенного резервирования (DRP) для передачи данных в сетях кольцевой топологии. Это может предотвратить широковещательные штормы для кольцевых сетей. Когда канал или узел неисправен, резервный канал может взять на себя обслуживание в режиме реального времени, чтобы обеспечить непрерывную передачу данных.

В соответствии со стандартом IEC 62439-6 DRP использует механизм выбора устройства Master без его фиксации. DRP обеспечивает следующие функции:

- Время восстановления, не зависящее от масштаба сети.

DRP обеспечивает время восстановления, не зависящее от масштаба сети, за счет оптимизации механизма пересылки пакетов обнаружения кольца. DRP позволяет сетям восстанавливаться в течение 20 мс благодаря введению отчетов о прерывании в реальном времени, что повышает надежность передачи данных в реальном времени. Эта функция позволяет коммутаторам обеспечивать более высокую надежность для приложений в энергетике, железнодорожном транспорте и многих других отраслях, требующих управления в режиме реального времени.

- Различные функции проверки линии связи

Для повышения стабильности сети DRP предоставляет разнообразные функции обнаружения каналов для типичных сетевых сбоев, включая обнаружение быстрого отключения, обнаружение однонаправленных каналов оптоволокна, проверку качества каналов и проверку работоспособности оборудования, обеспечивая правильную передачу данных.

- Применимость к нескольким сетевым топологиям

Помимо быстрого восстановления для простых кольцевых сетей, DRP также поддерживает сложные кольцевые топологии, такие как пересекающиеся кольца и соприкасающиеся кольца. Кроме того, DRP поддерживает многовариантные решения на основе VLAN, что подходит для различных сетевых приложений с гибкой сетью.

- Мощные функции диагностики и обслуживания

DRP предоставляет мощные механизмы запросов о состоянии и сигналов тревоги для диагностики и обслуживания сети, а также механизм предотвращения непреднамеренных операций и неправильных конфигураций, которые могут привести к кольцевым сетевым штормам.

7.5.2.2 Основные понятия

1. Режимы DRP

DRP имеет два режима: DRP-Port-Based и DRP-VLAN-Based.

DRP-Port-Based: перенаправляет или блокирует пакеты на основе определенных портов.

DRP-VLAN-Based: перенаправляет или блокирует пакеты на основе VLAN. Если порт находится в состоянии блокировки, блокируются только пакеты данных указанной VLAN. Таким образом, на портах соприкасающихся колец можно настроить несколько VLAN. Порт может принадлежать разным кольцам DRP в соответствии с конфигурациями VLAN.

2. Состояния порта DRP

Состояние пересылки: Если порт находится в состоянии пересылки, порт может и принимать, и отправлять пакеты данных. Состояние блокировки: Если порт находится в состоянии блокировки, порт может и принимать пакеты DRP, но не другие пакеты данных.

Основной порт: указывает кольцевой порт (для коммутатора Root), состояние которого настроено как принудительная переадресация пользователем, когда кольцо замкнуто.

Предупреждение:

- Если для коммутатора Root не настроен основной порт, им будет первый порт, состояние связи которого изменилось на «работает» (когда кольцо замкнуто), и он будет в состоянии пересылки.

  Остальные кольцевые порты находятся в состоянии блокировки.

- Порт на устройстве Root в состоянии блокировки может активно отправлять пакеты DRP.

3. Режимы DRP

DRP определяет роли коммутаторов, пересылая пакеты Announce, предотвращая образование петель в кольцах резервирования.

INIT: указывает устройство, на котором включен DRP, а два кольцевых порта находятся в состоянии Link down.

INIT: указывает устройство, на котором включен DRP, а хотя бы один кольцевой порт находится в состоянии Link up. В кольце Root выбирается в соответствии с векторами пакетов Announce. Это может измениться в зависимости от топологии сети. Root периодически отправляет свои собственные пакеты Announce на другие устройства. Состояния кольцевых портов: Один кольцевой порт находится в состоянии пересылки, а другой — в состоянии блокировки. Получив пакет Announce от другого устройства, Root сравнивает вектор пакета с вектором своего собственного пакета Announce. Если вектор полученного пакета больше, Root меняет свою роль на Normal или B-Root в зависимости от состояния канала и ухудшения CRC портов.

B-Root: указывает устройство, на котором включен DRP, отвечающее хотя бы одному из следующих условий: один кольцевой порт находится в состоянии Link up, а другой — в состоянии Link down, деградация CRC, приоритет не менее 200. B-Root сравнивает и пересылает пакеты Announce. Если вектор полученного пакета Announce меньше вектора его собственного пакета Announce, B-Root меняет свою роль на Root; в противном случае он пересылает полученный пакет и не меняет свою роль. Состояния кольцевых портов: Один кольцевой порт находится в состоянии пересылки.

Normal: указывает устройство, на котором включен DRP, и оба кольцевых порта находятся в состоянии Link up без ухудшения CRC, а приоритет больше 200. Normal только пересылает пакеты Announce, но не проверяет содержимое пакетов.

Состояния кольцевых портов: Оба кольцевых порта находятся в состоянии пересылки.

Примечание:
Ухудшение CRC: указывает, что количество пакетов CRC превышает пороговое значение за 15 минут.

7.5.2.3 Реализация

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

Вектор пакета Announce содержит следующую информацию для назначения роли.

Таблица 5 Вектор пакета Announce

Состояние канала	Состояние ухудшения CRC	Скорость ухудшения CRC	Приоритет роли	IP-адрес устройства	MAC-адрес устройства

Состояние канала: Значение устанавливается равным 1, если один кольцевой порт находится в состоянии Link down, и устанавливается в 0, если оба кольцевых порта находятся в состоянии Link up.

Состояние ухудшения CRC: Если ухудшение CRC происходит на одном порту, значение устанавливается равным 1. Если ухудшение CRC не происходит на двух кольцевых портах, значение устанавливается равным 0.

Скорость ухудшения CRC: Соотношение количества пакетов CRC и порогового значения за 15 минут.

Приоритет роли: Значение можно задать через веб-интерфейс.

Параметры в таблице 5 Вектор пакета Announce сравниваются в следующей процедуре:

1. Сначала проверяется значение состояния канала. Устройство с большим значением состояния канала считается имеющим больший вектор.
2. Если два сравниваемых устройства имеют одинаковое значение состояния канала, сравниваются значения состояния ухудшения CRC. Устройство с большим значением состояния ухудшения CRC считается имеющим больший вектор. Если

значение состояния ухудшения CRC всех сравниваемых устройств равно 1, считается, что устройство с большим значением скорости ухудшения CRC имеет больший вектор.

3. Если два сравниваемых устройства имеют одинаковое значение состояния канала и значение ухудшения CRC, значения приоритета ролей, IP-адресов и MAC-адресов сравниваются последовательно.

Устройство с большим значением считается имеющим больший вектор.

4. Устройство с большим вектором будет выбрано в качестве Root.

Примечание:

Только когда значение состояния ухудшения CRC равно 1, значение скорости ухудшения CRC участвует в сравнении векторов. В противном случае векторы сравниваются независимо от значения скорости ухудшения CRC.

➢Реализация режима DRP-Port-Based Роли коммутаторов следующие:

1. При запуске все коммутаторы находятся в состоянии INIT. Когда состояние одного порта изменяется на Link up, коммутатор становится коммутатором Root и отправляет пакеты Announce другим коммутаторам в кольце для выбора.
2. Коммутатор с большим вектором пакета Announce будет выбран в качестве Root. Кольцевой порт, который первым на Root переходит в состояние Link up, находится в состоянии пересылки, а другой кольцевой порт находится в состоянии блокировки. Среди других коммутаторов в кольце коммутатор с одним кольцевым портом в состоянии Link down или ухудшения CRC является коммутатором B-Root. Коммутатор с обоими кольцевыми портами в состоянии Link up и без ухудшения CRC является коммутатором Normal.

Процедура устранения отказов показана на рисунке 125:

1. В исходной топологии A является Root; порт 1 находится в состоянии пересылки, а порт 2 в состоянии блокировки.

B, C и D – коммутаторы Normal, и их кольцевые порты находятся в состоянии пересылки.

2. Когда линия связи CD неисправна, DRP изменяет состояние порта 6 и порта 7 на состояние блокировки. В результате C и D становятся коммутаторами Root. Поскольку коммутаторы A, C и D в настоящий момент являются коммутаторами Root, все они отправляют пакеты Announce. Векторы C и D больше, чем векторы A, потому что порты 7 и 6 находятся в состоянии Link down. В этом случае, если вектор D больше, чем вектор C, D выбирается в качестве Root, а C становится B-Root. При получении пакета Announce от D, A обнаруживает, что вектор D больше, чем его собственный вектор, и оба его кольцевых порта находятся в состоянии Link up. Таким образом, A становится Normal и меняет статус порта 2 на пересылку.
3. Когда связь CD восстанавливается, D по-прежнему является Root, поскольку его вектор больше, чем вектор C.

- Если на D не настроен основной порт, порт 7 по-прежнему находится в состоянии блокировки, а порт 8 — в состоянии пересылки.
- Если порт 7 на D настроен как основной порт, порт 7 переходит в состояние пересылки, а порт 8 — в состояние блокировки.

DRP меняет статус порта 6 на пересылку. В результате C становится коммутатором Normal. Поэтому роли коммутаторов не меняется для восстановления связи.

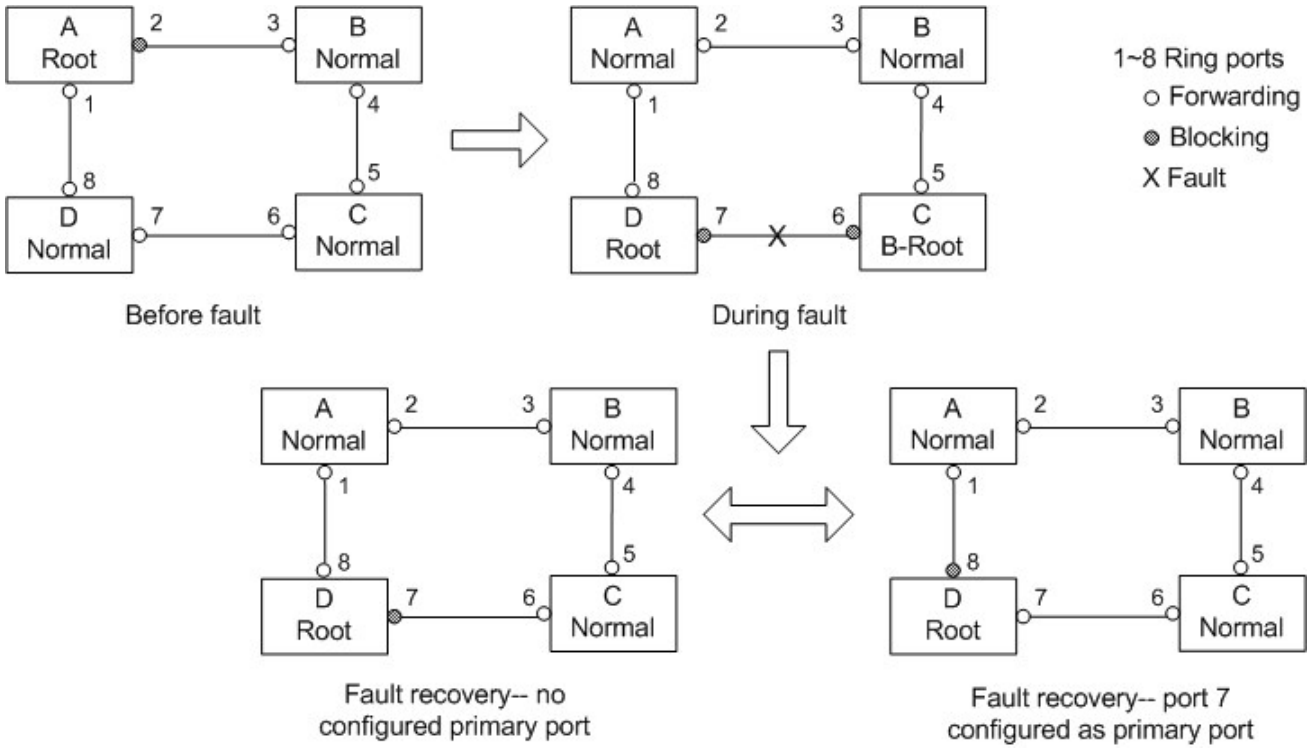


Рисунок 125 Отказ канала DRP

Примечание:

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

- Реализация режима DRP-VLAN-Based

Кольцо DRP-VLAN-Based позволяет пересылать пакеты из разных VLAN по разным путям. Каждый путь пересылки для VLAN образует DRP-VLAN-Based. Различные кольца на основе DRP-VLAN могут иметь разные корневые коммутаторы. Нак показано на следующем рисунке, сконфигурированы два кольца DRP-VLAN-Based.

Линии связи DRP-VLAN10/20-Based: AB-BC-CD-DE-EA.

Линии связи DRP-VLAN30-Based: FB-BC-CD-DE-EF.

Два кольца соприкасаются линиями связи BC, CD и DE. Коммутатор C и коммутатор D используют одни и те же порты в двух кольцах, но используют разные логические каналы на основе VLAN.

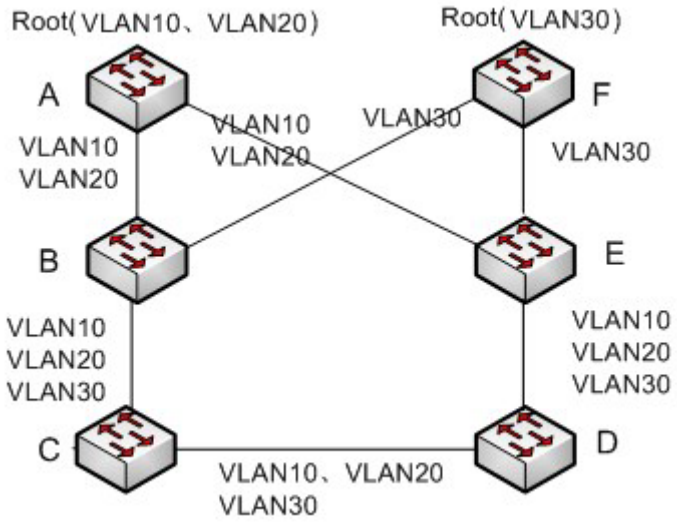


Рисунок 126 DRP-VLAN-Based

Примечание:
Статус порта и назначение ролей для каждого кольца на DRP-VLAN-Based такие же, как и для кольца DRP-Port-Based.

- Резервирование DRP

DRP также может обеспечивать резервирование двух колец DRP, предотвращая образование петель и обеспечивая нормальный обмен данными между кольцами.

Порт резервирования: указывает порт связи между кольцами DRP. Можно настроить несколько портов резервирования, но они должны находиться в одном кольце. Первый резервный порт в состоянии Link up – это резервный порт Master, который находится в состоянии пересылки. Все остальные порты являются портами Slave. Они находятся в состоянии блокировки.

Как показано на рисунке 127, на каждом коммутаторе можно настроить один резервный порт. Резервный порт Master находится в состоянии пересылки, а другие резервные порты — в состоянии блокировки. Если резервный порт Master или его канал выходят из строя, для пересылки данных будет выбран резервный порт Slave.

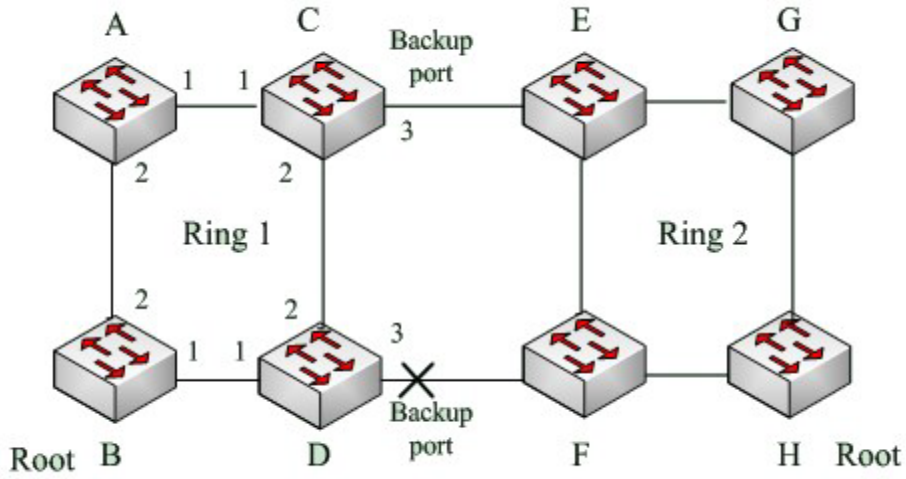


Рисунок 127 Резервирование DRP

Предупреждение:
Изменение статуса соединения влияет на статус резервных портов.

7.5.3 DHP

7.5.3.1 Обзор

Как показано на рисунке 128, коммутаторы A, B, C и D подключены к кольцу. Протокол Dual Homing (DHP) выполняет следующие функции, если он включен на A, B, C и D:

- A, B, C и D могут взаимодействовать друг с другом, не влияя на правильную работу устройств в кольце.
- Если связь между A и B неисправна, A все еще может обмениваться данными с B, C и D через Устройство 1 и Устройство 2.

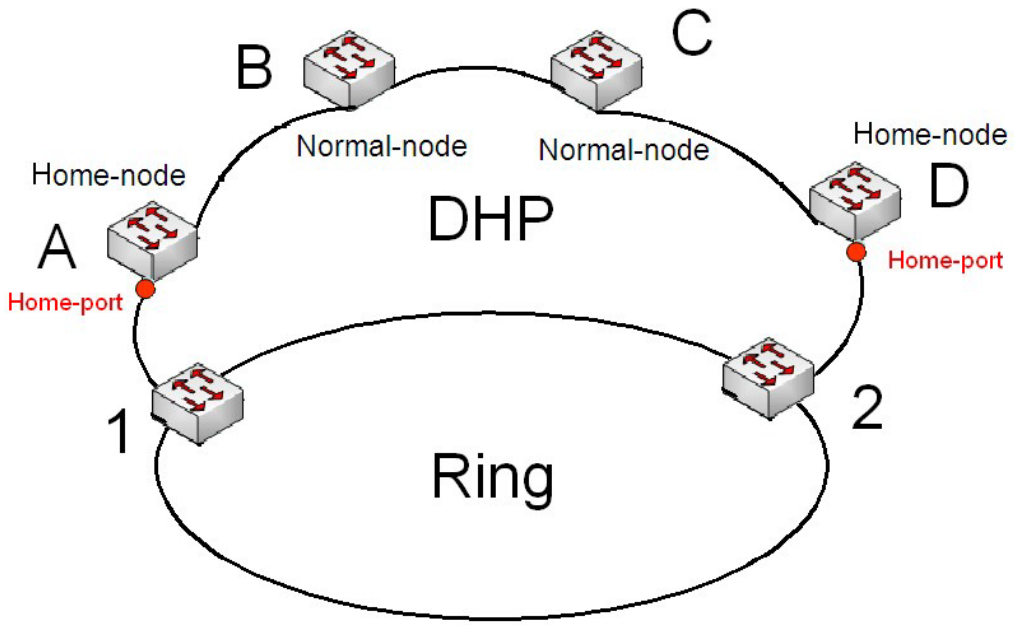


Рисунок 128 Использование DHP

7.5.3.2 Основные понятия

Реализация DHP основана на DRP. Механизм выбора и назначения ролей в DHP такой же, как и в DRP. DHP обеспечивает резервирование канала посредством настройки узла Home, узла Normal и порта Home.

Узел Home: указывает устройства на обоих концах канала DHP и завершает пакеты DRP.

Порт Home: указывает порт, соединяющий узел Home с внешней сетью. Порт Home обеспечивает следующие функции:

- Отправка ответных пакетов Root после получения пакетов Announce от Root. Если Root получает ответные пакеты, состояние кольца идентифицируется как замкнутое. Если Root получает не ответные пакеты, состояние кольца идентифицируется как разомкнутое.
- Блокировка пакетов DRP внешних сетей и изоляция канала DHP от внешних сетей.
- Отправка пакетов очистки входа на подключенные устройства во внешних сетях при изменении топологии канала DHP.

Узел Normal: указывает устройства в канале DHP, за исключением устройств на обоих концах.

Узлы Normal передают ответные пакеты домашних узлов Home.

7.5.3.3 Реализация

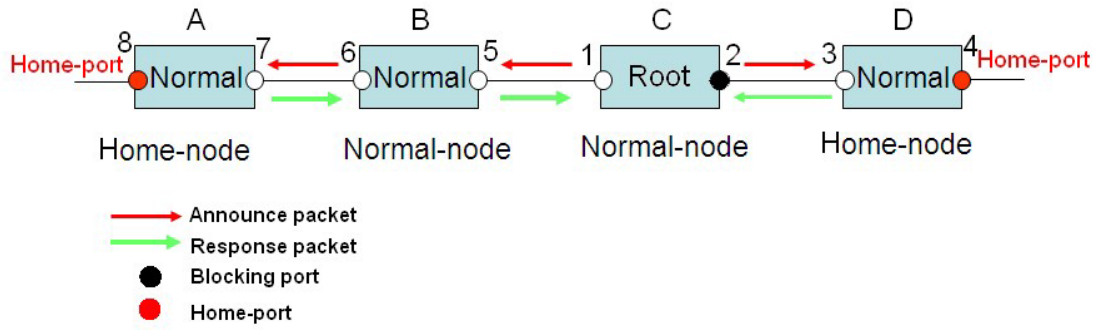


Рисунок 129 Конфигурация DHP

Как показано на рисунке 128, конфигурации A, B, C и D на рисунке 129 следующие:

- Конфигурация DRP: C — Root; порт 2 находится в состоянии блокировки; A, B и D являются узлами Normal; все остальные порты кольца находятся в состоянии пересылки.
- Конфигурация DHP A и D — узлы Home; порт 8 и порт 4 — порты Home; B и C являются узлами Normal.

Реализация:

1. C, Root, отправляет пакеты Announce через два своих кольцевых порта. Порт Home 8 и порт Home 4 завершают полученные пакеты Announce и отправляют ответные пакеты на C. C идентифицирует состояние кольца как замкнутое. Порт 2 находится в состоянии блокировки.
2. Когда канал между A и B заблокирован, топология включает два канала: A и B-C-D.

- A выбран в качестве Root. Порт 7 находится в состоянии блокировки.
- B канале B-C-D B выбран в качестве Root. Порт 6 находится в состоянии блокировки. C становится узлом Normal. Порт 2 находится в состоянии пересылки. A может обмениваться данными с B, C и D через Устройство 1 и Устройство 2, как показано на рисунке 130.

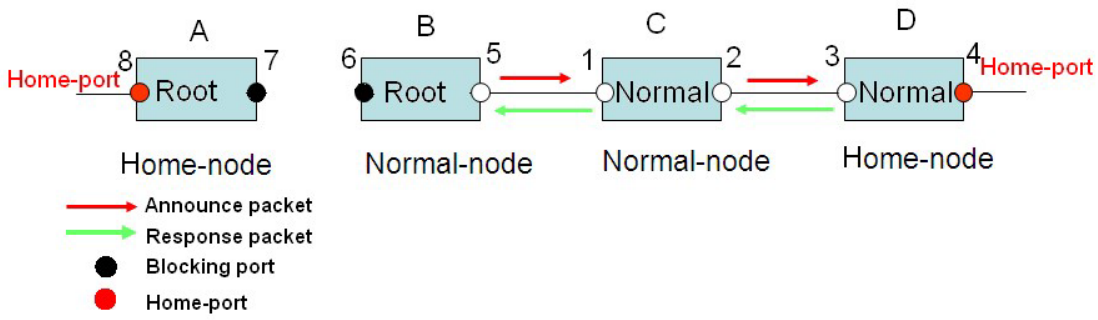


Рисунок 130 Устранение отказа DHP

7.5.3.4 Описание

Конфигурации DRP отвечают следующим требованиям:

- Все коммутаторы в одном кольце должны иметь одинаковый номер домена.
- Одно кольцо содержит только один узел Root, но может содержать несколько узлов B-Root или Normal.
- На каждом коммутаторе можно настроить только два порта для кольца.
- Для двух объединенных колец резервные порты можно настроить только в одном кольце.
- В одном кольце можно настроить несколько портов резервирования.
- На коммутаторе в одном кольце может быть настроен только один резервный порт.

7.5.3.5 Настройка через веб-интерфейс

1. Настройте режим резервирования DRP, как показано на рисунке 131.

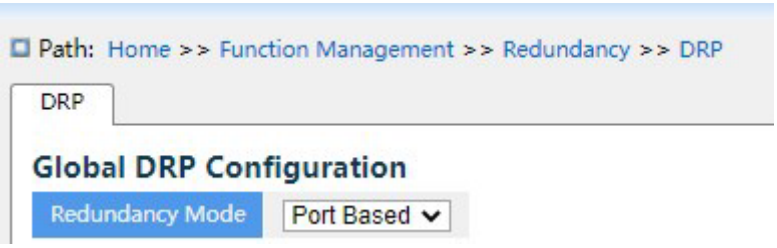


Рисунок 131 Настройка режима резервирования DRP

Режим резервирования

Варианты конфигурации: Port Based/Vlan Based

Конфигурация по умолчанию: Port Based

Функция: Настройка режима резервирования DRP

Предупреждение:

- К кольцевым протоколам на основе портов относятся RSTP, DT-Ring-Port и DRP-Port, а к протоколам на основе VLAN – MSTP, DT-Ring-VLAN и DRP-VLAN.
- Кольцевые протоколы на основе VLAN являются взаимоисключающими, и для одного устройства можно настроить только 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. Настройте DRP-Port-Based и DRP-VLAN-Based, как показано на рисунке 132 и рисунке 133.

DRP Configuration

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	aaa	1	2	Ring Port-1	Normal-Node	---	100	128	---			Disable	Details

Рисунок 132 Настройка DRP-Port-Based

DRP Configuration

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

Рисунок 133 Настройка DRP-VLAN-Based

Domain ID

Диапазон настройки: 1~32

Функция: Каждое кольцо имеет уникальный идентификатор домена. Один коммутатор поддерживает максимум 8

колец на основе VLAN, количество колец на основе портов зависит от количества портов коммутатора.

Domain Name

Диапазон настройки: 1~31 символ

Функция: Задание доменного имени.

Ring Port-1/Ring Port-2

Варианты: все порты коммутатора. Функция:

Выбор двух кольцевых портов.

Предупреждение:

- Кольцевой порт DRP или резервный порт и канал портов являются взаимоисключающими. Кольцевой порт DRP или резервный порт не могут быть добавлены к каналу портов; порт в канале портов не может быть настроен в качестве кольцевого порта DRP или резервного порта.

- Кольцевые порты между кольцевыми протоколами на основе портов RSTP, DT-Ring-Port и DRP-Port являются взаимоисключающими, то есть кольцевой порт и резервный порт DRP-Port не могут быть настроены как порт RSTP; Порт RSTP нельзя настроить как кольцевой порт DRP-Port или резервный порт.

Основной порт

Варианты: --/Ring Port-1/Ring Port-2

Конфигурация по умолчанию: --

Функция: Настройка основного порта. Когда кольцо замкнуто, основной порт коммутатора Root находится в состоянии пересылки.

Режим DHP

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

Конфигурация по умолчанию: Disable

Функция: Отключение DHP или настройка режима DHP.

DHP Home Port

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

Функция: Настройка порта Home для узла Home DHP.

Описание: Если в канале DHP есть только одно устройство, оба кольцевых порта узла Home должны быть настроены как порты Home.

CRC Threshold

Диапазон настройки: 25~65535

Конфигурация по умолчанию: 100

Функция: Настройка порогового значения CRC.

Описание: Этот параметр используется при выборе коммутатора Root. Система подсчитывает количество полученных CRC. Если количество CRC одного кольцевого порта превышает пороговое значение, система считает, что порт имеет ухудшение CRC. В результате в векторе пакета Announce порта значение ухудшения CRC устанавливается равным 1.

Приоритет роли

Диапазон настройки: 0~255

Конфигурация по умолчанию: 128

Функция: Настройка приоритета коммутатора.

Резервный порт

Варианты: все порты коммутатора. Функция:

Настройка резервного порта.

Предупреждение:
Не следует настраивать кольцевой порт в качестве резервного.

VLAN List

Варианты конфигурации: Все созданные VLAN

Функция: Выбор VLAN, управляемой данным кольцом DRP-VLAN-Based

Protocol Vlan ID

Диапазон настройки: 1~4093

Описание: VLAN ID должен быть идентификатором сервисной VLAN.

Функция: Пакеты DRP с VLAN ID служат основой для диагностики и обслуживания кольца DRP-VLAN-Based.

Включение протокола

Варианты конфигурации: Enable/Disable

Функция: Включение протокола DRP для указанного домена.

3. Просмотрите и измените конфигурацию DRP, как показано ниже.

Рисунок 134 Просмотр и изменение конфигурации DRP

Выберите запись DRP, щелкните <Modify>, чтобы редактировать конфигурацию DRP; щелкните <Delete>, чтобы удалить выбранную запись DRP.

4．Настройка Out-Home-Port показана ниже.

Рисунок 135 Настройка Out-Home-Port

Port

Область действия настройки: Все порты коммутатора.

Функция: Механизм обнаружения двойной атрибуции в сочетании со стандартным кольцевым протоколом RSTP (протокол быстрого связующего дерева) обеспечивает двойные каналы атрибуции и предотвращает временные петли при включении и отключении промежуточных каналов, а также обеспечивает быстрое переключение путей пересылки. Когда порт DHP включен, кольцо, образованное нисходящим каналом и основным кольцом, будет находиться в состоянии замыкания кольца, обеспечивая нормальную связь между всеми устройствами.

5. Щелкните запись DRP на рисунке 134, чтобы отобразить роли и состояние портов коммутаторов в кольце DRP, как показано на рисунке 136.

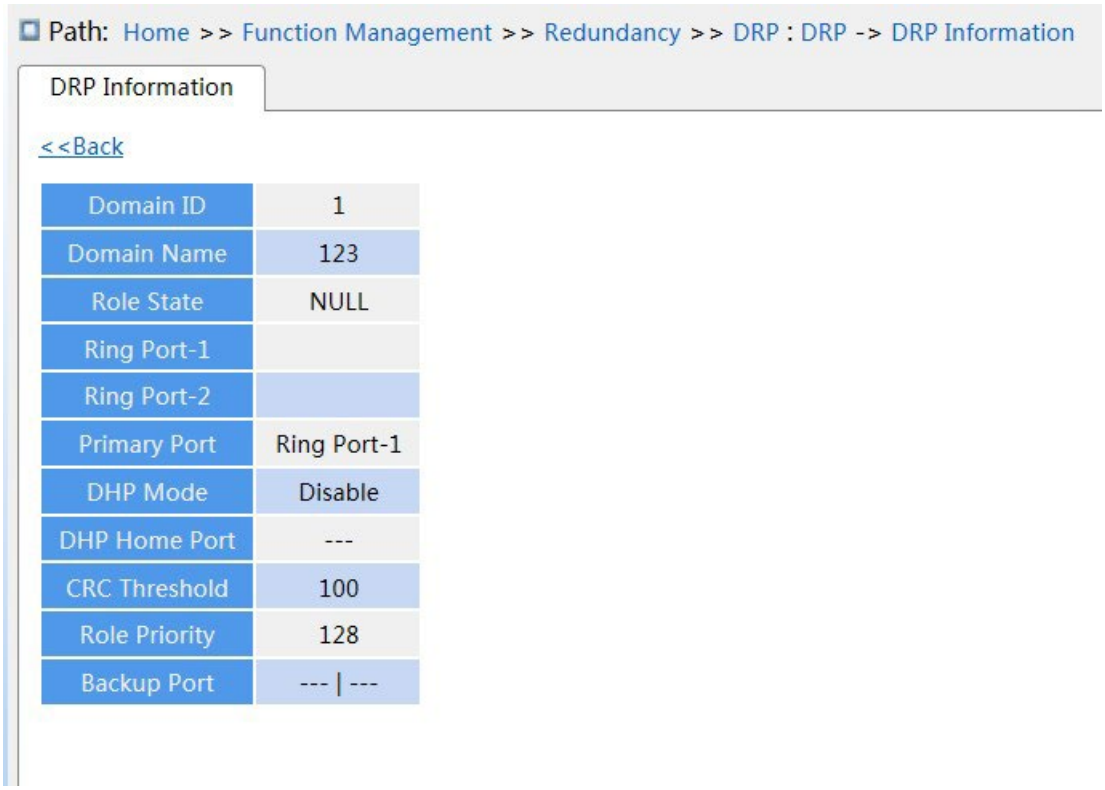


Рисунок 136 Состояние DRP

7.5.3.6 Пример типовой конфигурации

Как показано на рисунке 127, A, B, C и D образуют кольцо 1; E, F, G и H образуют кольцо 2; CE и DF являются резервными каналами Ring 1 и Ring 2.

Конфигурация коммутатора A и коммутатора B:

1. Установите Domain ID 1 и Domain name a. Выберите кольцевой порт 1 и кольцевой порт 2. Сохраните значения по умолчанию для приоритета роли и резервного порта, как показано на рисунке 132.

Конфигурация коммутатора C и коммутатора D:

2. Установите Domain ID 1, Domain name a, резервный порт 3. Выберите кольцевой порт 1 и кольцевой порт 2. Сохраните значения по умолчанию для приоритета роли, как показано на рисунке 132.

Конфигурация коммутаторов E, F, G и H:

3. Установите Domain ID 2 и Domain name b. Выберите кольцевой порт 1 и кольцевой порт 2. Сохраните значения по умолчанию для приоритета роли и резервного порта, как показано на рисунке 132.

7.5.4 Настройка RSTP/STP

7.5.4.1 Введение

Стандартизированный в IEEE802.1D протокол Spanning Tree Protocol (STP) представляет собой протокол локальной сети, используемый для предотвращения широковещательных штормов, вызванных петлями канала, и обеспечения резервирования канала. Устройства с поддержкой STP обмениваются пакетами и блокируют определенные порты, чтобы сократить «петли» на «деревья», предотвращая распространение и бесконечные петли. Недостаток STP заключается в том, что порт, чтобы перейти в состояние пересылки, должен ждать в два раза дольше, чем задержка пересылки.

Чтобы преодолеть этот недостаток, IEEE создает стандарт 802.1w в дополнение к 802.1D. IEEE802.1w определяет протокол Rapid Spanning Tree Protocol (RSTP). По сравнению с STP, RSTP достигает гораздо более быстрой конвергенции, добавляя альтернативный порт и резервный порт для корневого порта и назначенного порта соответственно. Когда корневой порт выходит из строя, альтернативный порт может быстро войти в состояние пересылки.

7.5.4.2 Основные понятия

Корневой мост: служит корнем 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: указывает наилучший порт для передачи от некорневых мостов к корневому мосту. Лучший порт — это порт с наименьшей стоимостью пути до 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: указывает порт для пересылки BPDU на другие устройства или локальные сети. Все порты корневого моста являются назначенными портами.

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

Резервный 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 Сообщения конфигурации BPDU

Для предотвращения образования петель все мосты локальной сети вычисляют связующее дерево. Процесс вычисления включает в себя передачу BPDU между устройствами для определения топологии сети. В таблице 6 показана структура данных BPDU.

Таблица 6 BPDU

…	ID корн. моста	Стоим. корн. пути	ID моста назн.	ID порта назн.	Возр. сообщ.	Макс. возр.	Инт. Hello	Задерж. отпр.	…
…	8 байт	4 байта	8 байт	2 байта	2 байта	2 байта	2 байта	2 байта	…

ID корневого моста: приоритет корневого моста (2 байта) +MAC-адрес корневого моста (6 байт).

Стоимость корневого пути: стоимость пути к корневому мосту.

ID назначенного моста: приоритет назначенного моста (2 байта) +MAC-адрес назначенного моста (6 байт).

ID назначенного порта: приоритет порта+номер порта.

Возраст сообщения: продолжительность распространения BPDU по сети.

Макс. возраст: максимальная продолжительность хранения BPDU на устройстве. Когда возраст сообщения больше чем макс. возраст, BPDU отбрасывается.

Интервал Hello: интервал времени для отправки BPDU.

Задержка отправки: задержка изменения статуса (отбрасывание--обнаружение или обнаружение--пересылка).

7.5.4.4 Реализация

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

1. В начальной фазе

Каждый порт всех устройств генерирует BPDU с самим собой в качестве корневого моста; и идентификатор корневого моста, и идентификатор назначенного моста являются идентификатором локального устройства; стоимость корневого пути равна 0; назначенный порт является локальным портом.

2. Выбор лучшего BPDU

Все устройства отправляют свои собственные BPDU и получают BPDU от других устройств. При получении BPDU каждый порт сравнивает полученный BPDU со своим.

- Если приоритет собственного BPDU выше, то порт не выполняет никаких операций.
- Если приоритет полученного BPDU выше, то порт заменяет локальный BPDU полученным.

Устройства сравнивают BPDU всех портов и определяют лучший BPDU. Принципы сравнения BPDU следующие:

- BPDU с меньшим идентификатором корневого моста имеет более высокий приоритет.
- Если идентификаторы корневого моста двух BPDU совпадают, сравнивается их стоимость корневого пути. Если стоимость корневого пути в BPDU плюс стоимость пути локального порта меньше, приоритет BPDU выше.
- Если стоимость корневого пути двух BPDU также одинакова, идентификаторы назначенного моста, идентификаторы назначенного порта и идентификаторы порта, получающего BPDU, дополнительно сравниваются по порядку. BPDU с меньшим идентификатором имеет более высокий приоритет. BPDU с меньшим идентификатором корневого моста имеет более высокий приоритет.

3. Выбор корневого моста

Корневой мост связующего дерева — это мост с наименьшим идентификатором моста.

4. Выбор корневого порта

Устройство без корневого моста выбирает порт, получающий лучший BPDU, в качестве корневого порта.

5. Расчет BPDU назначенного порта

На основе BPDU корневого порта и стоимости пути корневого порта устройство вычисляет BPDU назначенного порта для каждого порта следующим образом:

- Идентификатор корневого моста заменяется идентификатором корневого моста BPDU корневого порта.
- Стоимость корневого пути заменяется на стоимость корневого пути BPDU корневого порта плюс стоимость пути корневого порта.
- Идентификатор назначенного моста заменяется идентификатором локального устройства.
- Идентификатор назначенного порта заменяется идентификатором локального порта.

6. Выбор назначенного порта.

Если рассчитанный BPDU лучше, то устройство выбирает порт в качестве назначенного порта, заменяет BPDU порта рассчитанным BPDU и отправляет рассчитанный BPDU. Если BPDU порта лучше, то устройство не обновляет BPDU порта и блокирует порт.

Заблокированные порты могут получать и пересылать только пакеты RSTP, но не другие пакеты.

7.5.4.5 Настройка через веб-интерфейс

Задайте параметры времени сетевого моста, как показано ниже.

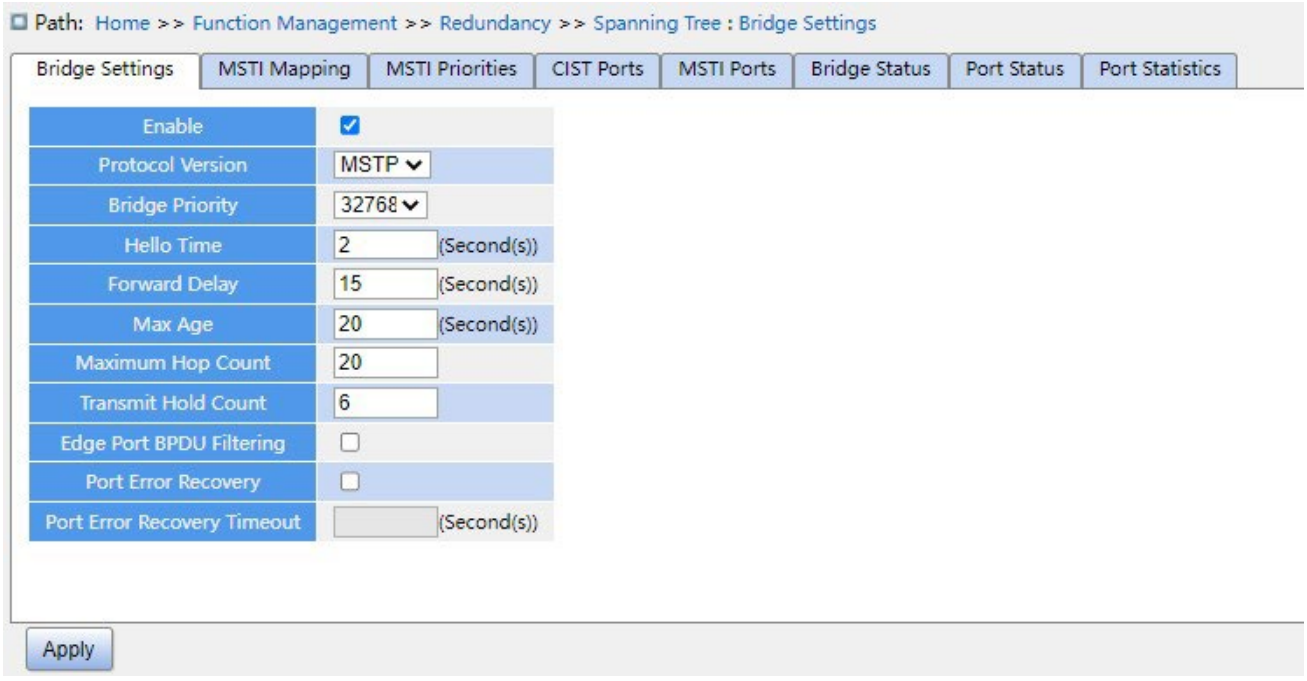


Рисунок 137 Задание параметров времени сетевого моста

Глобальная настройка

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включить или выключить связующее дерево.

Предупреждение:

- К кольцевым протоколам на основе портов относятся RSTP, а к протоколам на основе VLAN – MSTP и DRP-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.

Protocol Priority

Варианты конфигурации: MSTP/RSTP/STP

Конфигурация по умолчанию: MSTP

Функция: Выбор протокола связующего дерева.

Bridge Priority

Диапазон настройки: 0~61440. Шаг составляет 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 настройки: 1~10 с

Конфигурация по умолчанию: 2 с

Функция: Настройка интервала времени для отправки BPDU.

Forward Delay

Диапазон настройки: 4~30 с

Конфигурация по умолчанию: 15 с

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

Max Age

Диапазон настройки: 6~40 с

Конфигурация по умолчанию: 20 с

Функция: Максимальная продолжительность хранения BPDU на устройстве.

Описание: Если значение возраста сообщения в BPDU больше указанного значения, то BPDU отбрасывается.

Предупреждение:

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

Maximum Hop Count

Диапазон настройки: 6~40

Конфигурация по умолчанию: 20

Функция: Настройка максимального числа транзитных участков региона MST. Максимальное число транзитных участков региона MST ограничивает масштаб региона MST; максимальное количество транзитных участков регионального корня равно максимальному количеству транзитных участков региона MST.

Описание: Начиная с корневого моста связующего дерева в регионе MST, из числа транзитных участков вычитается 1, когда BPDU проходит через устройство в регионе. Устройство отбрасывает BPDU с количеством транзитных участков 0.

Предупреждение:

- Действительна конфигурация только с максимальным количеством транзитных участков корневого моста в регионе MST. Устройство, не являющее корневым, использует конфигурацию транзитных участков корневого моста.

- Рекомендуется использовать настройки по умолчанию.

Transmit Hold Count

Диапазон настройки: 1~10

Конфигурация по умолчанию: 6

Функция: Задание максимального количества пакетов BPDU, которое может быть отправлено портом в течение каждого промежутка Hello Time.

Edge Port BPDU Filtering

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение и выключения режима получения и отправки граничным портом пакетов BPDU.

Port Error Recovery

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Контроль возможности порта автоматически восстанавливаться из состояния ошибки в нормальное состояние.

Port Error Recovery Timeout

Диапазон настройки: 30~86400 с

Функция: Задание для порта времени для восстановления из состояния ошибки в нормальное состояние.

2. Настройте порт RSTP, как показано ниже.

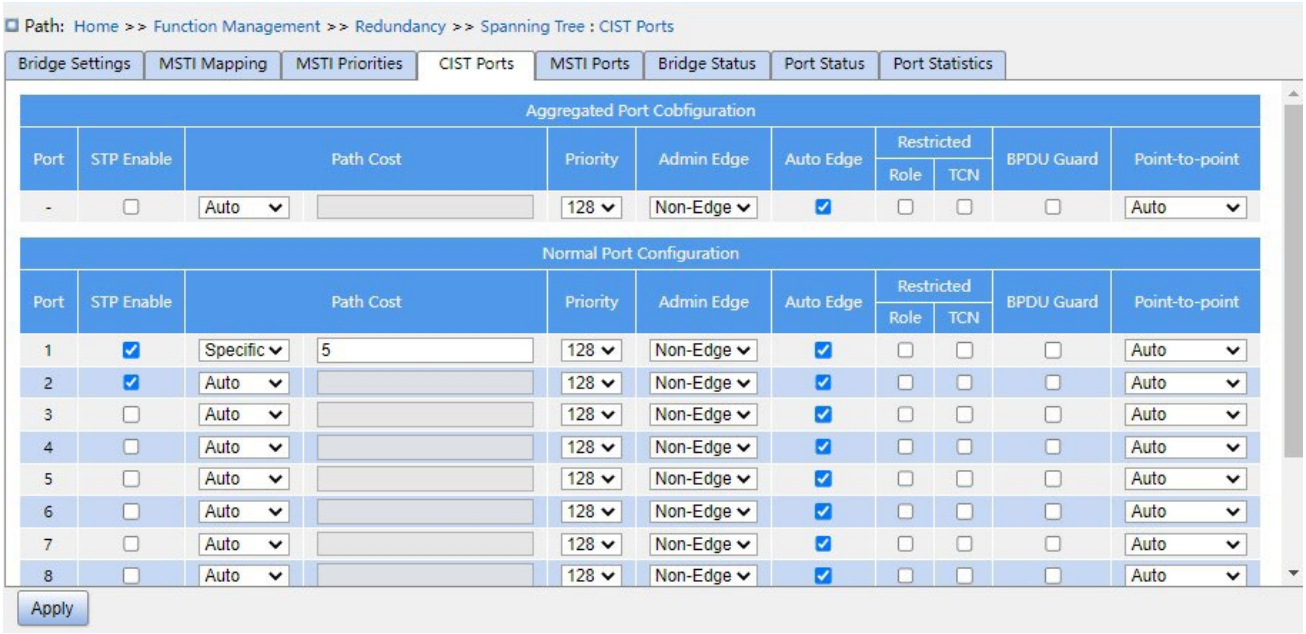


Рисунок 138 Настройка порта RSTP

CIST

Функция: Рассмотрение группы агрегации как порта CIST и настройка ее служебных данных и приоритета пути в указанном экземпляре.

STP Enabled

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение или выключение STP/RSTP для порта.

Предупреждение:

- Канал портов и порт RSTP являются взаимоисключающими. Порты в канале портов нельзя настроить как порт RSTP, а порт RSTP нельзя добавить в канал портов.
- Кольцевые порты между кольцевыми протоколами на основе портов RSTP, DT-Ring-Port и DRP-Port являются взаимоисключающими, то есть порт RSTP нельзя настроить как кольцевой порт DRP-Port/DT-Ring-Port или резервный порт DRP-Port/DT-Ring-Port; Кольцевой порт DRP-Port/DT-Ring-Port и резервный порт DRP-Port/DT-Ring-Port нельзя настроить как порт RSTP.

Path Cost

Варианты конфигурации: Auto/Specific (1~200000000)

Конфигурация по умолчанию: Auto

Описание: Стоимость пути порта используется для расчета наилучшего пути. Значение параметра зависит от полосы пропускания. Чем больше значение, тем ниже стоимость. Можно изменить роль порта, изменив значение параметра стоимости пути. Чтобы настроить значение вручную, выберите значение No для параметра Cost Count.

Priority

Диапазон настройки: 0~240. Шаг составляет 16.

Конфигурация по умолчанию: 128

Функция: Настройка приоритета порта, определяющего роли портов.

Admin Edge

Варианты конфигурации: Non-Edge/Edge

Конфигурация по умолчанию: Non-Edge

Функция: Настройка порта в режим граничного порта.

Описание: Когда порт напрямую подключен к терминалу и не подключен к другим устройствам или общему сегменту сети, этот порт считается граничным портом. Граничный порт может быстро перейти из состояния блокировки в состояние пересылки без задержки ожидания. После того как граничный порт получает пакеты BPDU, он перестает быть граничным портом.

Auto Edge

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Enable

Функция: Включение функции автоматического обнаружения граничного порта.

Restricted Role

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Порт с ограничением роли никогда не будет выбран в качестве корневого узла, даже если ему предоставлен 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: Режим контроля перехода граничного порта в состояние Error-Disable и закрытия при получении пакетов BPDU.

Point-to-point

Варианты конфигурации: Auto/Forced True/Forced False

Конфигурация по умолчанию: Auto

Функция: Настройка типа соединения для порта. Если порт подключен к каналу «точка-точка», порт может быстро перейти в другое состояние.

Описание: **Auto** указывает, что коммутатор автоматически определяет тип канала на основе того, что порт работает в дуплексном режиме. Когда порт работает в полнодуплексном режиме, коммутатор считает, что тип соединения, подключенного к порту, — «точка-точка»; когда порт работает в полудуплексном режиме, коммутатор считает, что тип соединения, подключенного к порту, является общим. Принудительное задание соединения «точка-точка» означает, что соединение, подключенное к порту, является соединением «точка-точка», а принудительное задание совместного использования означает, что соединение, подключенное к порту, является общим соединением.

7.5.4.6 Пример типовой конфигурации

Приоритеты коммутаторов A, B и C: 0, 4096 и 8192. Стоимость пути для соединений составляет 4, 5 и 10, как показано на рисунке 139.

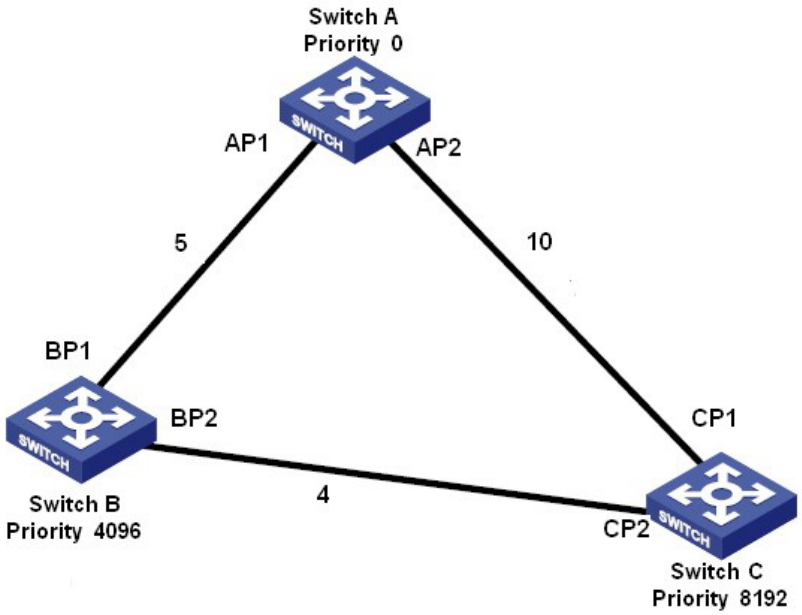


Рисунок 139 Пример настроек RSTP

Конфигурация коммутатора A:

1. Установите приоритет моста 0 и значения по умолчанию для временных параметров, как показано на рисунке 137.
2. Установите стоимость пути для порта 1 – 5 и для порта 2 – 10, как показано на рисунке 138.

Конфигурация коммутатора B:

1. Установите приоритет моста 4096 и значения по умолчанию для временных параметров, как показано на рисунке 137.
2. Установите стоимость пути для порта 1 – 5 и для порта 2 – 4, как показано на рисунке 138.

Конфигурация коммутатора C:

1. Установите приоритет моста 8192 и значения по умолчанию для временных параметров, как показано на рисунке 137.
2. Установите стоимость пути для порта 1 – 10 и для порта 2 – 4, как показано на рисунке 138.

- Приоритет коммутатора A равен 0, а его корневой идентификатор наименьший. Таким образом, коммутатор A является корневым мостом.
- Стоимость пути от AP1 к BP1 равна 5, а от AP2 к BP2 равна 14. Таким образом, BP1 является корневым портом.

- Стоимость пути от AP1 к CP2 равна 9, а от AP2 к CP1 равна 10. Таким образом, CP2 является корневым портом, а BP2 является назначенным портом.

7.5.5 Настройка MSTP

7.5.5.1 Введение

Хотя протокол RSTP обеспечивает быструю конвергенцию, у него, как и у STP, есть следующий недостаток: все мосты в локальной сети совместно используют одно связующее дерево, и пакеты всех VLAN пересылаются по связующему дереву. Как показано на рисунке 140, некоторые конфигурации могут блокировать соединение между коммутатором A и коммутатором C. Поскольку коммутатор B и коммутатор D не входят в сеть VLAN 1, они не могут пересылать пакеты сети VLAN 1. В результате порт VLAN 1 коммутатора A не может обмениваться данными с портом коммутатора C.

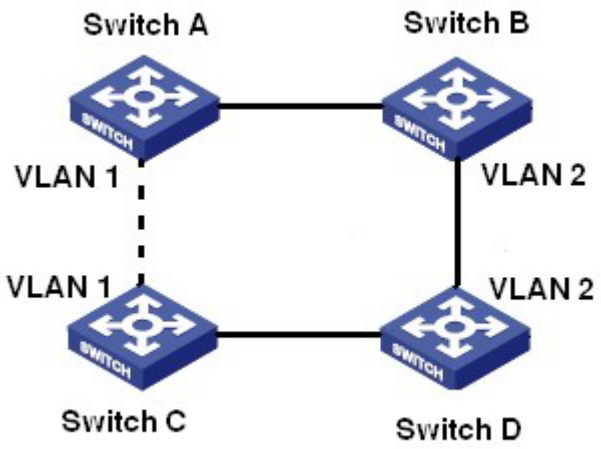


Рисунок 140 Недостатки RSTP

Чтобы решить эту проблему, появился протокол Multiple Spanning Tree Protocol (MSTP). Он обеспечивает как быструю конвергенцию, так и отдельные пути пересылки для трафика разных VLAN, обеспечивая лучший механизм распределения нагрузки для избыточных каналов.

MSTP отображает одну или несколько VLAN в один экземпляр. Коммутаторы с одинаковой конфигурацией образуют регион. Каждый регион содержит несколько

взаимно независимых связующих деревьев. Регион выступает коммутационным узлом. Он участвует в вычислении с другими регионами на основе алгоритма связующего дерева, вычисляя общее связующее дерево. На основе этого алгоритма сеть на рисунке 140 формирует топологию, показанную на рисунке 141. Коммутатор A и коммутатора B находятся в Region1. Ни одна связь не заблокирована, так как регион не содержит петель. То же самое и с Region2. Region1 и Region2 аналогичны узлам коммутатора. Эти два «коммутатора» образуют петлю. Таким образом, связь должна быть заблокирована.

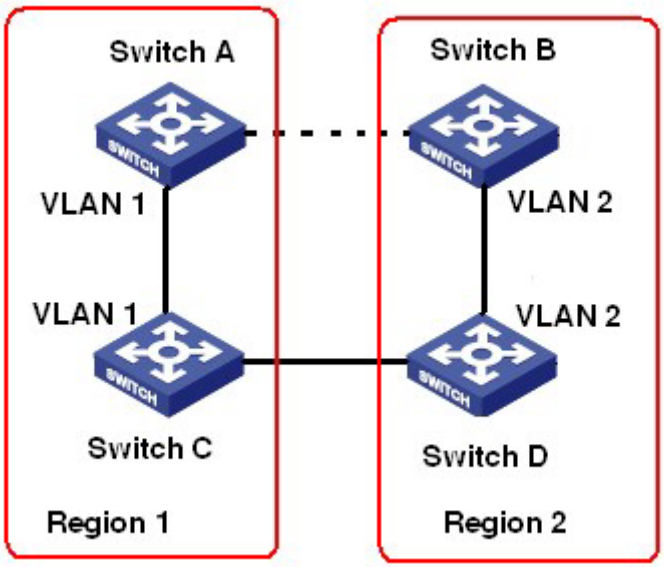


Рисунок 141 Топология MSTP

7.5.5.2 Основные понятия

Ознакомьтесь с концепцией MSTP, показанной на рисунке 142 и рисунке 145.

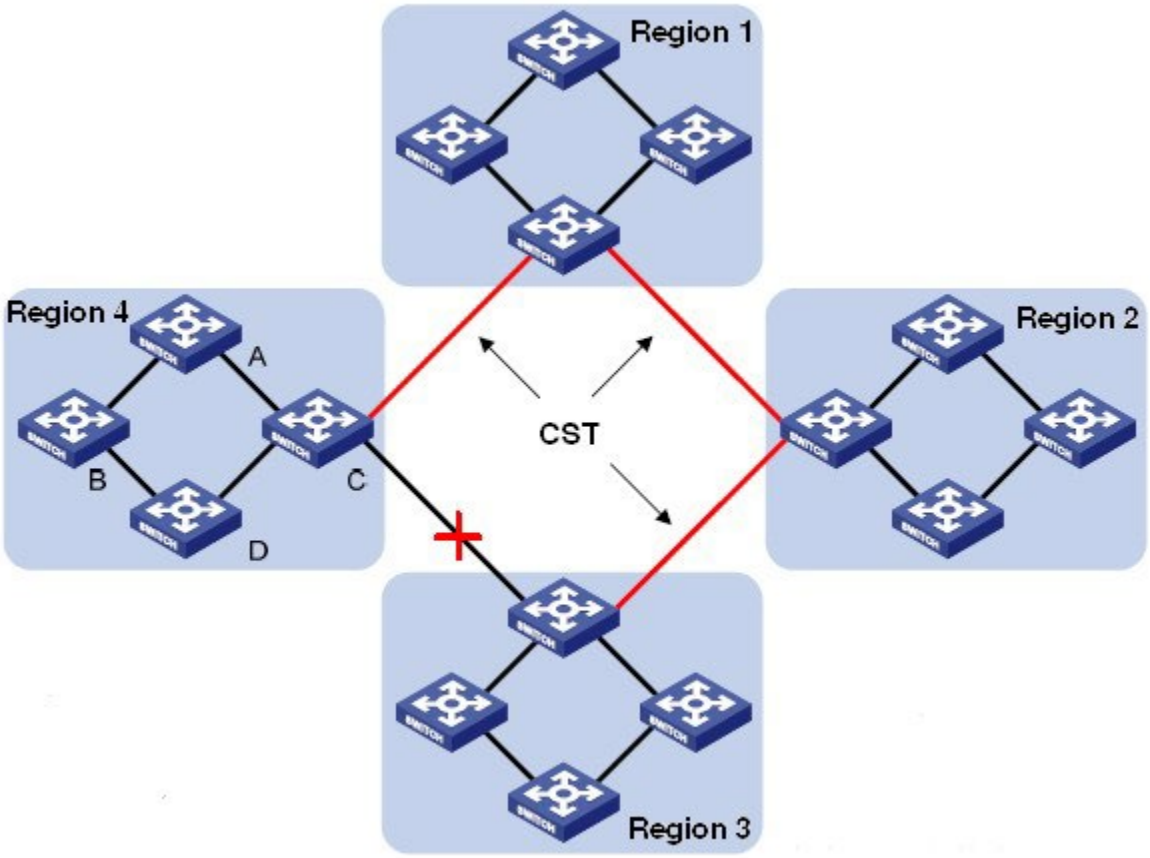


Рисунок 142 Концепция MSTP

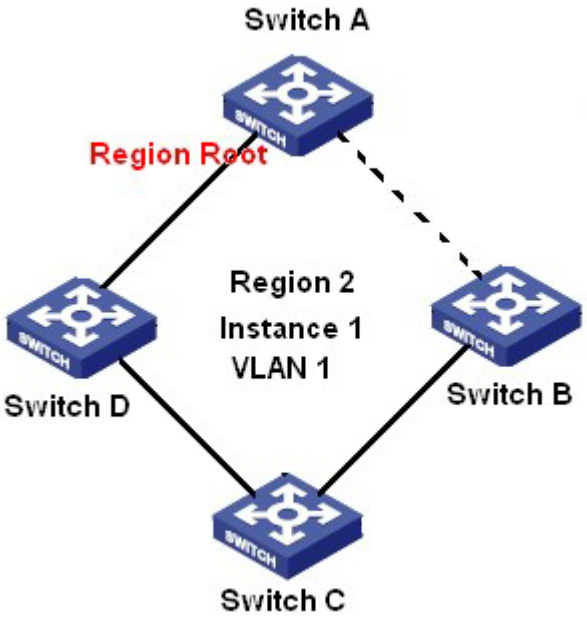


Рисунок 143 Сопоставление VLAN 1 с экземпляром 1

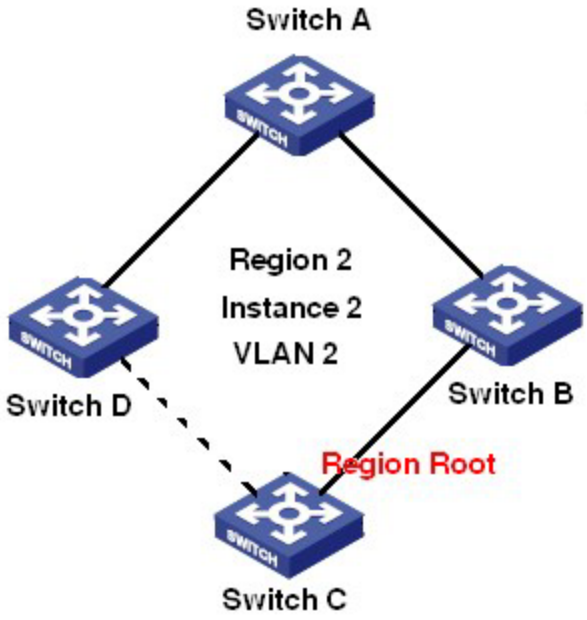


Рисунок 144 Сопоставление VLAN 2 с экземпляром 2

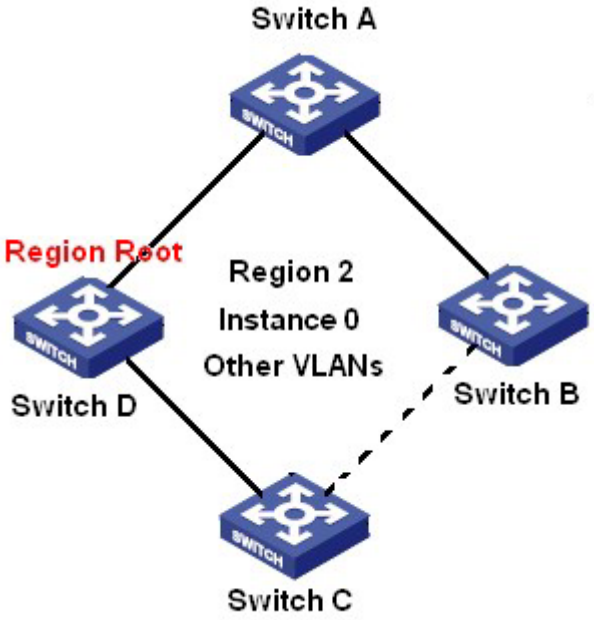


Рисунок 145 Сопоставление другой VLAN с экземпляром 0

Экземпляр: набор из нескольких VLAN. Одна VLAN (как показано на рисунке 143 и рисунке 144) или несколько VLAN с одинаковой топологией (как показано на рисунке 145) могут быть сопоставлены с одним экземпляром; то есть одна VLAN может образовывать связующее дерево, а несколько VLAN могут совместно использовать одно связующее дерево. Разные экземпляры сопоставляются с разными связующими деревьями. Экземпляр 0 – это связующее дерево для устройств всех регионов, в то

время как остальные экземпляры – это связующие деревья для устройств конкретного региона.

Multiple Spanning Tree Region (регион MST): Коммутаторы с одинаковым именем региона MSTP, уровнем версии и сопоставлением VLAN–экземпляр принадлежат одному региону MST. Как показано на рисунке 142, регион 1, регион 2, регион 3 и регион 4 – это четыре различных региона MST.

Таблица сопоставления VLAN: состоит из сопоставления VLAN и связующих деревьев. На

рисунке 142, таблица сопоставления VLAN региона 2 – это сопоставление VLAN 1 и экземпляра 1, как показано на рисунке 143; VLAN 2 сопоставляется с экземпляром 2, как показано на рисунке 144. Другие VLAN сопоставляются с экземпляром 0, как показано на рисунке 145.

Общее и внутреннее связующее дерево (CIST): указывает экземпляр 0, то есть связующее дерево, охватывающее все устройства в коммутируемой сети. Как показано на рисунке 142, CIST состоит из IST и CST.

Внутреннее связующее дерево (IST): указывает сегмент CIST в регионе MST, то есть экземпляр 0 каждого региона, как показано на рисунке 145.

Общее связующее дерево (CST): указывает связующее дерево, соединяющее все регионы MST в коммутируемой сети. Если каждый регион MST является узлом, CST - это связующее дерево, вычисленное этими узлами на основе STP/RSTP. Как показано на рисунке 142, красные линии обозначают связующее дерево.

MSTI (Несколько экземпляров связующего дерева): один регион MST может образовывать несколько связующих деревьев, и они не зависят друг от друга. Каждое связующее дерево является MSTI, как показано на рисунке 143 и рисунке 144. IST также является специальным MSTI.

Общий корень: указывает корневой мост CIST. Коммутатор с наименьшим идентификатором корневого моста в сети является общим корневым коммутатором.

В регионе MST связующие деревья имеют разную топологию и их корни регионов также могут быть разными. Как показано на рисунке 143, рисунке 144 и рисунке 145, эти три экземпляра имеют разные корни региона. Корневой мост MSTI

рассчитывается на основе STP/RSTP в текущем регионе MST. Корневой мост IST — это устройство, которое подключено к другому региону MST и выбрано на основе полученной информации о приоритете.

Граничный порт: указывает порт, который соединяет регион MST с другим регионом MST, рабочим регионом STP или рабочим регионом RSTP.

Состояние порта: Порт может находиться в одном из следующих состояний в зависимости от того, изучает ли он MAC-адреса и пересылает ли трафик.

Состояние Forwarding: указывает, что порт изучает MAC-адреса и пересылает трафик.

Состояние Learning: указывает, что порт изучает MAC-адреса, но не пересылает трафик.

Состояние Discarding: указывает, что порт не изучает MAC-адреса и не пересылает трафик. Корневой порт: указывает лучший порт от некорневого моста к корневому мосту, то есть порт с наименьшей стоимостью 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 Forwarding, Learning или Discarding.

Назначенный порт: указывает порт для пересылки BPDU на другие устройства или локальные сети. Все порты корневого моста являются назначенными портами. Назначенный порт может находиться в состоянии Forwarding, Learning или Discarding.

Главный порт: указывает порт, который соединяет регион MST с общим корнем. Порт имеет кратчайший путь к общему корню. Исходя из CST, главный порт - это корневой порт региона (как узел). Главный порт - это специальный граничный порт. Это корневой порт для CIST и главный порт для других экземпляров. Главный порт может находиться в состоянии Forwarding, Learning или Discarding.

Альтернативный порт: указывает резервный порт корневого порта или главного порта. Если корневой порт или главный порт выходит из строя, альтернативный порт становится новым корневым портом или главным портом. Главный порт может находиться в только состоянии Discarding.

Резервный порт: указывает резервный порт назначенного порта. Когда назначенный порт выходит из строя, резервный порт становится новым назначенным портом и

пересылает данные без задержки. Резервный порт может находиться в только состоянии Discarding.

7.5.5.3 Реализация MSTP

MSTP делит сеть на несколько регионов MST. CST рассчитывается между регионами. Для региона рассчитывается несколько связующих деревьев. Каждое связующее дерево – это MSTI. Экземпляр 0 – это IST, остальные экземпляры – MSTI.

1. Расчет CIST

- Устройство отправляет и получает пакеты BPDU. На основе сравнения сообщений конфигурации MSTP устройство с наивысшим приоритетом выбирается в качестве общего корня CIST.
- IST вычисляется в каждом регионе MST.
- Каждый регион MST рассматривается как отдельное устройство, и CST рассчитывается между регионами.
- CST и IST составляют CIST всей сети.

2. Расчет MSTI

В регионе MST MSTP создает различные связующие деревья для VLAN на основе сопоставления между VLAN и связующими деревьями. Каждое связующее дерево рассчитывается независимо. Процесс расчета подобен процессу в STP.

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

7.5.5.4 Настройка через веб-интерфейс

1. Задайте параметры времени сетевого моста, как показано ниже.

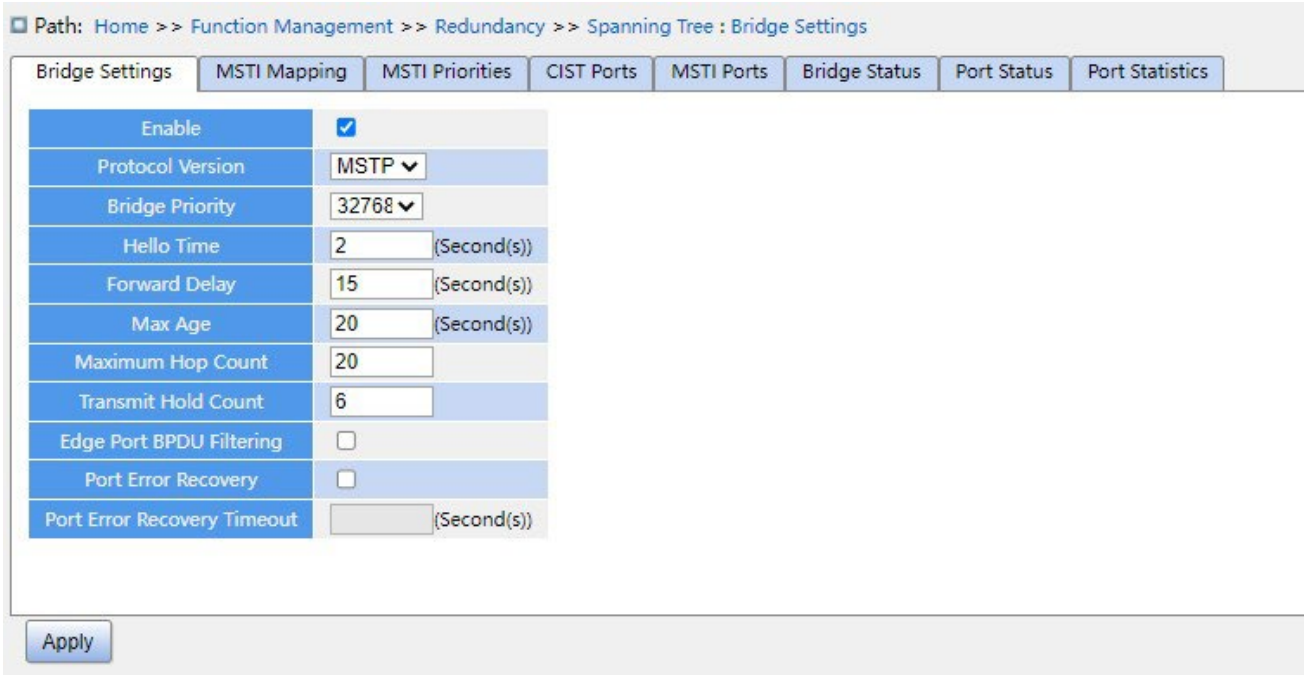


Рисунок 146 Задание параметров времени сетевого моста

Глобальная настройка

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включить или выключить связующее дерево.

Предупреждение:

- К кольцевым протоколам на основе портов относятся RSTP и DRP-Port, а к протоколам на основе VLAN – MSTP и DRP-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.

Protocol Priority

Варианты конфигурации: MSTP/RSTP/STP

Конфигурация по умолчанию: MSTP

Функция: Выбор протокола связующего дерева.

Bridge Priority

Диапазон настройки: 0~61440. Шаг составляет 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 настройки: 1~10 с

Конфигурация по умолчанию: 2 с

Функция: Настройка интервала времени для отправки BPDU.

Forward Delay

Диапазон настройки: 4~30 с

Конфигурация по умолчанию: 15 с

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

Max Age

Диапазон настройки: 6~40 с

Конфигурация по умолчанию: 20 с

Функция: Максимальная продолжительность хранения BPDU на устройстве.

Описание: Если значение возраста сообщения в BPDU больше указанного значения, то BPDU отбрасывается.

Предупреждение:

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

Maximum Hop Count

Диапазон настройки: 6~40

Конфигурация по умолчанию: 20

Функция: Настройка максимального числа транзитных участков региона MST. Максимальное число транзитных участков региона MST ограничивает масштаб региона MST; максимальное количество транзитных участков регионального корня равно максимальному количеству транзитных участков региона MST.

Описание: Начиная с корневого моста связующего дерева в регионе MST, из числа транзитных участков вычитается 1, когда BPDU проходит через устройство в регионе. Устройство отбрасывает BPDU с количеством транзитных участков 0.

Предупреждение:

- Действительна конфигурация только с максимальным количеством транзитных участков корневого моста в регионе MST. Устройство, не являющее корневым, использует конфигурацию транзитных участков корневого моста.
- Рекомендуется использовать настройки по умолчанию.

Transmit Hold Count

Диапазон настройки: 1~10

Конфигурация по умолчанию: 6

Функция: Задание максимального количества пакетов BPDU, которое может быть отправлено портом в течение каждого промежутка Hello Time.

Edge Port BPDU Filtering

Варианты конфигурации: Enable/Disable

: Disable

Функция: Включение и выключения режима получения и отправки граничным портом пакетов BPDU.

Port Error Recovery

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Контроль возможности порта автоматически восстанавливаться из состояния ошибки в нормальное состояние.

Port Error Recovery Timeout

Диапазон настройки: 30~86400 с

Функция: Задание для порта времени для восстановления из состояния ошибки в нормальное состояние.

2. Настройте сопоставление MSTI, как показано ниже.

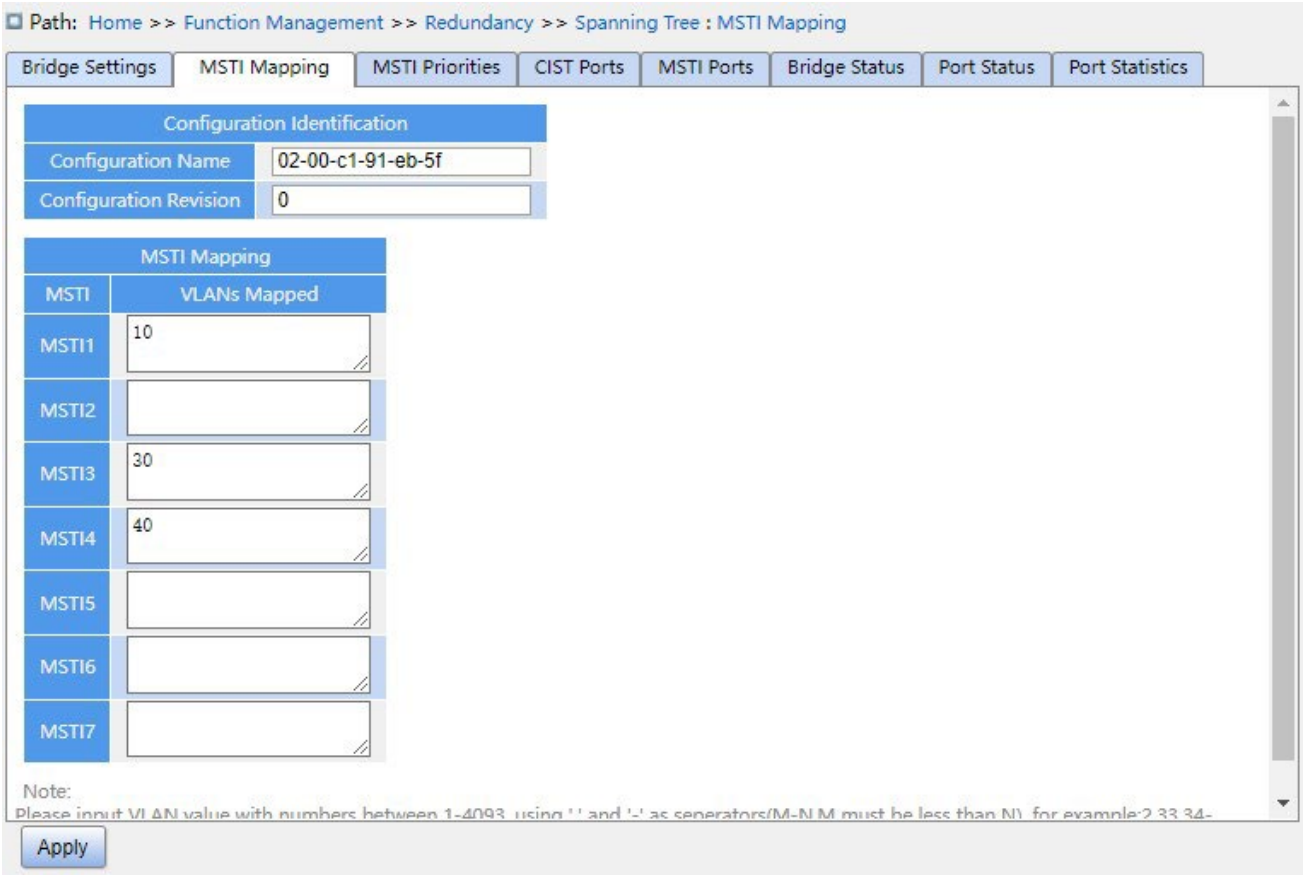


Рисунок 147 Настройка сопоставления MSTI

Configuration Name

Диапазон настройки: 1-32 символа. По умолчанию: MAC-адрес устройства

Функция: Задание имени региона MST.

Configuration Revision

Варианты конфигурации: 0~65535

Конфигурация по умолчанию: 0

Функция: Настройка параметра версии региона MSTP.

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

VLANs Mapped

Диапазон настройки: 1~4094

Функция: Настройка таблицы сопоставления VLAN в регионе MST. При наличии нескольких VLAN их можно разделить запятой (,) и дефисом (-), где дефис используется для разделения двух последовательных идентификаторов VLAN, а запятая — для разделения двух непоследовательных идентификаторов VLAN.

Описание: По умолчанию все VLAN сопоставлены экземпляру 0. Одна VLAN сопоставляется только одному экземпляру 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 с экземпляром 0.

3. Настройте приоритета моста коммутатора в назначенном экземпляре, как показано ниже.

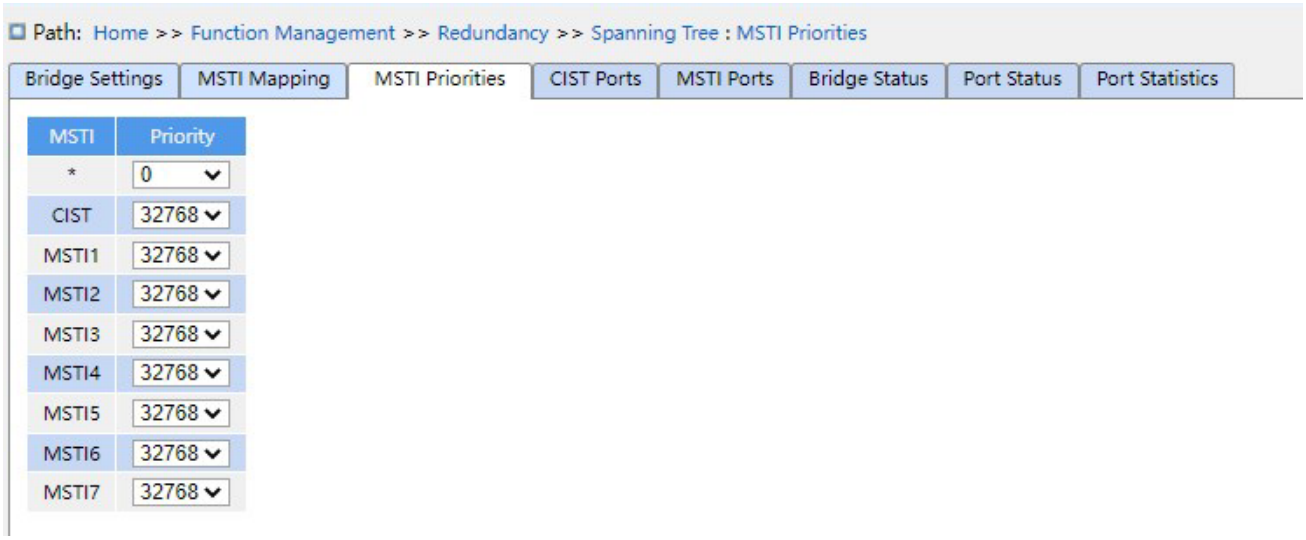


Рисунок 148 Настройка приоритета моста коммутатора в назначенном экземпляре

Priority

Диапазон настройки: 0~61440 с шагом 4096

Конфигурация по умолчанию:: 32768

Функция: Настройка приоритета моста коммутатора в назначенном экземпляре.

Описание: Приоритет моста определяет, может ли коммутатор быть выбран в качестве регионального корня экземпляра связующего дерева. Чем меньше значение, тем выше приоритет. Установив более низкий приоритет, можно назначить определенное устройство корневым мостом связующего дерева. Устройство с поддержкой MSTP можно настроить с разными приоритетами в разных экземплярах связующего дерева.

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

4. Настройте порты CIST, как показано ниже.

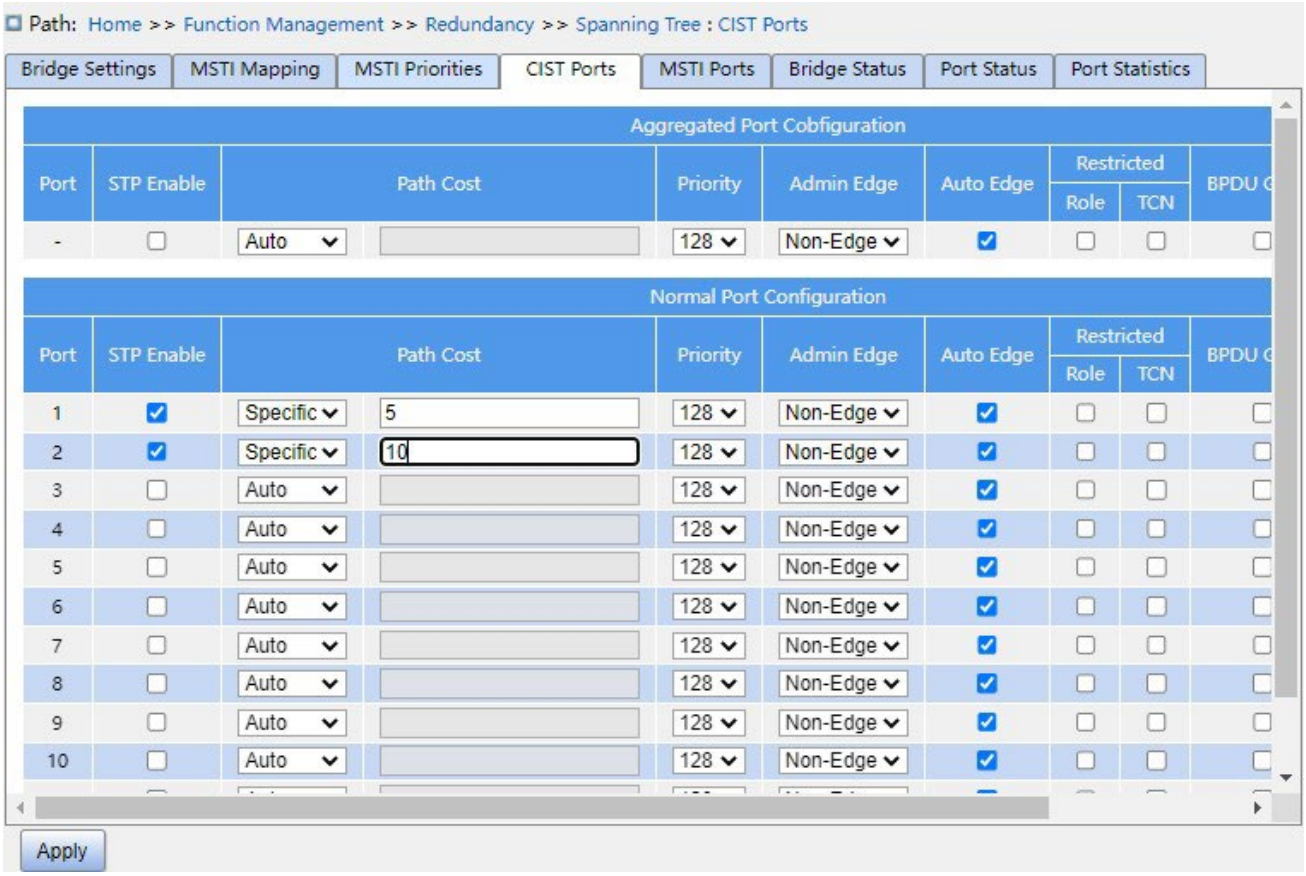


Рисунок 149 Настройка портов CIST

STP Enabled

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение или выключение STP/RSTP для порта.

Предупреждение:
Канал портов и порт MSTP являются взаимоисключающими. Порты в канале портов нельзя настроить как порт MSTP, а порт MSTP нельзя добавить в канал портов.

Path Cost

Варианты конфигурации: Auto/Specific (1~200000000)

Конфигурация по умолчанию: Auto

Описание: Стоимость пути порта используется для расчета наилучшего пути. Значение параметра зависит от полосы пропускания. Чем больше значение, тем ниже стоимость. Можно изменить роль порта, изменив значение параметра стоимости пути. Чтобы настроить значение вручную, выберите значение No для параметра Cost Count.

Priority

Диапазон настройки: 0~240. Шаг составляет 16.

Конфигурация по умолчанию: 128

Функция: Настройка приоритета порта, определяющего роли портов.

Admin Edge

Варианты конфигурации: Non-Edge/Edge

Конфигурация по умолчанию: Non-Edge

Функция: Настройка порта в режим граничного порта.

Описание: Когда порт напрямую подключен к терминалу и не подключен к другим устройствам или общему сегменту сети, этот порт считается граничным портом. Граничный порт может быстро перейти из состояния блокировки в состояние пересылки без задержки ожидания. После того как граничный порт получает пакеты BPDU, он перестает быть граничным портом.

Auto Edge

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Enable

Функция: Включение функции автоматического обнаружения граничного порта.

Restricted Role

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Порт с ограничением роли никогда не будет выбран в качестве корневого узла, даже если ему предоставлен 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: Режим контроля перехода граничного порта в состояние Error-Disable и закрытия при получении пакетов BPDU.

Point-to-point

Варианты конфигурации: Auto/Forced True/Forced False

Конфигурация по умолчанию: Auto

Функция: Настройка типа соединения для порта. Если порт подключен к каналу «точка-точка», порт может быстро перейти в другое состояние.

Описание: Auto указывает, что коммутатор автоматически определяет тип канала на основе того, что порт работает в дуплексном режиме. Когда порт работает в полнодуплексном режиме, коммутатор считает, что тип соединения, подключенного к порту, — «точка-точка»; когда порт работает в полудуплексном режиме, коммутатор считает, что тип соединения, подключенного к порту, является общим. Принудительное задание соединения «точка-точка» означает, что соединение, подключенное к порту, является соединением «точка-точка», а принудительное задание совместного использования означает, что соединение, подключенное к порту, является общим соединением.

5. Настройте порты MSTI, как показано ниже.

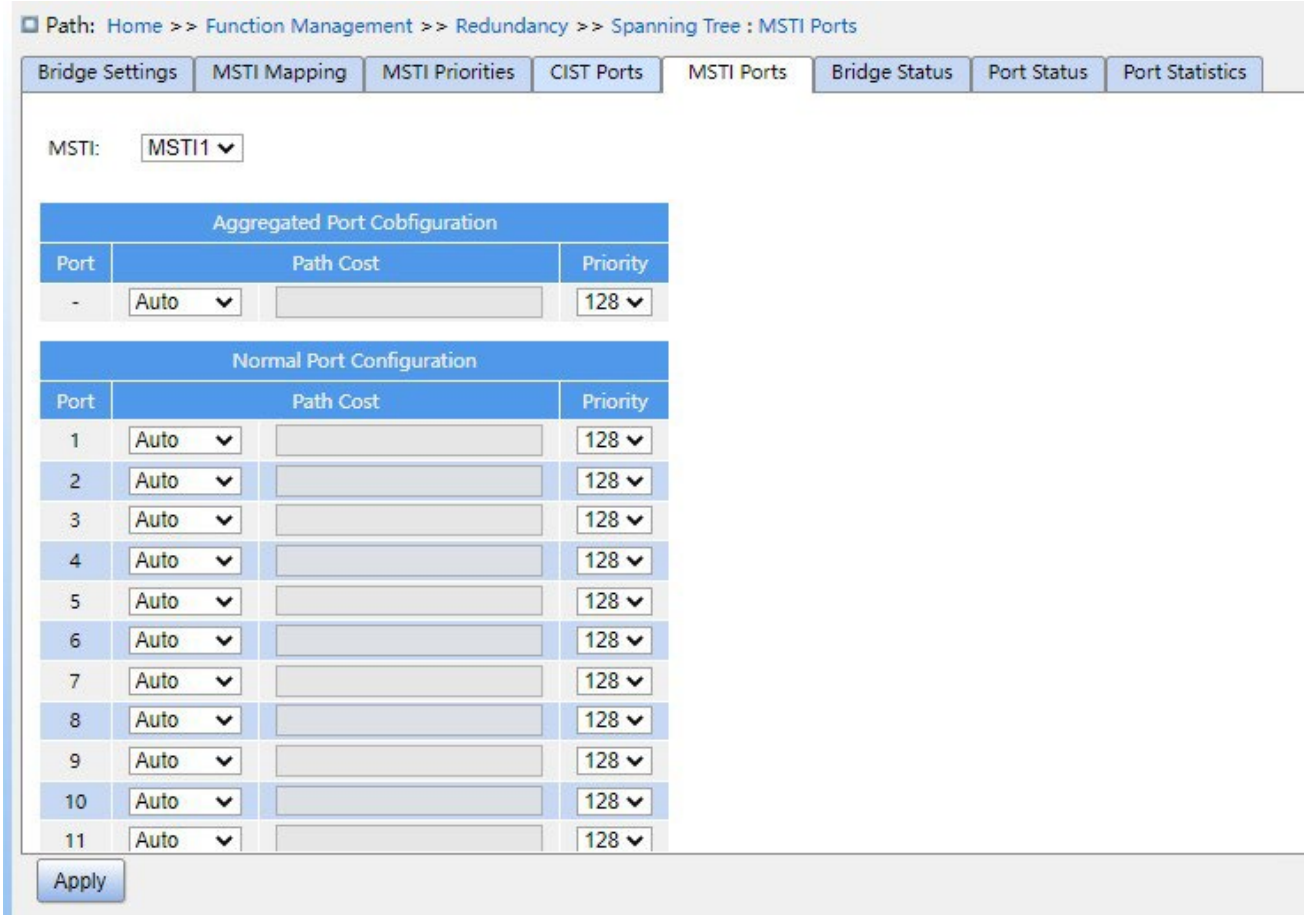


Рисунок 150 Выбор MSTI

Select MSTI

Диапазон настройки: MST1~MST7

Конфигурация по умолчанию: MST1

Функция: Выбор MSTI.

Настройка агрегированного порта MSTI

Функция: Настройка группы агрегации как порта MSTP и настройка стоимости и приоритета ее пути в указанном экземпляре.

Path Cost

Варианты конфигурации: Auto/Specific (1~200000000)

Конфигурация по умолчанию: Auto

Функция: Настройка стоимости пути для порта в назначенном экземпляре.

Описание: Стоимость пути порта используется для расчета наилучшего пути. Этот параметр зависит от полосы пропускания. Чем шире полоса пропускания, тем ниже

стоимость. Изменение стоимости пути порта может изменить путь передачи между устройством и корневым мостом, тем самым изменив роль порта.

Устройство с поддержкой MSTP можно настроить с разными стоимостями пути в разных экземплярах связующего дерева.

Priority

Диапазон настройки: 0~240. Шаг составляет 16.

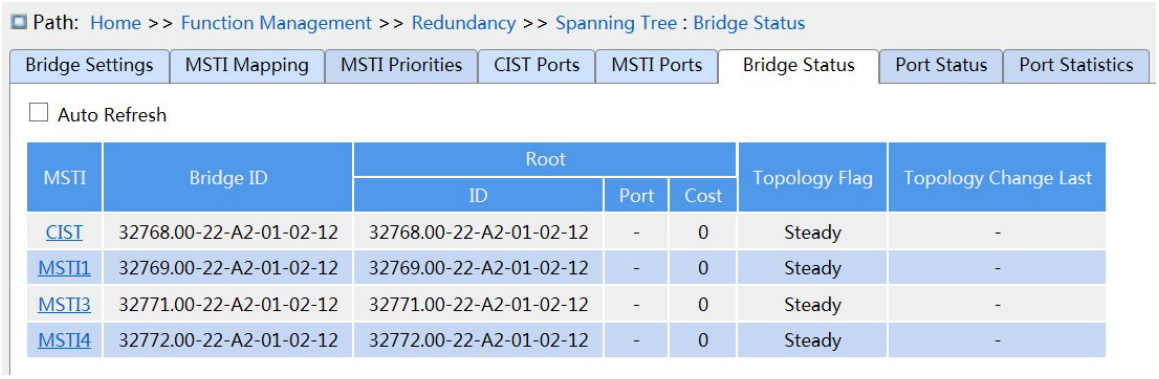
Конфигурация по умолчанию: 128

Функция: Настройка приоритета для порта в назначенном экземпляре.

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

Щелкните <Apply>, чтобы применить текущую конфигурацию.

6. Просмотрите состояние моста, как показано ниже.



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	-

Рисунок 151 Просмотр состояния моста

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 корневого моста текущего экземпляра связующего дерева этого устройства. ID: Указывает идентификатор корневого моста текущего экземпляра связующего дерева этого устройства. Port: Указывает корневой порт текущего экземпляра связующего дерева. Cost: Указывает стоимость пути от корневого порта до корневого моста в текущем экземпляре связующего дерева. **Topology Flag**

Функция: Указывает текущее рабочее состояние экземпляра связующего дерева.

Duration after topology change

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

7. Просмотрите статус портов STP, как показано ниже.

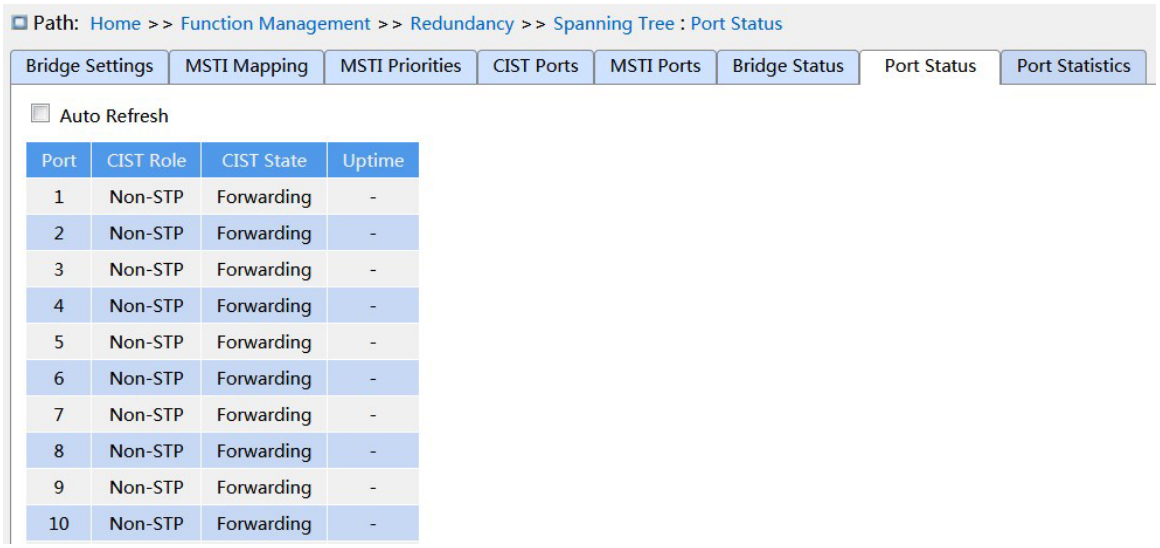


Рисунок 152 Просмотр статуса портов STP

Port

Функция: Текущий номер порта устройства.

CIST Role

Функция: Текущая роль порта в STP.

CIST State

Функция: Указывает состояние порта в STP.

Uptime

Функция: Время работы этого порта под управлением STP.

8. Просмотрите статистику пакетов портов STP, как показано ниже.

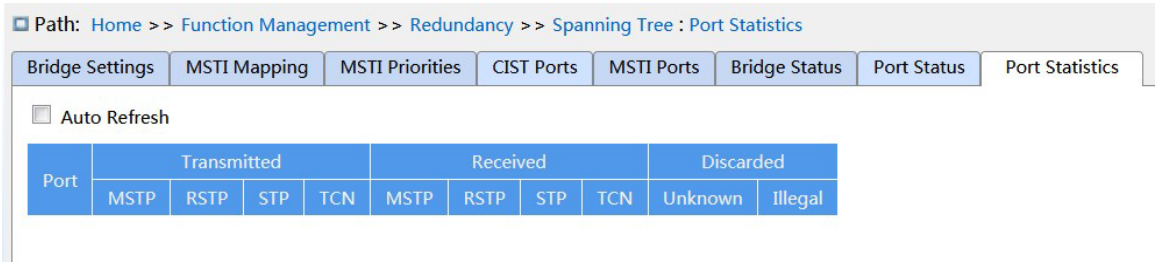


Рисунок 153 Просмотр статистики пакетов портов STP

Функция: число сообщений MSTP/RSTP/STP/TCN, отправленных/полученных портом. Discarded Количество неизвестных/недопустимых сообщений STP.

7.5.5.5 Пример типовой конфигурации

Как показано на рисунке 154, коммутаторы A, B, C и D принадлежат одному региону MST. Сети VLAN, отмеченные красным, указывают, что пакеты VLAN могут передаваться по линиям связи. После завершения настройки пакеты VLAN можно пересылать по разным экземплярам связующего дерева. Пакеты VLAN 10 пересылаются по экземпляру 1, а корневым мостом экземпляра 1 является коммутатор A; Пакеты VLAN 30 пересылаются по экземпляру 3, а корневой мост экземпляра 3 — это коммутатор B. Пакеты VLAN 40 пересылаются по экземпляру 4, а корневой мост экземпляра 4 — это коммутатор C. Пакеты VLAN 20 пересылаются по экземпляру 0, а корневым мостом экземпляра 0 является коммутатор B.

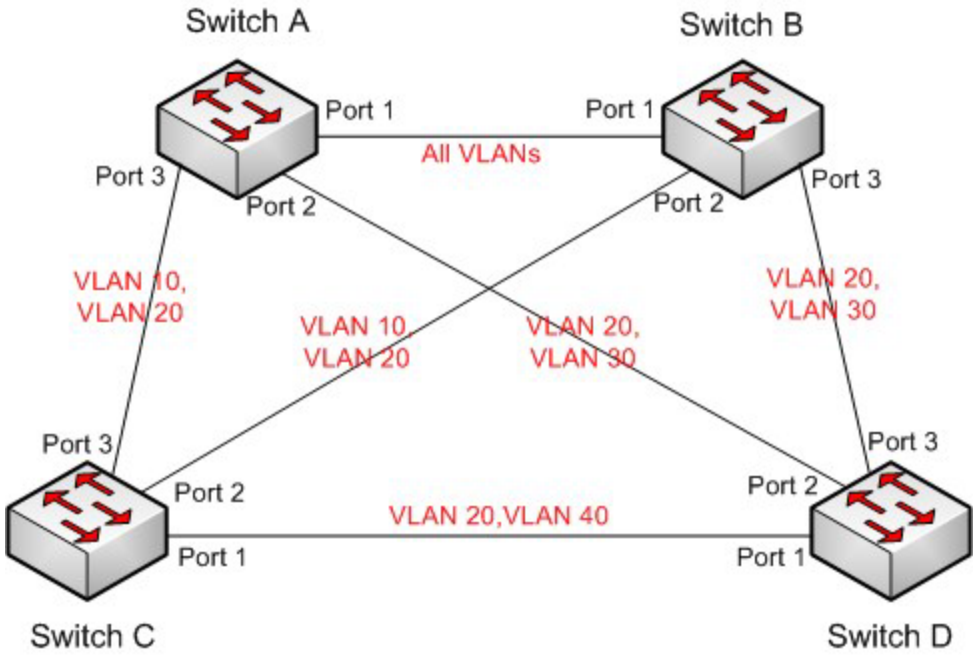


Рисунок 154 Пример типовой конфигурации MSTP

Конфигурация коммутатора A:

1. Создайте VLAN 10, 20 и 30 на коммутаторе A; настройте порты и разрешите прохождение пакетов соответствующих VLAN.
2. Включите глобальный протокол MSTP, как показано на рисунке 146.
3. Установите имя региона MST Region, а параметр версии 0, как показано на рисунке 150.
4. Создайте MSTI 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с экземплярами 1, 3 и 4 соответственно, как показано на рисунке 150.
5. Установите приоритет моста коммутатора в MSTI 1 равным 4096 и сохраните приоритет по умолчанию в других экземплярах, как показано на рисунке 148.

Конфигурация коммутатора B:

6. Создайте VLAN 10, 20 и 30 на коммутаторе B; настройте порты и разрешите прохождение пакетов соответствующих VLAN.
7. Включите глобальный протокол MSTP, как показано на рисунке 146.
8. Установите имя региона MST Region, а параметр версии 0, как показано на рисунке 150.
9. Создайте MSTI 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с экземплярами 1, 3 и 4 соответственно, как показано на рисунке 150.
10. Установите приоритет моста коммутатора в MSTI 3 равным 4096 и сохраните приоритет по умолчанию в других экземплярах, как показано на рисунке 148.

Конфигурация коммутатора C:

11. Создайте VLAN 10, 20 и 40 на коммутаторе C; настройте порты и разрешите прохождение пакетов соответствующих VLAN.
12. Включите глобальный протокол MSTP, как показано на рисунке 146.
13. Установите имя региона MST Region, а параметр версии 0, как показано на рисунке 150.
14. Создайте MSTI 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с экземплярами 1, 3 и 4 соответственно, как показано на рисунке 150.
15. Установите приоритет моста коммутатора в MSTI 4 равным 4096 и сохраните приоритет по умолчанию в других экземплярах, как показано на рисунке 148.

Конфигурация коммутатора D:

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

17. Включите глобальный протокол MSTP, как показано на рисунке 146.
18. Установите имя региона MST Region, а параметр версии 0, как показано на рисунке 150.
19. Создайте MSTI 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с экземплярами 1, 3 и 4 соответственно, как показано на рисунке 150.

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

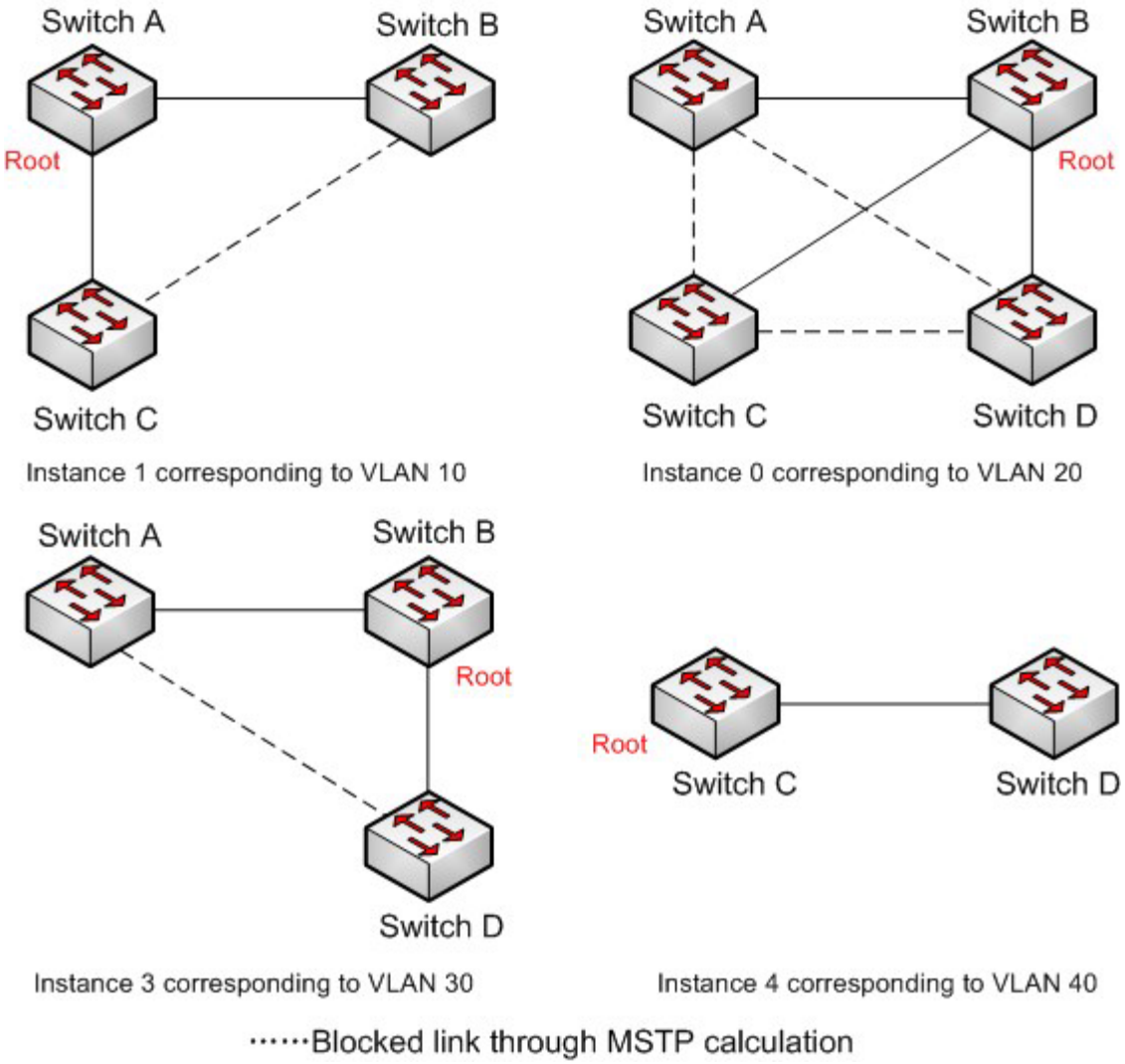


Рисунок 155 Экземпляры связующего дерева для каждой VLAN

7.6 Настройка ARP

7.6.1 Введение

Протокол разрешения адресов (ARP) разрешает сопоставление между IP-адресами и MAC-адресами с помощью механизма запроса и ответа адреса. Коммутатор получает информацию о сопоставлении между IP-адресами и MAC-адресами других хостов в том же сегменте сети. Он также поддерживает статические записи ARP для определения соответствия между IP-адресами и MAC-адресами. Динамические записи ARP периодически устаревают, обеспечивая согласованность между записями ARP и реальными приложениями.

Коммутаторы этой серии обеспечивают не только функцию коммутации уровня 2, но и функцию ARP для разрешения IP-адресов других хостов в том же сегменте сети, обеспечивая связь между NMS и управляемыми хостами.

7.6.2 Описание

Элементы таблицы ARP делятся на динамические элементы таблицы ARP и статические элементы таблицы ARP. Динамические элементы таблицы генерируются и поддерживаются автоматически посредством взаимодействия с сообщениями ARP, которые могут устаревать, обновляться новыми сообщениями ARP и перезаписываться статическими элементами таблицы ARP.

Статические элементы таблицы настраиваются и обслуживаются вручную, не устаревают и не перезаписываются динамическими элементами таблицы ARP.

7.6.3 Proxy ARP

Если запрос ARP отправляется от хоста одной сети к другому хосту в том же сегменте сети, но не в той же физической сети, то шлюз с функцией прокси-ARP, который напрямую подключен к исходному хосту, может ответить на сообщение запроса. Это называется прокси-ARP.

Процесс прокси-ARP выглядит так:

1、Хост-источник отправляет запрос ARP хосту другой физической сети;

2、Шлюз, напрямую подключенный к исходному хосту, включил функцию прокси-ARP интерфейса VLAN. Если существует нормальный маршрут к хосту назначения, хост назначения будет заменен для воспроизведения MAC-адреса своего собственного интерфейса.

3、IP-сообщения, отправляемые с исходного хоста на хост назначения, отправляются на устройство с включенной функцией proxy ARP.

4、Шлюз выполняет обычную IP-маршрутизацию сообщений.

5、IP-сообщения, которые должны быть отправлены на хост назначения, достигают хоста назначения через сеть.

7.6.4 Настройка через веб-интерфейс

1. Настройте элементы таблицы статических адресов ARP, как показано ниже.

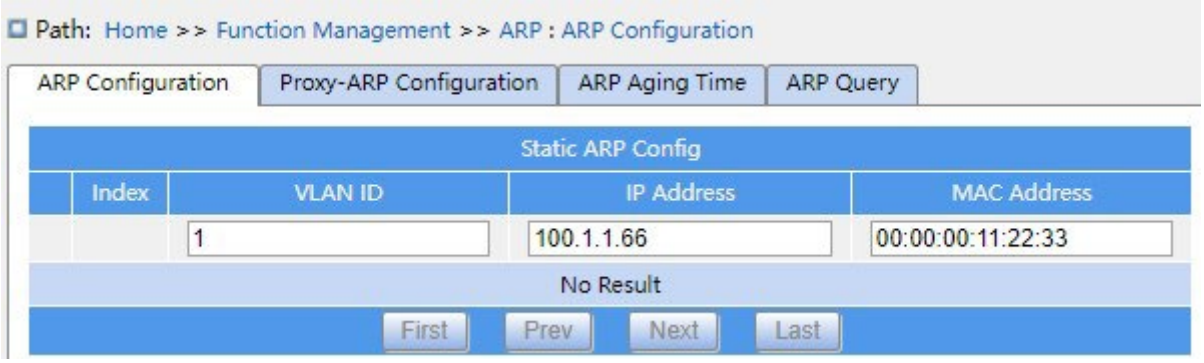


Рисунок 156 Настройка элементов таблицы статических адресов ARP

VLAN ID

Настройка: Созданный интерфейс L3 VLAN, диапазон 1-4094

Функция: выбор интерфейса L3 VLAN текущего элемента таблицы ARP.

IP Address

Формат: A.B.C.D

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

MAC address

Формат: HH-HH-HH-HH-HH-HH (H – шестнадцатеричное число) Функция: Настройка MAC-адреса статических записей таблицы ARP.

Предупреждение:

Как правило, коммутатор автоматически запоминает записи ARP, у администратора нет необходимости конфигурировать статические записи таблицы.

2. Конфигурация прокси-ARP показана ниже.

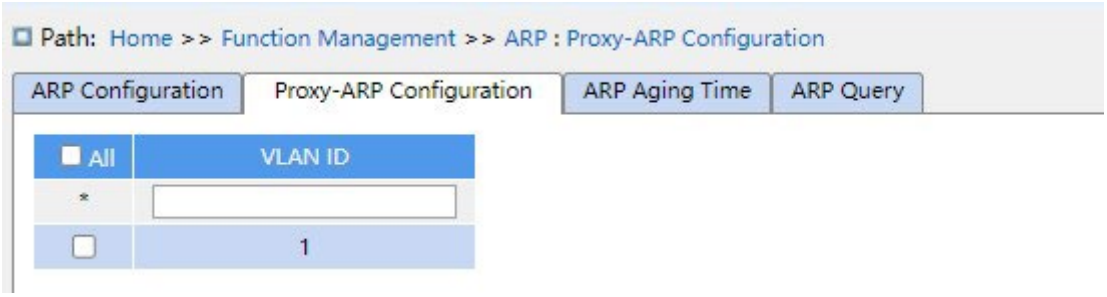


Рисунок 157 Конфигурация прокси-ARP

VLAN ID

Диапазон настройки: 1-4094

Функция: Выбор интерфейса L3 для включения прокси-ARP.

3. Настройка времени устаревания ARP показана ниже.

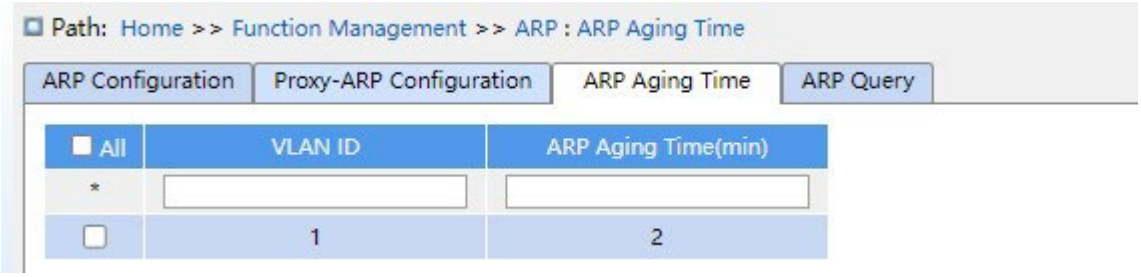


Рисунок 158 Настройка времени устаревания ARP

VLAN ID

Диапазон настройки: 1-4094

Функция: Указание интерфейса L3 с настройкой времени устаревания ARP.

ARP Aging Time

Диапазон настройки: 1 ~ 60 минут

Функция: Время устаревания ARP.

Описание: Время устаревания ARP означает начало отсчета времени путем добавления динамического элемента таблицы ARP в таблицу адресов, и элемент таблицы динамических адресов будет удален из списка ARP по истечении времени устаревания.

4. Запрос ARP показан ниже.

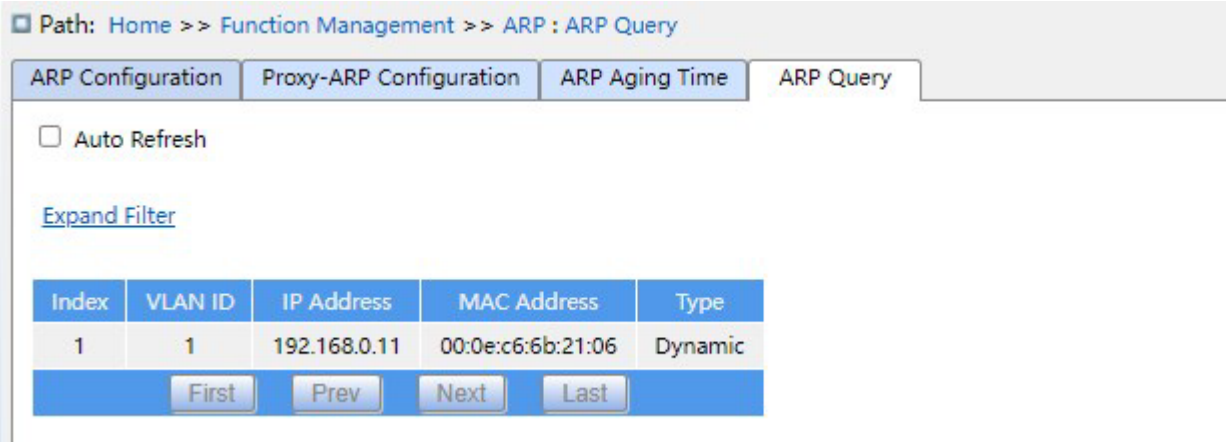


Рисунок 159 Запрос ARP

ARP Query

Отображение элемента: {index, VLAN ID, IP address, MAC address, type}

Функция: отображение элемента таблицы ARP.

Описание: В списке отображаются все элементы таблицы ARP, соответствующие порту в состоянии LinkUp, включая статические и динамические элементы таблицы.

7.7 Настройка ACL

7.7.1 Обзор

С развитием сетевых технологий вопросы безопасности становятся все более заметными, что требует механизма контроля доступа. Благодаря функции списка управления доступом Access Control List (ACL) коммутатор сопоставляет пакеты со списком для реализации контроля доступа.

7.7.2 Реализация

Коммутаторы серии осуществляют фильтрацию пакетов в соответствии с согласованным ACL. Каждая запись состоит из нескольких условий в логической связи И. Записи ACL не зависят друг от друга.

Коммутатор сравнивает пакет с записями ACL в порядке возрастания идентификаторов записей. Как только совпадение найдено, действие выполнено, и дальнейшее сравнение не проводится, как показано на следующем рисунке.

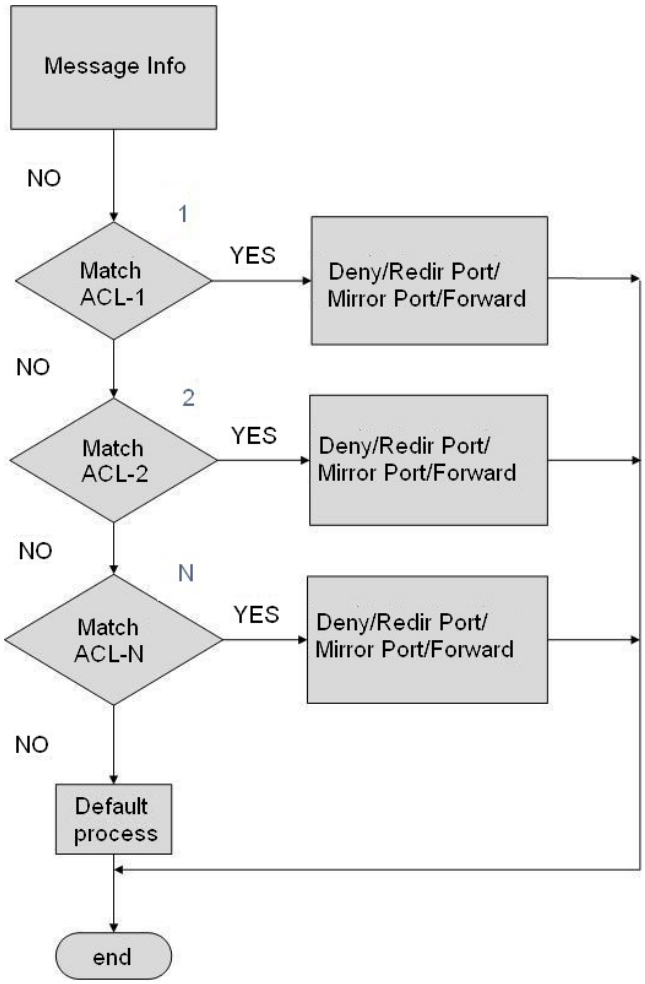


Рисунок 160 Схема обработки ACL

Примечание:
Процесс по умолчанию указывает режим обработки пакетов, не соответствующих записи ACL.

7.7.3 Настройка на веб-странице

1. Настройте записи таблицы ACL

Щелкните [Function Management] → [ACL] в дереве навигации→, чтобы войти в интерфейс настройки ACL, как показано на следующем рисунке:

Рисунок 161 Настройка записей таблицы ACL

ACL ID

Диапазон настройки: 1~1024

Функция: Настройка ID записи таблицы ACL.

Описание: Изделие поддерживает до 512 записей таблицы ACL. Если записи таблицы применяются к нескольким портам, применение под каждым портом представляет собой одну запись таблицы ACL.

Предупреждение:
Поскольку для устройства существуют некоторые системные записи таблицы ACL, количество записей таблицы ACL, которые фактически может настроить пользователь, составляет менее 512.

Описание

Диапазон настройки: 1~127 символов

Функция: Добавление описательной информации к записи таблицы ACL.

Priority

Диапазон настройки: 1-1024

Функция: Чем меньше значение, тем выше приоритет.

2. Щелкните одну из записей таблицы, созданной на рисунке 161, чтобы войти в интерфейс, показанный на рисунке 162, и щелкните кнопку <Add Rule> ниже, чтобы настроить правила записи таблицы ACL.

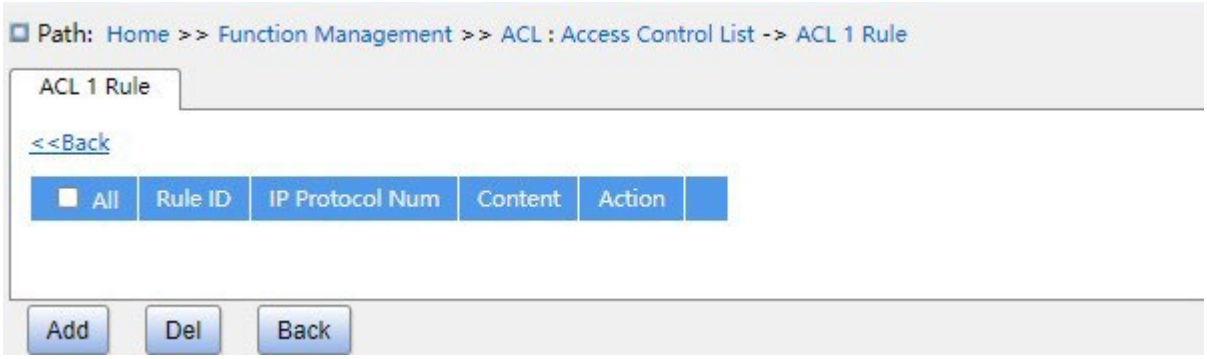


Рисунок 162 Редактирование записи в таблице ACL

3. Настройте число правил записей таблицы ACL1, как показано на следующем рисунке.

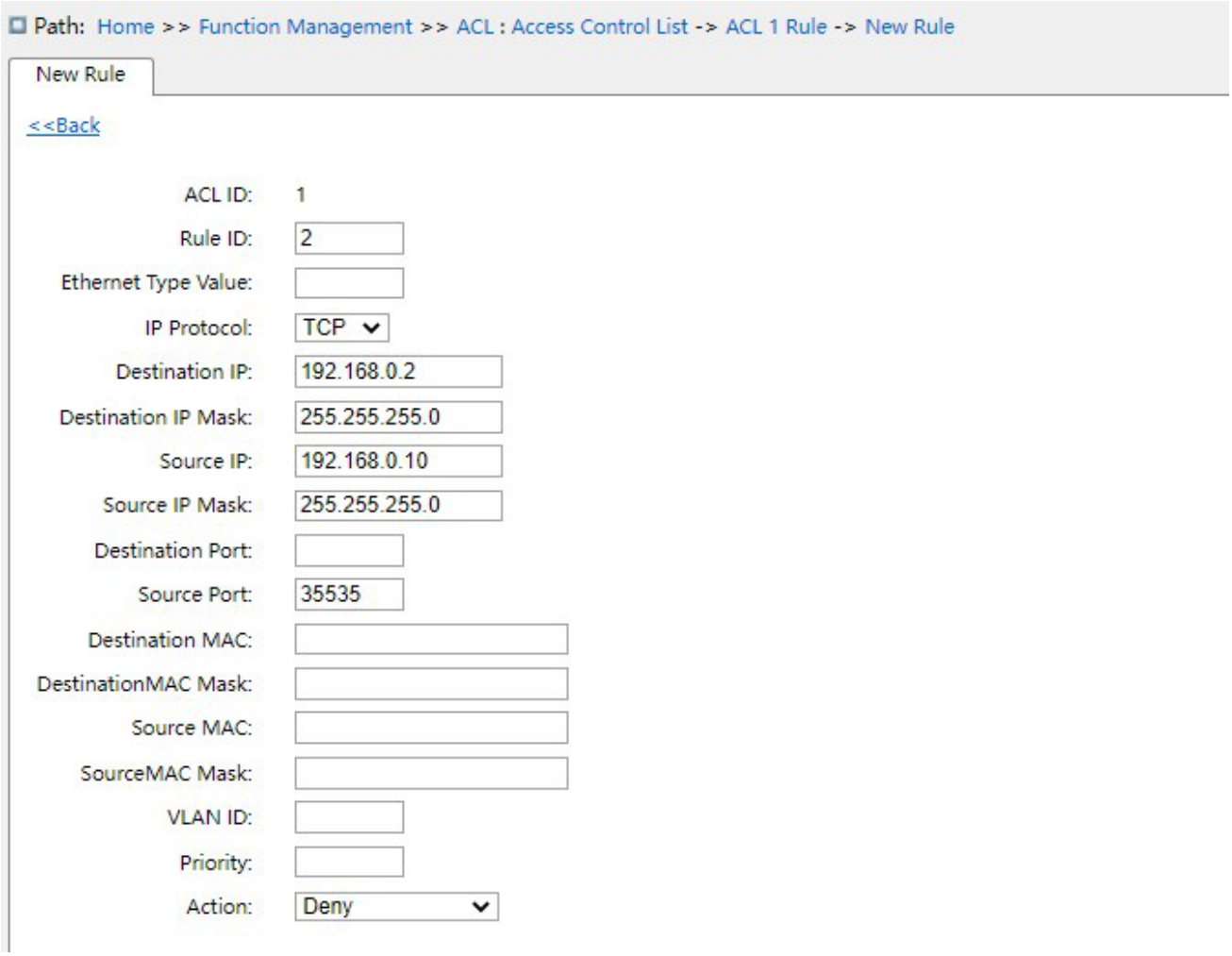


Рисунок 163 Настройка правил ACL

Rule ID

Диапазон настройки: 1~1024

Функция: Настройка номера правила записи таблицы ACL.

Описание: Каждая запись ACL поддерживает до 512 правил, а общее количество правил во всех ACL не может превышать 512.

Ethernet Type Value

Диапазон настройки: 0x600~0xFFFF

Функция: Настройка типа протокола для правила.

IP Protocol

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

Конфигурация по умолчанию: Any

Функция: Настройка параметра условия — тип протокола сообщений IPv4. Если выбрано значечние ICMP/UDP/TCP, необходимо настроить соответствующий параметр; если выбрано Other, необходимо настроить номер протокола. Когда тип протокола в сообщении IPv4, полученном портом, соответствует настройкам этого параметра, условие успешно выполнено.

Destination IP/ Destination IP Mask

Функция: Настройка информации об IP-адресе назначения для правила. 1 в IP-маске назначения представляет собой интересующий бит IP-адреса назначения, а 0 представляет бит IP-адреса назначения, который следует игнорировать.

Source IP/ Source IP Mask

Функция: Настройка информации об IP-адресе источника для правила. 1 в IP-маске назначения представляет собой интересующий бит IP-адреса источника, а 0 представляет бит IP-адреса источника, который следует игнорировать.

Destination port

Диапазон настройки: 0~65535

Функция: Настройка номера порта назначения TCP/UDP.

Source Port

Диапазон настройки: 0~65535

Функция: Настройка номера исходного порта TCP/UDP.

Destination MAC/ Destination MAC Mask

Функция: Настройка информации об MAC-адресе назначения для правила. 1 в MAC-маске назначения представляет собой интересующий бит MAC-адреса назначения, а 0 представляет бит MAC-адреса назначения, который следует игнорировать.

Source MAC/ Source MAC Mask

Функция: Настройка информации об MAC-адресе источника для правила. 1 в MAC-маске назначения представляет собой интересующий бит MAC-адреса источника, а 0 представляет бит MAC-адреса источника, который следует игнорировать.

VLAN ID

Варианты конфигурации: 1~4093

Функция: Настройка VLAN ID для правила.

Priority

Варианты конфигурации: 0~7 (значение COS)

Функция: Настройка значения перемаркировки уровня приоритета.

Описание: Политика перемаркировки будет применена для значения приоритета в сообщениях, соответствующих критериям.

Action

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

Конфигурация по умолчанию: Permit

Функция: Настройка обработки успешно сопоставленных сообщений.

Описание: Permit означает получение успешного совпадения; Deny означает отбросить успешное совпадение; Mirror to CPU означает получить успешное совпадение и отразить его на ЦП; Mirror to Port означает получение успешного совпадения и зеркалирование его на указанный порт; Redirect to CPU означает перенаправление успешного совпадения на ЦП; Redirect to Port означает перенаправление совпадающих сообщений на указанный порт. Limit To kbps означает ограничение скорости кбит/с соответствующего сообщения; Limit To mbps означает ограничение скорости в Мбит/с соответствующего сообщения; Limit To pps означает ограничение скорости pps соответствующего сообщения; Modify DSCP означает изменение значения DSCP соответствующего сообщения; Modify Queue означает изменить значение очереди соответствующего сообщения. Modify VLAN означает изменить значение идентификатора VLAN успешного сообщения. Modify Cos означает изменить значение Cos успешного сообщения.

4. Настройте объект применения записи таблицы ACL1, как показано на следующем рисунке.

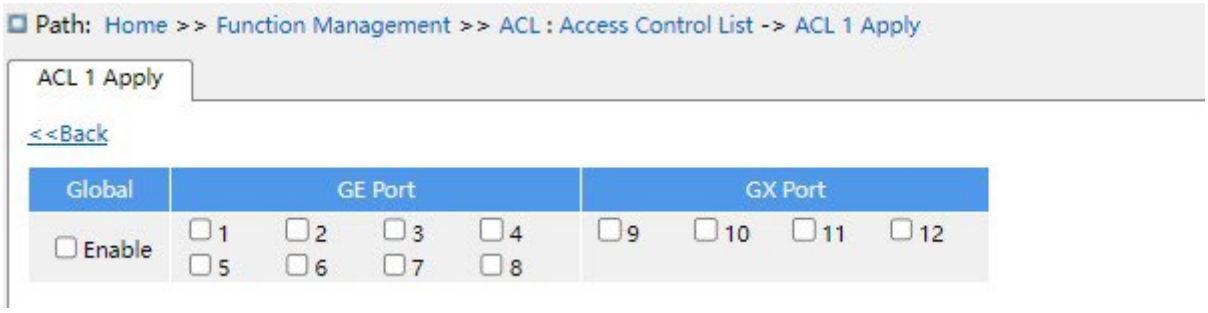


Рисунок 164 Настройка объекта применения записи таблицы ACL

ACL1 Application object

Варианты конфигурации: Global/FE port/FX port

При глобальном применении правило ACL вступит в силу для всех портов, т. е. вступит в силу глобальное включение. При применении к порту правило ACL будет действовать только на включенном порту.

7.8 Настройка MAC-адреса

7.8.1 Введение

При пересылке пакета коммутатор ищет порт пересылки в таблице MAC-адресов на основе MAC-адреса получателя 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 действует постоянно.

Динамические MAC-адреса коммутатор узнает при пересылке данных. Они действительны только в течение определенного периода. Коммутатор периодически обновляет свою таблицу MAC-адресов. При получении кадра данных для пересылки коммутатор узнает исходный MAC-адрес кадра, устанавливает сопоставление с принимающим портом и запрашивает порт пересылки в таблице MAC-адресов на основе MAC-адреса получателя кадра. Если совпадение найдено, коммутатор пересылает кадр данных с соответствующего порта. Если совпадений не найдено, коммутатор передает кадр в своем широковещательном домене.

Время устаревания начинается с момента добавления динамического MAC-адреса в таблицу MAC-адресов. Если ни один порт не получает кадр с MAC-адресом в течение

времени, в 1-2 раза превышающего время устаревания, коммутатор удаляет запись MAC-адреса из таблицы динамических адресов пересылки.

Статические MAC-адреса не включают понятие времени устаревания.

7.8.2 Настройка через веб-интерфейс

1. Настройте время устаревания MAC-адреса, как показано ниже.

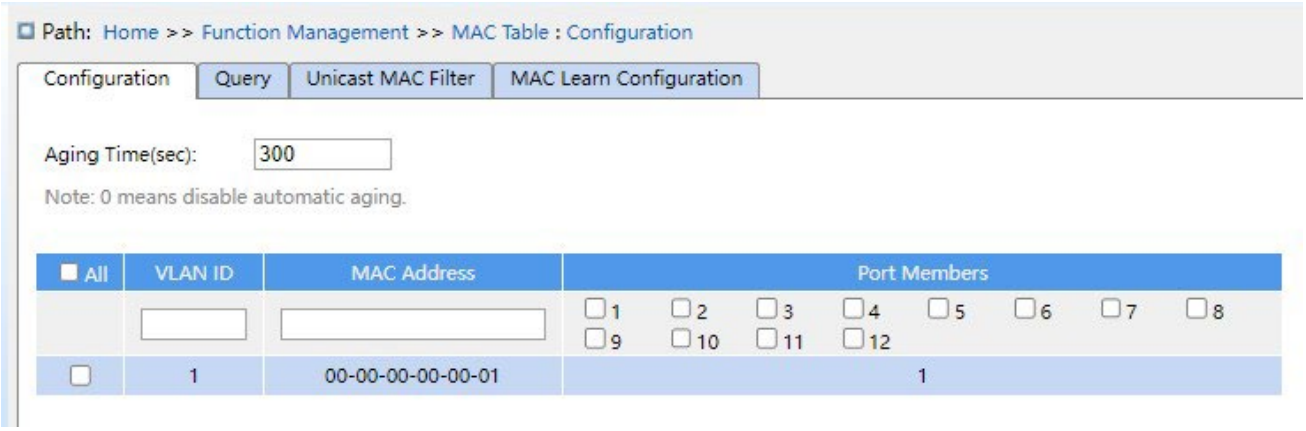


Рисунок 165 Настройка времени устаревания MAC-адреса

Aging Time

Диапазон настройки: 0 или 10~1000000 с

Конфигурация по умолчанию: 300 с

Функция: Задание времени устаревания для записи динамического MAC-адреса.

VLAN ID

Варианты: все созданные VLAN ID

Конфигурация по умолчанию: VLAN 1

Функция: Настройка VLAN ID статического MAC-адреса.

MAC address

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

Функция: Настройка MAC-адреса. Для MAC-адреса одноадресной рассылки младший бит в первом байте равен 0. Для MAC-адреса многоадресной рассылки младший бит в первом байте равен 1.

Port members

Функция: Выбор портов для пересылки пакетов с этим MAC-адресом назначения.

2. Просмотрите таблицу MAC-адресов, как показано ниже.

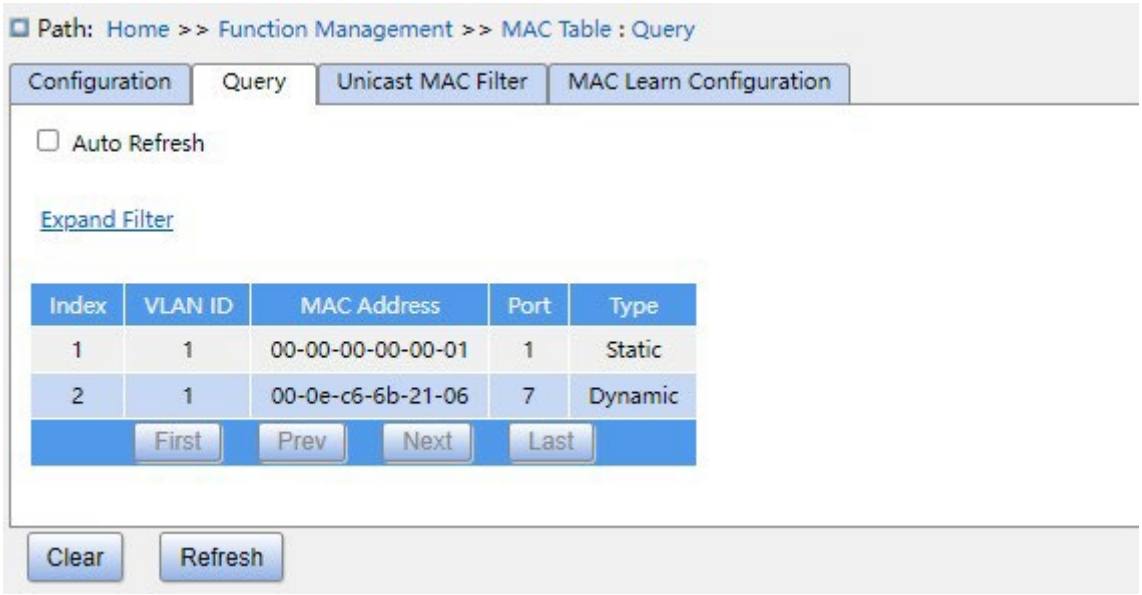


Рисунок 166 Просмотр таблицы MAC-адресов

VLAN ID

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

Конфигурация по умолчанию: *

Функция: Отображение таблицы MAC-адресов в соответствии с настроенными VLAN ID.

MAC Address

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

Конфигурация по умолчанию: *

Функция: Отображение таблицы MAC-адресов в соответствии с настроенными MAC-адресами.

Port

Варианты конфигурации: */include/not include

Конфигурация по умолчанию: *

Функция: Отображение таблицы MAC-адресов в соответствии с настроенным портом.

Type

Варианты конфигурации: */static/dynamic

Конфигурация по умолчанию: *

Функция: Отображение таблицы MAC-адресов в соответствии с настроенными типом.

3. Настройте запись таблицы фильтрации одноадресных MAC-адресов, как показано на следующем рисунке.

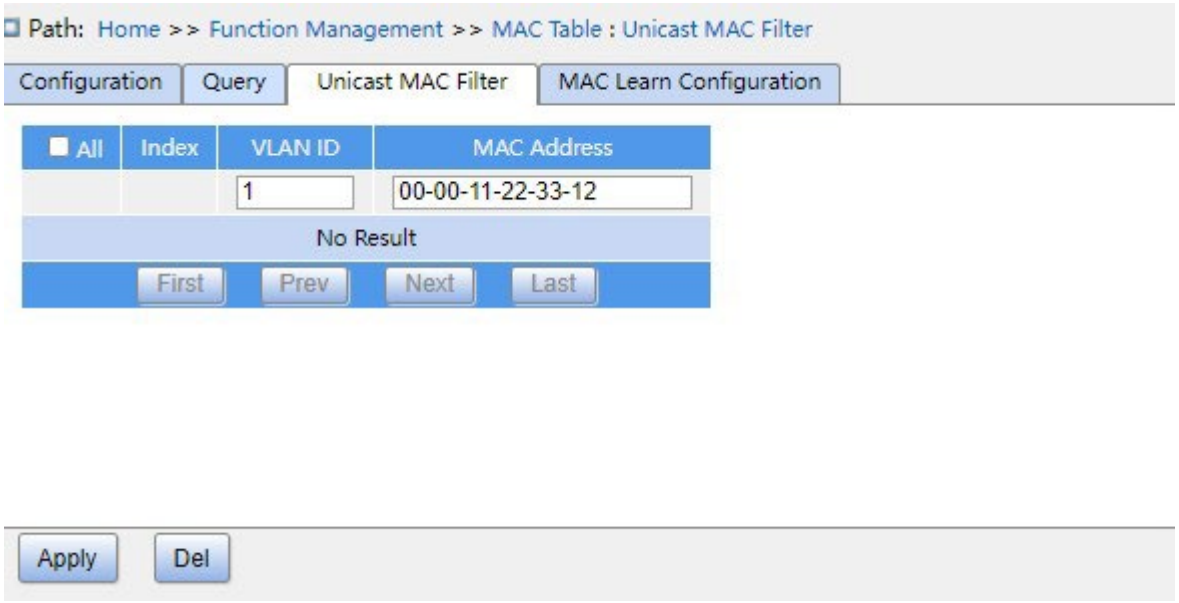


Рисунок 167 Настройка записи таблицы фильтрации одноадресных MAC-адресов

VLAN ID

Варианты конфигурации: Все созданные VLAN ID.

Функция: Настройка VLAN ID для таблицы статических MAC-адресов.

MAC Address

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

Функция: Настройка MAC-адреса. Младший бит старшего байта одноадресного MAC-адреса равен 0; младший бит старшего байта многоадресного MAC-адреса равен 1.

4. На странице настройки обучения MAC можно настроить каждый порт для включения обучения MAC, как показано на следующем рисунке.

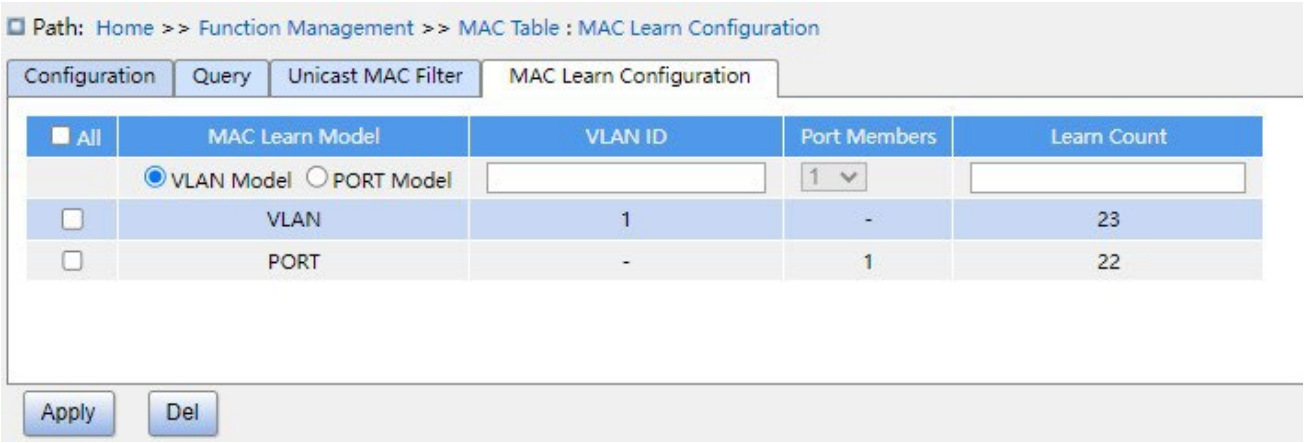


Рисунок 168 Настройка обучения MAC.

MAC Learn Model

Варианты конфигурации: VLAN mode / PORT mode

Функция: Настройка режима ограничения обучения MAC, который может ограничить количество обучения MAC для VLAN или порта.

VLAN ID

Варианты конфигурации: 1-4093

Функция: Настройка VLAN, ограничивающий обучение MAC.

Port members

Диапазон настройки: Все порты устройства.

Функция: Включить ограничение изучения таблицы MAC-адресов.

Learn Count

Диапазон настройки: 1~8192

Функция: Настройка количества ограниченных изучений MAC.

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 расстояние надежной подачи питания составляет до 100 м. Технология PoE эффективно решает проблему централизованного электропитания для IP-телефона, беспроводной точки доступа, зарядного устройства портативного устройства, камеры, сбора данных и т. д., независимо от проводки внутренней системы электропитания, PoE может подавать питание на оборудования одновременно с его подключением к сети.
Коммутатор серии POE соответствует стандарту IEEE 802.3at, он включает в себя PSE и PD, PSE (Power Sourcing Equipment) — это устройство, которое подает питание на другое устройство, а PD (Powered Device) — это устройство, которое получает питание в системе питания PoE.

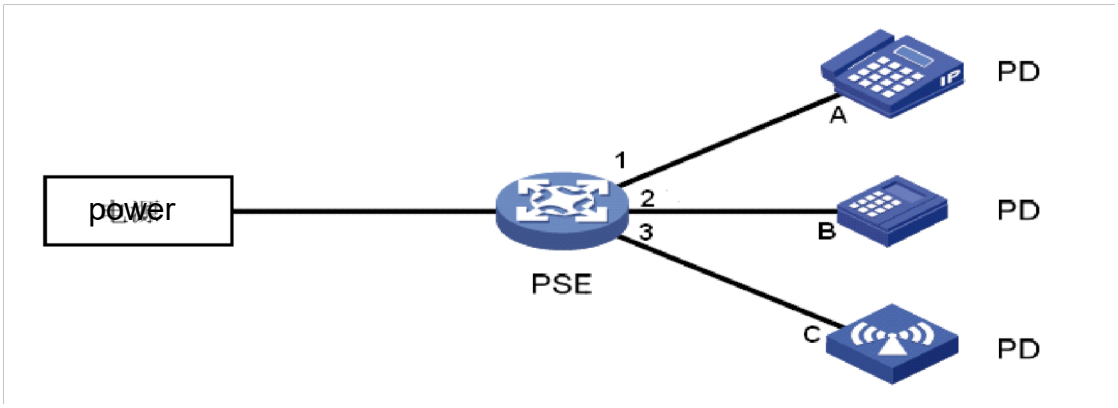


Рисунок 169 Система питания POE

7.9.2 Настройка через веб-интерфейс

1. Настройте PoE для порта, как показано ниже.

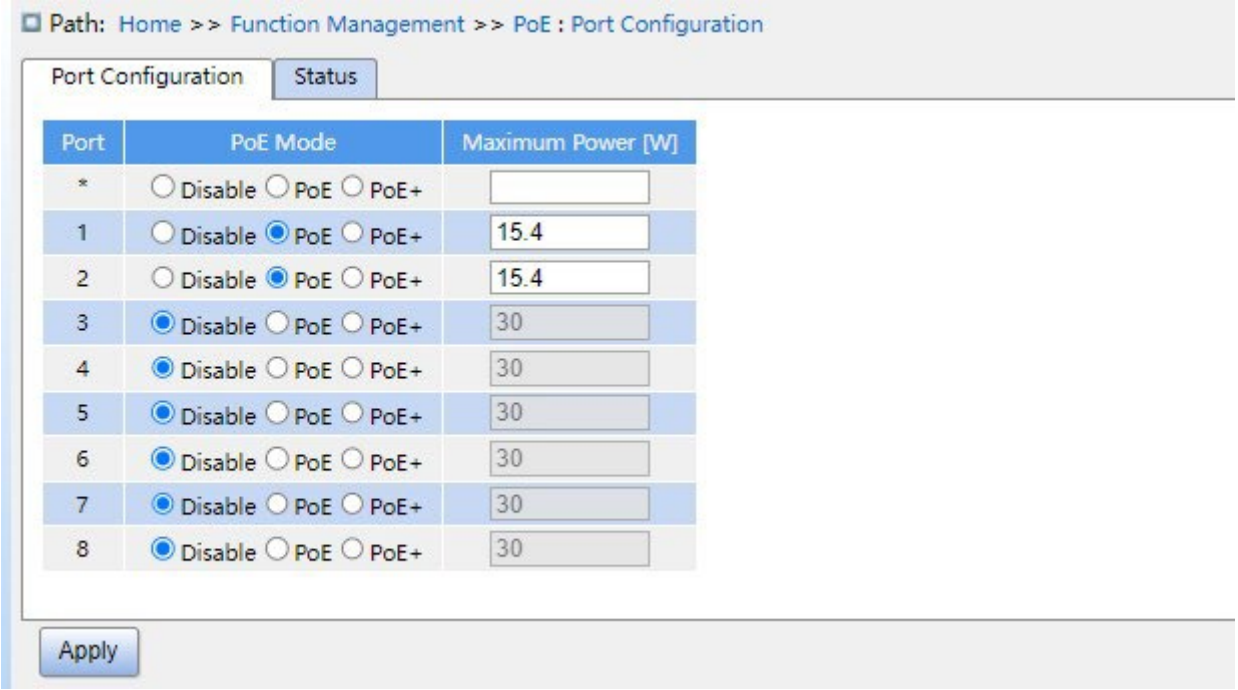


Рисунок 170 Настройка PoE для порта

PoE Mode

Варианты конфигурации: Disable/PoE/PoE+

Конфигурация по умолчанию: Disable

Функция: Включение PoE для порта. PoE: 100M Ethernet поддерживает выход PoE, отвечающий IEEE802.3af; PoE+: 100M Ethernet поддерживает выход PoE, отвечающий IEEE802.3at.

Maximum Power [W]

Диапазон настройки: 1~15,4 Вт (PoE) /1~30,0 Вт (PoE+)

Функция: настройка максимальной выходной мощности порта PoE. Если мощность, потребляемая подключенным к порту устройством PD, превышает это значение, питание устройства PD невозможно. В соответствии с фактическими потребностями пользователь может разумно настроить предел выходной мощности каждого порта коммутатора, чтобы эффективно удовлетворить требования к источнику питания каждого порта.

2. Просмотрите состояние PoE, как показано ниже.

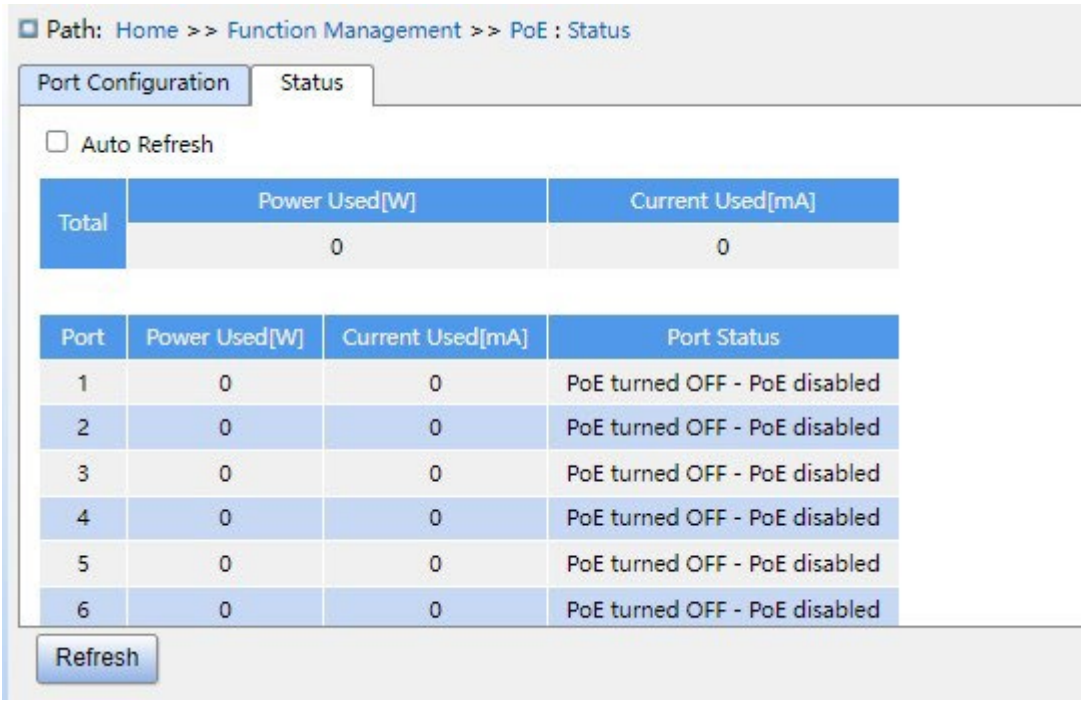


Рисунок 171 Отображение состояния порта PoE

Power Used/Current Used

Функция: Отображение потребляемой мощности, тока и параметров приоритета 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: Отображение статуса PoE для порта.

Пояснение: No PD detected означает включение PoE, при этом устройство PD не обнаружено.

Invalid PD означает включение PoE, обнаружение PD, но питание нарушено.

PoE turned ON означает включение PoE, обнаружение PD, нормальное питание. PoE turned OFF-PoE disabled означает отключение PoE.

PoE turned OFF-Power budget exceeded означает включение PoE, обнаружение устройства PD, но доступ к устройству PD приведет к тому, что общее энергопотребление всех устройств PD превысит максимальное энергопотребление, обеспечиваемое устройством в целом, и устройство PD не может быть запитано.

PoE turned OFF-Power budget exceeded означает включение PoE, обнаружение устройства PD, при этом общая потребляемая мощность всеми устройствами PD не превышает максимальную потребляемую мощность, обеспечиваемую устройством в целом, но потребляемая мощность устройства PD превышает максимальную выходную мощность порта PoE, устройство PD не может быть запитано.

PoE turned ON-PD forced ON означает включение PoE и принудительное запитывание.

7.9.3 Пример типового использования

Как показано на рисунке 169, максимальная мощность, обеспечиваемая коммутатором в режиме PSE, составляет 11 Вт, порты коммутатора 1 и 2 подключены к устройствам A и B, максимальная потребляемая мощность A — 5 Вт, максимальная потребляемая мощность B — 4 Вт. Ожидается, что порт коммутатора 3 будет подключен к устройству C, а максимальная потребляемая мощность C составляет 5 Вт.

Требование:

1. Коммутатор подключен только к устройствам A и B, он может нормально подавать питание;
2. Если устройство PD C подключено к порту 3 коммутатора, общая потребляемая мощность всеми устройствами PD превышает максимальную мощность, которую может обеспечить коммутатор, необходимо сначала обеспечить питание устройства C, которое подключено к порту 3 коммутатора.

Конфигурация PSE следующая:

1. Настройте для порта 1 режим PoE, как покащано на рисунке 170.
2. Включите функцию PoE для портов 1~3, остальные настройки по умолчанию.

7.10 IGMP Snooping

7.10.1 Введение

Отслеживание IGMP — это протокол многоадресной рассылки на канальном уровне. Он используется для управления и контроля групп многоадресной рассылки. Коммутаторы с поддержкой IGMP Snooping анализируют полученные пакеты IGMP, устанавливают сопоставление между портами и MAC-адресами многоадресной рассылки и пересылают многоадресные пакеты в соответствии с сопоставлением.

Есть три версии протокола IGMP: IGMPv1, IGMPv2 и IGMPv3. Версия IGMPv1 определена в RFC1112, IGMPv2 определена в RFC2236, а IGMPv3 определена в RFC3376.

IGMPv1 поддерживает два типа пакетов (пакеты отчетов и запросов) и определяет базовый процесс запроса и отчета члена группы.

Протокол IGMPv2, построенный на основе IGMPv1, предоставляет пакет выхода механизма быстрого выхода для членов группы. При использовании этого механизма, когда последний участник покидает группу многоадресной рассылки, маршрутизатор получает указание провести быструю конвергенцию. По сравнению с IGMPv1, IGMPv2 поддерживает два типа пакетов запросов: общий пакет запроса и пакет запроса для конкретной группы. Коммутатор периодически отправляет пакет общего запроса для запроса членства. Когда хост покидает группу многоадресной рассылки, после получения коммутатором сообщения о выходе коммутатор отправляет пакет запроса для конкретной группы, чтобы определить, все ли члены покидают группу многоадресной рассылки. В IGMPv3 добавлена функция фильтрации источника хоста. Эта функция позволяет хосту указать, следует ли принимать или отклонять пакеты от определенных источников группы многоадресной рассылки.

7.10.2 Основные понятия

Генератор запросов Querier: периодически отправляет пакеты общего запроса IGMP для запроса статуса членов в группе многоадресной рассылки, сохраняя информацию о группе многоадресной рассылки. Когда в сети существует несколько генераторов запросов, автоматически выбирается тот, у которого наименьший IP-адрес, в качестве запрашивающего. Только выбранный генератор запросов периодически отправляет пакеты

общего запроса IGMP. Другие генераторы запросов только получают и пересылают пакеты запросов IGMP.

Маршрутизирующий порт: получает пакеты общего запроса (на коммутаторе с поддержкой IGMP) от генератор запросов. После получения ответа IGMP коммутатор создает запись многоадресной рассылки и добавляет порт, который получает отчет IGMP, в список портов-участников. Если маршрутизирующий порт существует, он также добавляется в список портов-участников. Затем коммутатор пересылает отчет IGMP другим устройствам через маршрутизирующий порт, чтобы другие устройства создали ту же запись многоадресной рассылки.

Прокси IGMP Snooping: Функция прокси-сервера IGMP snooping настраивается на граничном устройстве, чтобы уменьшить количество пакетов отчетов IGMP и оставить пакеты, полученные вышестоящим устройством, тем самым повышая общую производительность вышестоящего устройства. Устройство, на котором настроена функция прокси-сервера IGMP snooping, работает как хост для вышестоящего устройства и работает как генератор запросов для нижестоящего хоста.

7.10.3 Принцип работы

IGMP Snooping управляет и поддерживает членов группы многоадресной рассылки путем обмена пакетами related между устройствами с поддержкой IGMP. Пакеты related следующие:

Пакет общего запроса: Генератор запросов периодически отправляет пакеты общего запроса (IP-адрес назначения 224.0.0.1) чтобы подтвердить, есть ли в группе многоадресной рассылки порты-участники. После получения пакета запроса устройство, не являющееся генератором запросов, пересылает пакет на все подключенные к нему порты.

Пакет конкретного запроса: Если устройство хочет выйти из группы многоадресной рассылки, оно отправляет пакет IGMP leave. После получения пакета leave запрашивающая сторона отправляет пакет конкретного запроса (IP-адрес назначения: IP-адрес группы многоадресной рассылки), чтобы убедиться, что группа содержит другие порты-участники.

Пакет с отчетом участника: Если устройство хочет получить данные группы многоадресной рассылки, оно отправляет пакет IGMP report (IP-адрес назначения: IP-адрес группы многоадресной рассылки) немедленно в ответ на пакет запроса IGMP группы.

Пакет выхода: Если устройство хочет выйти из группы многоадресной рассылки, оно отправляет пакет IGMP leave (IP-адрес назначения: 224.0.0.2).

7.10.4 Настройка через веб-интерфейс

1. Включите IGMP Snooping, как показано ниже.

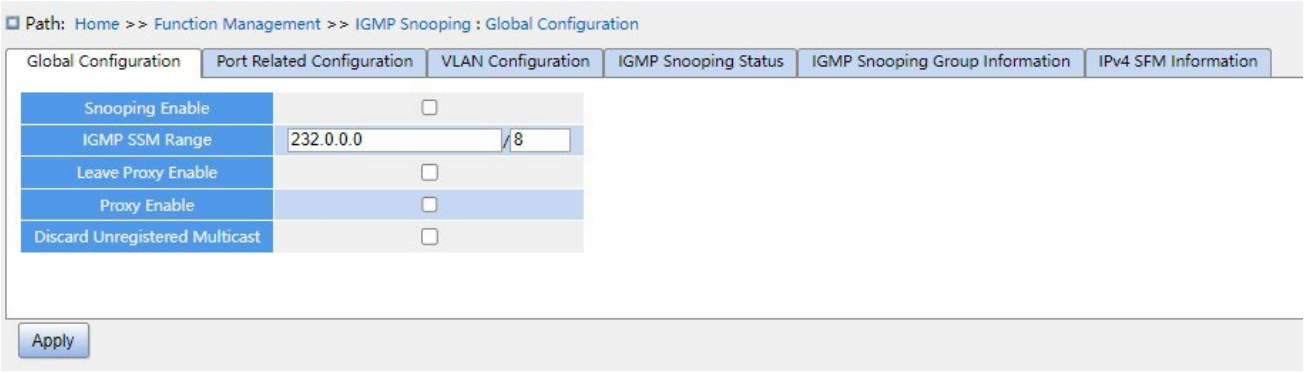


Рисунок 172 Настройка IGMP Snooping

Snooping Enable

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение или выключение глобального протокола IGMP Snooping.

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 модель службы многоадресной рассылки IGMP (SSM) при условии, что хосты и маршрутизаторы поддерживают модель службы IGMP SSM. Модель службы SSM предоставляет пользователям услугу передачи, определяющую источники многоадресной рассылки для клиента.

Leave Proxy Enable

Варианты конфигурации: Enabled/Disabled

Конфигурация по умолчанию: Disabled

Функция: Включение/выключение функции пересылки пакетов leave генератору запросов. Когда функция включена, пакеты leave не пересылаются.

Proxy Enable

Варианты конфигурации: Enabled/Disabled

Конфигурация по умолчанию: Disabled

Функция: Включение/выключение функции пересылки пакетов leave и пакетов отчетов участников генератору запросов. Когда функция включена, пакеты leave и пакеты отчетов участников не пересылаются.

Discard Unregistered Multicast

Варианты конфигурации: Enabled/Disabled

Конфигурация по умолчанию: Disabled

Функция: Включение отбрасывания коммутатором неизвестных многоадресных пакетов.

2. Настройте порт IGMP, как показано ниже.

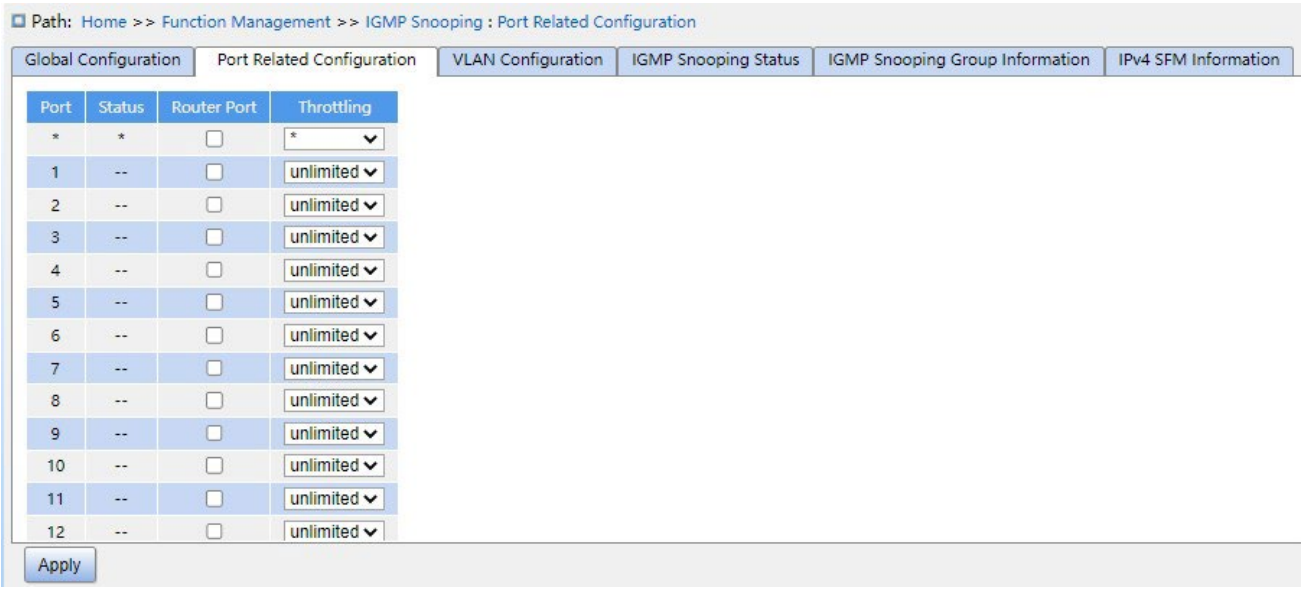


Рисунок 173 Настройка порта IGMP

Status

Варианты конфигурации: --/static/dynamic/both

Функция: Отображение статуса порта маршрутизатора. **Static** указывает, что порт статически настроен как маршрутизирующий порт, **Dynamic** указывает, что порт динамически определяется как маршрутизирующий порт. **Both** указывает, что порт

динамически настраивается как маршрутизирующий порт или динамически определяется как маршрутизирующий порт.

Router Port

Варианты конфигурации: Enabled/Disabled

Конфигурация по умолчанию: Disabled

Функция: Настройка порта маршрутизатора.

Throttling

Варианты конфигурации: unlimited/1~10

Конфигурация по умолчанию: unlimited

Функция: Включение/выключение функции ограничения количества записей многоадресной рассылки, полученных портом.

3. Настройте IGMP Snooping VLAN, как показано ниже.

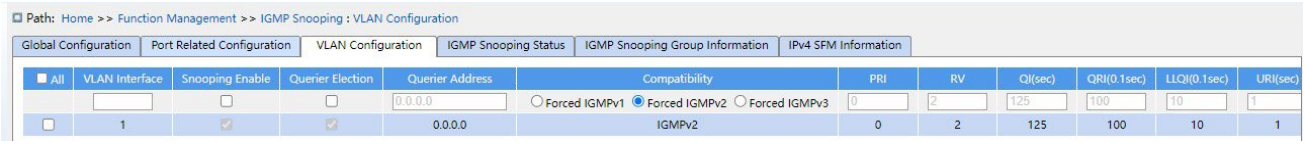


Рисунок 174 Настройка IGMP Snooping VLAN

VLAN Interface

Варианты: все созданные VLAN ID

Snooping Enable

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение или выключение функции 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: Включение или выключение функции IGMP query для выбранной VLAN. Предварительным условием для этой функции является включение глобальной функции IGMP Snooping и функции VLAN IGMP Snooping.

Описание: Когда в сети существует несколько генераторов запросов, автоматически выбирается тот, у которого наименьший IP-адрес, в качестве запрашивающего. Если есть только одно устройство, на котором включена функция IGMP query, оно будет генератором запросов.

Querier Address

Формат: A.B.C.D

Функция: Настройка исходящего IP-адреса для отправки пакетов с запросом. Если установлено значение

0.0.0.0, IP-адрес порта VLAN используется в качестве адреса запроса.

Compatibility

Варианты конфигурации: Forced IGMPv1/Forced IGMPv2/Forced IGMPv3

Конфигурация по умолчанию: Forced IGMPv2

Функция: Настройка версии IGMP.

PRI (Priority of Interface)

Диапазон настройки: 0~7

Конфигурация по умолчанию: 0

Функция: Настройка приоритета пакета управления IGMP.

RV (Robustness Variable)

Диапазон настройки: 1~255

Конфигурация по умолчанию: 2

Функция: Настройка параметра 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 настройки: 1~31744 с

Конфигурация по умолчанию: 125 с

Функция: Настройка интервала отправки пакета общего запроса.

QRI (Query Response Interval)

Диапазон настройки: 0~255 (ед. изм.: 0,1 с)

Конфигурация по умолчанию: 100

Функция: Настройка максимального времени ответа на пакет общего запроса.

LLQI (Last Member Query Interval)

Диапазон настройки: 0~31744（ед. изм: 0,1 с)

Конфигурация по умолчанию: 10

Функция: Настройка максимального времени ответа на пакет конкретного запроса.

Предупреждение:
Конфигурация QI, QRI и LLQI действительна только для генератора запросов.

URI (Unsolicited Report Interval)

Диапазон настройки: 0~31744 с

Конфигурация по умолчанию: 1 с

Функция: Задание интервала повторной отправки хостом пакета отчета для присоединения к группе многоадресной рассылки. Щелкните <Add New IGMP VLAN>, чтобы настроить запись IGMP Snooping VLAN. Поддерживается не более 32 записей IGMP Snooping VLAN.

4. Просмотрите статус IGMP Snooping, как показано ниже.

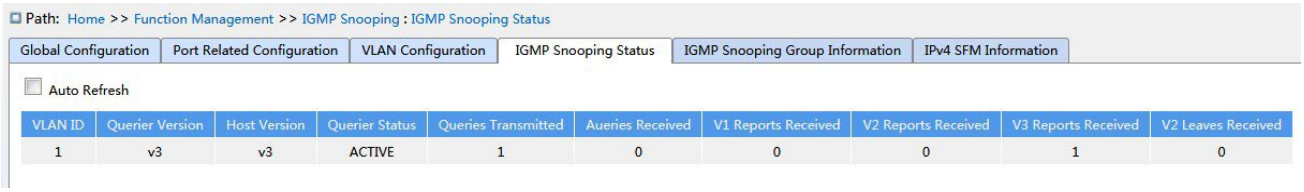


Рисунок 175 Просмотр статуса IGMP Snooping

Функция: На этой странице показаны подробности IGMP Snooping в интерфейсе VLAN.

VLAN ID: Интерфейс VLAN, на котором включен IGMP Snooping.

Query version: Версия запроса IGMP Snooping в интерфейсе VLAN, т. е. версия отправленных сообщений IGMP.

Host version: Версия хоста IGMP Snooping в интерфейсе VLAN, т. е. версия, которая получает сообщения IGMP.

Query status: включен ли запрос в интерфейсе VLAN.

Query sent/received: количество сообщений запроса, отправленных или полученных в интерфейсе VLAN.

Report Received v1/v2/v3: Количество отчетов IGMP версии v1/v2/v3, полученных в интерфейсе VLAN.

V2 Leave Receive: Количество сообщений IGMP Leave, полученных в интерфейсе VLAN для версии V2.

5. Просмотрите список участников многоадресной рассылки, как показано ниже.

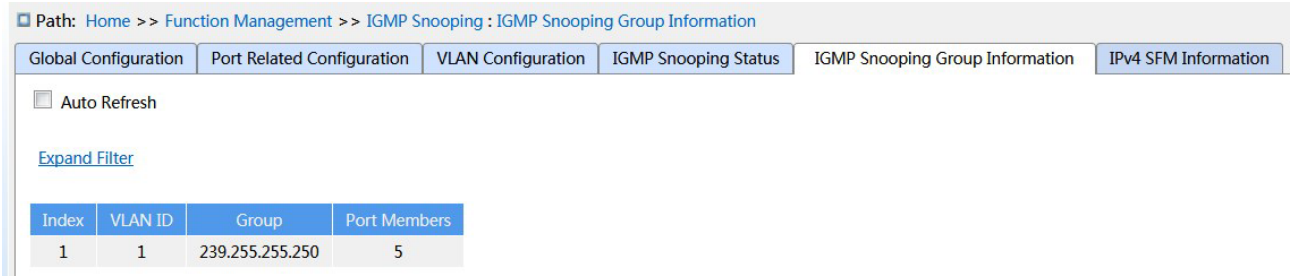


Рисунок 176 Список участников IGMP Snooping

VLAN ID

Варианты конфигурации: */>=/<=/диапазон выбора

Конфигурация по умолчанию: *

Функция: Отображение информации группы в соответствии с настроенными VLAN ID.

Group

Варианты конфигурации: */>=/<=/диапазон выбора

Конфигурация по умолчанию: *

Функция: Отображение информации группы в соответствии с настроенным адресом группы.

Port

Варианты конфигурации: */include/not include

Конфигурация по умолчанию: *

Функция: Отображение информации группы в соответствии с настроенным портом.

6. Просмотрите информацию Ipv4 SMF, как показано ниже.

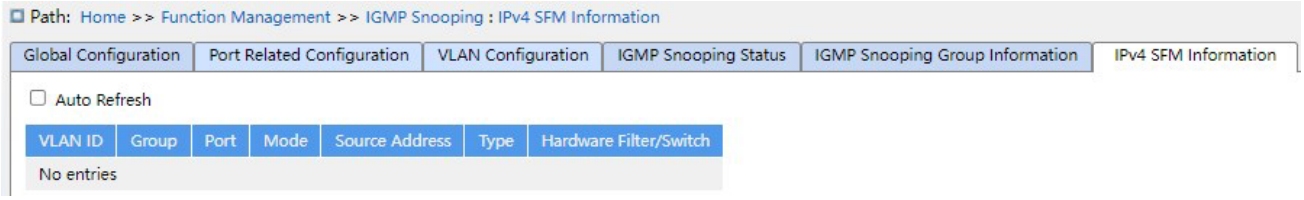


Рисунок 177 Информация IGMP Snooping IPv4 SFM

Функция: Когда устройство использует протокол v3, хосты могут явно запрашивать получение или отказ от получения данных многоадресной рассылки от определенного

источника многоадресной рассылки при присоединении к группе многоадресной рассылки, и эта информация включается в просмотр списка участников многоадресной рассылки на этой странице.

7.10.5 Пример типового использования

Как показано на рисунке 178, включите IGMP Snooping на коммутаторе 1, коммутаторе 2 и коммутаторе 3. Включите функцию автоматического запроса на коммутаторе 2 и коммутаторе 3. IP-адрес коммутатора 2 192.168.1.2, а IP-адрес коммутатора 3 192.168.0.2, таким образом коммутатор 3 выбран в качестве генератора запросов.

1. Включите IGMP Snooping.
2. Включите IGMP Snooping и автозапрос.
3. Включите IGMP Snooping и автозапрос.

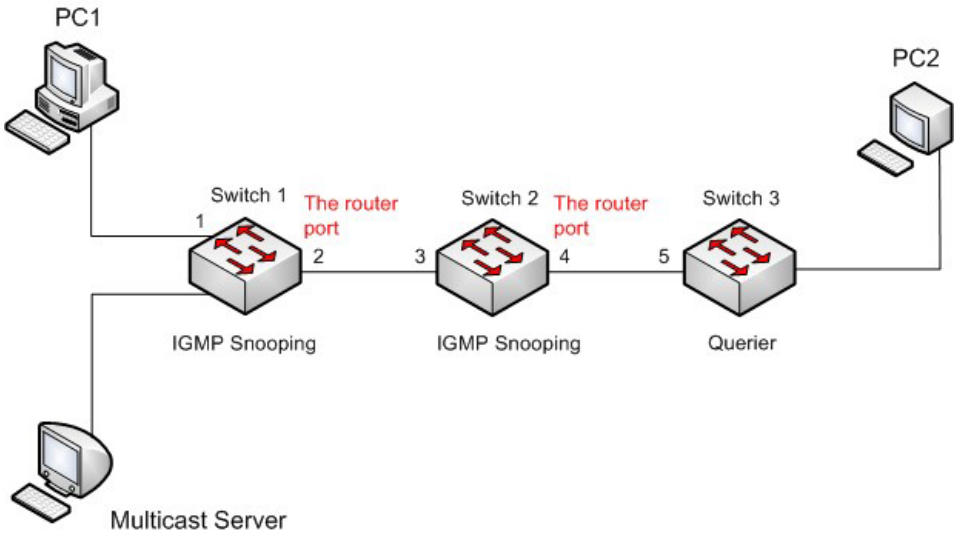


Рисунок 178 Пример использования IGMP Snooping

- Поскольку коммутатор 3 выбран в качестве генератора запросов, он периодически отправляет сообщение общего запроса.
- Порт 4 коммутатора 2 получает сообщение запроса. Он становится портом маршрутизатора. Между тем, коммутатор 2 пересылает сообщение запроса с порта 3. Затем порт 2 коммутатора 1 выбирается в качестве порта маршрутизатора, как только он получает запрос от коммутатора 2.
- Когда ПК 1 присоединяется к группе многоадресной рассылки 225.1.1.1, он отправляет сообщение отчета IGMP, поэтому порт 1 и маршрутизирующий порт 2 коммутатора 1

также присоединяются к группе многоадресной рассылки 225.1.1.1. Затем сообщение с отчетом IGMP будет перенаправлено на коммутатор 2 через маршрутизирующий порт 2, поэтому порт 3 и порт 4 коммутатора 2 также присоединятся к 225.1.1.1, а затем сообщение с отчетом IGMP будет перенаправлено на коммутатор 3 через маршрутизирующий порт 4, поэтому порт 5 коммутатора 3 также присоединится к 225.1.1.1.

- Когда многоадресные данные сервера многоадресной рассылки достигают коммутатора 1, данные будут перенаправлены на ПК1 через порт 1; поскольку маршрутизирующий порт 2 также является участником группы многоадресной рассылки, данные многоадресной рассылки будут пересылаться маршрутизирующим портом. Таким образом, когда данные достигнут порта 5 коммутатора 3, их пересылка прекратится, поскольку приемника больше нет, но если ПК2 также присоединится к группе 255.1.1.1, данные многоадресной рассылки будут перенаправлены на ПК2.

7.11 Настройка DHCP

С непрерывным расширением масштаба и ростом сложности сети, в условиях частого перемещения компьютеров (таких как ноутбуки или беспроводная сеть) и числа компьютеров, превышающего выделяемые IP-адреса, протокол BootP, специально предназначенный для статической конфигурации хоста, оказывается неспособным удовлетворить фактические потребности. Для быстрого доступа и выхода из сети и улучшения коэффициента использования ресурсов IP-адресов нам необходимо разработать автоматический механизм на основе BootP для назначения IP-адресов. Для решения этих проблем был введен DHCP (протокол динамической конфигурации хоста).

DHCP использует модель взаимодействия клиент-сервер. Клиент отправляет запрос конфигурации на сервер, а затем сервер отправляет параметры конфигурации, такие как IP-адрес, клиенту, достигая динамической конфигурации IP-адресов. Структура типичного использования DHCP показана на рисунке 179.

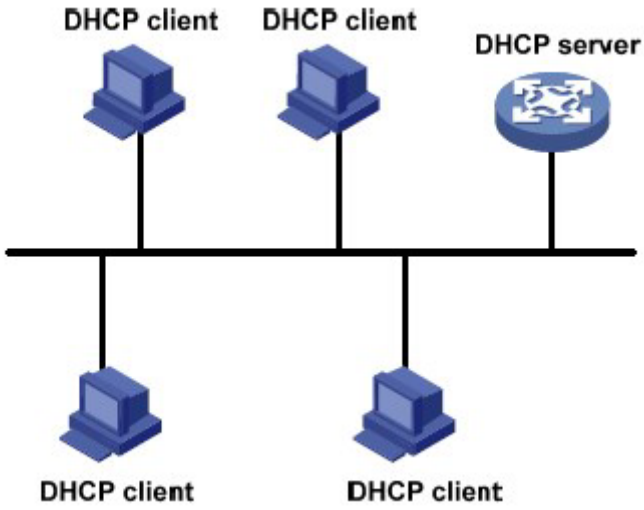


Рисунок 179 Типичное использование DHCP

Предупреждение:
В процессе динамического получения IP-адресов сообщения рассылаются путем широковещательной рассылки, поэтому требуется, чтобы DHCP-клиент и DHCP-сервер находились в одном сегменте. Если они находятся в разных сегментах, клиент может связаться с сервером через DHCP Relay, чтобы получить IP-адреса и параметры конфигурации.

DHCP поддерживает два типа механизмов распределения IP-адресов.

Статическое распределение: сетевой администратор статически привязывает фиксированные IP-адреса к нескольким конкретным клиентам, таким как WWW-сервер, и отправляет привязанные IP-адреса клиентам по DHCP. При статическом распределении адреса закрепляются постоянно.

Динамическое распределение: Сервер DHCP динамически выделяет IP-адрес клиенту. Этот механизм выделения может выделить клиенту постоянный IP-адрес или IP-адрес с ограниченным сроком аренды. Когда срок аренды истекает, клиенту необходимо повторно запросить IP-адрес.

Сетевой администратор может выбрать механизм распределения DHCP для каждого клиента.

7.11.1 Настройка сервера DHCP

7.11.1.1 Введение

DHCP-сервер — поставщик услуг DHCP. Он использует DHCP-сообщения для связи с DHCP-клиентом, чтобы выделить клиенту подходящий IP-адрес и при необходимости назначить ему другие сетевые параметры. DHCP-сервер обычно используется для выделения IP-адресов в следующих случаях.

- Большой масштаб сети. Трудоемкость ручной настройки велика, и трудно управлять всей сетью.
- Количество хостов превышает количество назначаемых IP-адресов, и нет возможности выделить фиксированный IP-адрес каждому хосту.

Лишь несколько хостов в сети нуждаются в фиксированных IP-адресах.

7.11.1.2 Пул адресов DHCP

DHCP-сервер выбирает IP-адрес из пула адресов и выделяет его клиенту вместе с другими параметрами. Последовательность распределения IP-адресов следующая:

1. IP-адрес статически привязан к MAC-адресу клиента.
2. Записанный на DHCP-сервере IP-адрес, который когда-либо был выделен клиенту.
3. IP-адрес, указанный в сообщении запроса, отправленном от клиента.
4. Первый доступный IP-адрес, найденный в пуле адресов.
5. Если нет доступного IP адреса, проверяется IP адрес, срок действия которого истекает, и у которого были конфликты в процессе использования. Если такой IP адрес найден, он присваивается клиенту. Если нет, то ничего не происходит.

7.11.1.3 Настройка через веб-интерфейс

1. Включите сервер DHCP, как показано ниже.

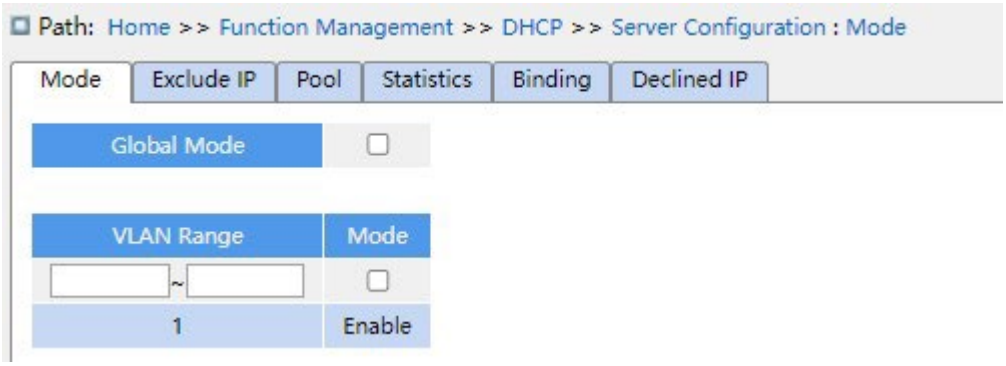


Рисунок 180 Запуск сервера DHCP

Режим Global Mode

Варианты конфигурации: Disabled/Enabled

Конфигурация по умолчанию: Disabled

Функция: Выбор текущего коммутатора как сервера DHCP, чтобы выделить или не выделять IP-адрес клиенту.

{VLAN Range, Mode}

Диапазон настройки: {1~4093, Disabled/Enabled}

Функция: Если для VLAN клиента, подающего заявку на получение IP-адреса, установлено значение Enabled, DHCP-сервер выделяет клиенту IP-адрес. В противном случае DHCP-сервер не выделяет клиенту IP-адрес.

2. Создайте пул адресов DHCP, как показано ниже.

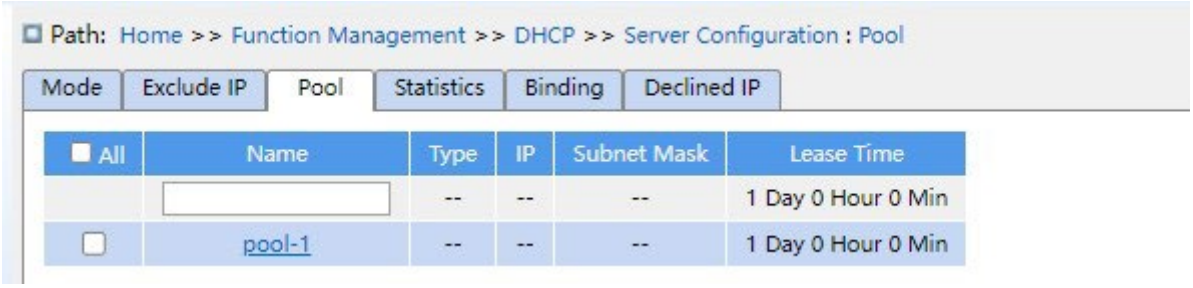


Рисунок 181 Создание пула адресов DHCP

Name

Диапазон настройки: 1~32 символа

Функция: задание имени пула IP-адресов.

Щелкните <Apply>, чтобы создать новый пул адресов DHCP.

3. Настройте пул адресов DHCP. Щелкните <Name> (см. рис. 181), чтобы настроить пул адресов DHCP, как показано ниже.

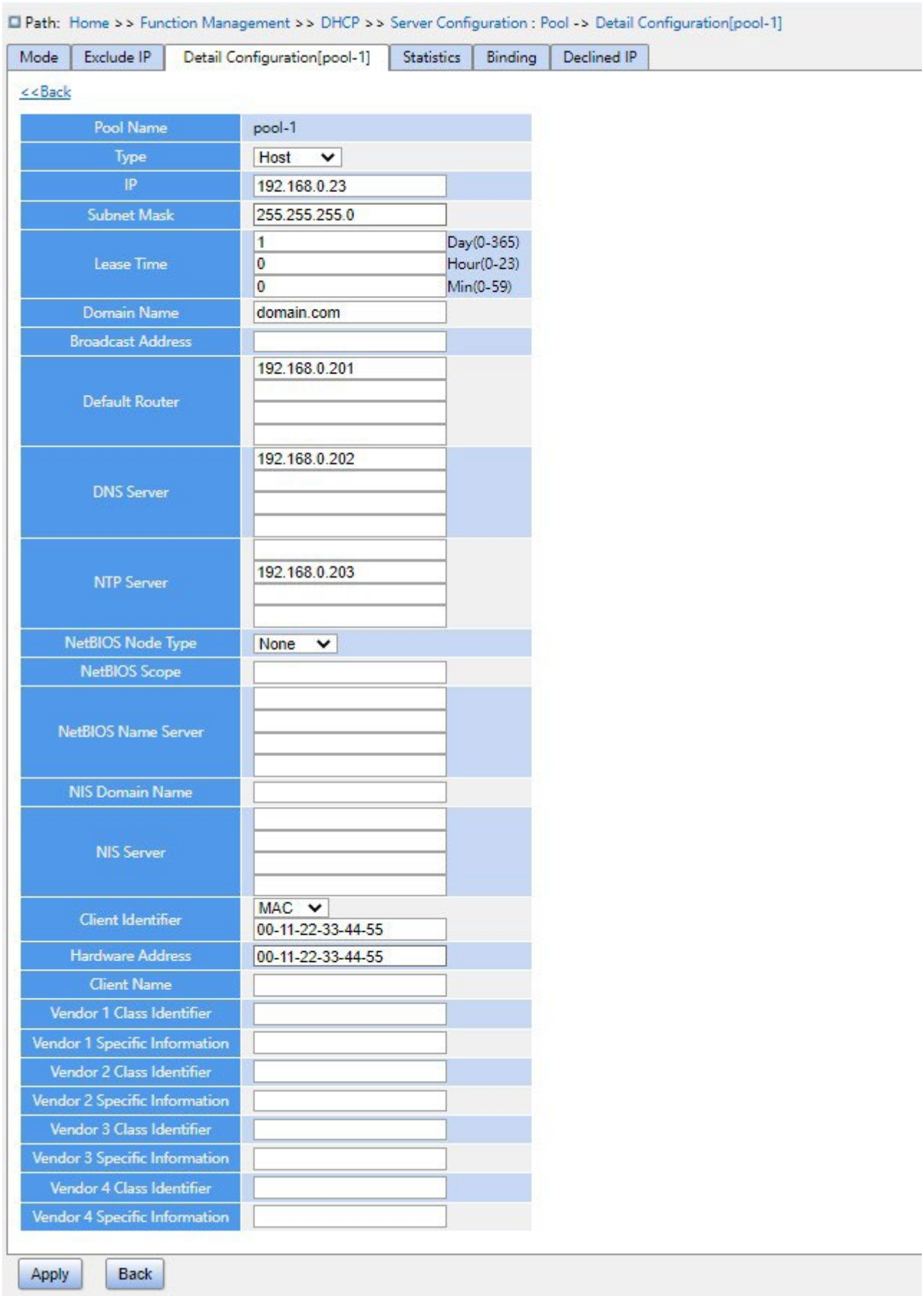


Рисунок 182 Настройка пула IP-адресов

Type

Варианты конфигурации: None/Network/Host

Конфигурация по умолчанию: None

Функция: Настройка типа пула адресов. Network: коммутатор динамически выделяет IP-адреса нескольким DHCP-клиентам. Host: коммутатор поддерживает статическое выделение IP-адресов специальным DHCP-клиентам.

{IP, Subnet Mask}

Функция: Network означает, что можно настроить диапазон пула IP-адресов, а диапазон адресов определяется маской подсети Маска подсети представляет собой число длиной 32 бита, состоящее из строки 1 и строки 0. «1» соответствует полям номера сети и полям номера подсети, а «0» соответствует полям номера хоста. Значение обычно настроено как 255.255.255.0.

Host указывает, что можно настроить статически привязанный IP-адрес клиента. Назначение статического IP-адреса реализовано путем связывания 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 выделения выше, чем у динамического выделения IP-адресов, а срок аренды является постоянным.

Lease Time

Диапазон настройки: 0 дней 0 часов 0 минут~365 дней 23 часа 59 минут

Конфигурация по умолчанию: 1 день 0 часов 0 минут

Описание: Настройка тайм-аута динамического выделения адресов. Для разных пулов адресов сервер DHCP может установить разное время аренды адреса, но адреса в одном пуле адресов DHCP имеют одинаковое время аренды.

Domain Name

Диапазон настройки: 1~36 символов

Функция: Задание доменного имени пула IP-адресов. При выделении IP-адреса клиенту ему также отправляется суффикс доменного имени.

Broadcast Address

Формат: A.B.C.D

Функция: Настройка широковещательного адреса клиента, выделенного DHCP-сервером.

Default Router

Формат: A.B.C.D

Функция: Настройка адреса клиентского шлюза, выделенного DHCP-сервером.

Пояснение: когда DHCP-клиент посещает хост, находящийся в другом сегменте, данные должны пересылаться через шлюзы. Когда DHCP-сервер выделяет клиентам IP-адреса, он может одновременно указывать адреса шлюза. Для пула адресов DHCP можно настроить не более 4 шлюзов.

DNS Server

Формат: A.B.C.D

Функция: Настройка адреса сервера DNS, выделенного DHCP-сервером.

Пояснение: При посещении сетевого хоста через доменное имя доменное имя должно быть преобразовано в IP-адрес. Это реализуется DNS (системой доменных имен). Для того, чтобы DHCP-клиент мог посещать сетевой хост через доменное имя, при выделении IP-адресов клиентам DHCP-сервер может одновременно указывать IP-адреса серверов доменных имен. Для пула адресов DHCP можно настроить не более 4 серверов DNS.

NTP Server

Формат: A.B.C.D

Функция: Настройка адреса сервера NTP, выделенного DHCP-сервером.

NetBIOS Node Type

Варианты конфигурации: None/B-node/P-node/M-node/H-node

Конфигурация по умолчанию: None

Функция: Настройка типа узла NetBIOS, выделенного DHCP-сервером. Когда DHCP-клиент использует протокол NetBIOS для связи в сети, необходимо установить соответствие между именем хоста и IP-адресом. Различные типы узлов получают сопоставление в разных режимах.

Описание: B-узел получает сопоставление в широковещательном режиме. P-узел получает сопоставление, отправляя одноадресный пакет для связи с WINS-сервером в первый раз. M-узел получает сопоставление, отправив широковещательный пакет в первый раз. Если M-узел не может получить сопоставление в первый раз, он получает сопоставление,

отправив одноадресный пакет для связи с WINS-сервером во второй раз. H-узел получает сопоставление, отправляя одноадресный пакет для связи с WINS-сервером в первый раз. Если H-узел не может получить сопоставление в первый раз, он получает сопоставление, отправив широковещательный пакет во второй раз.

NetBIOS Scope

Диапазон настройки: 1~36 символов

Функция: Настройка имени NetBIOS.

NetBIOS Name Server

Формат: A.B.C.D

Функция: Настройка адреса сервера WINS, выделенного DHCP-сервером.

Пояснение: Для клиента, работающего под управлением операционной системы (ОС) Microsoft Windows, сервер Windows Internet Naming Service (WINS) предоставляет услугу преобразования имени хоста в IP-адрес для хоста, использующего протокол NetBIOS для передачи данных. Поэтому для большинства клиентов на базе ОС Windows требуется настройка WINS. Чтобы DHCP-клиент мог преобразовать имя хоста в IP-адрес, следует указать адрес WINS-сервера, когда DHCP-сервер выделяет IP-адрес клиенту. Для пула адресов DHCP можно настроить не более 4 серверов WINS.

NIS Domain Name

Диапазон настройки: 1~36 символов

Функция: Настройка адреса доменного имени NIS, выделенного DHCP-сервером.

NIS Server

Формат: A.B.C.D

Функция: Настройка адреса сервера NIS, выделенного DHCP-сервером.

Client Identifier

Варианты конфигурации: None/FQDN/MAC

Конфигурация по умолчанию: None

Функция: Если тип пула - хост, необходимо указать уникальный идентификатор клиента.

Hardware Address

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

Функция: Если тип пула - хост, необходимо указать статически привязанный MAC-адрес.

Client Name

Диапазон настройки: 1~32 символа

Функция: Настройка имени пользователя клиента.

Vendor i Class Identifier

Диапазон настройки: 1~64 символа

Функция: Настройка идентификатора класса вендора, выделенного DHCP-сервером.

Vendor i Specific Information

Диапазон настройки: 1~64 шестнадцатеричных числа

Функция: Настройка специфичной информации вендора, выданной DHCP-сервером.

4. Настройте исключенные IP-адреса (IP-адреса не выделяются динамически в пуле адресов DHCP), как показано ниже.

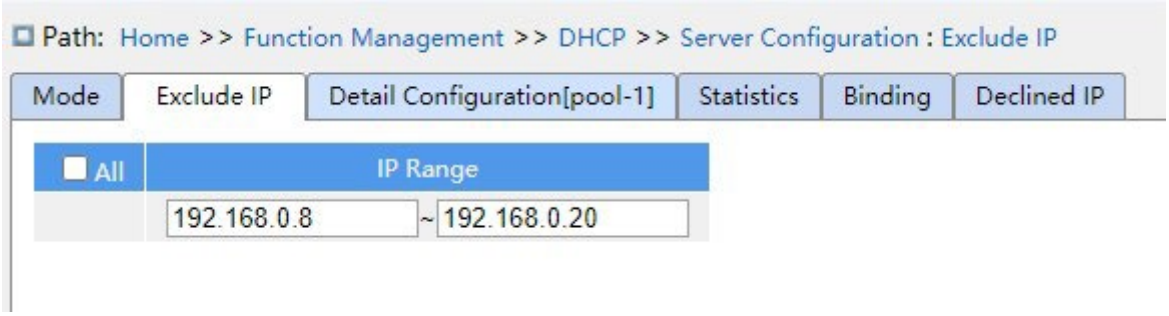


Рисунок 183 Настройка исключенных IP-адресов

IP Range

Функция: Настройка диапазона IP-адресов, которые не выделяются динамически в пуле адресов DHCP. При распределении IP-адресов DHCP-сервер должен исключить занятый IP-адрес (например, IP-адреса шлюза и DNS-сервера). В противном случае один и тот же IP-адрес может быть назначен двум клиентам, что приведет к конфликту IP-адресов.

5. Просмотрите статистику сервера DHCP, как показано ниже.

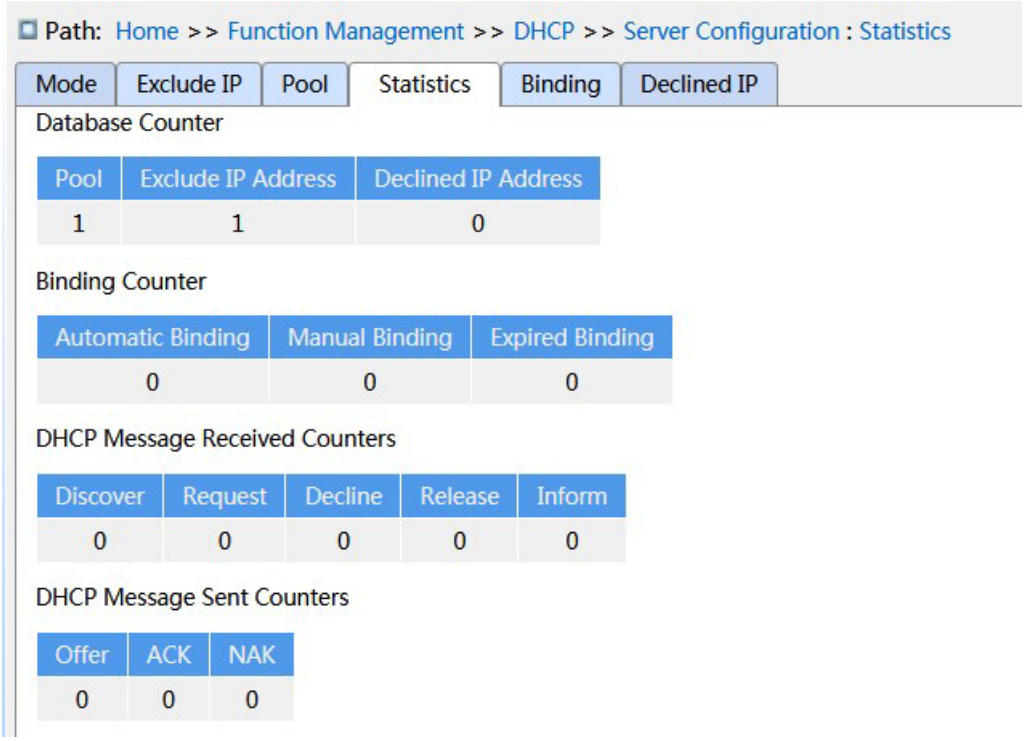


Рисунок 184 Просмотр статистики сервера DHCP

6. Просмотрите информацию об IP-адресах, выделенных сервером DHCP, как показано ниже.

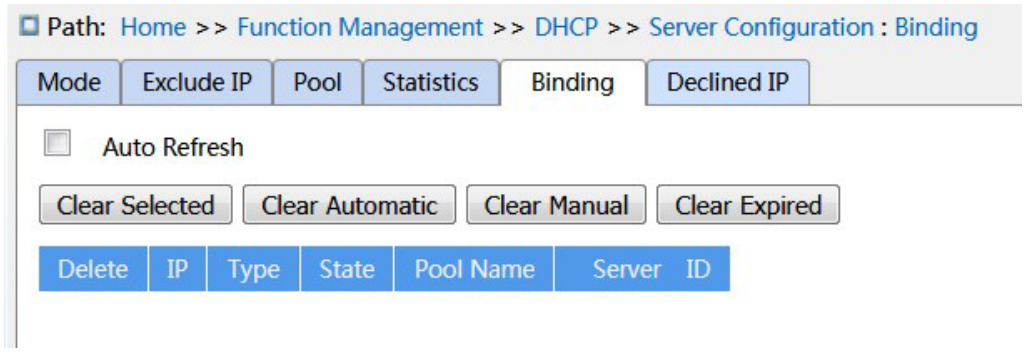


Рисунок 185 Просмотр информации об IP-адресах, выделенных сервером DHCP

Функция: Отображение информации об IP-адресах, которые в данный момент назначены через DHCP.. ip: Назначенный IP-адрес. Type: Тип назначенного адреса. Status: Статус использования назначенного IP-адреса. Address pool name: Имя пула адресов, использованного для назначения IP-адреса. Server ID: Идентификатор сервера, использованного для назначения IP-адреса.

7. Просмотрите IP-адреса, отклоненные DHCP-клиентами, как показано ниже.

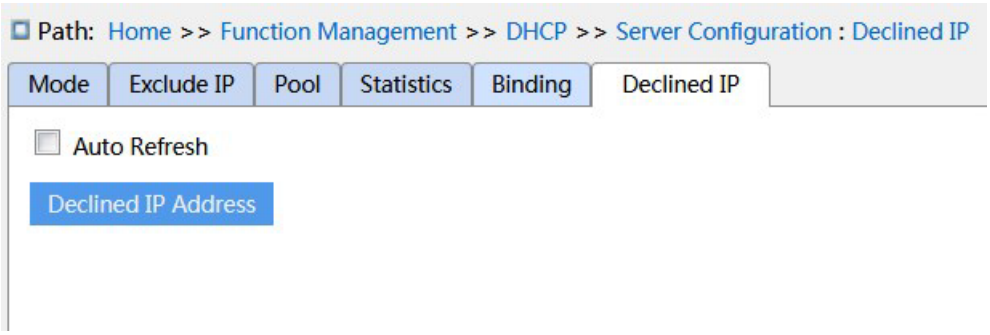


Рисунок 186 Просмотр IP-адресов, отклоненных DHCP-клиентами

Если клиент обнаруживает, что IP-адрес, выделенный сервером, конфликтует со статическим IP-адресом в том же сегменте сети, он отправляет на сервер пакет отклонения, чтобы отклонить этот IP-адрес. Сервер записывает IP-адрес, отклоненный клиентом, и не будет выделять этот IP-адрес другим клиентам в течение определенного периода времени.

7.11.1.4 Пример типовой конфигурации

Как показано на рисунке 187, коммутатор A работает как сервер DHCP, а коммутатор B работает как DHCP-клиент. Порт 3 коммутатора A подключается к порту 4 коммутатора B. Клиент отправляет сообщения с запросом IP-адреса, и сервер может выделить IP-адрес клиенту двумя способами. Для динамического выделения IP-адресов диапазон исключенных адресов 192.168.0.1~192.168.0.10.

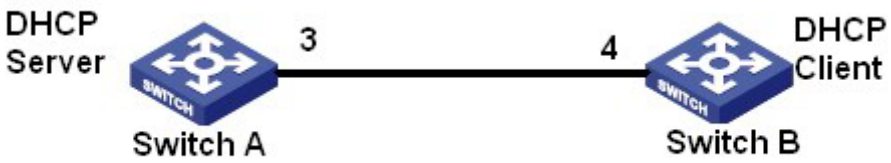


Рисунок 187 Пример типовой конфигурации DHCP

Статически выделите IP-адрес

➢ Конфигурация коммутатора A:

1. Запустите сервер DHCP в соответствующих VLANs, как показано на рисунке 180.
2. Создайте IP-пул DHCP: pool-1, как показано на рисунке 181.
3. Установите тип пула Host; IP-адрес 192.168.0.6, маску 255.255.255.0; Привяжите MAC-адрес коммутатора B: 00-11-22-33-44-55, как показано на рисунке 182.

➢Конфигурация коммутатора B:

1. Настройте коммутатор B для автоматического получения 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 рисунке 188.

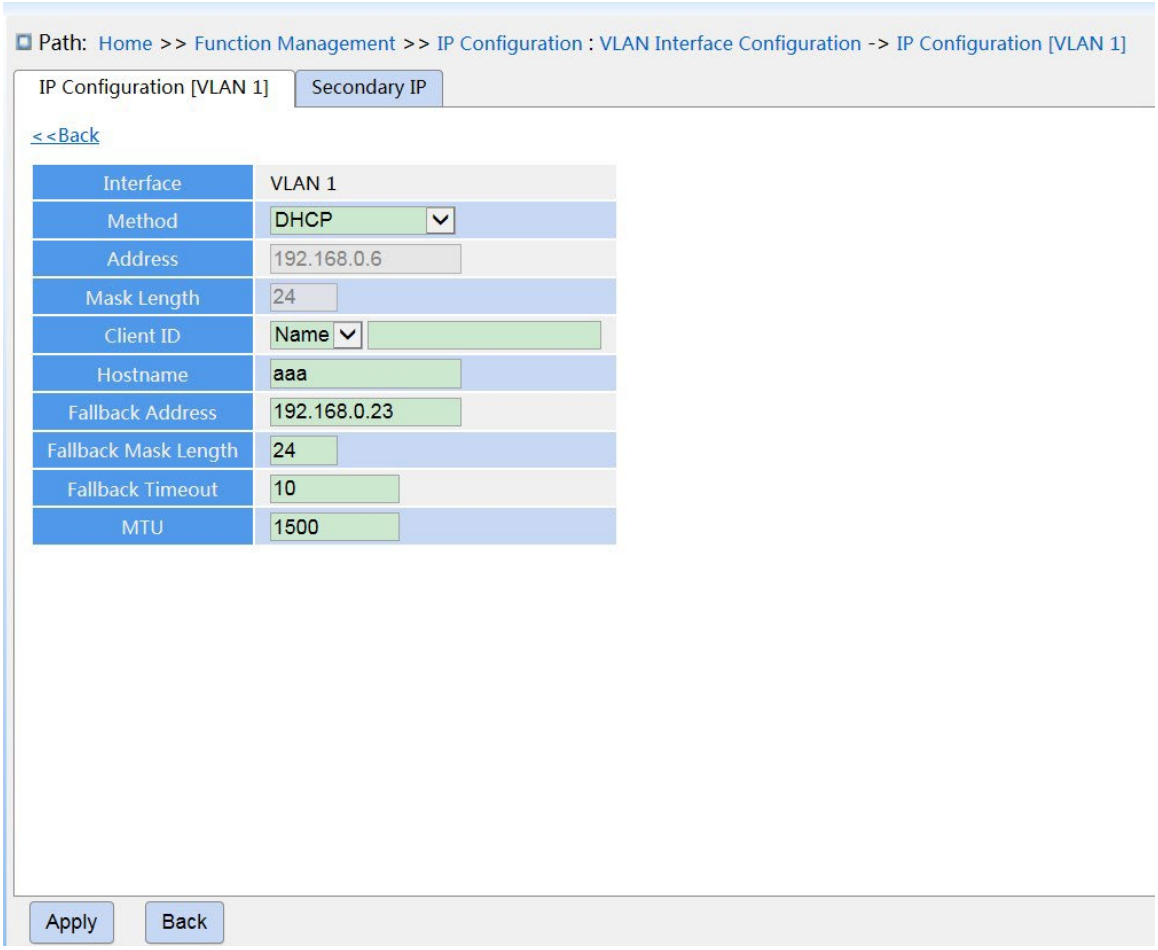


Рисунок 188 Клиент DHCP получает IP-адрес-1

Динамически выделите IP-адрес

➢ Конфигурация коммутатора A:

1. Запустите сервер DHCP в соответствующих VLANs, как показано на рисунке 180.
2. Создайте IP-пул DHCP: pool-1, как показано на рисунке 181.
3. Установите тип пула Network; IP-адрес 192.168.0.6, маску 255.255.255.0, остальные настройки по умолчанию.
4. Настройте диапазон исключенных IP-адресов 192.168.0.1~192.168.0.10., как показано на рисунке 183.

➢Конфигурация коммутатора B:

1. Настройте коммутатор B для автоматического получения IP-адреса через DHCP.

2. DHCP-сервер ищет доступные IP-адреса в пуле адресов по порядку и выделяет первый найденный доступный IP-адрес и другие сетевые параметры коммутатору B.

Маска подсети 255.255.255.0, как показано на рисунке 189.

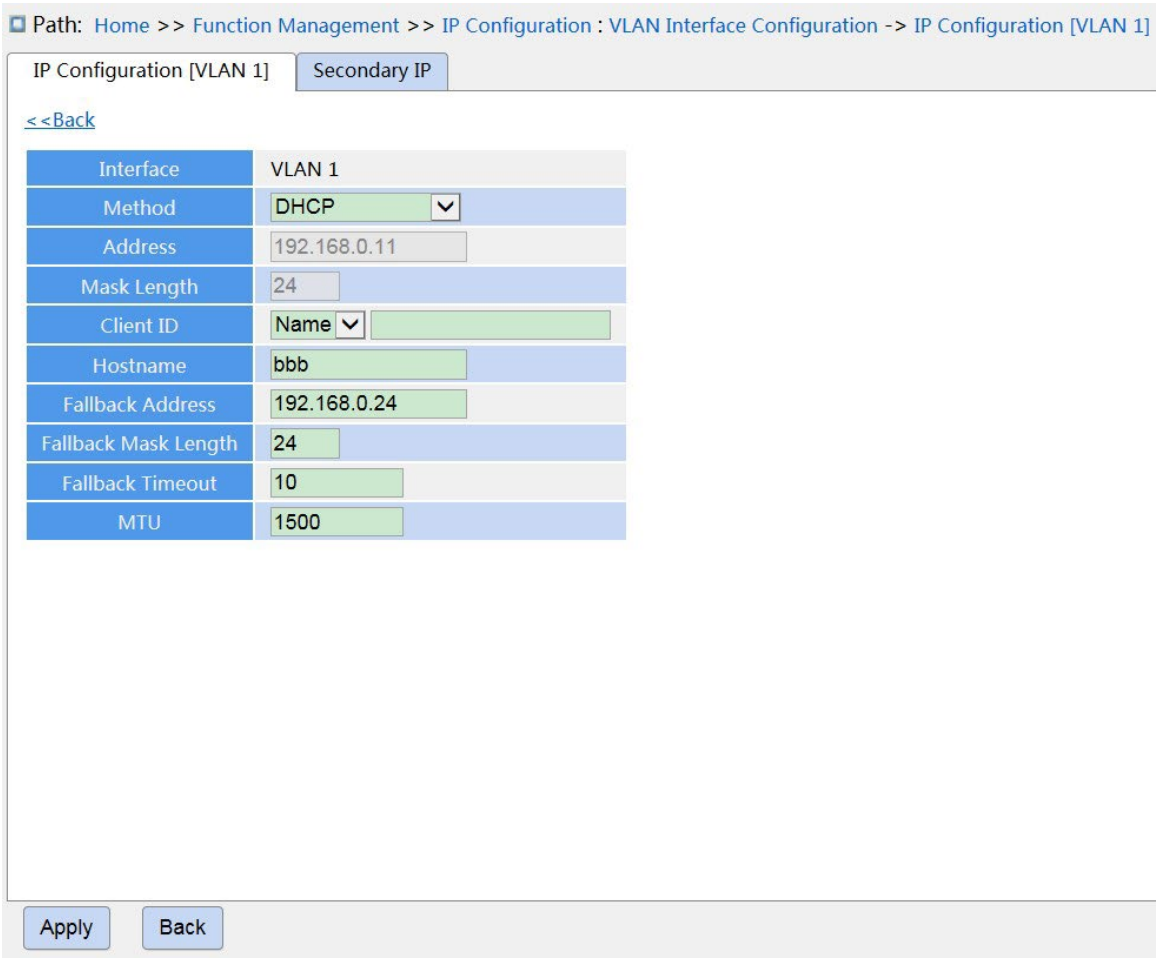


Рисунок 189 Клиент DHCP получает IP-адрес-2

7.11.2 DHCP Snooping

7.11.2.1 Введение

Отслеживание DHCP — это функция мониторинга служб DHCP на уровне 2 и функция безопасности DHCP, обеспечивающая дополнительную безопасность клиента. Механизм безопасности DHCP Snooping может контролировать, что только доверенный порт может пересылать сообщение запроса DHCP-клиента на легальный сервер, в то же время он может контролировать источник ответного сообщения DHCP-сервера, гарантируя, что клиент получит IP-адрес от действительного сервера, и

предотвращая выделения IP-адресов или других параметров конфигурации другим хостам поддельным или недействительным DHCP-сервером.

Механизм безопасности DHCP Snooping делит порты на доверенные и ненадежные. Доверенный порт: порт, который прямо или косвенно подключается к действительному DHCP-серверу. Доверенный порт пересылает сообщения запросов DHCP-клиентов и ответные сообщения DHCP-серверов, чтобы гарантировать, что DHCP-клиенты могут получить допустимые IP-адреса. Ненадежный порт: это порт, который подключается к недействительному DHCP-серверу. Ненадежный порт не пересылает сообщения запросов DHCP-клиентов и ответные сообщения DHCP-серверов, чтобы предотвратить получение DHCP-клиентами недопустимых IP-адресов.

7.11.2.2 Настройка через веб-интерфейс

1. Включите функцию DHCP Snooping, как показано ниже.

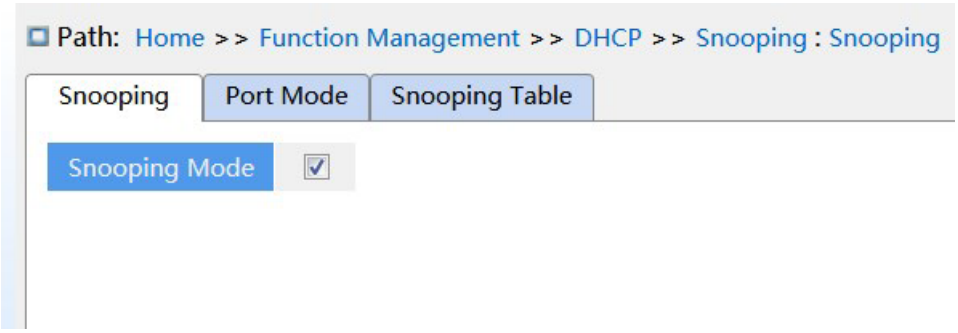


Рисунок 190 Состояние функции DHCP Snooping

DHCP Snooping Mode

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение/выключение функции DHCP Snooping

Предупреждение:

У коммутатора, который работает и как сервер DHCP и как клиент, нельзя включить функцию DHCP Snooping.

2. Настройте доверенные порты, как показано ниже.

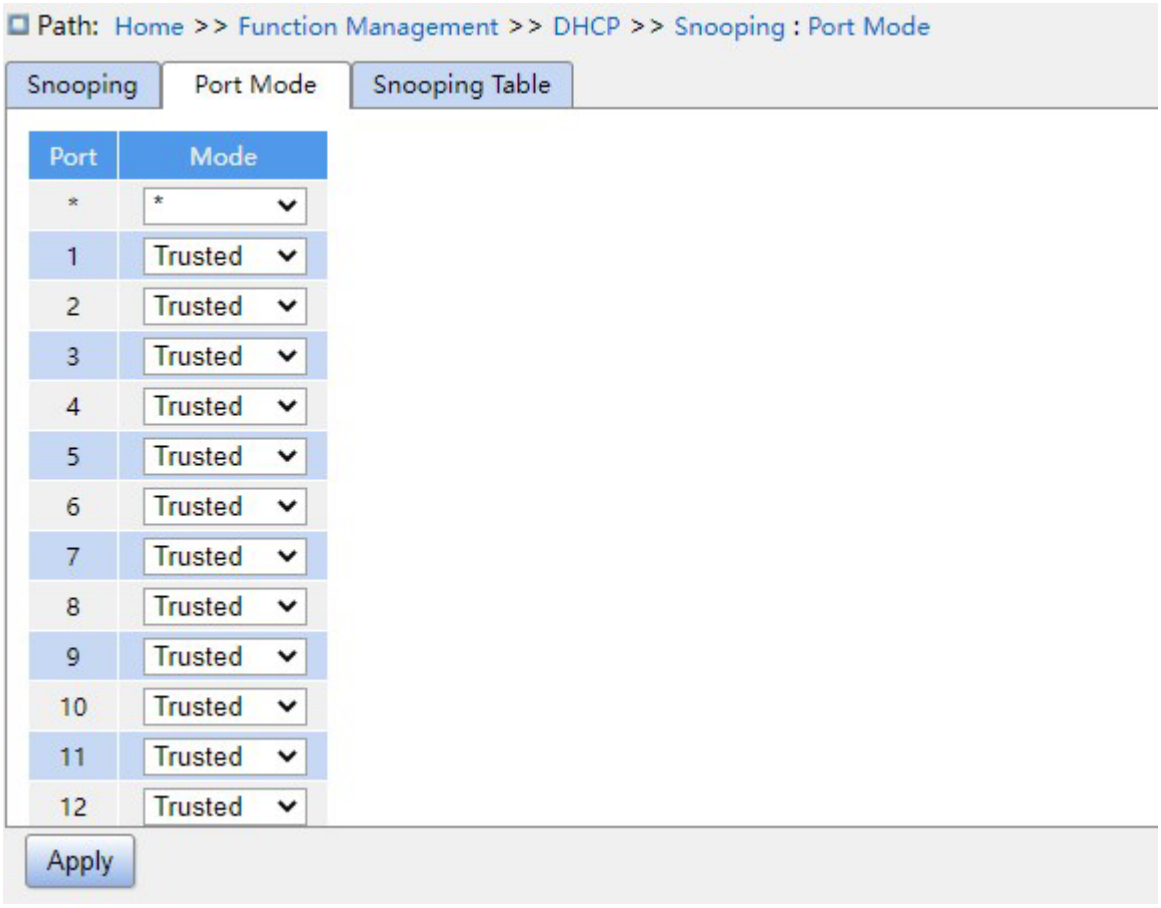


Рисунок 191 Настройка доверенных портов

Mode

Варианты конфигурации: Trusted/Untrusted

Конфигурация по умолчанию: Untrusted

Функция: настройка порта как доверенного или ненадежного. Порты, которые прямо или косвенно подключаются к действительному DHCP-серверу – это доверенные порты.

3. Просмотрите записи DHCP Snooping, как показано ниже.

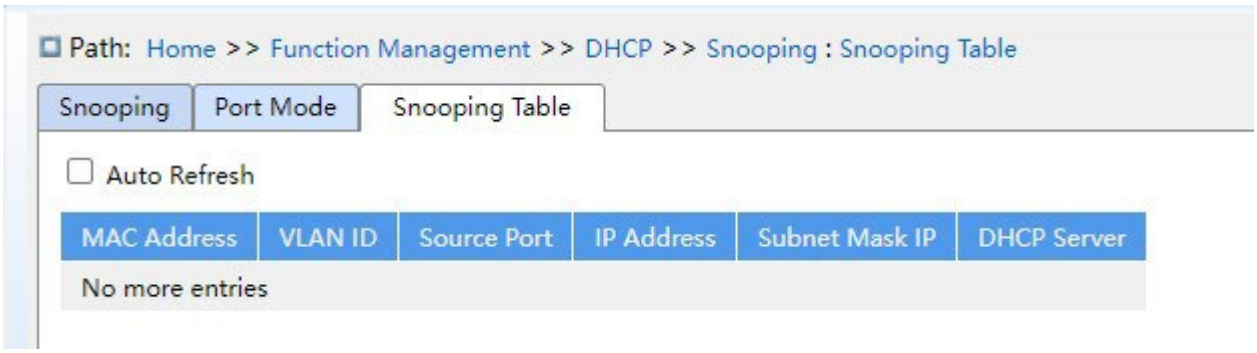


Рисунок 192 Просмотр записей DHCP Snooping

7.11.2.3 Пример типовой конфигурации

Как показано на рисунке 193, DHCP-клиент запрашивает IP-адрес от сервера DHCP. В сети существует неавторизованный DHCP-сервер. Порт 1 настроен как доверенный порт с помощью DHCP Snooping, чтобы пересылать сообщение запроса DHCP-клиента на DHCP-сервер и пересылать ответное сообщение DHCP-сервера на DHCP-клиент. Порт 3 настроен в качестве ненадежного порта, который не может пересылать сообщение запроса DHCP-клиента и ответное сообщение неавторизованного DHCP-сервера, гарантируя, что клиент может получить действительный IP-адрес от действительного DHCP-сервера.

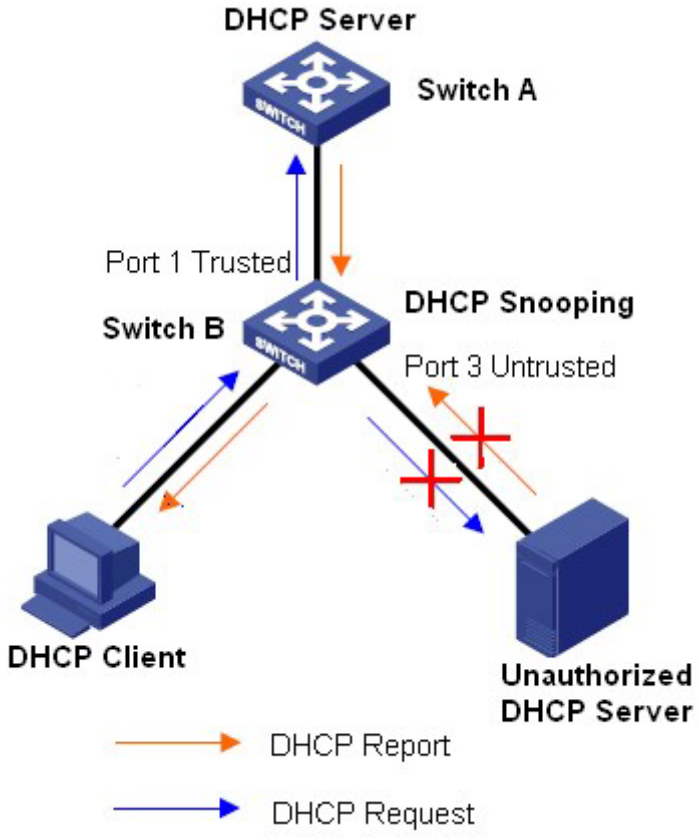


Рисунок 193 Пример типовой конфигурации DHCP

Конфигурация коммутатора B:

- Включите функцию DHCP Snooping, как показано на рисунке 190.
- Настройте порт 1 коммутатора B как доверенный порт, а порт 3 как ненадежный порт, как показано на рисунке 191.

7.11.3 DHCP Relay

7.11.3.1 Введение

1. DHCP Relay

Ретрансляция DHCP — это пересылка пакетов DHCP между DHCP-сервером и клиентом. Если клиент DHCP не находится в той же подсети, что и сервер, должен быть ретранслятор DHCP для пересылки сообщений запроса и ответа DHCP. Пересылка данных ретрансляции DHCP отличается от обычной переадресации маршрута. Обычная переадресация маршрута относительно прозрачна, и устройство обычно не изменяет содержимое IP-пакета. Однако после получения сообщения DHCP ретранслятор DHCP повторно сгенерирует сообщение DHCP и затем перешлет его. С позиции клиента DHCP агент ретрансляции DHCP подобен DHCP-серверу; с позиции DHCP-сервера агент ретрансляции DHCP аналогичен DHCP-клиенту.

Ретранслятор DHCP пересылает полученный пакет запроса DHCP на сервер DHCP в одноадресном режиме и пересылает полученный пакет ответа DHCP клиенту DHCP. Ретранслятор DHCP эквивалентен станции пересылки и отвечает за связь с DHCP-клиентами и DHCP-серверами, расположенными в разных сегментах сети. Он реализует динамическое управление IP-адресами для нескольких сегментов сети, пока установлен DHCP-сервер, то есть динамическое управление IP-адресами DHCP в режиме «клиент-ретранслятор-сервер», как показано ниже.

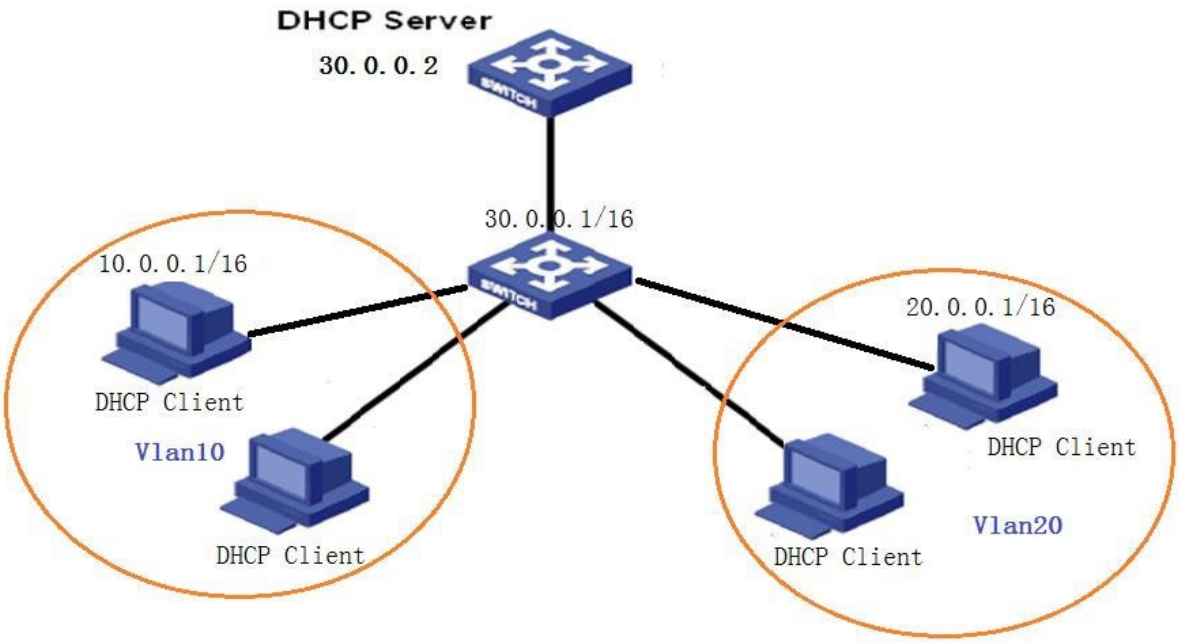


Рисунок 194 Режим «клиент-ретранслятор-сервер»

2. Информация об агенте ретрансляции DHCP (Функция option 82)

Когда ретрансляционное устройство выполняет ретрансляцию DHCP, можно добавить некоторые параметры, чтобы указать некоторую сетевую информацию клиента DHCP, чтобы сервер мог назначать пользователям разные IP-адреса в соответствии с более точной информацией. Согласно RFC3046, номер используемой опции — 82, поэтому ее также называют option 82.

Функция Option 82 (запись информации об агенте ретрансляции) записывает информацию о клиенте. Когда DHCP Snooping, поддерживаемый Option 82, получает сообщение запроса от DHCP-клиента, в сообщения добавляется соответствующее поле Option 82, а затем сообщение пересылается на DHCP-сервер. Сервер, поддерживающий Option 82, может гибко распределять адреса в соответствии с сообщением Option 82.

После включения функции Option 82 поле Option 82 будет добавлено в сообщение. Поле Option82 коммутаторов этой серии содержит два параметра: параметр 1 (Circuit ID) и параметр 2 (Remote ID). Формат двух параметров показан ниже:

- Параметр 1 содержит идентификатор VLAN ID и номер порта, который получает сообщение запроса от DHCP-клиента, как показано в Таблице 7.

Таблица 7 Формат поля параметра 1

Тип параметра（0x01）	Длина（0x04）	VLAN ID	Номер порта
Один байт	Один байт	Два байта.	Два байта.

Тип параметра: Тип параметра 1 – 1.

Длина: количество байтов, которые занимают идентификатор VLAN и номер порта.

VLAN ID: На устройстве DHCP Relay — идентификатор VLAN порта, который получает сообщение запроса от DHCP-клиента.

Номер порта: На устройстве DHCP Relay — номер порта, который получает сообщение запроса от DHCP-клиента.

- Параметр 2 содержит MAC-адрес устройства DHCP Relay, которое получает сообщение запроса от DHCP-клиента, как показано в Таблице 8.

Таблица 8 Формат поля параметра 2 – MAC-адрес

Тип параметра（0x02）	Длина（0x06）	MAC-адрес
Один байт	Один байт	6 байт

Тип параметра: Тип параметра 2 – 2.

Длина: количество байтов, которые занимает содержание параметра 2. MAC-адрес занимает 6 байт, а строка символов занимает 16 байт.

MAC-адрес: содержимое параметра 2 — это MAC-адрес устройства DHCP Relay, которое получает сообщение запроса от DHCP-клиента.

Если устройство DHCP Relay поддерживает функцию Option 82, при получении DHCP Relay сообщения запроса DHCP сообщение обрабатывается в соответствии с тем, содержит ли сообщение Option 82 и политику клиента, а затем обработанное сообщение пересылается серверу DHCP. Метод обработки показан в таблице 9.

Таблица 9 Обработка сообщения запроса DHCP Relay

Получение сообщения запроса от DHCP-клиента.	**Политика конфигурации**	**Обработка сообщения запроса на устройстве DHCP Relay**

Сообщение запроса содержит Option 82	Drop	Отклонить сообщение запроса
	Keep	Сохранить формат сообщения без изменений и переслать сообщение
	Replace	Заменить поле Option 82 в сообщении полем Option 82 устройства Snooping и переслать новое сообщение
Сообщение запроса не содержит Option 82	Drop/Keep/Replace	Добавить поле Option 82 устройства Relay в сообщение и переслать его

Когда устройство DHCP Relay получает сообщение запроса от DHCP-сервера, если сообщение содержит поле Option 82, удалить поле Option 82 и переслать сообщение клиенту.

7.11.3.2 Настройка через веб-интерфейс

1. Глобальные настройки DHCP Relay показаны ниже.

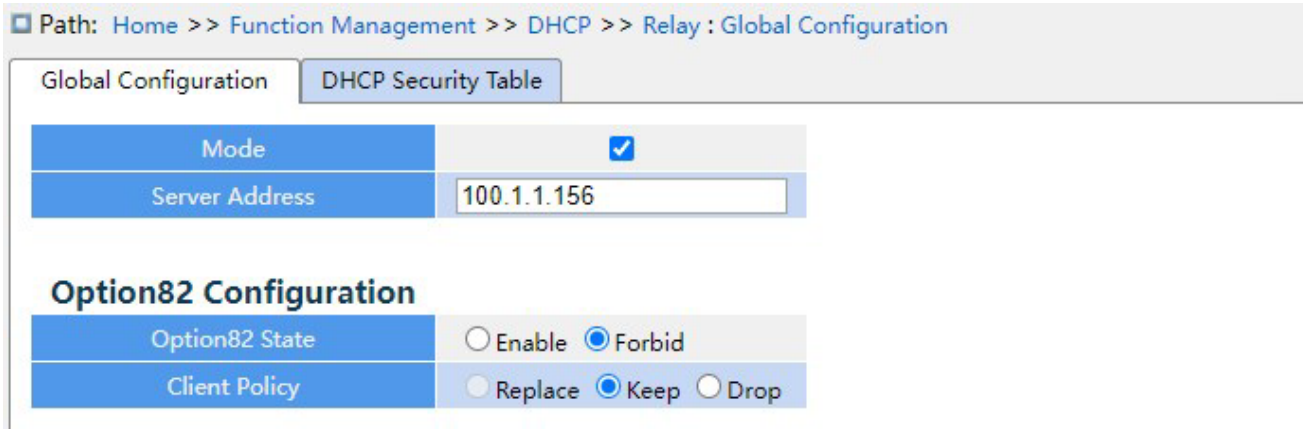


Рисунок 195 Глобальные настройки DHCP Relay

Mode

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: включение DHCP Relay

Server Address

Функция: Настройка адреса сервера DHCP.

Option82 State

Варианты конфигурации: Enable/Forbid

Конфигурация по умолчанию: Forbid

Функция: включение Option 82 DHCP Relay

Client Policy

Варианты конфигурации: Replace/keep/drop

Конфигурация по умолчанию: Keep

Функция: настроить политику клиента, ретрансляция DHCP обработает сообщение запроса, отправленное клиентом, в соответствии с политикой клиента. Метод обработки показан в таблице 9.

2. Настройте элементы таблицы безопасности DHCP, как показано ниже.

Рисунок 196 Просмотр таблицы безопасности DHCP

7.11.3.3 Пример типовой конфигурации

Как показано ниже, коммутатор A в качестве DHCP-сервера, коммутатор B в качестве ретранслятора DHCP, коммутатор C в качестве DHCP-клиента, порт 1 коммутатора A подключаются к порту 1 коммутатора B, порт 2 коммутатора B подключаются к порту 2 коммутатора. C. DHCP-сервер не находится в той же локальной сети, что и DHCP-клиент. Клиент динамически получает IP-адрес и другие сетевые параметры в режиме DHCP через ретранслятор DHCP.

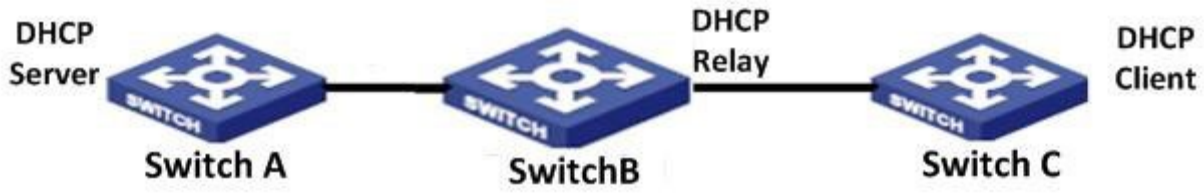


Рисунок 197 Пример типовой конфигурации

DHCP ➢Конфигурация коммутатора A:

1. Создайте VLAN1 и настройте IP: 100.1.1.156, как показано на рисунке 107.
2. Откройте вкладку состояния сервера DHCP VLAN 1, как показано на рисунке 107.
3. Создайте пул адресов pool-33, как показано на рисунке 181.
4. Выберите тип пула адресов Network; IP-адрес: 33.1.1.6; маску: 255.0.0.0;

➢Конфигурация коммутатора B:

1. Создайте VLAN1 и настройте IP: 100.1.1.180, как показано на рисунке 107.
2. Создайте VLAN33 и настройте IP: 33.1.1.2, как показано на рисунке 107.
3. Включите ретрансляцию DHCP, как показано на рисунке 195.
4. Настройте IP-адрес сервера: 100.1.1.156, как показано на рисунке 195. ➢ Конфигурация коммутатора C:

1. Создайте VLAN33 и включите клиент DHCP, как показано на рисунке 107.
2. Коммутатор A назначает IP-адрес 33.0.0.1 коммутатору C.

7.12 Настройка IEEE802.1X

7.12.1 Введение

Для обеспечения безопасности WLAN комитет IEEE802 LAN/WAN предложил протокол 802.1X. Как общий механизм управления доступом к портам LAN в Ethernet, 802.1X реализует аутентификацию и безопасность Ethernet.

802.1X — это управление доступом к сети на основе портов.

Управление доступом к сети на основе портов предназначено для реализации аутентификации и управления портами устройств доступа к локальной сети.

Если пользователь проходит аутентификацию, он может получить доступ к ресурсам в локальной сети. Если он не проходит аутентификацию, он не может получить доступ к ресурсам в локальной сети. Системы 802.1X используют структуру клиент/сервер, как показано ниже. Аутентификация и авторизация пользователя при управлении доступом на основе порта требуют следующих элементов:

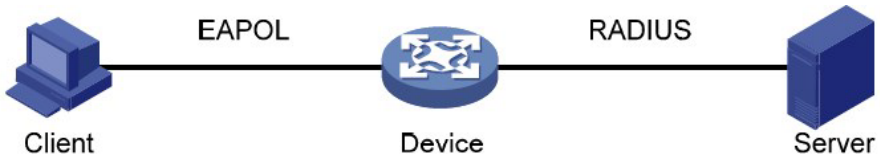


Рисунок 198 Структура IEEE802.1X

Клиент: обычно указывает пользовательский терминал. Когда пользователь хочет выйти в Интернет, он запускает клиентскую программу и вводит необходимое имя пользователя и пароль. Клиентская программа отправляет запрос на соединение. Клиент должен поддерживать EAPOL (Extensible Authentication Protocol over LAN).

Устройство: указывает коммутатор аутентификации в системе Ethernet. Он загружает и доставляет информацию об аутентификации пользователя, а также включает или отключает порт в зависимости от результата аутентификации.

Сервер аутентификации: указывает объект, предоставляющий службу аутентификации для устройств. Он проверяет, есть ли у пользователей разрешения на использование сетевых служб в соответствии с идентификаторами (именами пользователей и паролями), отправленными клиентами, и включает или отключает порты в соответствии с результатами аутентификации.

7.12.2 Настройка через веб-интерфейс

1. Конфигурация 802.1X Task Manager показана ниже.

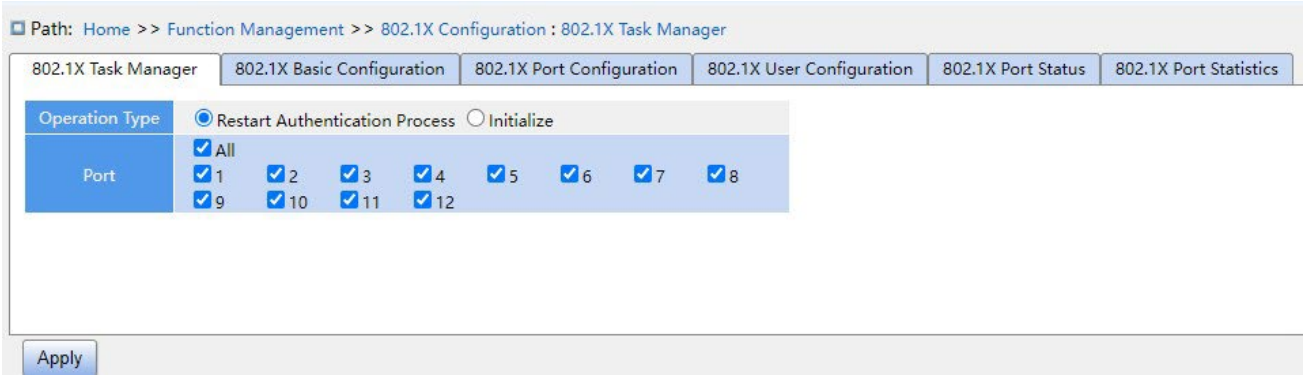


Рисунок 199 Конфигурация Task Manager

Operation type

Варианты конфигурации: Restart Authentication Process /initialization

Функция: Когда порт выбирает режим аутентификации 802.1X на базе Mac и порта, можно выбрать <Restart Authentication Process>/<Initialize> для повторной

аутентификации. Во время процесса повторной аутентификации статус порта переключается на состояние отсутствия аутентификации.

Port

Выбор порта, для которого необходимо запустить процесс Restart Authentication Process /initialize.

2. Основная конфигурация IEEE802.1X показана ниже.

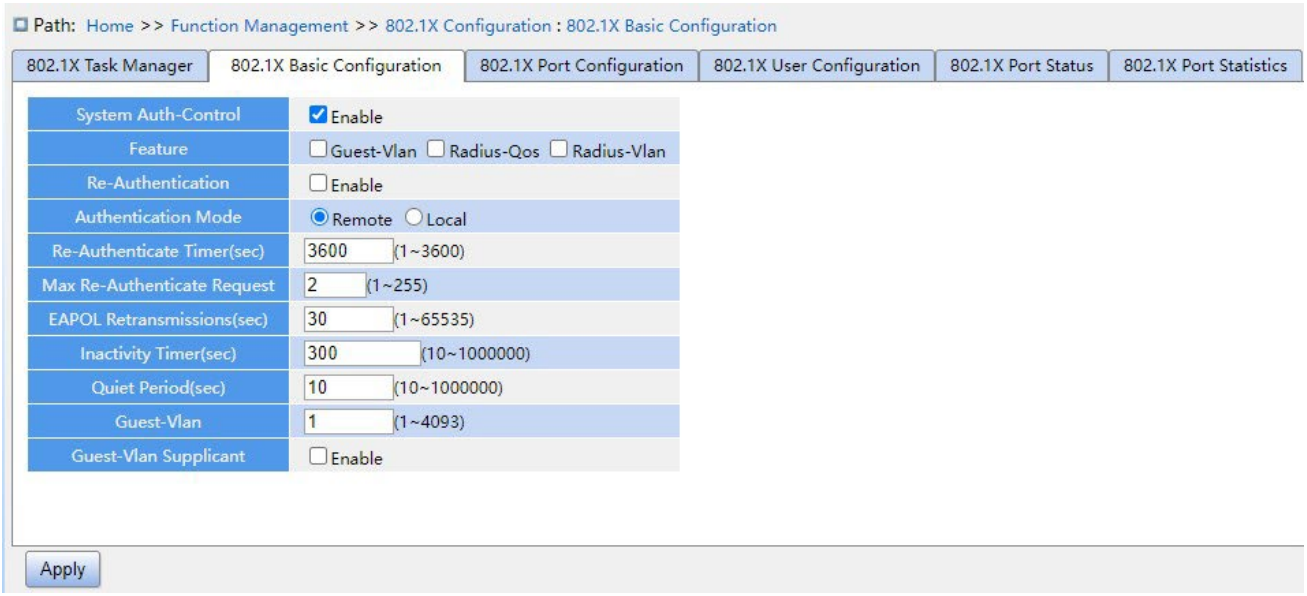


Рисунок 200 Основная конфигурация IEEE802.1X

System Auth-Control

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение/выключение глобальных функций безопасности IEEE802.1x.

Guest-VLAN

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: При значении Enable, если пользователь не прошел аутентификацию или в аутентификации отказано, устройство добавляет порт аутентификации клиента в гостевую VLAN. Все пользователи, имеющие доступ к этому порту, имеют право доступа к ресурсам в гостевой VLAN.

RADIUS-QOS

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Если этот параметр включен, после прохождения клиентом аутентификации сервер передает на устройство информацию об авторизации. Если на сервере установлен флаг **RADIUS QoS**, информация авторизации включает информацию CoS, назначенную для авторизации. Оборудование изменит значение CoS порта аутентификации клиента на основе присвоенного значения.

RADIUS-VLAN

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Если этот параметр включен, после прохождения клиентом аутентификации сервер передает на устройство информацию об авторизации. Если на сервере установлен флаг **RADIUS-VLAN**, информация авторизации включает информацию VLAN, назначенную для авторизации. Оборудование изменит значение VLAN порта аутентификации клиента на основе присвоенного значения.

Re-Authentication

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Требуется ли регулярная повторная аутентификация при успешной проверке аутентификации.

Authentication Mode

Варианты конфигурации: Remote/Local

Конфигурация по умолчанию: Remote

Функция: Настройте режим аутентификации Radius как удаленную или локальную аутентификацию.

Re-Authenticate Timer(sec)

Диапазон настройки: 1~3600 с

Конфигурация по умолчанию: 3600 с

Функция: Установка временного интервала для повторной аутентификации после успешной аутентификации.

Параметр **Re-Authenticate Timer** можно настроить только тогда, когда параметр **Re-Authentication** имеет значение Enable.

Max Re-Authenticate Request

Диапазон настройки: 1~255

Конфигурация по умолчанию: 2

Функция: Задание максимального количества попыток повторной передачи для пакетов запроса Identity EAPOL. Если устройство по-прежнему не получает ответных пакетов от клиента после максимальных попыток повторной передачи, устройство будет считать аутентификацию неудачной.

EAPOL Retransmissions

Диапазон настройки: 1~65535 с

Конфигурация по умолчанию: 30 с

Функция: Настройка времени для получения отклика от клиента. После отправки пакета запроса идентификации EAPOL устройство повторит передачу пакета запроса идентификации EAPOL, если оно по-прежнему не получит ответа от клиента по истечении указанного времени.

Inactivity Timer

Диапазон настройки: 0~1000000 с

Конфигурация по умолчанию: 300

с Функция:

После аутентификации MAC-адреса, если аутентификация прошла успешно и в течение этого времени не проходят пакеты, соответствующая запись безопасности удаляется.

Quiet Period(sec)

Диапазон настройки: 10~1000000 с

Конфигурация по умолчанию: 10 с

Функция: Если аутентификация не удалась, устройство переходит в режим молчания. В период молчания устройство не отвечает на запросы аутентификации от клиента.

Guest-VLAN

Диапазон настройки: 1~4095

Конфигурация по умолчанию: 1

Функция: Настройка VLAN ID гостевой сети.

Guest-VLAN Supplicant

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: При значении Enable, если пользователь не прошел аутентификацию или в аутентификации отказано, устройство добавляет порт аутентификации клиента в гостевую VLAN. При значении Disable устройство добавляет порт в гостевую VLAN только в том случае, если этот порт не имеет записи кадра EAPOL.

Предупреждение:

- Предварительным условием для настройки **Guest-VLAN**, **Max Re-Authenticate Request** и **Guest-Vlan Supplicant** является включение **Guest -VLAN**.
  - Если порт имеет тип аутентификации Trunk или Hybrid, рекомендуется для параметров Radius-Vlan и **Guest -VLAN** задать значение Disable.
  - Значение CoS, назначенное для авторизации, не меняет и не влияет на конфигурацию порта. Однако приоритет значения COS, назначенного для авторизации, выше, чем приоритет значения COS, настроенного пользователем. Иными словами, действительным после аутентификации является значение CoS, назначенное для авторизации. Если пользователь не проходит аутентификацию или выходит из сети, значение CoS, настроенное пользователем, вступает в силу.
  - Назначенная для авторизации VLAN или гостевая VLAN не меняют и не влияют на конфигурацию порта. Однако назначенная для авторизации VLAN или гостевая VLAN имеет более высокий приоритет, чем VLAN, настроенная пользователем.

После того, как пользователь инициирует аутентификацию, и если аутентификация прошла успешно:

Если на порту включен режим **RADIUS-VLAN**, порт добавляется в VLAN, назначенную сервером RADIUS.

Если на порту не включен режим **RADIUS-VLAN**, порт добавляется в VLAN, настроенную пользователем.

Если пользователь не проходит аутентификацию или выходит из сети:

Если на порту включены режимы **Guest-VLAN** и **Guest-Vlan Supplicant**, порт добавляется в VLAN.

Если для порта включен режим **Guest-VLAN**, но не включен режим **Guest-Vlan Supplicant,** порт добавляется в гостевую VLAN, если нет доступной записи кадра EAPOL, и добавляется в VLAN, настроенную пользователем, если запись кадра EAPOL доступна.

Если на порту не включен режим **Guest-VLAN**, порт добавляется в VLAN, настроенную пользователем.

---

3. Настройте порт IEEE802.1X, как показано ниже.

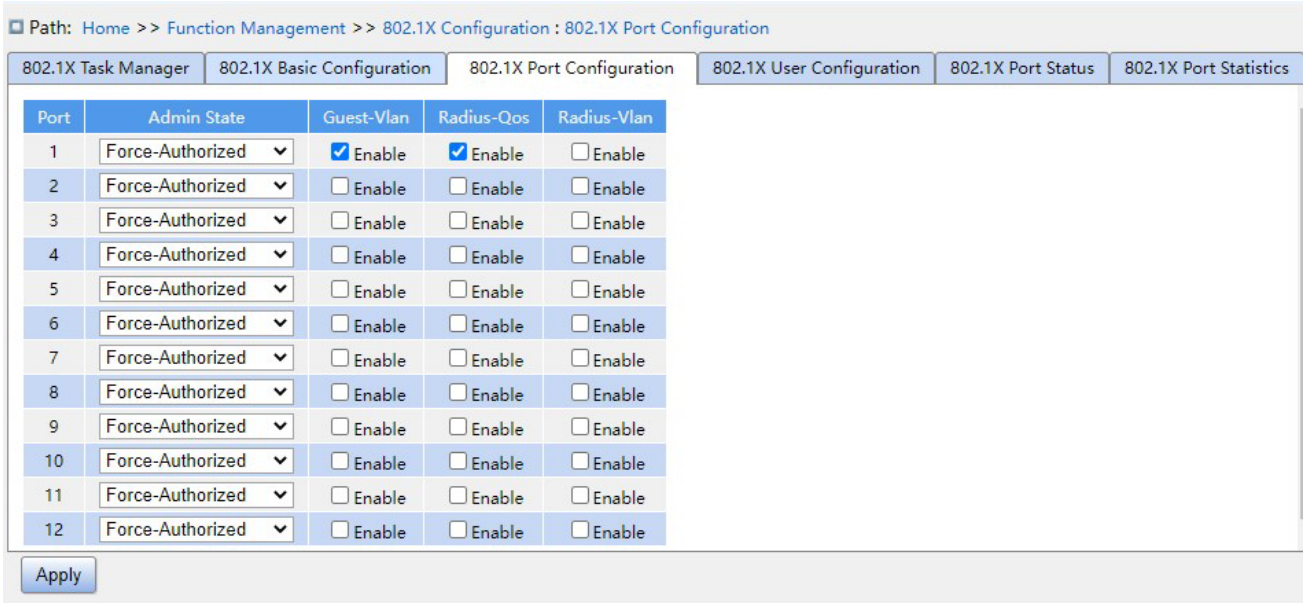


Рисунок 201 Настройка порта IEEE802.1X

Port

Варианты: все порты коммутатора.

Admin State

Варианты конфигурации: Force Authorized/Force Unauthorized/Port-based/MAC-based

Конфигурация по умолчанию: Force Authorized

Функция: Выбор режима аутентификации для порта.

Описание: **Force Authorized** означает, что порт всегда находится в авторизованном состоянии и позволяет пользователям получать доступ к сетевым ресурсам 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 получают доступ к

коммутатору через этот порт. **MAC–Based** указывает, что пользователи, использующие порт, должны пройти соответствующую аутентификацию. Когда пользователь находится в автономном режиме, только этот пользователь не может использовать сеть. **Port-based** указывает, что пользователи проходят аутентификацию на основе порта. После того как первый пользователь, использующий порт, проходит аутентификацию, всем другим пользователям, использующим порт, аутентификация не требуется. Однако, когда первый пользователь находится в автономном режиме, порт отключается, и все остальные пользователи, использующие этот порт, не могут использовать сеть.

RADIUS-QOS

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение или выключение назначенного RADIUS QoS для порта.

RADIUS-VLAN

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение или выключение назначенной RADIUS VLAN для порта.

Примечание:

Эта функция доступна только тогда, когда параметры RADIUS-QOS / RADIUS-VLAN включены и на глобальном уровне, и на уровне порта.

4. Настройки пользователя IEEE802.1X показаны ниже.

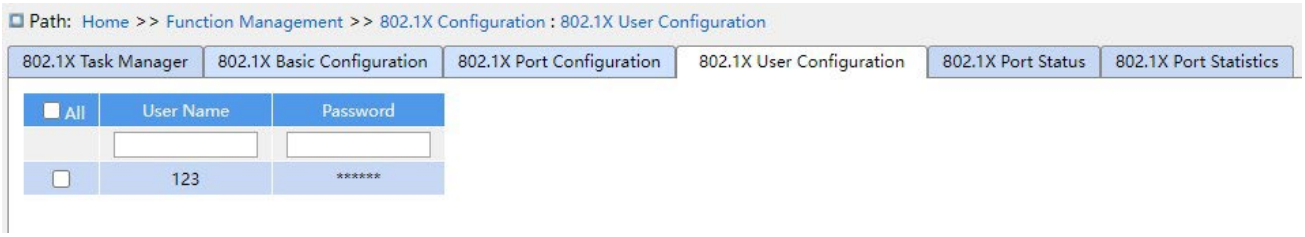


Рисунок 202 Настройки пользователя IEEE802.1x

User Name

Диапазон настройки: 1~16 символов

Конфигурация по умолчанию: None

Функция: Настройка имени пользователя для локальной аутентификации.

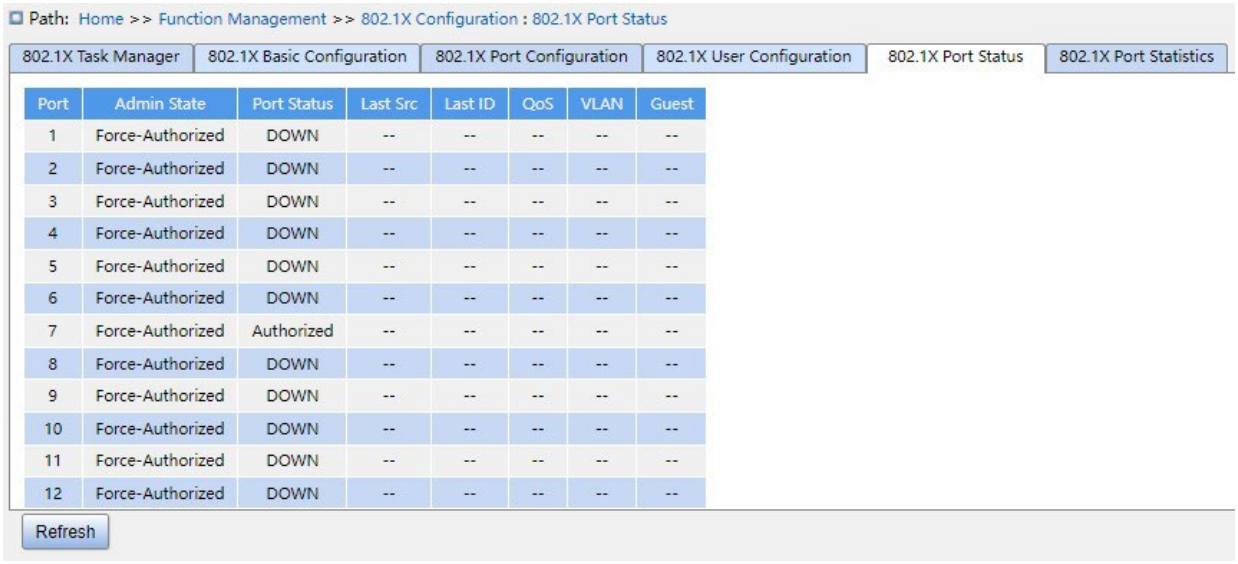
Password

Диапазон настройки: 1~16 символов

Конфигурация по умолчанию: None

Функция: Настройка пароля для локальной аутентификации.

5. Просмотрите статус порта IEEE802.1X, как показано ниже.



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	--	--	--	--	--

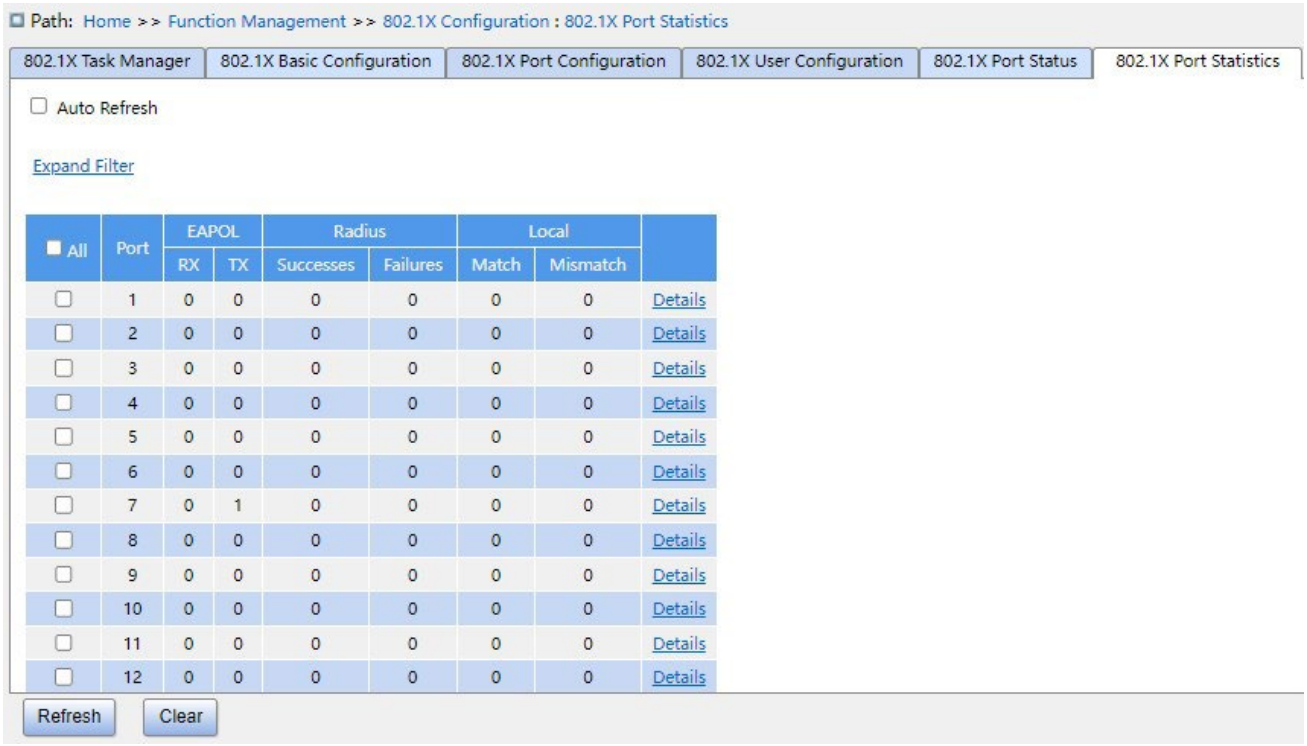
Рисунок 203 Статус порта IEEE802.1X

Port Status

Варианты конфигурации: Globally Disabled (Disable), Authorized (Auth), Unauthorized (UnAuth), Link Down (DOWN), x Auth/y Unauth (x A/y UnA)

Функция: Отображение состояния аутентификации для порта. **Disable** означает, что IEEE802.1X отключен глобально; **Auth** указывает, что пользователь, подключенный к порту, проходит аутентификацию; **UnAuth** указывает, что пользователю, подключенному к порту, не удалось пройти аутентификацию; **DOWN** указывает на то, что порт не работает; **x A/y UnA** указывает, что пользователи x авторизованы, а пользователи y не авторизованы, если режим аутентификации порта — аутентификация на основе MAC-адреса.

6. Просмотрите статистику IEEE802.1X, как показано ниже.



All	Port	EAPOL RX	EAPOL TX	Radius Successes	Radius Failures	Local Match	Local Mismatch	
☐	1	0	0	0	0	0	0	Details
☐	2	0	0	0	0	0	0	Details
☐	3	0	0	0	0	0	0	Details
☐	4	0	0	0	0	0	0	Details
☐	5	0	0	0	0	0	0	Details
☐	6	0	0	0	0	0	0	Details
☐	7	0	1	0	0	0	0	Details
☐	8	0	0	0	0	0	0	Details
☐	9	0	0	0	0	0	0	Details
☐	10	0	0	0	0	0	0	Details
☐	11	0	0	0	0	0	0	Details
☐	12	0	0	0	0	0	0	Details

Рисунок 204 Просмотр статистики IEEE802.1X

Щелкните **Details** порта, чтобы войти в интерфейс статистики IEEE802.1X соответствующего порта, как показано ниже.

<<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

Рисунок 205 Просмотр подробной статистики портов IEEE802.1X

7.12.3 Пример типовой конфигурации

Как показано ниже, клиент подключен к порту 1 коммутатора. Включите IEEE802.1x для порта 1 и выберите режим аутентификации **Port-based**. Имя пользователя и пароль для удаленной аутентификации ddd, остальные настройки по умолчанию.

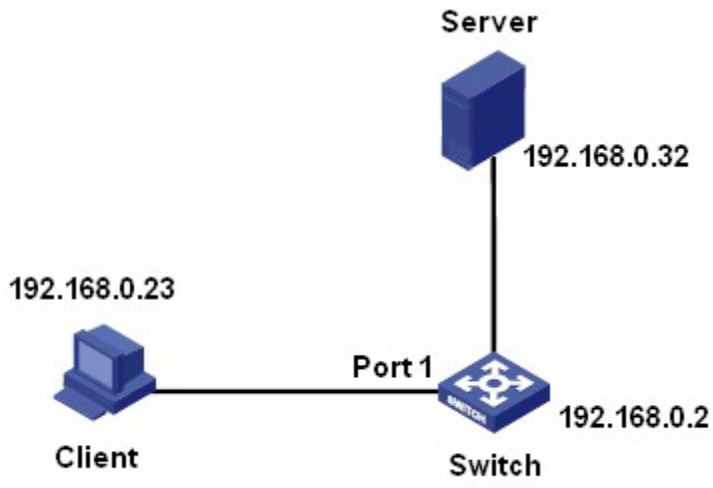


Рисунок 206 Пример настроек IEEE802.1X

Можно ознакомиться с примером типовой конфигурации в разделе 5.6 Настройка RADIUS.

7.13 GMRP

7.13.1 Введение в GARP

Протокол GARP (Generic Attribute Registration Protocol) используется для распространения, регистрации и отмены определенной информации (VLAN, адрес многоадресной рассылки) между коммутаторами в одной сети.

При использовании GARP информация о конфигурации участника GARP будет распространяться по всей сети коммутатора. Устройства, поддерживающие GARP, передают друг другу инструкции о регистрации или отмене тех или иных настроек путём отправки соответствующих сообщений join/leave. Участник также регистрирует или отменяет информацию о конфигурации других участников на основе сообщений join/leave, отправленных другими участниками.

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

- Когда прикладной объект GARP хочет зарегистрировать свою собственную информацию на других коммутаторах, объект отправляет сообщение Join. Сообщения Join делятся на два типа: JoinEmpty и JoinIn. Сообщение JoinIn

отправляется для объявления зарегистрированного атрибута, а сообщение JoinEmpty отправляется для объявления еще не зарегистрированного атрибута.

- Когда прикладной объект GARP хочет удалить свою собственную информацию на других коммутаторах, объект отправляет сообщение Leave. Сообщения Leave делятся на два типа: LeaveEmpty и LeaveIn. Сообщение LeaveIn отправляется для отмены зарегистрированного атрибута, а сообщение LeaveEmpty отправляется для отмены еще не зарегистрированного атрибута.
- После запуска объекта GARP он запускает таймер LeaveAll. Когда период таймера истекает, объект отправляет сообщение LeaveAll.

Примечание:
Объект указывает порт с поддержкой GARP.

Таймеры GARP – это таймер Hold, таймер Join, таймер Leave и таймер LeaveAll.

Hold Timer: При получении регистрационного сообщения объект GARP не сразу отправляет сообщение о присоединении, а запускает таймер Hold. Когда период таймера истекает, объект отправляет все регистрационные сообщения, полученные в течение предшествующего периода, в одном сообщении о присоединении, сокращая отправку пакетов для повышения стабильности сети.

Join Timer: Чтобы гарантировать получение сообщений Join другими прикладными объектами, прикладной объект GARP запускает таймер Join после отправки сообщения Join. Если сообщение JoinIn не получено до истечения периода таймера Join, объект снова отправляет сообщение Join. Если сообщение JoinIn

получено до истечения периода таймера Join, объект не отправляет второе сообщение Join. **Leave Timer**: Когда прикладной объект GARP хочет удалить информацию об атрибуте, объект отправляет сообщение Leave. Объект, получивший сообщение, запускает таймер Leave. Если сообщение Join не получено до истечения периода таймера, объект, получивший сообщение, удаляет информацию об атрибуте.

LeaveAll Timer: После запуска объекта GARP он запускает таймер LeaveAll. Когда период таймера истекает, объект отправляет сообщение LeaveAll, чтобы другие прикладные объекты GARP перерегистрировали все атрибуты. Затем объект снова запускает таймер LeaveAll для нового цикла.

7.13.2 Протокол GMRP

GARP Multicast Registration Protocol (GMRP) – это протокол регистрации многоадресной передачи, основанный на GARP. Он используется для поддержки регистрационной информации многоадресной рассылки коммутаторов. Все коммутаторы с поддержкой GMRP могут получать информацию о регистрации многоадресной рассылки от других коммутаторов, динамически обновлять информацию о регистрации локальной многоадресной рассылки и распространять информацию о регистрации локальной многоадресной рассылки на другие коммутаторы. Этот механизм обмена информацией обеспечивает согласованность многоадресной информации, поддерживаемой всеми коммутаторами с поддержкой GMRP в сети.

Если коммутатор или терминал хочет присоединиться к группе многоадресной рассылки или выйти из нее, порт с поддержкой GMRP передает информацию на все порты в той же VLAN.

7.13.3 Пояснения

Порт агента: указывает порт, на котором включены GMRP и функция агента.

Порт распространения: указывает порт, на котором включен только GMRP, но не функция прокси.

Динамически изученная запись многоадресной рассылки GMRP и запись агента перенаправляются портом распространения на порты распространения устройств более низкого уровня.

Все таймеры GMRP в одной сети должны поддерживать согласованность во избежание взаимных помех. Таймеры должны соответствовать следующим правилам: Таймер Hold < таймер Join, 2*таймер Join < таймер Leave, таймер Leave <таймер LeaveAll.

7.13.4 Настройка через веб-интерфейс

1. Включите глобальный протокол GMRP и настройте глобальный таймер, как показано ниже.

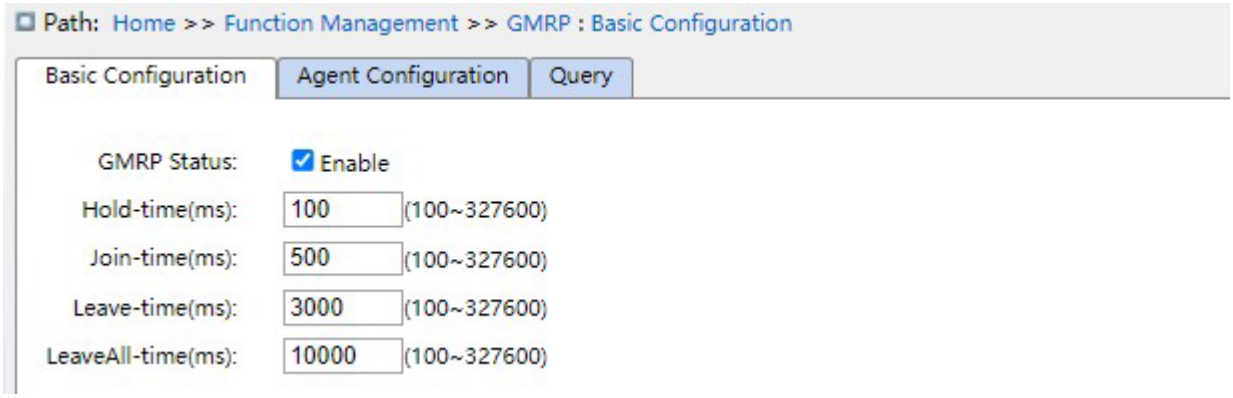


Рисунок 207 Глобальная настройка GMRP

GMRP Status

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение/выключение глобальной функции GMRP. Функцию нельзя использовать вместе с функцией IGMP Snooping.

Hold-timer

Диапазон настройки: 100 мс~327600 мс

Конфигурация по умолчанию: 100 мс

Описание: Значение должно быть кратно 100. Лучше установить одинаковое время таймеров Hold на всех портах с поддержкой GMRP.

Join-timer

Диапазон настройки: 100 мс~327600 мс

Конфигурация по умолчанию: 500 мс

Значение должно быть кратно 100. Лучше установить одинаковое время таймеров Join на всех портах с поддержкой GMRP.

Leave-timer

Диапазон настройки: 100 мс~327600 мс

Конфигурация по умолчанию: 3000 мс

Значение должно быть кратно 100. Лучше установить одинаковое время таймеров Leave на всех портах с поддержкой GMRP.

LeaveAll-timer

Диапазон настройки: 100 мс~327600 мс

Конфигурация по умолчанию: 10000 мс

Функция: Настройка интервала времени для отправки пакетов LeaveAll. Значение должно быть кратно 100.

Пояснение: Если таймеры LeaveAll на разных устройствах истекают одновременно, устройства отправят сообщение LeaveAll одновременно, что увеличит количество сообщений. Чтобы избежать одновременного истечения срока действия таймеров LeaveAll на разных устройствах фактическое время работы таймера LeaveAll является случайным значением и больше, чем значение таймера LeaveAll, и меньше чем 1,5 значения таймера LeaveAll.

2. Настройте функцию GMPR для порта, как показано ниже.

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	☐	☐	--

Рисунок 208 Настройка функции GMPR на порту

GMRP Enable

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение/выключение функции GMRP на порту.

GMRP Agent Enable

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение/выключение функции агента GMRP на порту.

Last PDU Origin

Функция: Исходный MAC-адрес пакета протокола, полученного портом последним.

Предупреждение:

➢Порт агента не может распространять запись агента.

➢Предпосылкой включения функции агента GMRP на порте является включение функции GMRP на порту.

3. Добавьте запись агента GMRP, как показано ниже.

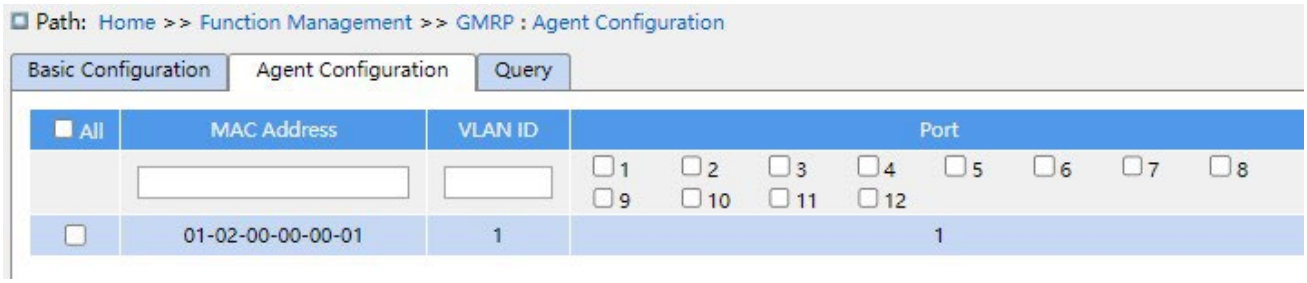


Рисунок 209 Настройка записи агента GMRP

MAC address

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

Функция: Настройка MAC-адреса многоадресной группы. Младший бит в первом байте равен 1.

VLAN ID

Варианты: все созданные номера VLAN

Функция: Настройка VLAN ID для записи агента GMRP.

Описание: Запись агента GMRP может быть перенаправлена только из порта распространения с идентификатором VLAN, совпадающим с идентификатором VLAN этой записи.

Port

Варианты: все настроенные порты агента 4.

Просмотрите настройки GMRP, как показано ниже.

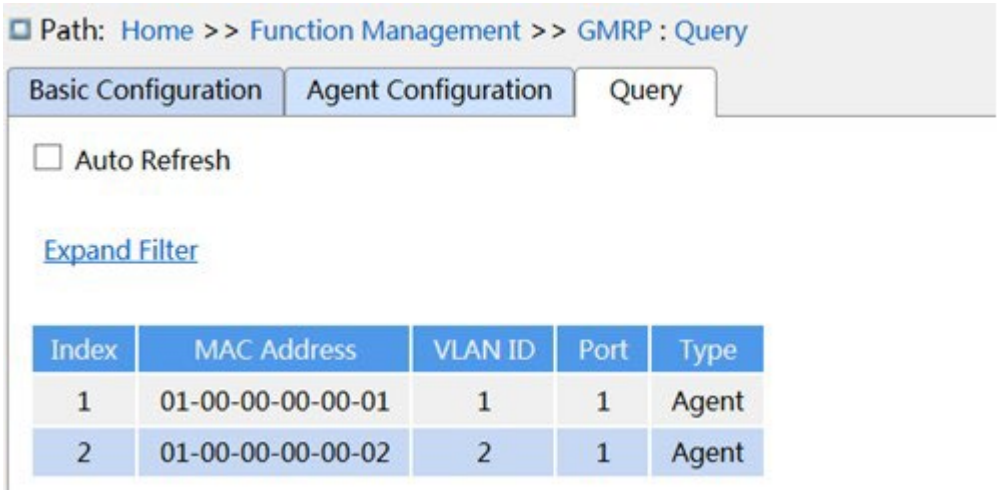


Рисунок 210 Информация о конфигурации GMRP

7.13.5 Пример типовой конфигурации

Как показано ниже, коммутатор A и коммутатор B соединены через порты 2. Порт 1 коммутатора A настроен как порт-агент и содержит 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 на портах наблюдайте за динамической регистрацией между коммутаторами и обновлением информации о многоадресной рассылке.

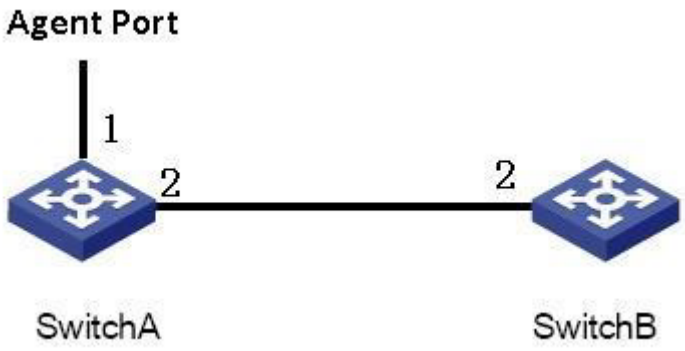


Рисунок 211 Сеть GMRP

Конфигурация коммутатора A:

1. Включите глобальную функцию GMRP на коммутаторе A; установите для таймера значение по умолчанию, как показано на рисунке

207.

2. Включите функцию GMRP и функцию агента на порту 1; включите только функцию GMRP на порту 2, как показано на рисунке 208.
3. Настройте запись агента многоадресной рассылки. Установите <MACaddress, VLAN ID, Member port> <01-00-00-00-00-01, 1, 1> и <01-00-00-00-00-02, 2, 1>, как показано на рисунке 209.

Конфигурация коммутатора B:

4. Включите глобальную функцию GMRP на коммутаторе B; установите для таймера значение по умолчанию, как показано на рисунке

207.

5. Включите функцию GMRP на порту 2; установите таймеры на значения по умолчанию, как показано на рисунке 208.

В таблице 10 перечислены динамически полученные записи многоадресной рассылки GMRP на коммутаторе B.

Таблица 10 Динамические записи многоадресной рассылки

Атрибуты порта 2 коммутатора A	**Атрибуты порта 2 коммутатора B**	**Записи многоадресной рассылки, полученные на коммутаторе B**
Access VID=1	Access VID=1	MAC: 01-00-00-00-00-01 VLAN ID: 1 Порт-участник 2
Access VID=2	Access VID=2	MAC: 01-00-00-00-00-02 VLAN ID: 2 Порт-участник 2
Access VID=1	Access VID=2	MAC: 01-00-00-00-00-01 VLAN ID: 2 Порт-участник 2

7.14 Настройка маршрутизации

7.14.1 Таблица маршрутизации

7.14.1.1 Введение

Статические маршруты настраиваются вручную. Если топология сети проста, 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, предотвращая незаконные изменения маршрутов. Недостатком использования статических маршрутов является то, что они не могут адаптироваться к изменениям топологии сети. Если в сети произойдет сбой или произойдет изменение топологии, соответствующие маршруты станут недоступны, и сеть разорвется. В этом случае сетевой администратор должен изменить статические маршруты вручную.

7.14.1.2 Настройка через веб-интерфейс

1. Настройка статической маршрутизации показана ниже.

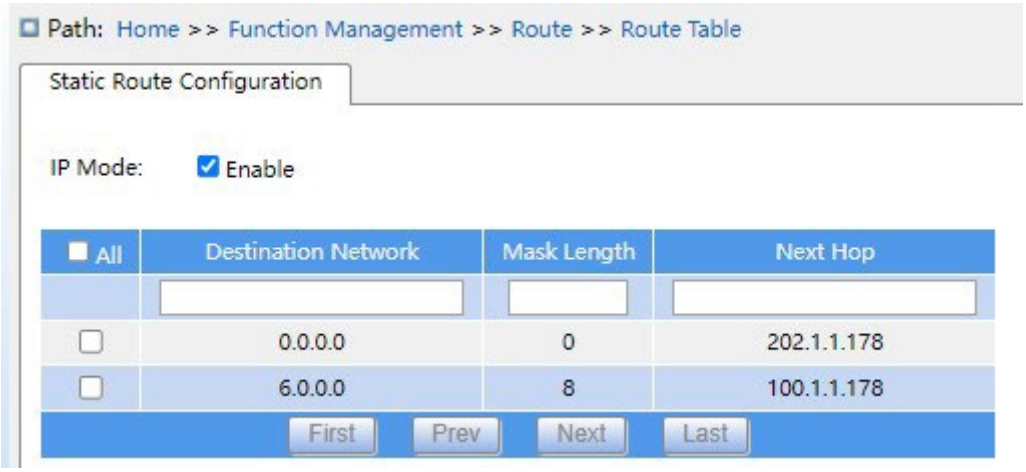


Рисунок 212 Настройка статической маршрутизации

IP Mode

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Для устройств Layer 3 значение по умолчанию Enable. Для устройств Layer 2 значение по умолчанию Disable.

Функция: Включение или выключение IP-режима.

Destination Network

Формат: A.B.C.D

Функция: Настройка целевого сетевого адреса в таблице статических маршрутов.

Mask Length

Функция: Маска подсети – это 32-разрядное число, состоящее из последовательности 1 и последовательности 0. «1» соответствует полям номера сети и полям номера подсети, а «0» соответствует полям номера хоста. Длина маски — это количество 1 в маске подсети.

Next Hop

Формат: A.B.C.D

Функция: Настройка IP-адреса следующего шага.

7.14.1.3 Пример типовой конфигурации

Как показано ниже, маски подсети всех коммутаторов уровня Layer-3 и ПК в сети имеют вид 255.255.255.0. Требуется настроить статические маршруты, чтобы любые хосты могли общаться друг с другом.

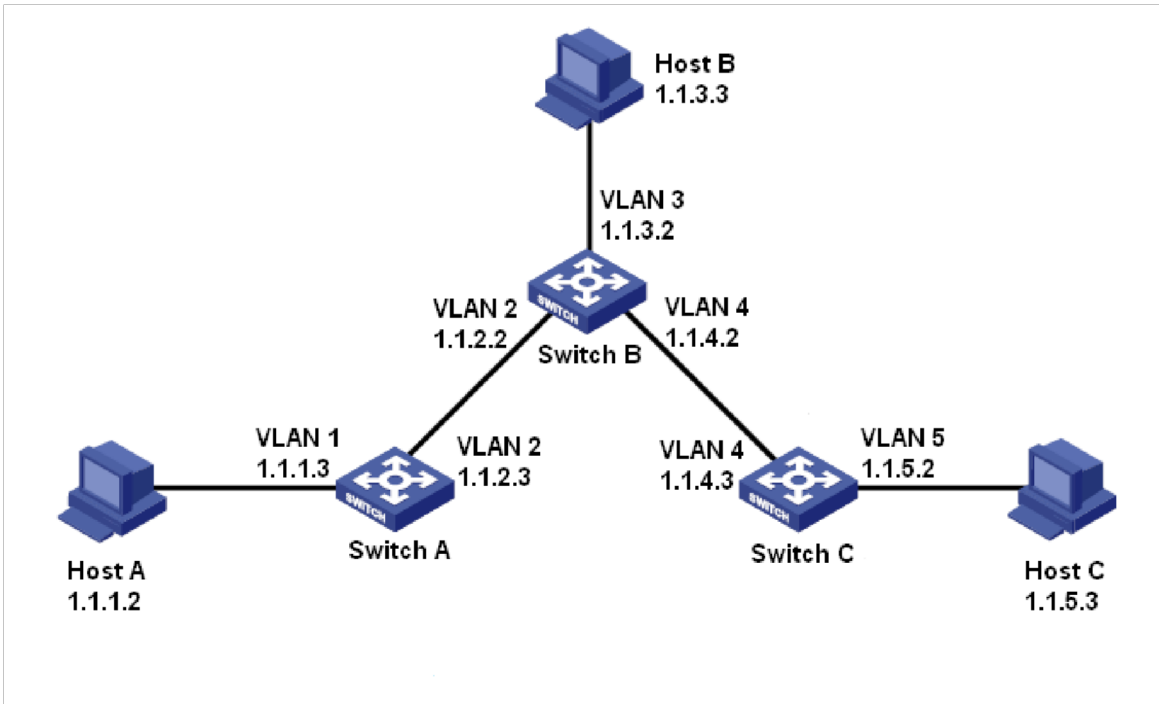


Рисунок 213 Пример настройки статических маршрутов

Конфигурация коммутатора A:

1. Задайте IP-адреса для интерфейсов VLAN.
2. Настройте статический маршрут со следующими параметрами:

IP-адрес назначения: 1.1.3.0; маска подсети назначения: 255.255.255.0; шлюз по умолчанию: 1.1.2.2; приоритет: 1, как показано на рисунке 212.

IP-адрес назначения: 1.1.5.0; маска подсети назначения: 255.255.255.0; шлюз по умолчанию:

1.1.2.2; приоритет: 1, как показано на рисунке 212.

Конфигурация коммутатора B:

3. Задайте IP-адреса для интерфейсов VLAN.
4. Настройте статический маршрут со следующими параметрами:

IP-адрес назначения: 1.1.1.0; маска подсети назначения: 255.255.255.0; шлюз по умолчанию: 1.1.2.3; приоритет: 1, как показано на рисунке 212.

IP-адрес назначения: 1.1.5.0; маска подсети назначения: 255.255.255.0; шлюз по умолчанию:

1.1.4.3; приоритет: 1, как показано на рисунке 212.

Конфигурация коммутатора C:

5. Задайте IP-адреса для интерфейсов VLAN.
6. Настройте статический маршрут со следующими параметрами:

IP-адрес назначения: 0.0.0.0; маска подсети назначения: 0.0.0.0; шлюз по умолчанию:

1.1.4.2; приоритет: 1, как показано на рисунке 212.

7. Настройте шлюзы по умолчанию для хоста A, хоста B и хоста C как 1.1.1.3, 1.1.3.2 и 1.1.5.2 соответственно.

7.15 Настройка QoS

7.15.1 Введение

Функция Quality of Service (QoS) позволяет предоставлять дифференцированные сервисы на основе различных требований при ограниченной пропускной способности

посредством управления трафиком и распределения ресурсов в IP-сетях. QoS пытается удовлетворить передачу различных сервисов, чтобы уменьшить перегрузку сети и свести к минимуму влияние перегрузки на сервисы с высоким приоритетом.

Классификация трафика, контроль трафика, формирование трафика, управление перегрузками и предотвращение перегрузок являются основными концепциями развертывания QoS. В основном выполняются следующие функции:

Классификация трафика: идентифицирует объект на основе определенных правил сопоставления Это основа и предпосылка QoS.

Контроль трафика: контролирует скорость трафика пакетов, которые передаются на устройство. Когда скорость трафика превышает указанную скорость трафика, устройство принимает меры ограничения или штрафа для защиты сетевых ресурсов от повреждения. Контроль трафика подразделяется на контроль трафика на основе портов и контроль трафика на основе очередей.

Формирование трафика: проактивно регулирует скорость вывода трафика. Оно направлено на адаптацию трафика к доступным сетевым ресурсам нисходящего устройства, чтобы предотвратить ненужное отбрасывание пакетов и перегрузку. Формирование трафика подразделяется на формирование трафика на основе портов и формирование трафика на основе очередей.

Управление перегрузками: Это обязательно для решения проблемы конкуренции за ресурсы. Управление перегрузками кэширует пакеты в очередях и определяет последовательность пересылки пакетов на основе определенного алгоритма планирования, обеспечивая приоритетную пересылку для ключевых служб.

Предотвращение перегрузки: Чрезмерная перегрузка может привести к повреждению сетевых ресурсов.

Функция предотвращения перегрузки отслеживает использование сетевых ресурсов. При обнаружении увеличения перегрузки функция использует упреждающее отбрасывание пакетов и настраивает объем трафика для устранения перегрузки.

Контроль трафика, формирование трафика, управление перегрузками и предотвращение перегрузок контролируют сетевой трафик и выделенные ресурсы с разных сторон. Они являются конкретным воплощением QoS. Например, коммутатор

контролирует пакеты, которые передаются в сеть, на основе установленной скорости. Он формирует пакеты до того, как пакеты покинут коммутатор. Он управляет планированием очереди в случае перегрузки и принимает меры по предотвращению перегрузки, когда перегрузка усиливается.

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 портом. Коммутаторы этой серии поддерживают классификацию трафика в следующих режимах сопоставления очередей: порт, информация заголовка 802.1Q, кодовая точка дифференцированного обслуживания (DSCP) и контрольный список QoS (QCL) с приоритетом в порядке возрастания.

При пересылке данных порт использует режим планирования для планирования данных в 8 очередях и пропускной способности каждой очереди. Коммутаторы этой серии поддерживают два режима планирования: 6 Queues Weighted и SP (Strict Priority). WRR (Weighted Round Robin) планирует потоки данных на основе соотношения весов. Очереди получают свою пропускную способность на основе соотношения весов. WRR отдает приоритет очередям с высоким весом. Больше пропускной способности выделяется очередям с более высоким весовым коэффициентом.

В режиме SP преимущественно пересылаются высокоприоритетные пакеты. Он в основном используется для передачи чувствительных сигналов. Если кадр поступает 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 из очереди с более низким приоритетом.

6 Queues Weighted указывает, что очередь 6 и очередь 7 используют режим планирования Strict Priority, а очередь 0 ~ очередь 5 используют режим планирования WRR. Данные в очереди 7 обрабатываются раньше данных в очереди 6. Когда и

очередь 7, и очередь 6 пусты, данные в очереди 0 ~ очереди 5 планируются на основе весовых коэффициентов.

7.15.3 Настройка через веб-интерфейс

1. Настройте режим перемаркировки 802.1p Mapped, как показано ниже.

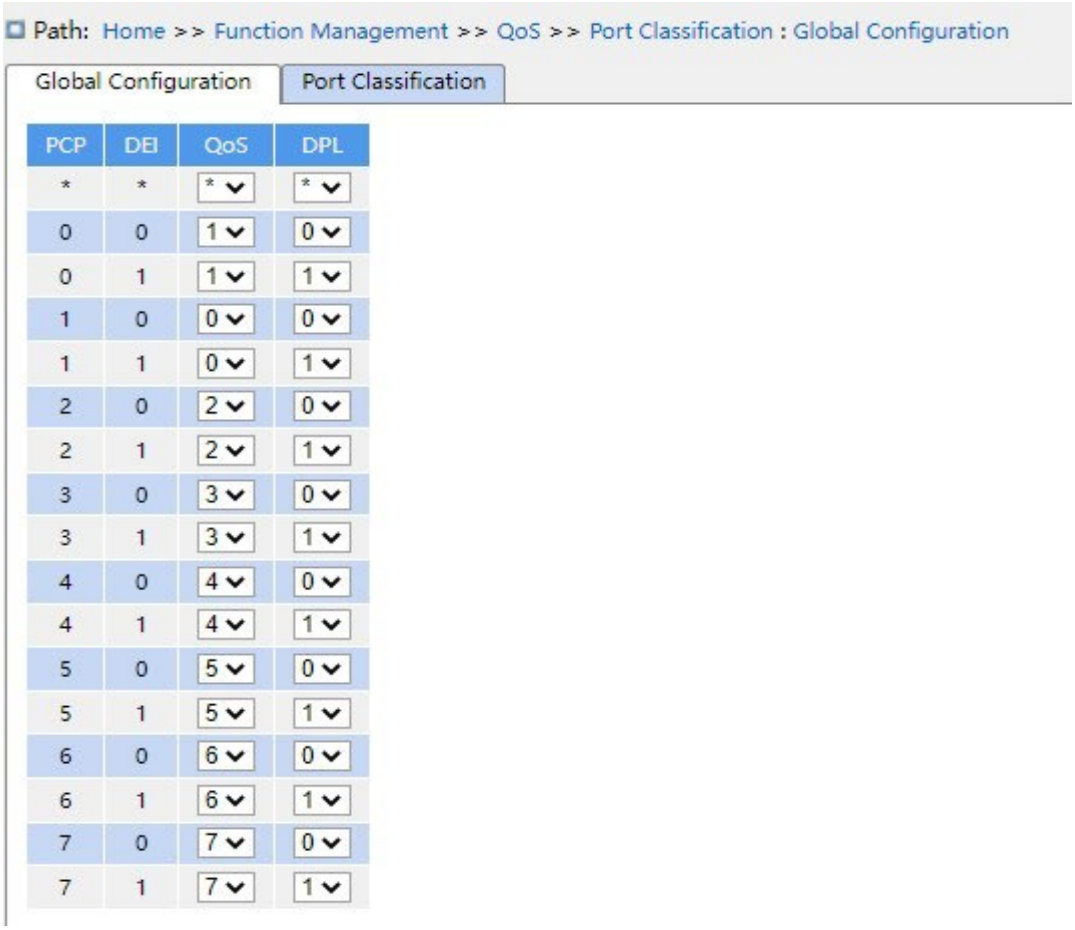


Рисунок 214 Настройка режим перемаркировки Mapped

Предупреждение:

Режим отображения очереди на основе информации заголовка 802.1Q подходит только для полученных сообщений с тегом.

(PCP, DEI) to (QoS class, DP level) mapping

Диапазон настройки: 0~7 (тип QoS) 0~1 (уровень DP)

Конфигурация по умолчанию: Значения PCP 0, 1, 2, 3, 4, 5, 6, 7 сопоставляются классу QoS 1, 0, 2, 3, 4, 5, 6, 7； значения DEI 0, 1 сопоставляются уровню DP 0, 1.

Функция: Задать сопоставление (PCP, DEI) с (CoS, DPL) на основе значений PCP и DEI в пакетах.

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 DPL. Если тип сообщения — тегированное и включает класс тега, значения CoS и DPL сообщения являются значением сопоставления из (PCP, DEI) в (CoS, DPL).

2. Включите режим иерархии портов, как показано ниже.

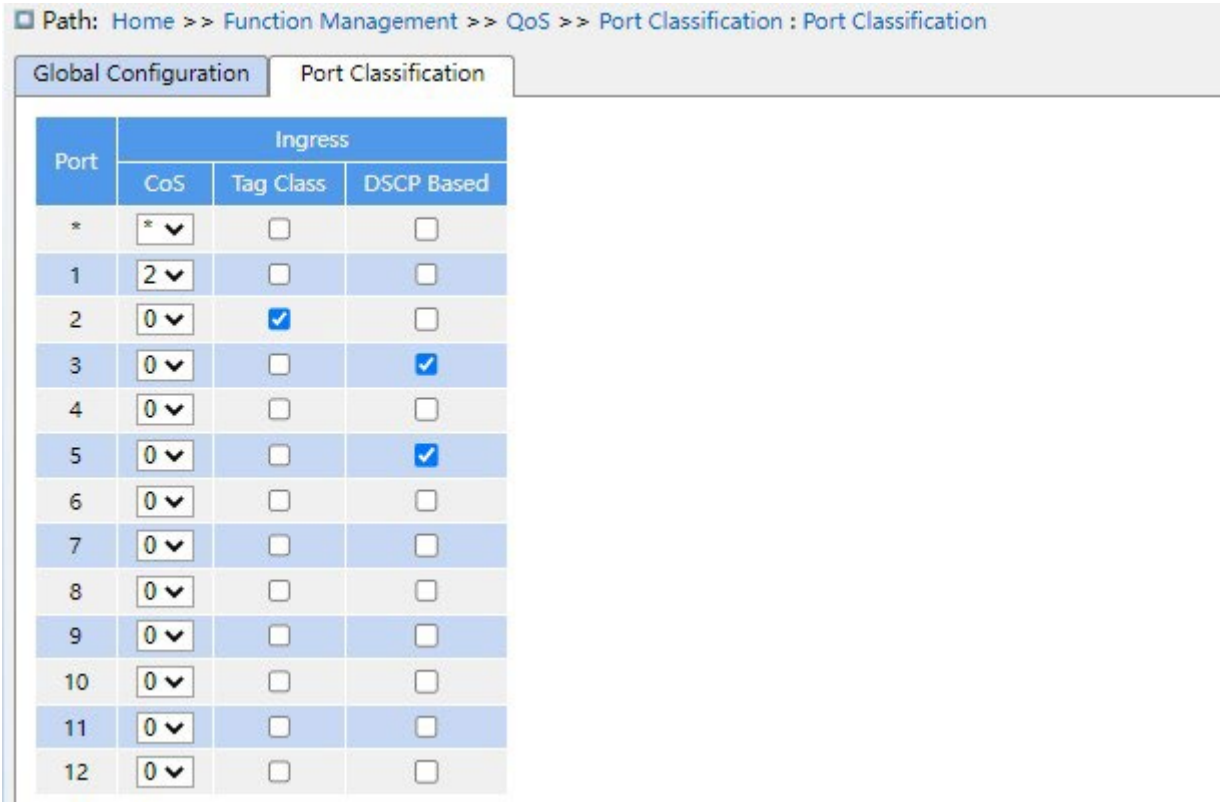


Рисунок 215 Настройка режима иерархии портов

DSCP Based

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: Включение или отключение режима сопоставления очередей на основе DSCP. Этот режим сопоставления очередей имеет более высокий приоритет по сравнению с режимом сопоставления очередей на основе информации заголовка 802.1Q.

CoS

Диапазон настройки: 0~7

Конфигурация по умолчанию: 0

Функция: Настройка значения CoS по умолчанию для порта.

Tag Class

Варианты конфигурации: enable/disable

Конфигурация по умолчанию: disable

Функция: Включение или отключение режима сопоставления очередей на основе информации заголовка 802.1Q.

3. Экран глобальной настройки перемаркировки 802.1p показан на рисунке 216; на этом экране показан режим повторной маркировки 802.1p, когда порт пересылает сообщения. Перемаркировка 802.1p означает, что порт обновляет значения PCP и DEI в сообщении при его пересылке.

Рисунок 216 Настройка режима перемаркировки 802.1p для глобальных портов

Предупреждение:

Функция повторной маркировки 802.1p недействительна, если исходящий порт пересылает сообщения, не содержащие теги.

- Установите режим перемаркировки 802.1p Classified, как показано на рисунке 216.

Tag Remarking Mode

Варианты конфигурации: Classified /Default

Конфигурация по умолчанию: Classified

Режим Classified: Значение PCP и значение DEI в пакетах не обновляются, когда выходной порт пересылает сообщение.

- Настройте режим перемаркировки 802.1p Default, как показано ниже.

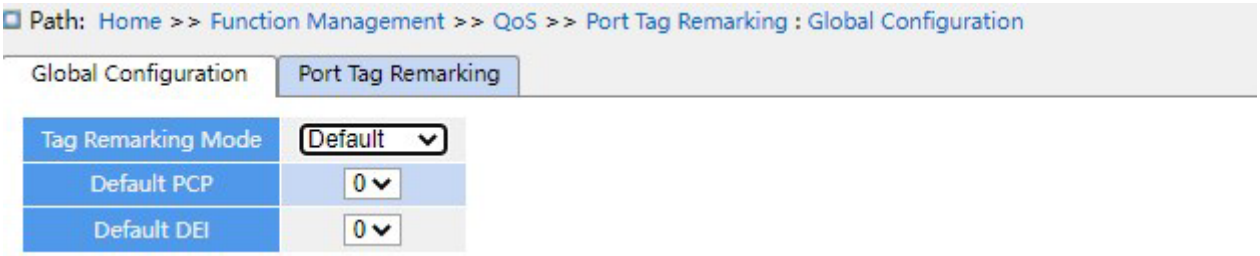


Рисунок 217 Настройка режима перемаркировки Default

Tag Remarking Mode

Варианты конфигурации: Classified /Default

Конфигурация по умолчанию: Classified

Функция: Настройка режима перемаркировки 802.1p По умолчанию: Когда выходной порт пересылает сообщение, значения PCP и DEI в обновленном сообщении являются значениями по умолчанию для выходного порта. (конфигурация, как показано ниже).

Default PCP

Диапазон настройки: 0~7

Конфигурация по умолчанию: 0

Функция: Настройка значения PCP по умолчанию для порта.

Default DEI

Диапазон настройки: 0~1

Конфигурация по умолчанию: 0

Функция: Настройка значения DEI по умолчанию для порта.

4 Настройте перемаркировку 802.1p, как показано ниже.

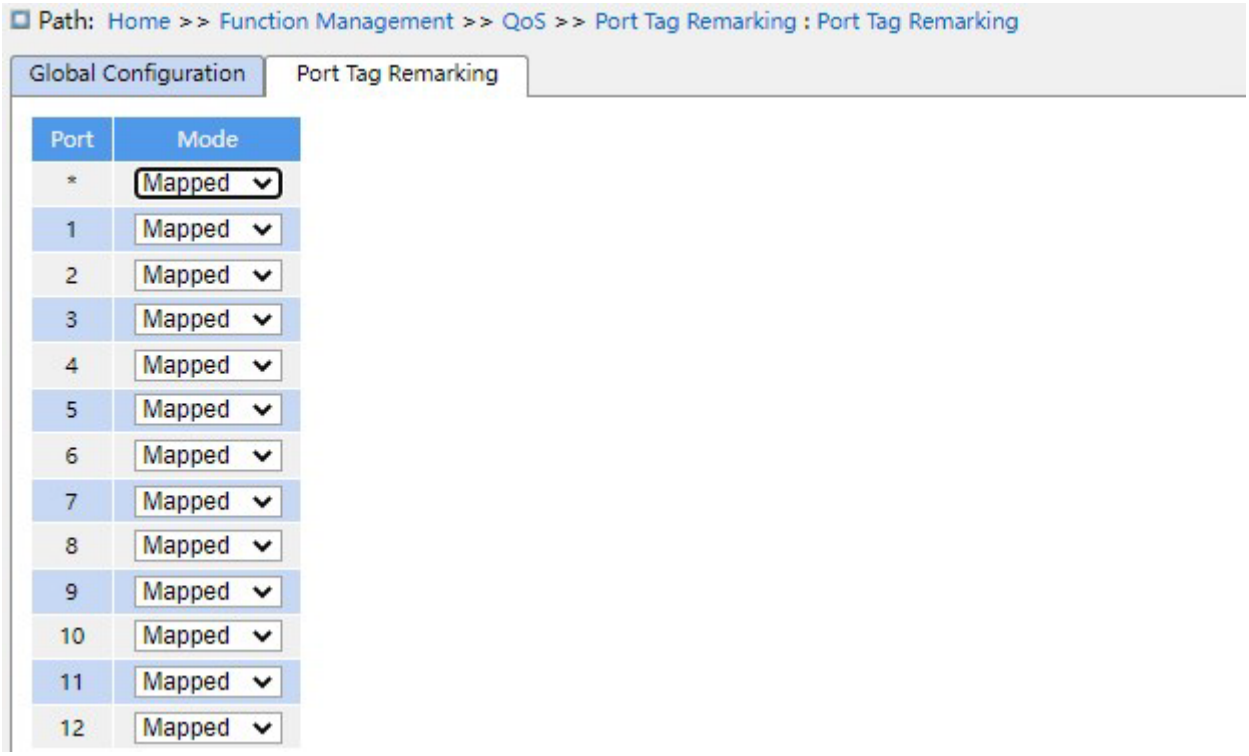


Рисунок 218 Настройка режима перемаркировки 802.1p для указанного порта

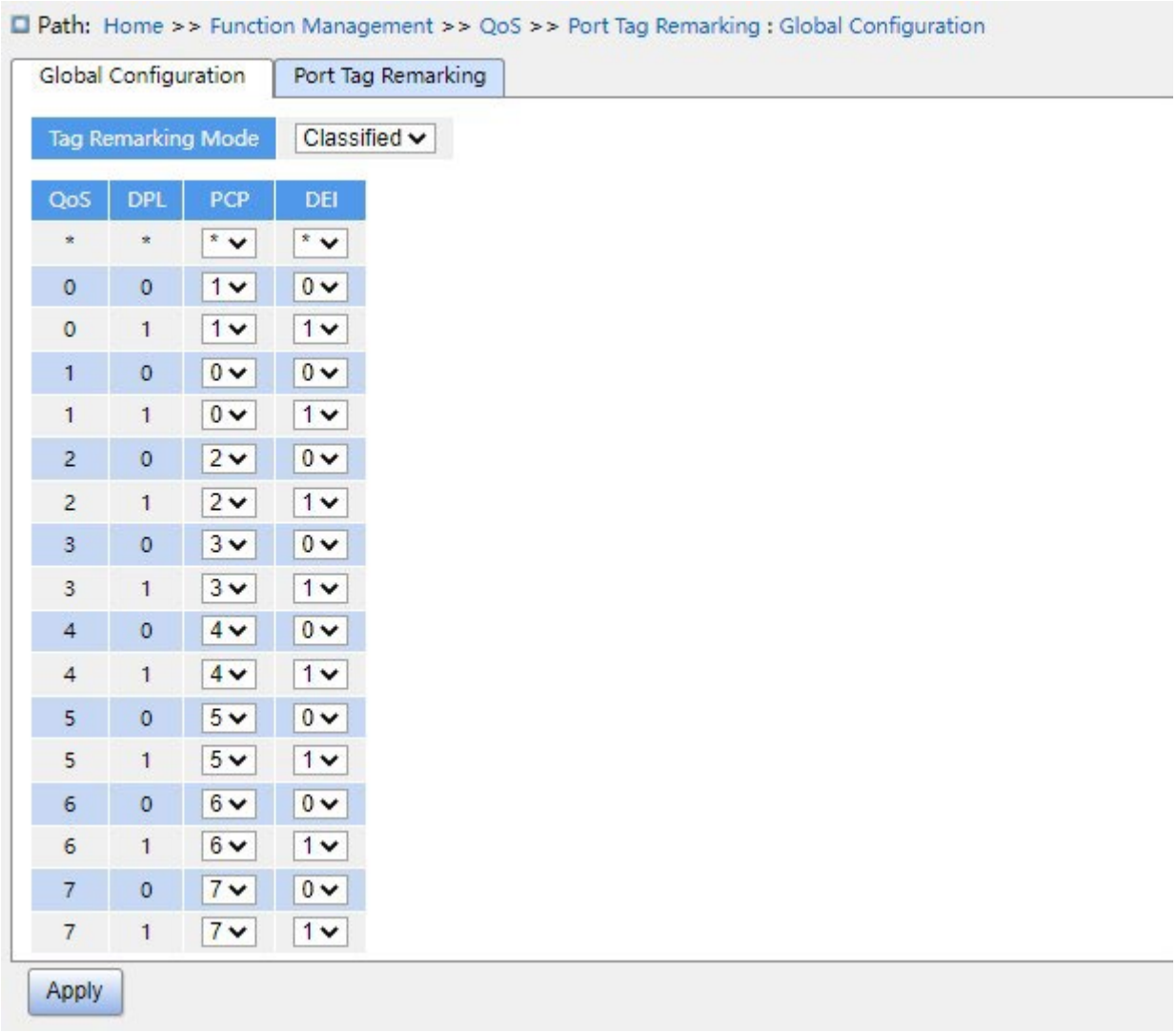


Рисунок 219 Настройка режим перемаркировки Mapped

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 являются значениями сопоставления (CoS, DPL) с (PCP, DEI). (Конфигурация сопоставления приведена ниже).

(QoS class, DP level) to (PCP, DEI) mapping

Варианты конфигурации: 0~7 (PCP) 0~1 (DEI)

Конфигурация по умолчанию: Класс QoS 0, 1, 2, 3, 4, 5, 6, 7 сопоставляется значению PCP 1, 0, 2, 3, 4, 5, 6, 7; уровень DP 0, 1 сопоставляется значению DEI 0, 1.

Функция: в соответствии со значением CoS и DPL в сообщении настройка сопоставления (CoS, DPL) с (PCP, DEI).

5. Включите преобразование входного порта, перезапись выходного порта, как показано ниже.

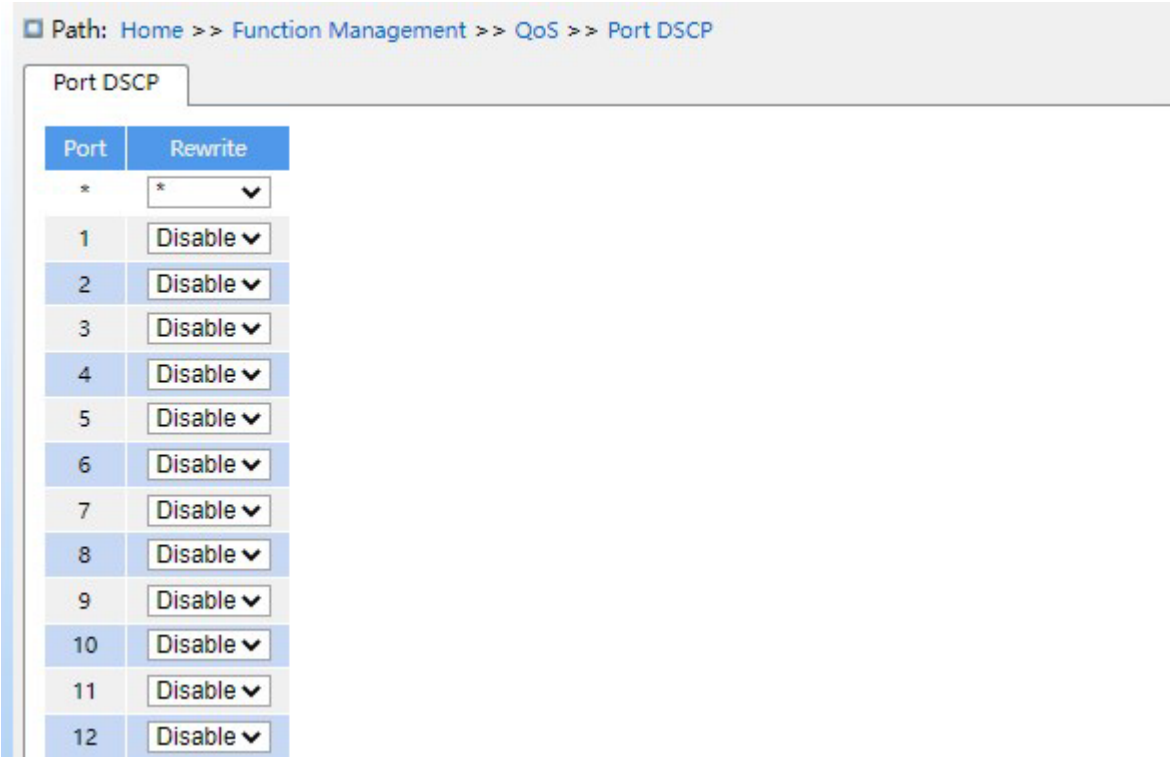


Рисунок 220 Настройка DSCP порта

Rewrite

Варианты конфигурации: Disable/enable/remap

Конфигурация по умолчанию: Disable

Функция: Установка режима перезаписи значения DSCP в пакетах, когда выходной порт пересылает пакеты.

Disable: Значение DSCP в пакетах не перезаписывается, когда выходной порт пересылает пакеты.

Enable: Когда выходной порт пересылает сообщение, следует ли перезаписать значение DSCP в сообщении в соответствии с настройкой классификации.

Remap: Когда выходной порт пересылает сообщение, DSCP в сообщении перезаписывается в соответствии с сопоставлением (DSCP, DPL) в DSCP.

6. Настройте режим сопоставления очередей на основе DSCP, как показано ниже.

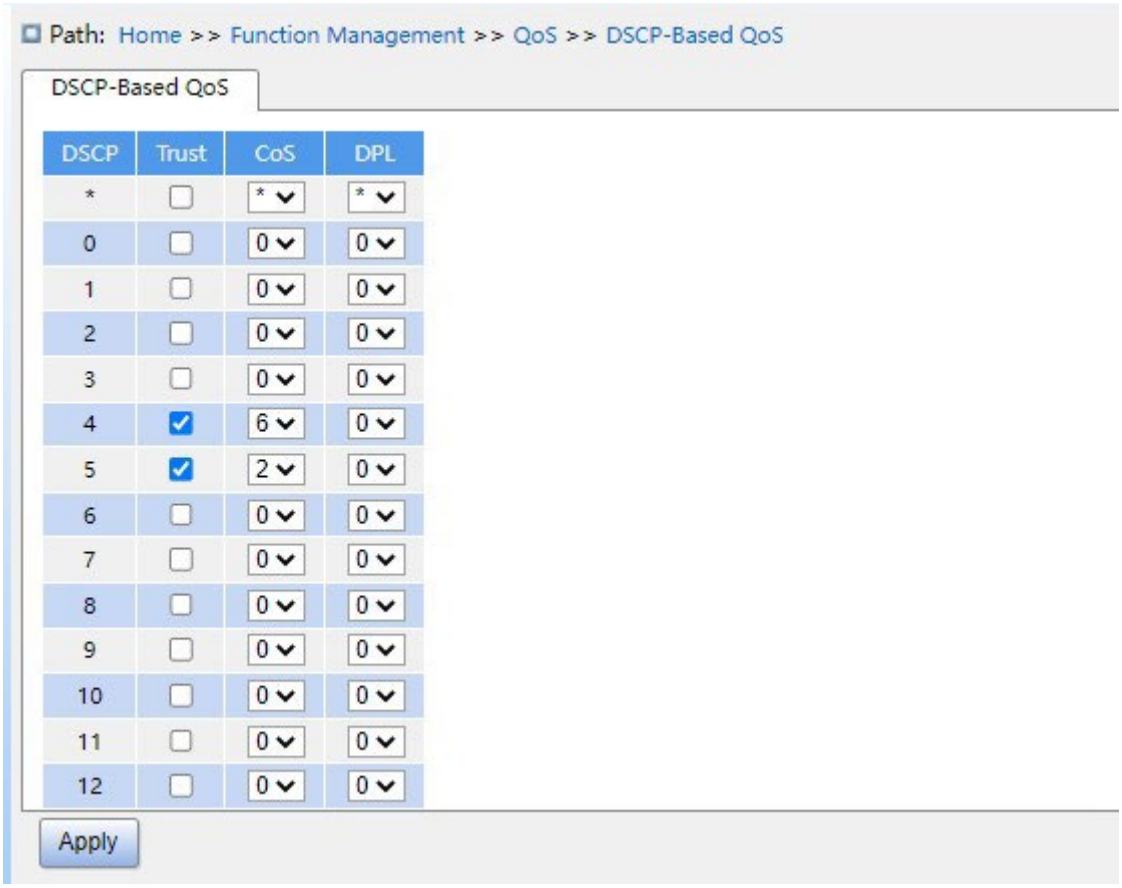


Рисунок 221 Настройка режима сопоставления очередей на основе DSCP.

Trust

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение и выключение доверенного режима значения DSCP.

Предупреждение:

Режим сопоставления очередей на основе DSCP применяется только к значению DSCP сообщения, полученного портом в качестве доверенного значения.

COS

Диапазон настройки: 0~7

Конфигурация по умолчанию: 0

Функция: Настройка сопоставления DSCP – CoS.

Описание: Значение CoS определяет сохраненную очередь сообщений, значение CoS 0–7, в свою очередь, соответствует очереди 0–7. Когда сообщение поступает на

коммутатор, коммутатор присваивает сообщению значения CoS в соответствии с сопоставлением DSCP – CoS.

Предупреждение:

Когда входной порт включает преобразование, коммутатор назначает значение CoS в соответствии с преобразованным значением DSCP; в противном случае коммутатор назначает значение CoS в соответствии с исходным значением DSCP в сообщении.

DPL

Диапазон настройки: 0~1

Конфигурация по умолчанию: 0

Функция: Настройка сопоставления DSCP – DPL.

Описание: После того, как сообщение со значением DSCP в качестве доверенного значения поступает в коммутатор, коммутатор присваивает сообщению значение DPL в соответствии с сопоставлением DSCP и DPL.

7. Настройте преобразование и перезапись DSCP, как показано ниже.

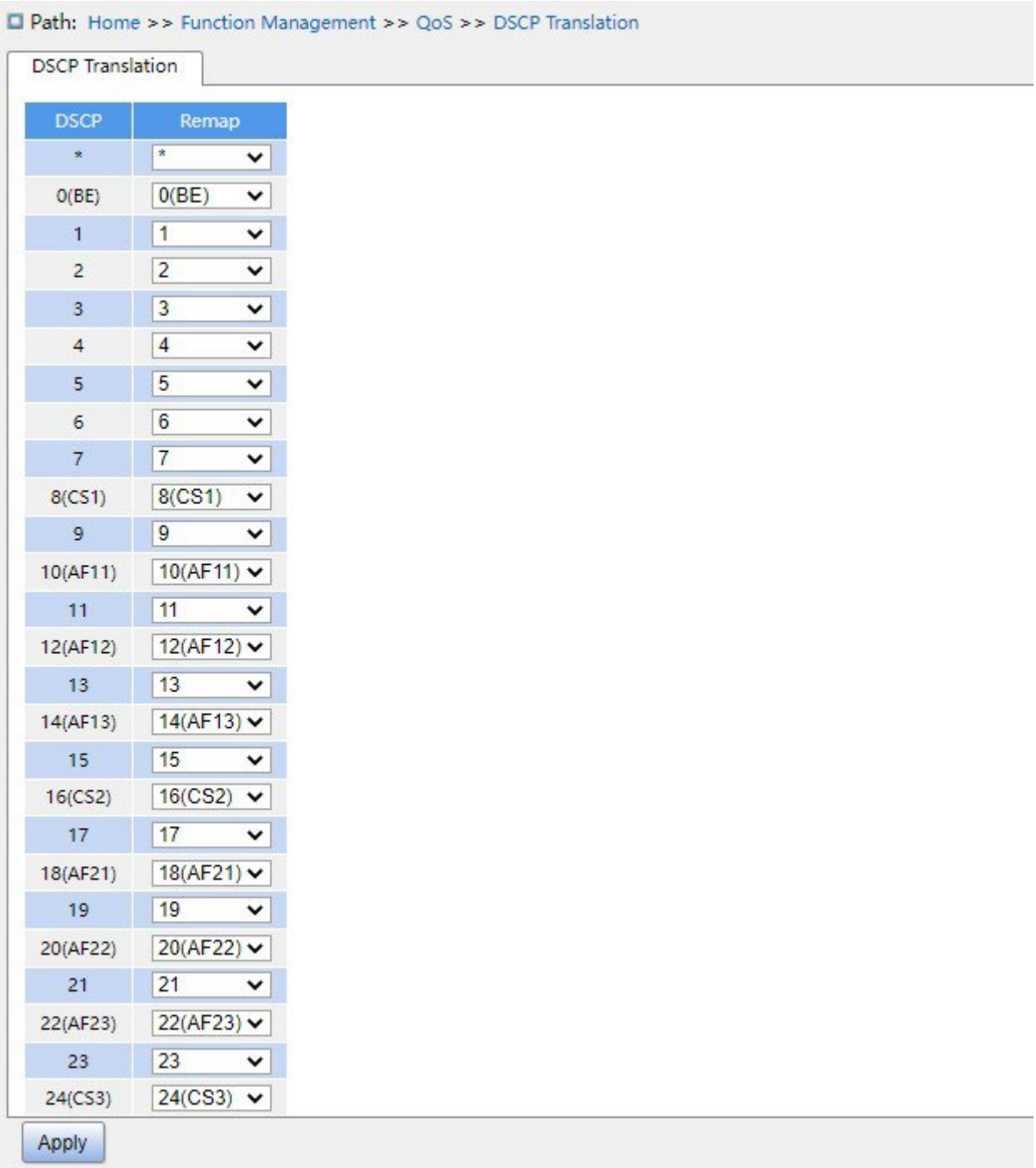


Рисунок 222 Настройка преобразования и перезаписи DSCP

Translate

Диапазон настройки: 0~63

Функция: Задание таблицы преобразования значений DSCP.

Предупреждение:
Когда входной порт включает преобразование, выбранное значение является преобразованным значением; в противном случае выбранной значение DHCP совпадает с исходным значением DSCP в сообщении.

Remap DP0

Диапазон настройки: 0~63

Функция: Настройка сопоставления (DSCP, DPL) – DSCP.

8. Настройте режим планировщика очереди портов, как показано на рисунке 223 и рисунке 224.

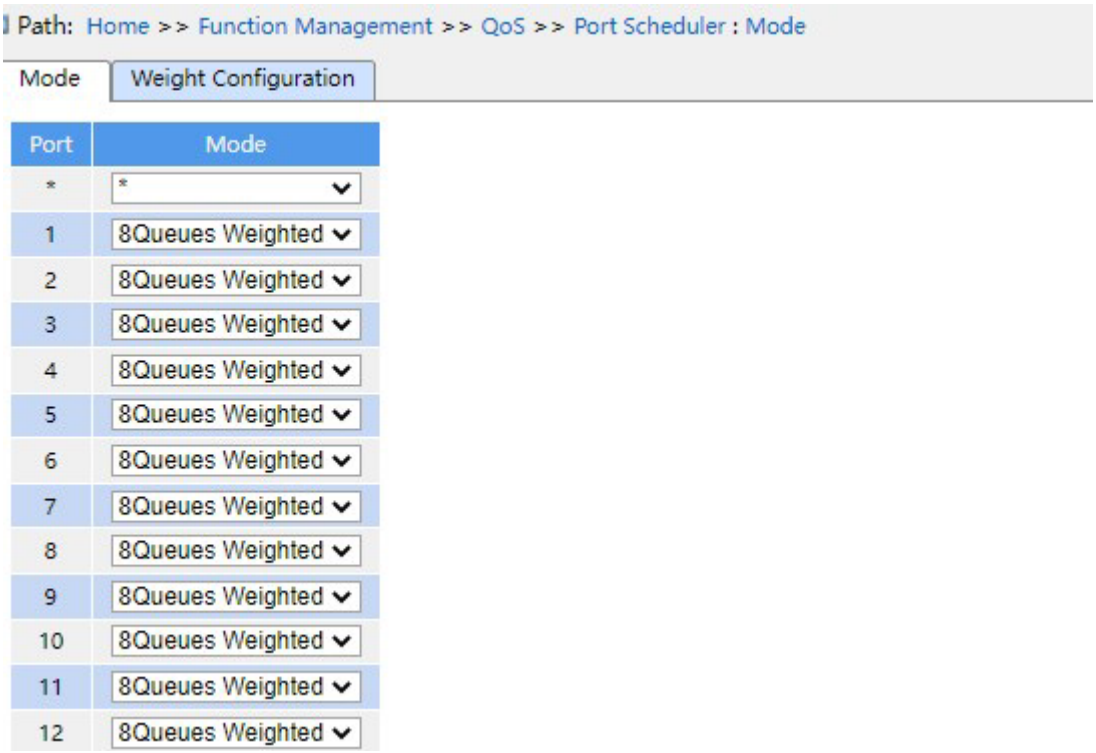


Рисунок 223 Настройка режима планировщика очереди портов

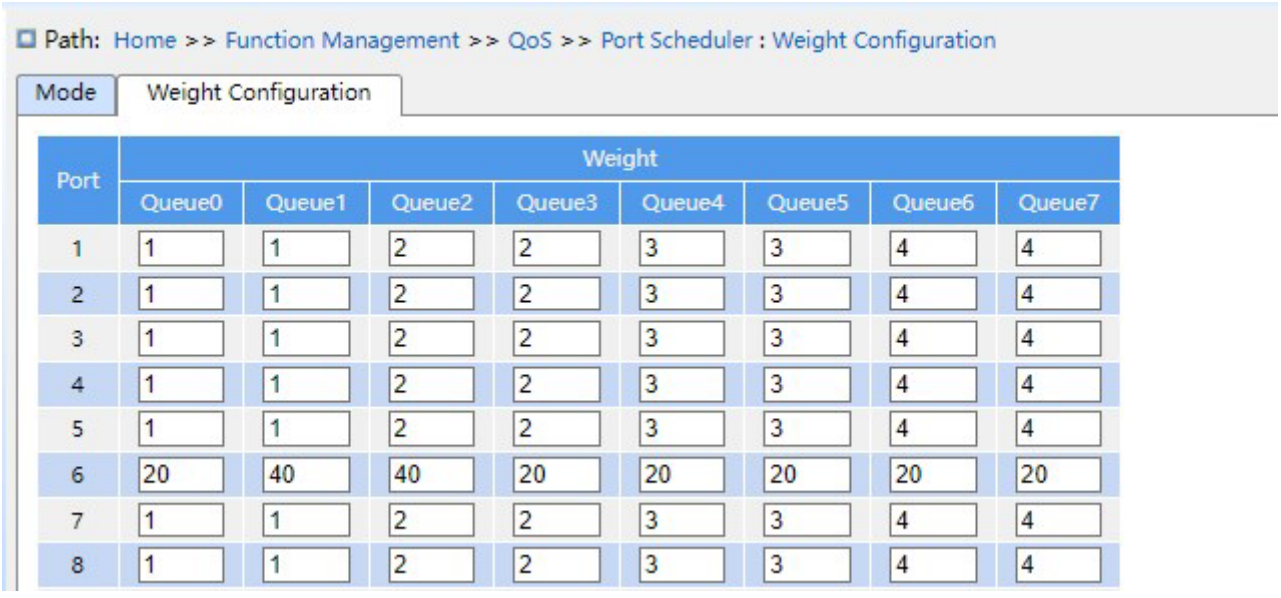


Рисунок 224 Настройка весов портов планировщика

Scheduler Mode

Варианты конфигурации: Strict Priority /2-8 queues weighted

Конфигурация по умолчанию: Strict Priority

Функция: Настройка режима планировщика очереди портов

Вес

Диапазон настройки: 1~100

Конфигурация по умолчанию: 17

Функция: Настройка веса очереди.

9. Настройте шейпинг порта, как показано ниже.

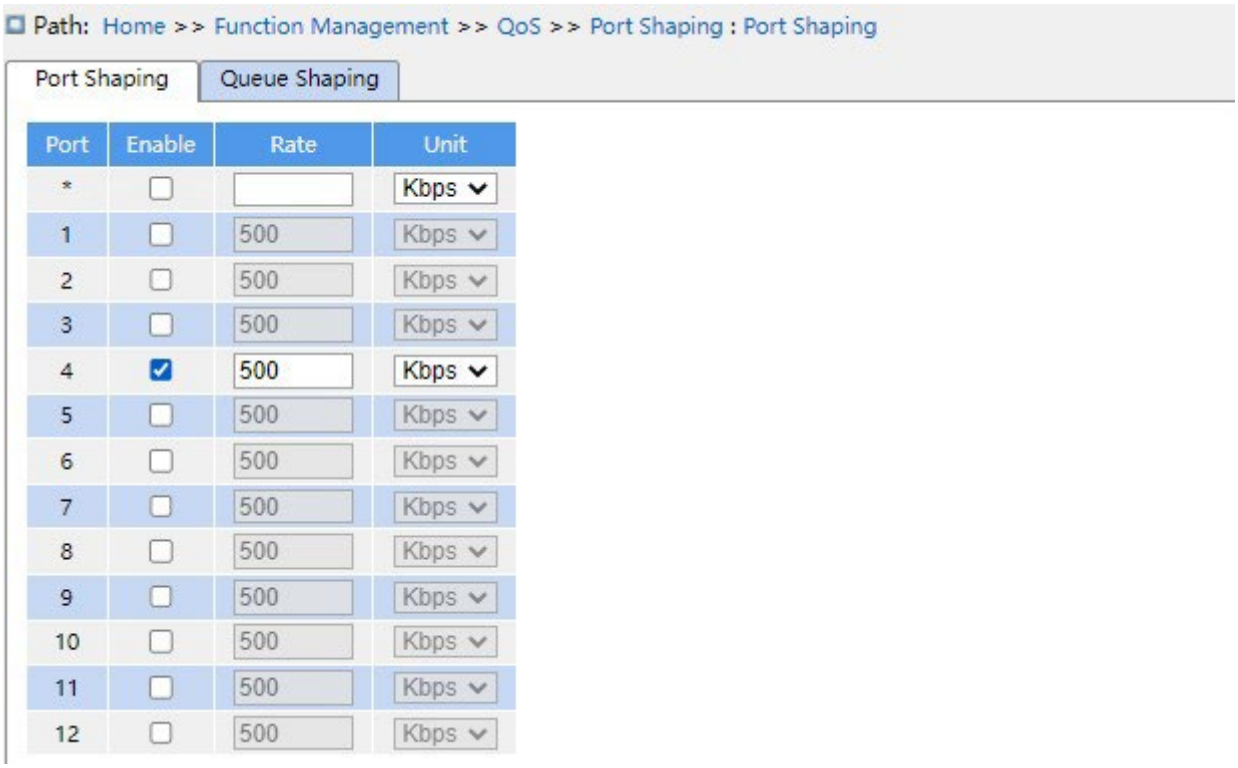


Рисунок 225 Настройка шейпинга порта

Enable

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: disable

Функция: включение шейпинга порта. Формирование трафика порта через ограничение скорости порта.

Rate, Unit

Диапазон настройки:16~1000000 кбит/с / 1~1000 Мбит/с

Функция: Ограничение количества кадров, передаваемых портом, и отбрасывание кадров, превышающих ограниченное значение.

10. Настройте шейпинг очереди, как показано ниже.

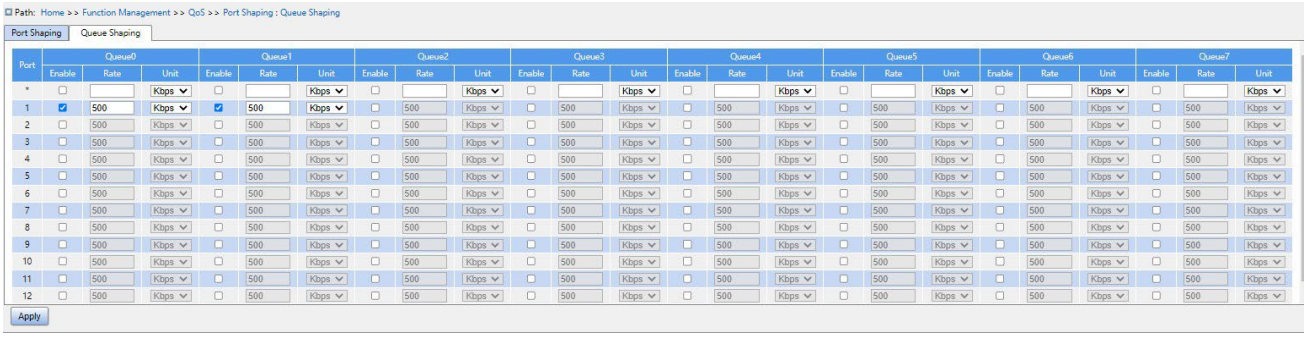


Рисунок 226 Настройка шейпинга очереди

Enable

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: disable

Функция: включение шейпинга очереди.

Rate, Unit

Диапазон настройки: 16~1000000 кбит/с / 1~1000 Мбит/с

Конфигурация по умолчанию: 500 kbps

Функция: Ограничение количества кадров, передаваемых очередью на порту, и отбрасывание кадров, превышающих ограниченное значение.

7.15.4 Пример типовой конфигурации

Как показано на рисунке 227, порты 1-5 пересылают пакет в порт 6. Среди них

Пакеты, полученные портом 1, имеют статус Untag, а пакеты, поступающие в порт 1, сопоставляются с очередью 2.

Значение PCP принятого пакета порта 2 равно 0, значение DEI равно 1, а пакеты, поступающие на порт 2, сопоставляются с очередью 3.

Значение DSCP принятого пакета порта 3 равно 4, а пакеты, поступающие в порт 3, сопоставляются с очередью 6.

Порт 4 включен для проверки формирования трафика порта, и поскольку формирование трафика действует в направлении исходящего порта, конфигурация отправляется на порт 6.

Значение DSCP принятого пакета порта 5 равно 5, а пакеты, поступающие в порт 5, сопоставляются с очередью 2.

Порт 6 использует режим планирования SP+WRR.

Процесс настройки:

1. Установите значение CoS порта 1 равным 2, как показано нарисунке 215.
2. Включите режим классификации тега порта 2 и сопоставьте (PCP=0, DEI=1) с CoS=3, как показано на рисунке 214.
3. Включите сопоставление на основе DSCP портов 3 и 5, как показано на рисунке 215.
4. Установите значения 4 и 5 DSCP и сопоставьте значение 4 DSCP с очередью 6, а значение 5 DSCP с очередью 2, как показано на рисунке 221.
5. Включите формирование трафика порта 6, чтобы ограничить скорость сообщений, отправляемых на порт 4, до 500 кбит/с, рисунок 225. 6. Настройте режим планирования очереди порта 6 на 6 Queues Weighted, вес очереди от Q0~Q5 до 20, 40, 40, 20, 20, 20, как показано на рисунках 223 и 224.

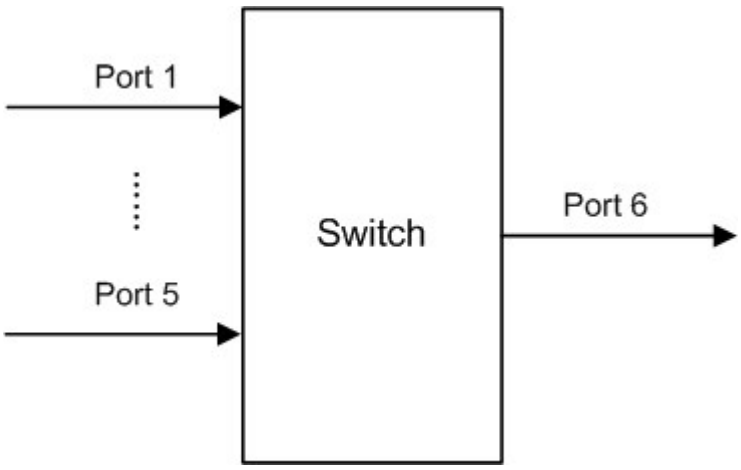


Рисунок 227 Пример настройки QoS

Пакеты порта 1 и порта 5 попадают в очередь 2, пакеты порта 2 попадают в очередь 3, пакеты порта 3 попадают в очередь 6, пакеты порта 4 попадают в очередь 5.

Очередь 6 и очередь 7 используют режим планирования со строгим приоритетом, а очереди с 0 по 5 используют режим планирования WRR. Данные в очереди 6 обрабатываются в первую очередь. Когда очередь 6 пуста, данные в очередях с 0 по 5 планируются по весовому соотношению.

Вес очереди 20, 40, 40, 20, 20, 20. Таким образом, доля полосы пропускания, выделенная пакетам во входной очереди 2, равна 40 /(20+40+40+20+20+20)=25%, а доля пропускной способности, выделенная пакетам во входной очереди 3, равна 20/(20+40+40. +20+20+20)=13%, а пакетам во входной очереди 5 выделяется 20/(20+40+40+20+20+20)=13%. Среди них пакеты порта 1 и порта 5 попадают в очередь 2, поэтому они пересылаются в соответствии с правилом First In, First out (FIFO), но общая пропорция пропускной способности порта 1 и порта 5 должна составлять 25%.

8 Настройка обнаружения петель Loop Detect

8.1 Обзор

После того, как обнаружение петель включено для порта, пакеты обнаружения петель будут отправлены через порт, чтобы определить, существуют ли петли в сети, подключенной к порту. ЦП периодически отправляет в порт пакеты обнаружения петель. Если какой-либо порт коммутатора получает пакеты обнаружения петель, определяется, что в сети существуют петли. Отключите порт, который отправляет пакеты обнаружения петли, и через некоторое время порт автоматически подключится и продолжит обнаружение. Интервал времени для отправки пакетов обнаружения петель и время восстановления порта можно настроить в программном обеспечении.

Примечание:

Обнаружение петель и DT-Ring/DRP/RSTP/MSTP являются взаимоисключающими. Порт, для которого включено обнаружение петель, не может быть настроен как резервный порт; резервный порт не может быть включен для обнаружения петель.

8.2 Настройка через веб-интерфейс

1. Настройте функцию обнаружения петель для порта, как показано на рисунке 228.

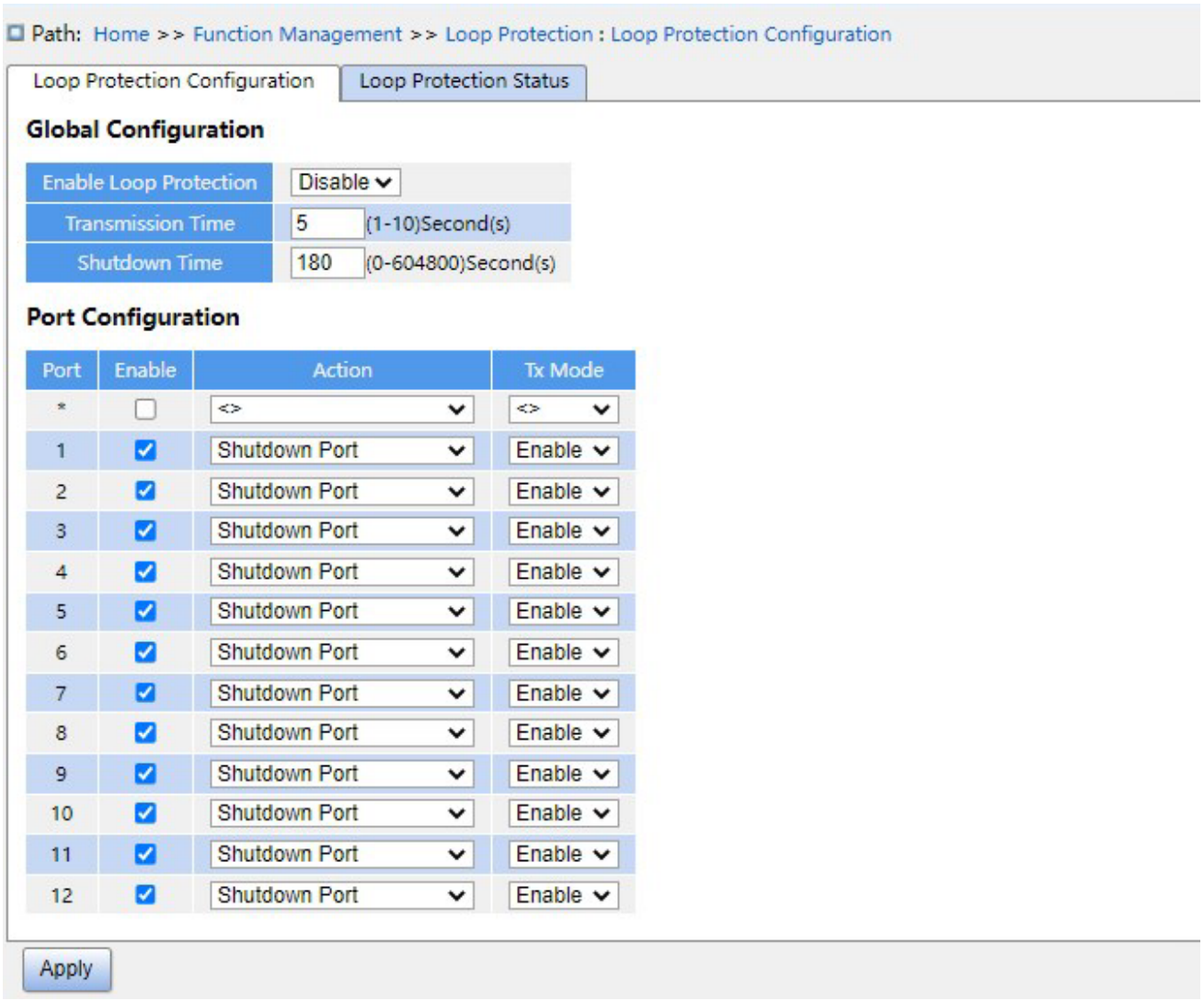


Рисунок 228 Включение функции обнаружения петель для порта

Enable Loop Protection

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение или выключение глобальной функции обнаружения петель для порта

Transmission Time

Диапазон: 1~10 с

По умолчанию: 5 с

Функция: Настройка интервала времени для отправки пакетов обнаружения петель.

Shutdown Time

Диапазон: 0~604800 с

По умолчанию: 180 с

Функция: Настройка времени восстановления порта, 0 указывает, что порт не может быть подключен автоматически до перезапуска устройства.

Enable

Варианты: Enable/Disable

По умолчанию: Enable

Функция: Включение или выключение функции обнаружения петель для порта.

Action

Варианты: Shutdown Port/Shutdown Port and Log/Log Only

По умолчанию: Shutdown Port

Функция: Действие, которое будет выполняться, когда порт обнаружит наличие петли.

Tx Mode

Варианты: Enable/Disable

По умолчанию: Enable

Функция: Отправлять ли пакеты обнаружения петель или нет.

Предупреждение:

Порт может точно определить, существует ли петля, только после того, как защита от петель включена глобально, защита от петель и режим Tx включены на порту.

2. Просмотрите статус защиты от петель, как показано на рисунке 229.

Port	Action	Transmitted	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	0	Down	--	--
2	Shutdown	Enabled	0	Down	--	--
3	Shutdown	Enabled	0	Down	--	--
4	Shutdown	Enabled	0	Down	--	--
5	Shutdown	Enabled	0	Down	--	--
6	Shutdown	Enabled	0	Down	--	--
7	Shutdown	Enabled	0	Up	--	--
8	Shutdown	Enabled	0	Down	--	--
9	Shutdown	Enabled	0	Down	--	--
10	Shutdown	Enabled	0	Down	--	--
11	Shutdown	Enabled	0	Down	--	--
12	Shutdown	Enabled	0	Down	--	--

Рисунок 229 Просмотр статуса защиты от петель

Loop Protection Status

Варианты: --/Loop

Функция: Показать наличие петель в сети, когда функция обнаружения петель порта включена. Loop указывает на наличие петель, а -- указывает на отсутствие петель.

8.3 Типовой пример конфигурации

Требования к сети

Порт 3 коммутатора подключен к внешней сети. При наличии петель в сети отключите порт 3, как показано на рисунке 230.

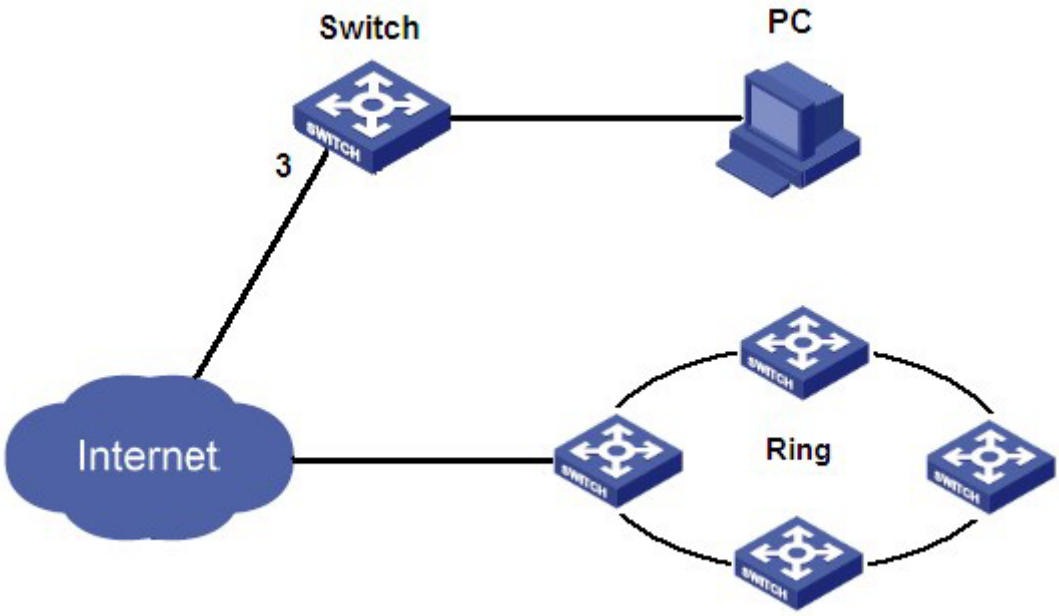


Рисунок 230 Пример обнаружения петли Конкретная конфигурация:

Включите функцию обнаружения петель для порта 3, как показано на рисунке 228.

9 Диагностика

9.1 Журнал

9.1.1 Введение

Функция журнала в основном записывает состояние системы, ошибки, отладку, аномалии и другую информацию. При соответствующей настройке коммутатор может загружать журналы на сервер с поддержкой Syslog в режиме реального времени. Журнал содержит информацию о сигналах тревоги, широковещательном шторме, перезагрузке, памяти и информацию об операциях пользователей.

9.1.2 Настройка через веб-интерфейс

1. Настройте системный журнал, как показано ниже.

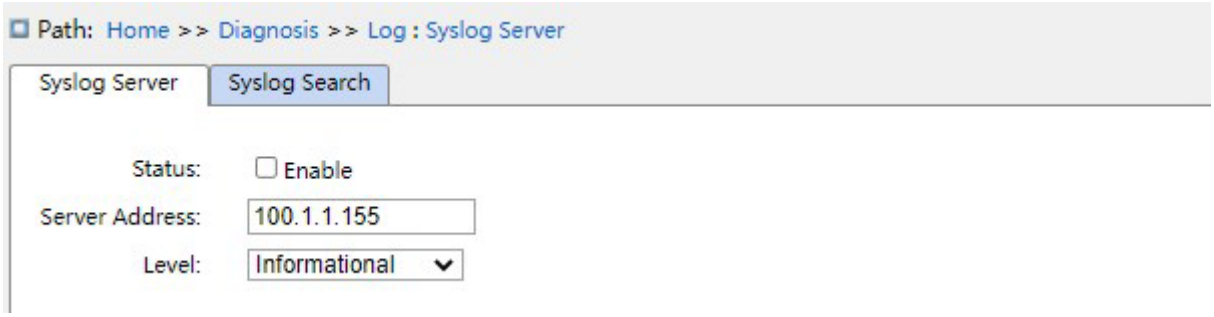


Рисунок 231 Настройка системного журнала

Status

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: включение сервера системного журнала.

Server Address

Формат: A.B.C.D

Настройка IP-адреса сервера журнала.

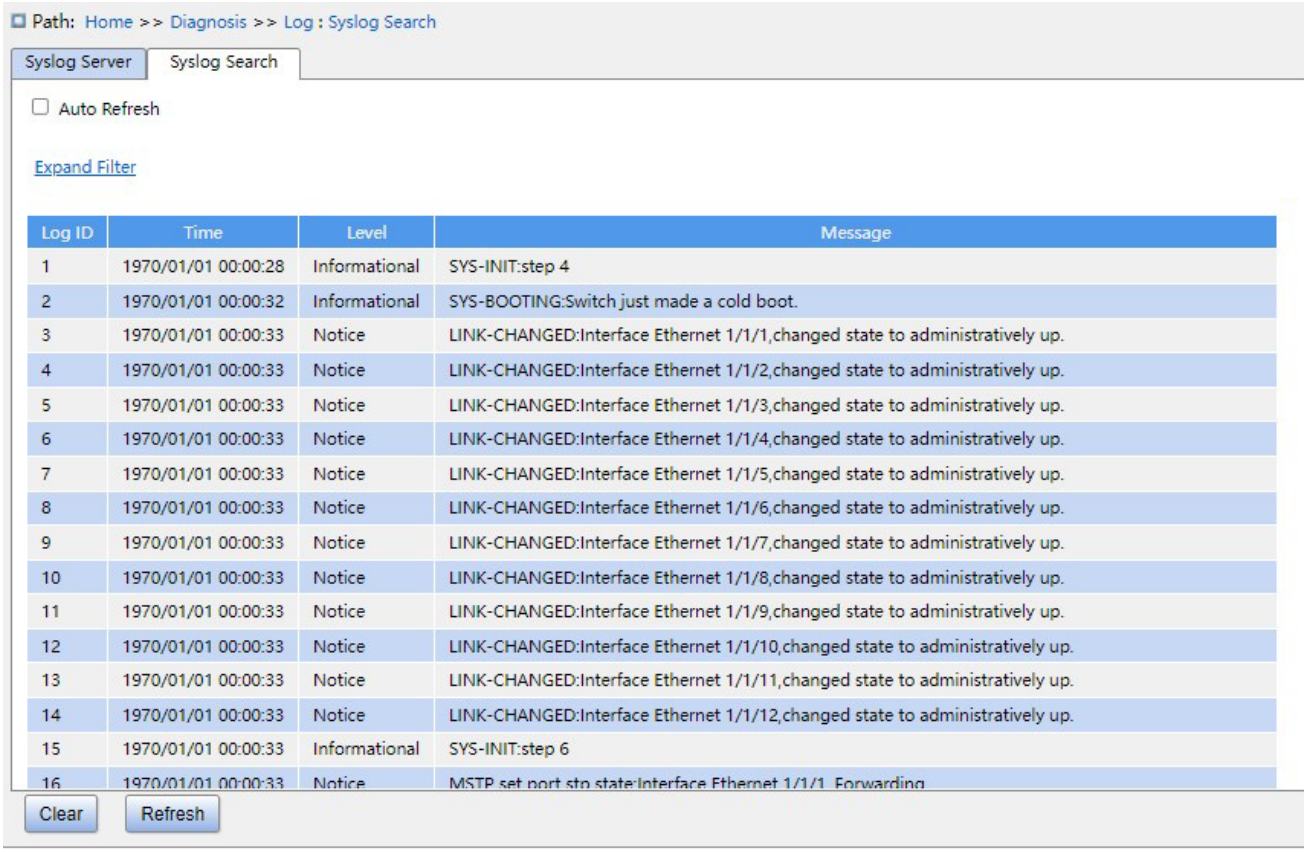
Level

Варианты конфигурации: Error/Warning/Notice/Information

Конфигурация по умолчанию: Information

Функция: Выбор отображаемого уровня информации журнала.

2. Поиск в журнале показан ниже.



Log ID	Time	Level	Message
1	1970/01/01 00:00:28	Informational	SYS-INIT:step 4
2	1970/01/01 00:00:32	Informational	SYS-BOOTING:Switch just made a cold boot.
3	1970/01/01 00:00:33	Notice	LINK-CHANGED:Interface Ethernet 1/1/1,changed state to administratively up.
4	1970/01/01 00:00:33	Notice	LINK-CHANGED:Interface Ethernet 1/1/2,changed state to administratively up.
5	1970/01/01 00:00:33	Notice	LINK-CHANGED:Interface Ethernet 1/1/3,changed state to administratively up.
6	1970/01/01 00:00:33	Notice	LINK-CHANGED:Interface Ethernet 1/1/4,changed state to administratively up.
7	1970/01/01 00:00:33	Notice	LINK-CHANGED:Interface Ethernet 1/1/5,changed state to administratively up.
8	1970/01/01 00:00:33	Notice	LINK-CHANGED:Interface Ethernet 1/1/6,changed state to administratively up.
9	1970/01/01 00:00:33	Notice	LINK-CHANGED:Interface Ethernet 1/1/7,changed state to administratively up.
10	1970/01/01 00:00:33	Notice	LINK-CHANGED:Interface Ethernet 1/1/8,changed state to administratively up.
11	1970/01/01 00:00:33	Notice	LINK-CHANGED:Interface Ethernet 1/1/9,changed state to administratively up.
12	1970/01/01 00:00:33	Notice	LINK-CHANGED:Interface Ethernet 1/1/10,changed state to administratively up.
13	1970/01/01 00:00:33	Notice	LINK-CHANGED:Interface Ethernet 1/1/11,changed state to administratively up.
14	1970/01/01 00:00:33	Notice	LINK-CHANGED:Interface Ethernet 1/1/12,changed state to administratively up.
15	1970/01/01 00:00:33	Informational	SYS-INIT:step 6
16	1970/01/01 00:00:33	Notice	MSTP set port stp state:Interface Ethernet 1/1/1 Forwarding

Рисунок 232 Поиск в журнале

Auto Refresh

Варианты настройки: флажок установлен/снят

Конфигурация по умолчанию: снят

Функция: включение Auto Refresh

Log ID

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

Конфигурация по умолчанию: *

Функция: Выбор идентификаторов отфильтрованных журналов. * означает все ID, >= означает журналы, ID которых больше или равен ID, <= означает журналы, ID которых меньше или равен ID, select range – ввод диапазона журналов вручную.

Time

Варианты конфигурации: */Start/end/select range

Конфигурация по умолчанию: *

Функция: Выбор интервала времени для отфильтрованных журналов, * означает все время, Start – время начала журнала, End – время завершения журнала, select range – выбор промежутка времени вручную.

Level

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

Конфигурация по умолчанию: *

Функция: Выбор уровней отфильтрованных журналов. * означает все уровни, >= означает журналы, уровень которых больше или равен заданному, <= означает журналы, уровень которых меньше или равен заданному, select range – ввод диапазона уровней вручную. Уровни включают в себя Error, Warning, Notice, Information.

Message

Варианты конфигурации: */include/not include

Конфигурация по умолчанию: *

Функция: Выбор отфильтрованных сообщений, * – все журналы, include – включить журналы для некоторых полей, not include – не включать журналы для некоторых полей.

3. Очистите журналы, как показано ниже.

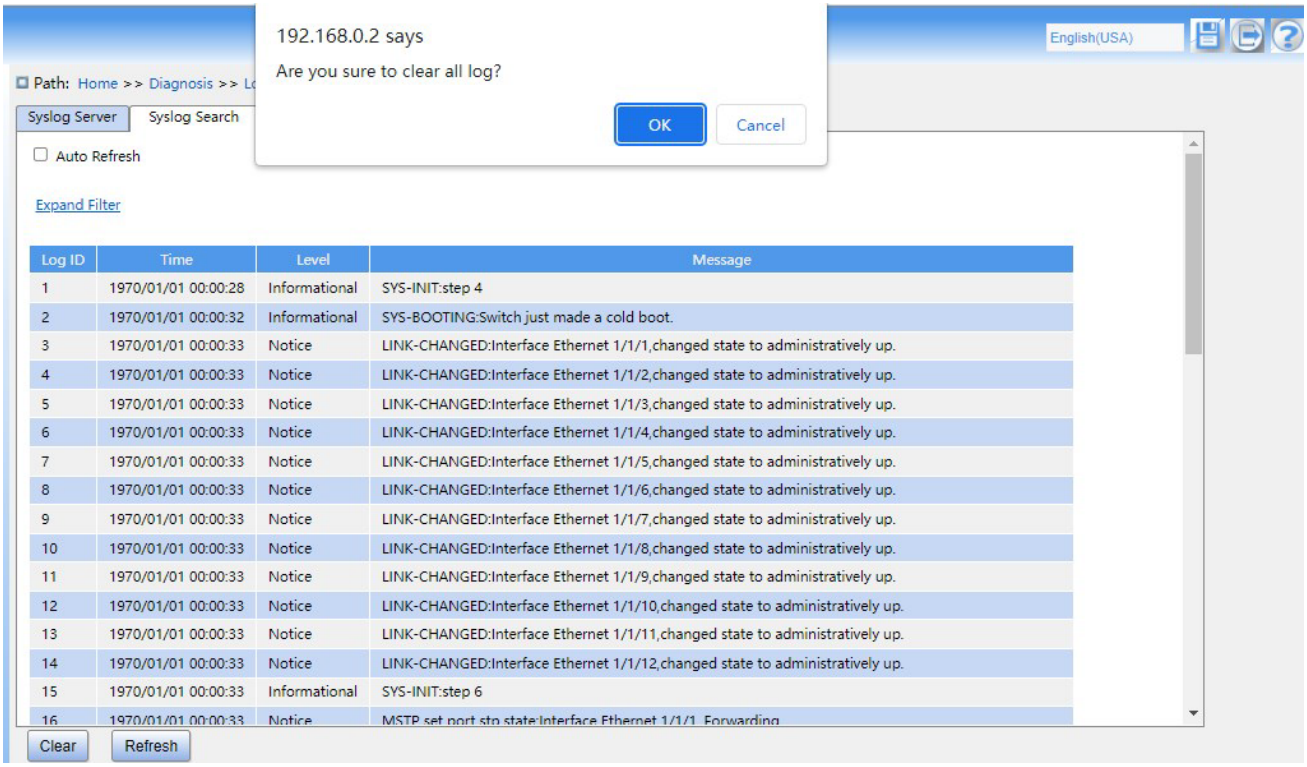


Рисунок 233 Очистка журналов

После завершения запросов нажмите кнопку <Clear> в нижнем левом углу, чтобы очистить журналы.

Сервер протокола системного журнала может установить на ПК программное обеспечение, поддерживающее сервер системного журнала, например, Tftp32. Информация журнала может отображаться в режиме реального времени на сервере Syslog, как показано ниже.

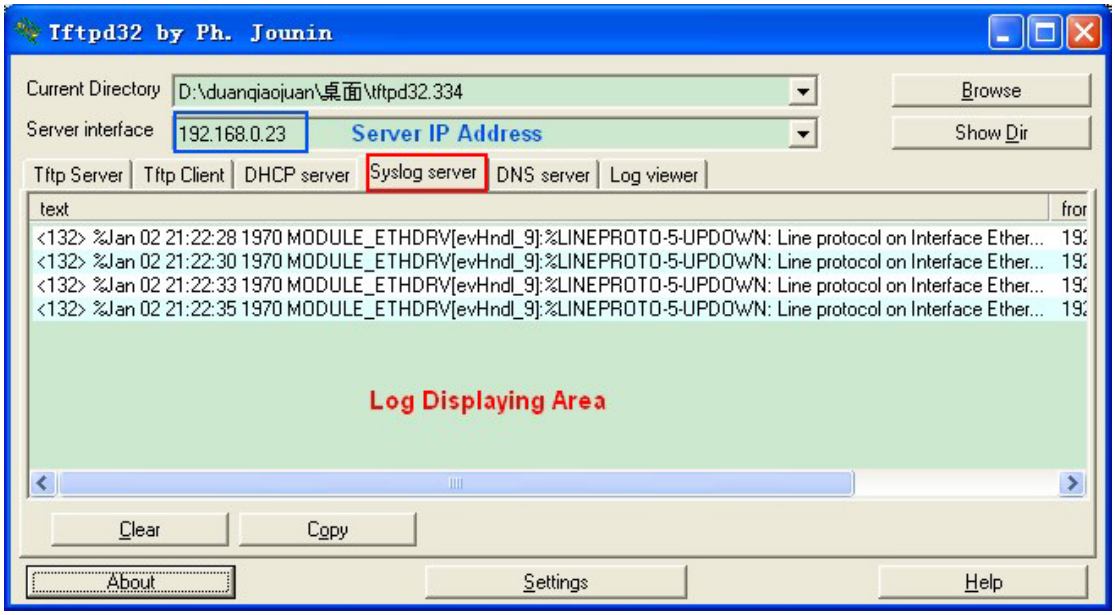


Рисунок 234 Выгрузка информации журнала в реальном времени

9.2 Зеркалирование портов

9.2.1 Введение

С функцией зеркалирования портов коммутатор копирует все полученные или переданные кадры данных в одном порту (исходный порт зеркалирования) на другой порт (порт назначения зеркалирования). Порт назначения зеркалирования подключается к анализатору протокола или монитору RMON для мониторинга сети, управления и диагностики неисправностей.

9.2.2 Пояснения

Коммутатор поддерживает только один порт назначения зеркалирования, но несколько портов-источников.

Несколько исходных портов могут находиться либо в одной VLAN, либо в разных VLAN.

Порт источника и порт назначения зеркалирования могут находиться в одной и той же VLAN или в разных VLAN.

Исходный порт и порт назначения не могут быть одним и тем же портом.

Предупреждение:

Динамическое изучение MAC-адресов должно быть отключено на порту назначения.

9.2.3 Настройка через веб-интерфейс

1. Настройте функцию зеркалирования порта, как показано ниже.

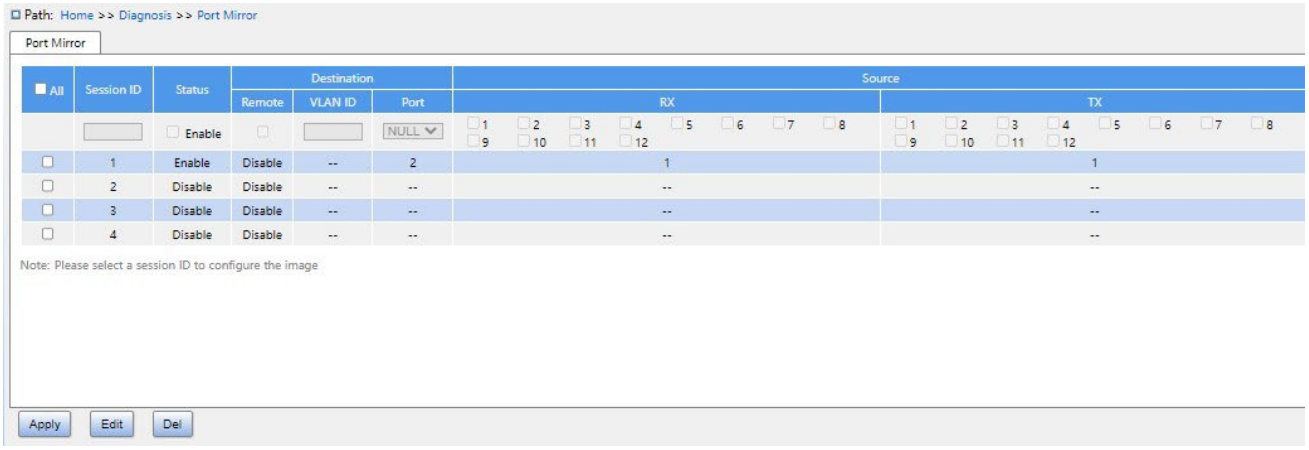


Рисунок 235 Настройка функции зеркалирования порта.

ALL

Варианты конфигурации: флажок установлен/снят

Конфигурация по умолчанию: Флажок снят

Функция: Выбор этой группы зеркалирования для редактирования и изменения.

Status

Варианты конфигурации: Enable/disable

Функция: включение зеркалирования порта.

Destination Port

Варианты конфигурации: NULL/Номер порта

Конфигурация по умолчанию: NULL

Функция: Выбор порта назначения зеркалирования, только один порт назначения зеркалирования.

Rx

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включить зеркалирование кадров, полученных из исходного порта.

Tx

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включить зеркалирование кадров, переданных из исходного порта.

2. Настройте режим Remote Mirror, как показано ниже.

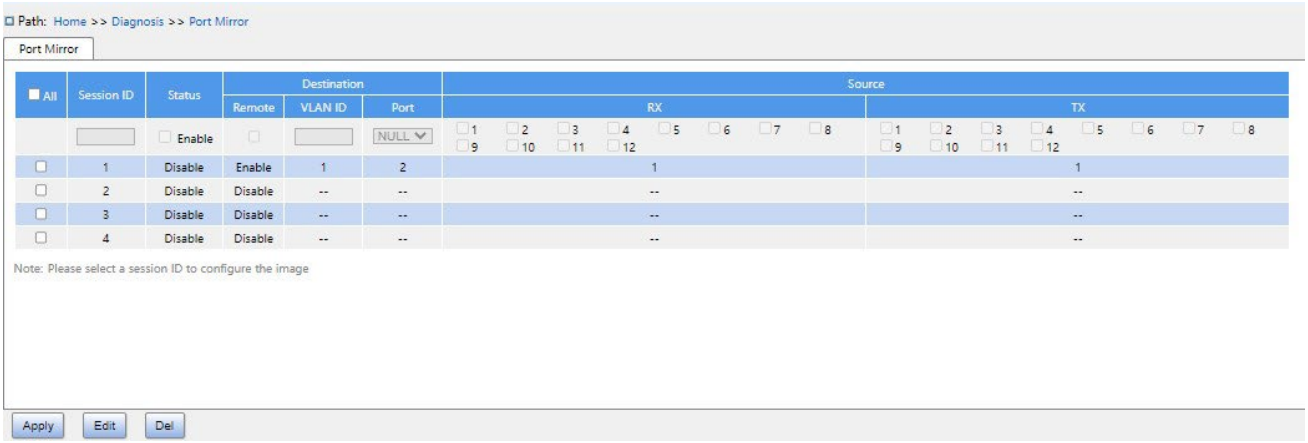


Рисунок 236 Настройка режима Remote Mirror

All

Варианты конфигурации: флажок установлен/снят

Конфигурация по умолчанию: Флажок снят

Функция: Выбор этой группы зеркалирования для редактирования и изменения.

Status

Варианты конфигурации: Enable/disable

Функция: включение зеркалирования порта.

Destination Remote

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: При включении удаленного зеркалирования, назначение и источник не могут быть включены одновременно. **Destination VLAN ID**

Диапазон настройки: 1~4093

Функция: Настройка VLAN ID удаленного зеркала назначения.

Destination Port

Варианты конфигурации: NULL/Номер порта

Конфигурация по умолчанию: NULL

Функция: При настройке удаленного зеркала назначения порт назначения используется в качестве порта отражения, а при настройке исходного удаленного зеркала порт назначения является портом назначения удаленного зеркала.

Rx

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включить зеркалирование кадров, полученных из исходного порта.

Tx

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включить зеркалирование кадров, переданных из исходного порта.

9.2.4 Пример типовой конфигурации

Как показано на рисунке 237, порт назначения зеркалирования — это порт 2, а исходный порт источника зеркалирования — порт 1. Как переданные, так и полученные пакеты порта 1 зеркалируются на порт 2.

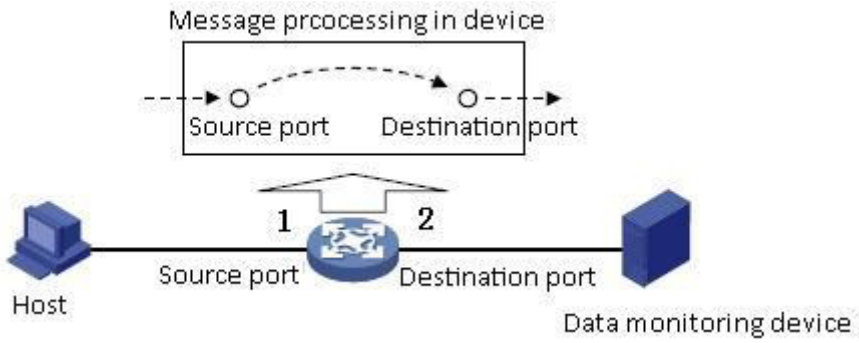


Рисунок 237 Пример зеркалирования порта

Процесс настройки:

1. Включите функцию зеркалирования порта, как показано на рисунке 235.

2. Установите порт 2 в качестве порта назначения зеркалирования, порт 1 в качестве исходного порта зеркалирования и режим зеркального отображения Both, как показано на рисунке 235.

9.3 LLDP

9.3.1 Введение

Протокол обнаружения канального уровня Link Layer Discovery Protocol (LLDP) предоставляет стандартный механизм обнаружения канального уровня. Он инкапсулирует информацию об устройстве, такую как возможности, адрес управления, идентификатор устройства и идентификатор интерфейса, в блок данных протокола обнаружения канального уровня (LLDPDU) и объявляет LLDPDU своим непосредственно подключенным соседям. Получив LLDPDU, соседи сохраняют эту информацию в MIB для запроса и проверки состояния канала NMS.

9.3.2 Настройка через веб-интерфейс

1. Настройте LLDP, как показано ниже.

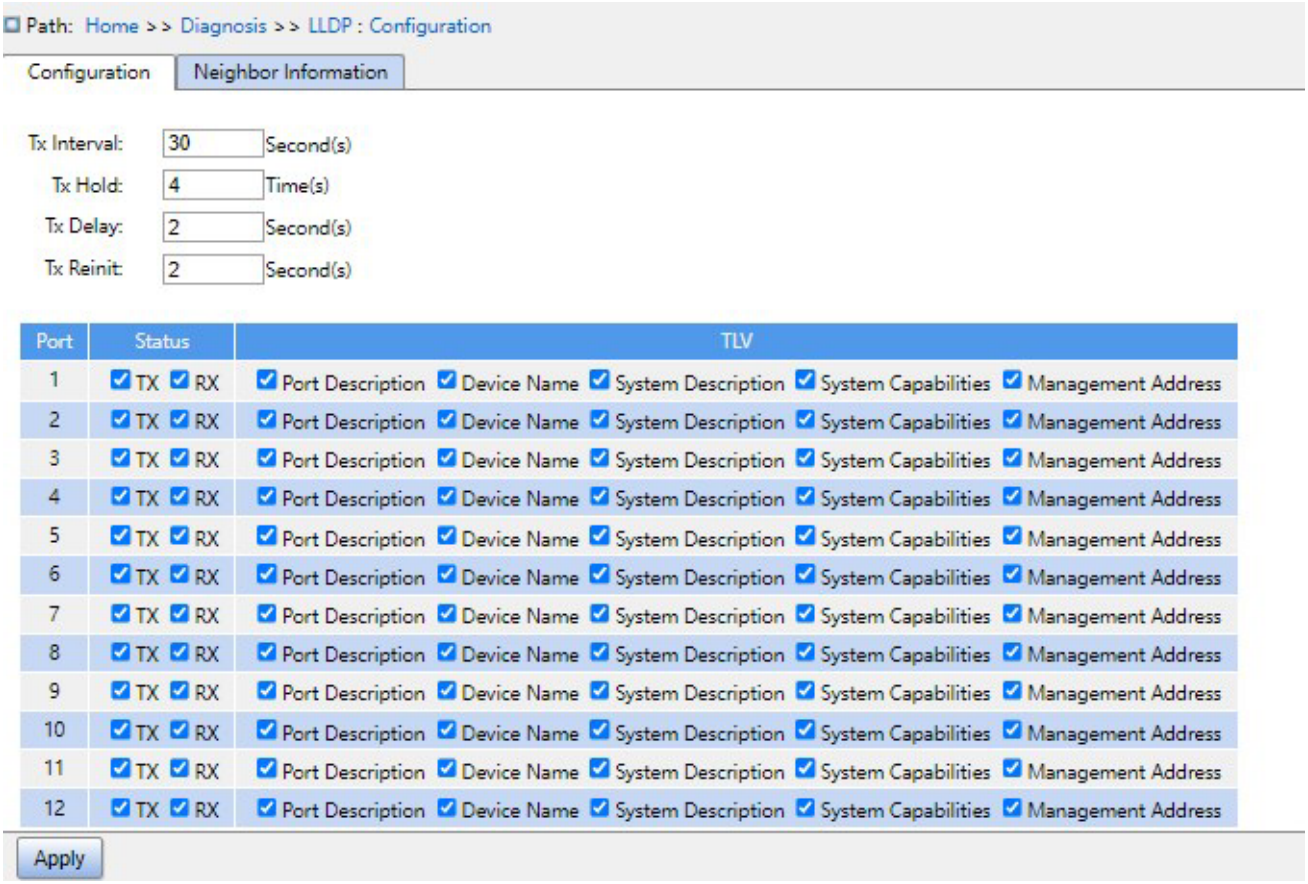


Рисунок 238 Настройка LLDP

Tx Interval

Диапазон настройки: 5~32768 с

Конфигурация по умолчанию: 30 с

Функция: Настройка интервала времени для отправки пакетов LLDP.

Tx Hold

Диапазон настройки: 2~10 раз

Конфигурация по умолчанию: 4 раза

Функция: Настройка количества удержаний Tx. Эффективная длительность пакета LLDP = Tx Interval x Tx Hold.

Tx Delay

Диапазон настройки: 1~8192 с

Конфигурация по умолчанию: 2 с

Функция: Задание интервала передачи между новым пакетом LLDP и предыдущим пакетом LLDP после изменения информации о конфигурации. Значение Tx Delay не может превышать 1/4 значения Tx Interval.

Tx Reinit

Диапазон настройки: 1~10 с

Конфигурация по умолчанию: 2 с

Функция: После отключения LLDP на порту или перезапуска коммутатора коммутатор отправляет кадр отключения LLDP соседнему узлу, чтобы объявить, что предыдущий пакет LLDP недействителен. Tx re-initialization относится к интервалу между передачей кадра выключения LLDP и повторной инициализацией пакета LLDP.

Status

Варианты конфигурации: Disable/TX/RX/TX&RX

Конфигурация по умолчанию: TX&RX

Функция: Настройка режима пакетов LLDP. Режим TX&RX указывает, что коммутатор может отправлять пакеты LLDP, а также получать и идентифицировать пакеты LLDP; режим Disable указывает, что коммутатор не отправляет пакеты LLDP и не принимает пакеты LLDP; режим только RX указывает, что коммутатор только принимает и идентифицирует пакеты LLDP; только TX указывает, что коммутатор только отправляет пакеты LLDP и не принимает пакеты LLDP.

Port Description

Варианты конфигурации: Enabled/Disabled

Конфигурация по умолчанию: Enabled

Функция: Enable указывает, что пакеты LLDP будут содержать описание порта.

Device Name

Варианты конфигурации: Enabled/Disabled

Конфигурация по умолчанию: Enabled

Функция: Enable указывает, что пакеты LLDP будут содержать имя системы.

System Description

Варианты конфигурации: Enabled/Disabled

Конфигурация по умолчанию: Enabled

Функция: Enable указывает, что пакеты LLDP будут содержать описание системы.

Sys Capability

Варианты конфигурации: Enabled/Disabled

Конфигурация по умолчанию: Enabled

Функция: Enable указывает, что пакеты LLDP будут содержать возможности системы.

Management Address

Варианты конфигурации: Enabled/Disabled

Конфигурация по умолчанию: Enabled

Функция: Enable указывает, что пакеты LLDP будут содержать адрес управления.

2. Просмотрите информацию LLDP, как показано ниже.

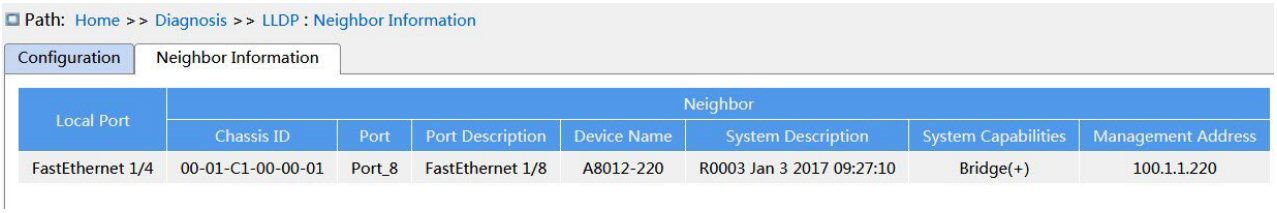


Рисунок 239 Просмотр информации LLDP

Предупреждение:

Для отображения информации LLDP необходимо включить LLDP на двух подключенных устройствах.

9.4 Трассировка

Трассировка маршрута позволяет увидеть маршрут пакетов IP-данных от одного хоста к другому.

1. Настройте трассировку, как показано ниже.

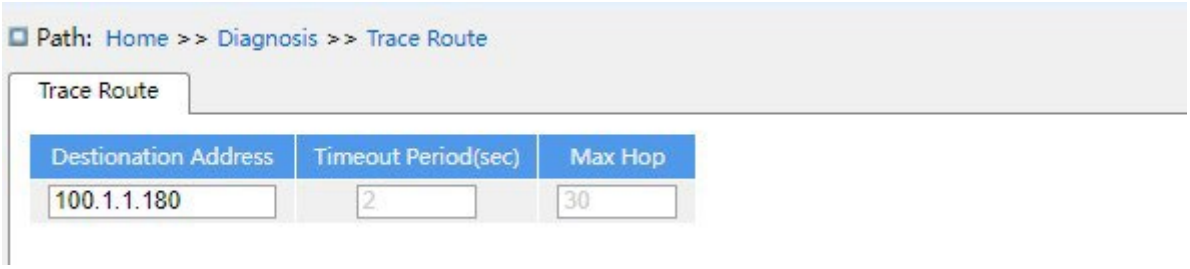


Рисунок 240 Настройка трассировки

Destination address

Формат: A.B.C.D

Функция: Настройка IP-адреса устройства назначения.

Timeout Period

Диапазон настройки: 1~10 с

Конфигурация по умолчанию: 2 с

Функция: Настройка периода ожидания. Если отправляющая сторона не получит ответное сообщение от принимающей стороны в течение этого времени, связь не удалась.

Max Hop

Диапазон настройки: 1~255

Конфигурация по умолчанию: 30

Функция: Проверка количества шлюзов, которые проходят пакеты на пути между отправляющим и принимающим устройствами.

2. Просмотрите результаты команды Traceroute, как показано ниже.

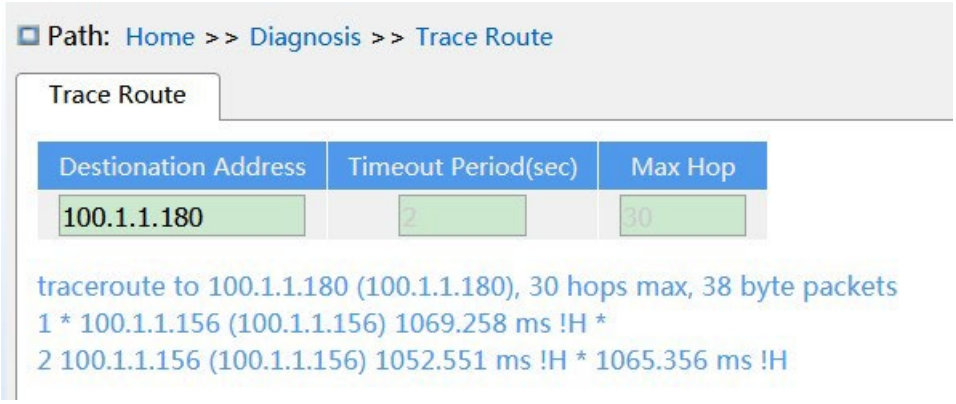


Рисунок 241 Просмотр результатов

9.5 Ping

Пользователи могут запустить команду ping, чтобы проверить, доступно ли устройство с указанным адресом и не повреждено ли сетевое подключение во время планового обслуживания системы.

1. Настройте команду ping, как показано ниже

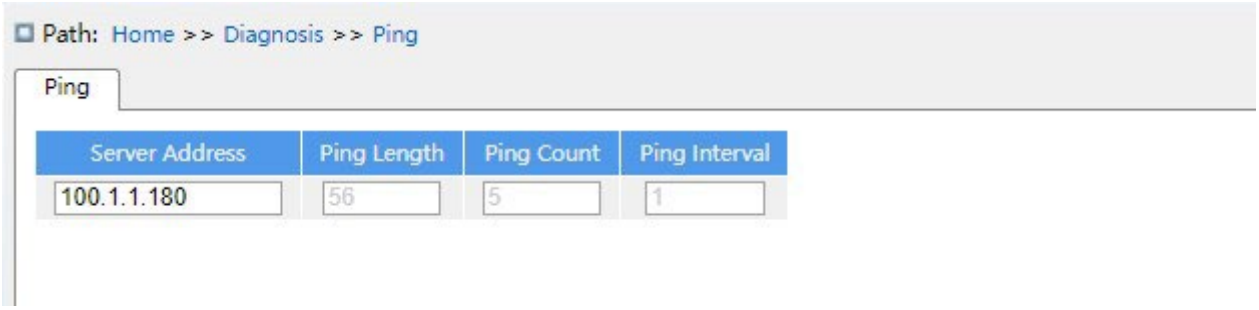


Рисунок 242 Настройка команды ping

Server Address

Формат: A.B.C.D

Описание: Ввод IP-адреса устройства назначения.

Ping Length

Диапазон настройки: 2~1452 байта

Конфигурация по умолчанию: 56 байт

Функция: Указание длины запроса ICMP (исключая заголовок IP и ICMP-пакета) для передачи.

Ping Count

Диапазон настройки: 1~60

Конфигурация по умолчанию: 5

Функция: Задание количества раз отправки ICMP-запроса.

Ping Interval

Диапазон настройки: 1~30 с

Конфигурация по умолчанию: 1 с

Функция: Задание интервала отправки ICMP-запроса.

2. Просмотрите результаты ping, как показано ниже

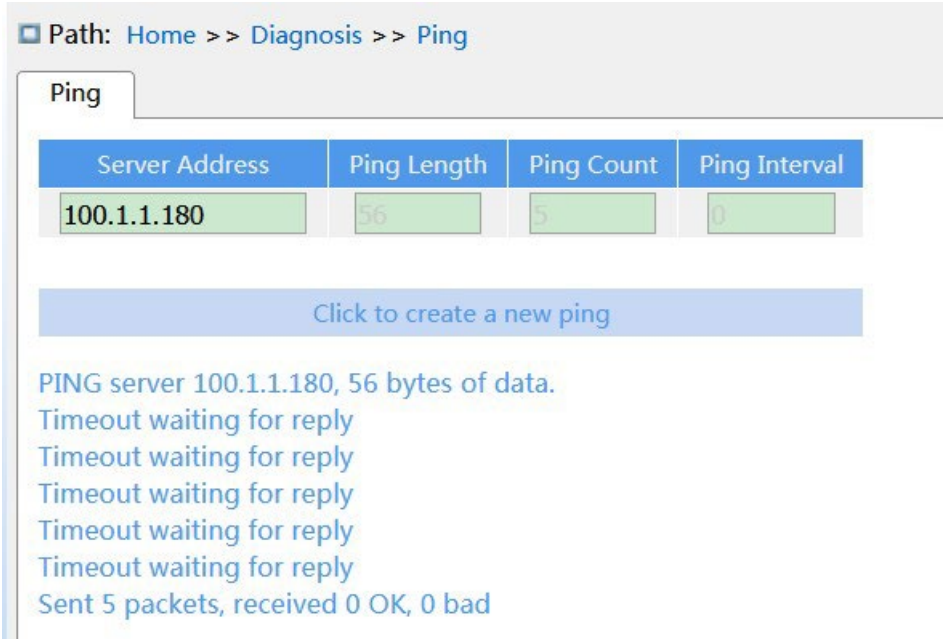


Рисунок 243 Просмотр результатов ping

Результаты команды ping включают в себя ответ целевого устройства на каждый пакет запроса ICMP и статистику пакетов, собранную во время выполнения команды ping.

9.6 IP Source Guard

9.6.1 Введение

Благодаря функции связывания IP Source Guard сообщения, пересылаемые портом, могут быть отфильтрованы, чтобы предотвратить прохождение незаконных сообщений через порт, таким образом, это ограничивает незаконное использование сетевых ресурсов (например, незаконный хост, поддельный IP-адрес законного пользователя, доступ к сеть), повышая безопасность порта.

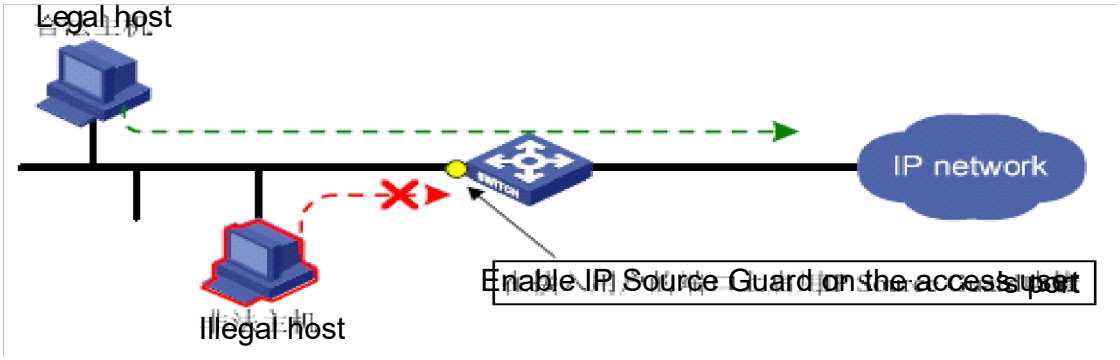


Рисунок 244 Схема работы IP Source Guard

9.6.2 Принцип работы

Настроенный порт с этой функцией после получения сообщения выполняет поиск в таблице привязки IP Source Guard. Если элемент функции в сообщении соответствует записанному элементу функции в таблице привязки, порт пересылает сообщение, в противном случае сообщение удаляется. Функция привязки предназначена для порта, один порт является привязкой, только этот порт ограничен, на другие порты привязка не влияет.

Функциональный элемент IP Source Guard включает в себя: IP-адрес источника, MAC-адрес источника и тег VLAN. И он поддерживает комбинацию портов со следующим функциональным элементом (коротко элемент таблицы привязки):

- IP, MAC, IP+MAC
- IP+VLAN, MAC+VLAN, IP+MAC+VLAN

Поддерживаемый тип привязки элементов таблицы по порту зависит от типа устройства и зависит от фактической ситуации с устройством.

IP Source Guard делится на статическую привязку и динамическую привязку в зависимости от режима формирования элементов таблицы привязки:

- **Статическая привязка:** Ручная настройка элементов таблицы привязки для управления портом подходит для случая, когда количество хостов в локальной сети невелико или хост необходимо привязать отдельно.
- **Динамическая привязка:** Функция управления портом осуществляется путем автоматического получения элементов таблицы привязки DHCP Snooping или DHCP Relay, которые подходят для многих хостов в локальной сети, а использование DHCP для настройки динамических хостов позволяет эффективно предотвращать конфликты IP-адресов и присвоение. Принцип заключается в том, что всякий раз, когда DHCP назначает пользователю элемент таблицы, функция динамической привязки добавляет соответствующий элемент таблицы привязки, чтобы позволить пользователю получить доступ к сети. Если пользователь устанавливает IP-адрес конфиденциально, он не сможет получить доступ к сети, поскольку это не активирует

элемент таблицы назначения DHCP, а функция динамической привязки не добавляет соответствующее правило разрешения доступа.

8.6.3 Настройка через веб-интерфейс

1. Включите IP Source Guard, как показано ниже.

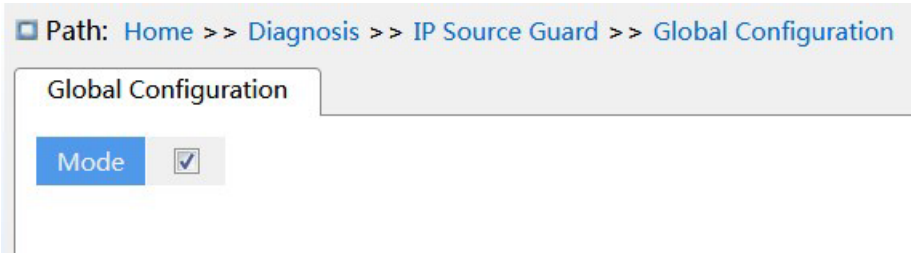


Рисунок 245 Настройка IP Source Guard

Mode

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение глобальной функции IP Source Guard.

2. Настройте IP Source Guard, как показано ниже.

Рисунок 246 Настройка IP Source Guard для порта

Enable

Варианты конфигурации: Enable/Disable

Конфигурация по умолчанию: Disable

Функция: Включение функции IP Source Guard для порта.

3. Настройка статической привязки показана ниже.

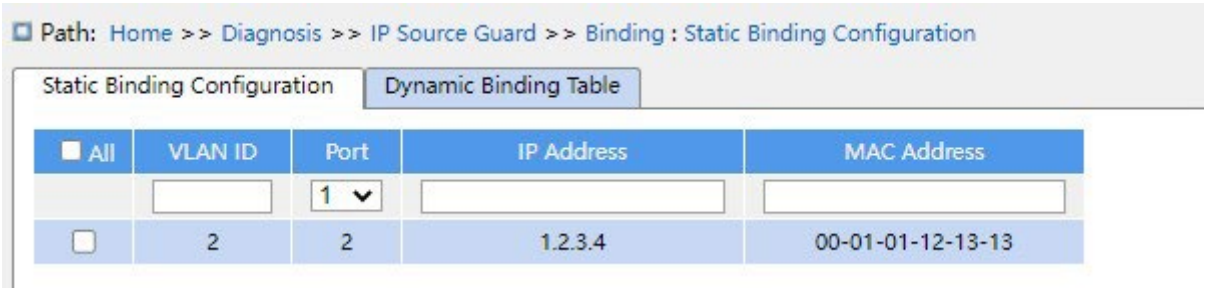


Рисунок 247 Настройка статической привязки

VLAN ID

Варианты конфигурации: Все VLAN ID

Настройка VLAN ID таблицы статической привязки.

Port

Функция: Выбор порт-участник таблицы статической привязки.

IP Address

Формат: A.B.C.D

Функция: Настройка IP-адреса таблицы статической привязки.

MAC address

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

Функция: Настройка MAC-адреса таблицы статической привязки, настраивать только как MAC-адрес одноадресной рассылки.

4. Просмотрите таблицу динамической привязки, как показано ниже.

Рисунок 248 Просмотр таблицы динамической привязки

Type

Варианты отображения: Relay/Snooping

Описание: Таблица динамической привязки генерируется устройствами DHCP Relay и DHCP Snooping, элементы таблицы типа Relay генерируются после включения глобальной функции IP Source Guard, элементы таблицы типа Snooping генерируются после включения функции IP Source Guard как глобально, так и для портов, которые подключаются к DHCP-клиенту.

8.6.4 Пример типовой конфигурации

1. Элементы таблицы IP Source Guard типа Relay

Как показано на рисунке 249, коммутатор A в качестве DHCP-сервера, коммутатор B в качестве ретранслятора DHCP, коммутатор C в качестве DHCP-клиента, порт 1 коммутатора A подключаются к порту 1 коммутатора B, порт 2 коммутатора B подключаются к порту 2 коммутатора C. DHCP-сервер не находится в той же локальной сети, что и DHCP-клиент. После включения IP Source Guard на устройстве ретрансляции клиент динамически получает IP-адрес и другие сетевые параметры в режиме DHCP через ретранслятор DHCP. Устройство ретрансляции формирует элементы таблицы IP Source Guard.

Рисунок 249 Пример типовой конфигурации

DHCP ➢ Конфигурация коммутатора A:

1. Создайте VLAN1 и настройте IP-адрес: 100.1.1.156;
2. Откройте вкладку состояния сервера DHCP VLAN 1, как показано на рисунке 180.
3. Создайте пул адресов pool-33, как показано на рисунке 181.
4. Выберите тип пула адресов Network; IP-адрес: 33.1.1.6; маска: 255.0.0.0, как показано на рисунке 182.

➢Конфигурация коммутатора B:

1. Создайте VLAN1 и настройте IP-адрес: 100.1.1.180;
2. Создайте VLAN33 и настройте IP-адрес: 33.1.1.2;
3. Включите ретрансляцию DHCP, как показано на рисунке 195.
4. Настройте IP-адрес сервера: 100.1.1.156, как показано на рисунке 195.
5. Включите глобальную функцию IP Source Guard, как показано на рисунке 245; ➢ Конфигурация коммутатора C:

1. Создайте VLAN33 и включите клиент DHCP;
2. Коммутатор A назначает IP-адрес 33.0.0.1 коммутатору C.

После того как коммутатор C получит адрес, таблицу IP Source Guard можно просмотреть на коммутаторе B, как показано на рисунке 248.

2. Элементы таблицы IP Source Guard типа Snooping

Как показано ниже, коммутатор A в качестве DHCP-сервера, коммутатор B в качестве DHCP Snooping, коммутатор C в качестве DHCP-клиента, порт 1 коммутатора A подключаются к порту 1 коммутатора B, порт 2 коммутатора B подключаются к порту 2 коммутатора C. DHCP-сервер не находится в той же локальной сети, что и DHCP-клиент. После включения IP Source Guard на устройстве Snooping клиент динамически получает IP-адрес и другие сетевые параметры в режиме DHCP через ретранслятор DHCP. Устройство ретрансляции формирует элементы таблицы IP Source Guard.

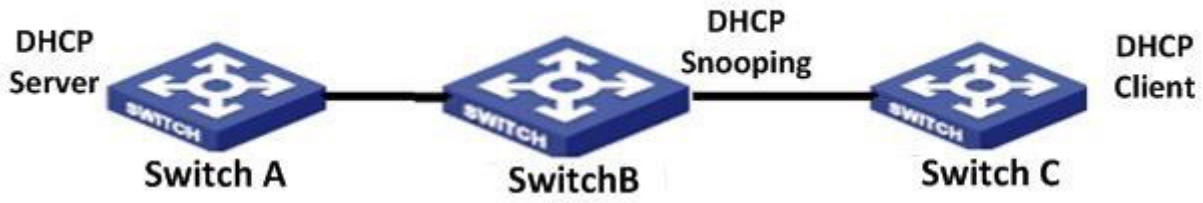


Рисунок 250 Пример типовой конфигурации

DHCP ➢ Конфигурация коммутатора A:

1. Создайте VLAN1 и настройте IP-адрес: 100.1.1.156;
2. Откройте вкладку состояния сервера DHCP VLAN 1, как показано на рисунке 180.
3. Создайте пул адресов pool-1;

4. Выберите тип пула адресов Network; IP-адрес: 33.1.1.6; маска: 255.0.0.0;

➢Конфигурация коммутатора B:

1. Создайте VLAN1 и настройте IP-адрес: 100.1.1.180;
2. Включите DHCP Snooping;
3. Настройте порт 1 как доверенный, как показано на рисунке 191.
4. Включите глобальную функцию IP Source Guard, как показано на рисунке 245;
5. Включите функцию IP Source Guard для порта 2, как показано на рисунке 246; ➢ Конфигурация коммутатора C:

1. Создайте VLAN1 и включите клиент DHCP;
2. Коммутатор A назначает IP-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

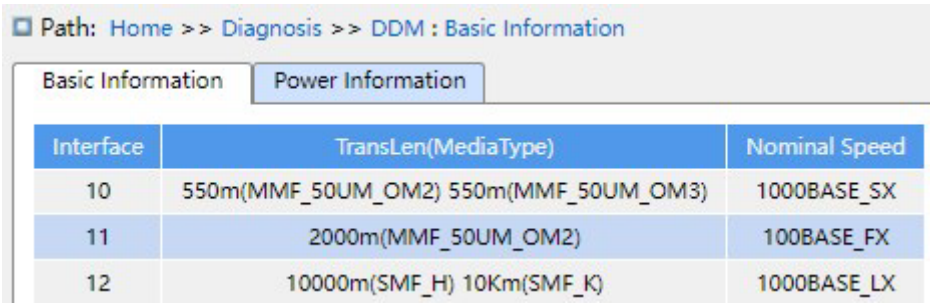
9.7.1 Введение

Цифровая диагностика является эффективным методом контроля важных рабочих параметров оптических модулей. Параметры, подлежащие контролю, включают оптическую мощность передачи, оптическую мощность приема, температуру, рабочее напряжение, ток смещения и аварийные сигналы. Благодаря функции цифровой диагностики оптического модуля блок управления сетью может получить доступ к оптическому модулю через двухпроводную последовательную шину и контролировать температуру, рабочее напряжение, ток смещения, передаваемую оптическую мощность и получаемую оптическую мощность модуля в реальном времени.

9.7.2 Настройка через веб-интерфейс

1. Основные сведения

По указанному ниже пути щелкните, чтобы просмотреть основную информацию об оптическом модуле, вставленном в устройство, как показано на следующем рисунке.


Path: Home >> Diagnosis >> DDM : Basic Information

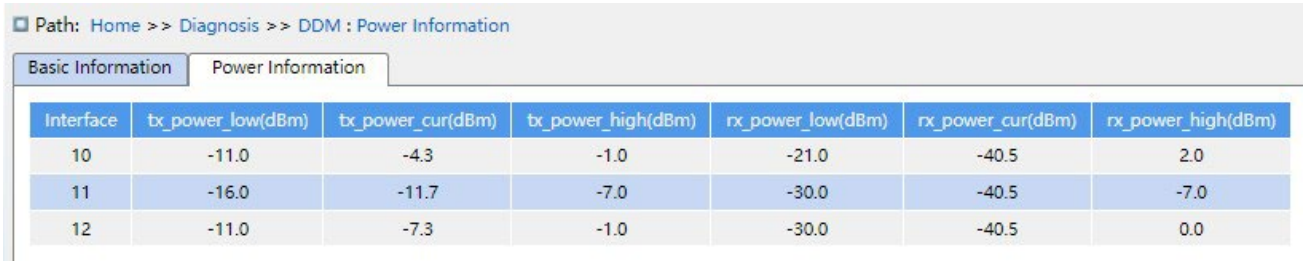
Basic Information | Power Information

Interface	TransLen(MediaType)	Nominal Speed
10	550m(MMF_50UM_OM2) 550m(MMF_50UM_OM3)	1000BASE_SX
11	2000m(MMF_50UM_OM2)	100BASE_FX
12	10000m(SMF_H) 10Km(SMF_K)	1000BASE_LX

Рисунок 251 Основные сведения об оптическом модуле

2. Сведения о мощности

По указанному ниже пути щелкните, чтобы просмотреть информацию о мощности для оптического модуля, как показано на следующем рисунке.


Path: Home >> Diagnosis >> DDM : Power Information

Basic Information | Power Information

Interface	tx_power_low(dBm)	tx_power_cur(dBm)	tx_power_high(dBm)	rx_power_low(dBm)	rx_power_cur(dBm)	rx_power_high(dBm)
10	-11.0	-4.3	-1.0	-21.0	-40.5	2.0
11	-16.0	-11.7	-7.0	-30.0	-40.5	-7.0
12	-11.0	-7.3	-1.0	-30.0	-40.5	0.0

Рисунок 252 Основные сведения об оптической мощности

Приложение: Аббревиатуры

Аббревиатур	Полное написание
ACE	Access Control Entry
ACL	Access Control List
ARP	Address Resolution Protocol
BootP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
CIST	Common and Internal Spanning Tree
CLI	Command Line Interface
CoS	Class of Service
CST	Common Spanning Tree
DHCP	Dynamic Host Configuration Protocol
DHP	Dual Homing Protocol
DNS	Domain Name System
DRP	Distributed Redundancy Protocol
DSCP	Differentiated Services CodePoint
DST	Daylight Saving Time
EAPOL	Extensible Authentication Protocol over LAN
GARP	Generic Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
GVRP	GARP VLAN Registration Protocol
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IGMP Snooping	Internet Group Management Protocol Snooping
IST	Internal Spanning Tree

LACP	Link Aggregation Control Protocol
LACPDU	Link Aggregation Control Protocol Data Unit
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
MIB	Management Information Base
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
NAS	Network Access Server
NetBIOS	Network Basic Input/Output System
NMS	Network Management Station
NTP	Network Time Protocol
OID	Object Identifier
PCP	Priority Code Point
PVLAN	Private VLAN
QCL	QoS Control List
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RMON	Remote Network Monitoring
RSTP	Rapid Spanning Tree Protocol
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SP	Strict Priority
SSH	Secure Shell
SSL	Secure Sockets Layer
SSM	Source Specific Multicast
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

USM	User-Based Security Model
VLAN	Virtual Local Area Network
WINS	Windows Internet Naming Service
WRR	Weighted Round Robin

Контакты

Для получения технической поддержки пишите на наш адрес электронной почты: *support@kyland-rus.ru*

Офис продаж: *sales@kyland-rus.ru*

Для получения информации об оборудовании, документации, актуальной информации обращайтесь на сайт: *https://kyland-rus.ru/*