Промышленный коммутатор серии SICOM3028GPT

Руководство по программной части

Версия 1.7

Сайт: https://kyland.com.ru/

Эл. почта:
sales@kyland.com.ru
support@kyland.com.ru

KYLAND

Содержание

Предисловие

Коммутаторы этой серии включают коммутаторы 2 уровня: SICOM3028GPT-L2GT, SICOM3028GPT-L2FT, SICOM3028GPT-L2G и SICOM3028GPT-L2F и коммутаторы 3 уровня: SICOM3028GPT-L3GT, SICOM3028GPT-L3FT, SICOM3028GPT-L3G и SICOM3028GPT-L3F.

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

Структура материала

Руководство пользователя содержи следующий материал:

Основное содержание	**Пояснения**
1. Введение	➢ Обзор ➢ Модели изделия ➢ Функции программного обеспечения
2. Доступ к коммутатору	➢ Варианты представления ➢ Доступ к коммутатору через порт консоли ➢ Доступ к коммутатору через Telnet ➢ Доступ к коммутатору через веб-интерфейс
3. Информация об устройстве	Основные сведения о коммутаторе
4. Обслуживание коммутатора	➢ Сохранение текущей конфигурации ➢ Загрузка настроек по умолчанию ➢ Перезагрузка ➢ Обновление программного обеспечения (по FTP, TFTP, SFTP) ➢ Выбор версии программного обеспечения

5. Основная конфигурация устройства	➢ Основная конфигурация (Основная конфигурация, настройка часов) ➢ Настройка управления пользователями ➢ Настройка порта (настройка физического порта, информация порта) ➢ Настройка QinQ ➢ Настройка PVLAN ➢ Зеркалирование портов ➢ Подавление штормов ➢ Изоляция портов ➢ Канал портов ➢ Настройка сервера Telnet ➢ Настройка сервера SSH ➢ Настройка SSL
6. Расширенна конфигурация устройства	➢ Настройка ARP ➢ Настройка интерфейса Layer-3 ➢ SNMPv2c, SNMPv3 ➢ DT-Ring ➢ Настройка DRP ➢ STP/RSTP ➢ MSTP ➢ Аварийная сигнализация ➢ Цифровая диагностика ➢ Настройка журнала ➢ Настройка статического маршрута* ➢ Настройка RIP* ➢ Настройка OSPF* ➢ Настройка сервера DHCP ➢ Настройка ACL

	➢ Настройка QoS ➢ Настройка IEC61850 ➢ Настройка GOOSE Trigger ➢ IGMP Snooping ➢ GMRP ➢ Статическая настройка многоадресной рассылки ➢ Настройка IGMP* ➢ PIM* ➢ LLDP ➢ RMON ➢ VRRP* ➢ Настройка SNTP ➢ Настройка NTP ➢ Настройка PTP# ➢ Настройка Sync Ethernet# ➢ Настройка GPS# ➢ Настройка IRIG-B# ➢ Настройка TACACS+ ➢ Настройка RADIUS ➢ Настройка IEEE802.1X ➢ Настройка аутентификации при входе ➢ Проверка канала связи ➢ Виртуальный кабельный тестер ➢ Настройка обнаружения петель ➢ Настройте функцию защита CRC порта.

Примечание:

* указывает, что функция недоступна в устройствах SICOM3028GPT-L2GT/SICOM3028GPT-L2FT/ SICOM3028GPT-L2G/SICOM3028GPT-L2F.

указывает, что функция недоступна в устройствах SICOM3028GPT-L2G/SICOM3028GPT-L2F/ SICOM3028GPT-L3G/SICOM3028GPT-L3F.

Условные обозначения в руководстве

1. Условные обозначения в тексте

Формат	**Пояснение**
< >	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
/	Выбор одного из двух или нескольких вариантов, разделенных знаком “/”. Например: “Добавление/вычитание” означает добавление или вычитание.
~	Обозначает диапазон. Например, “1~255” означает диапазон от 1 до 255.

2. Символы

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

Документация по изделию

Документация к промышленному коммутатору Ethernet SICOM3028GPT включает в себя:

Наименование документа	Содержание
SICOM3028GPT Series Industrial Ethernet Switches Hardware Installation Manual (Руководство пользователя по монтажу промышленного коммутатора серии SICOM3028GPT)	Описана конструкция оборудования, технические характеристики, способы монтажа и демонтажа.
SICOM3028GPT Industrial Ethernet Switch WebOperation Manual (Руководство пользователя по веб-интерфейсу промышленного коммутатора серии SICOM3028GPT)	Описаны функции ПО, способы настройки через веб-интерфейс и все функции.

Получение документации

Документацию по изделию можно получить:

- На сайте Kyland: https://kyland.com.ru/

1. Введение

1.1 Обзор

Коммутаторы этой серии, основанные на полностью гигабитной коммутационной платформе, являются первыми в мире промышленными Ethernet-коммутаторами, использующими технологию управления моделированием IEC61850 MMS, что обеспечивает унифицированное моделирование и управление. Благодаря ведущей в отрасли технологии синтеза тактовой частоты коммутаторы поддерживают IEEE1588-2008 PTP и протокол кольцевого резервирования IEC62439-6. Все они имеют модульную конструкцию для гибкой компоновки, расширяемый IRIG-B, GPS, последовательный порт, HSR и многие другие модули. Кроме того, коммутаторы соответствуют стандартам электроэнергетики IEC61850-3 и IEEE1613. Благодаря этим функциям коммутаторы хорошо подходят для индустрии интеллектуальных энергосистем.

Устройство поддерживает оптический модуль SFP с функцией цифровой диагностики, который используется для контроля температуры, напряжения питания, тока смещения лазера, передачи и приема оптической мощности. Используя такие измеренные параметры, блок управления может быстро обнаруживать ошибки, возникающие в оптических каналах, что помогает упростить техническое обслуживание и повысить надежность системы.

1.2 Функции программного обеспечения

Коммутаторы серии предоставляют обширный набор функций программного обеспечения, удовлетворяющих различные потребности заказчиков.

- Протоколы резервирования: STP/RSTP, MSTP, DT-Ring, VRRP и IEC62439-6
- Протоколы маршрутизации: OSPFv2, RIP, протокол статической маршрутизации
- Многоадресные протоколы: IGMP Snooping, GMRP и статическая многоадресная рассылка
- Атрибуты коммутации: VLAN, PVLAN, QoS и ARP
- Управление пропускной способностью: агрегация портов, ограничение скорости порта и подавление широковещательных штормов.

- Протоколы синхронизации: GPS, IRIG-B, PTP(IEEE1588-2008), ITU-T.G.8261/G.8262, SNTP и NTP
- Безопасность: IEEE802.1x, TACACS+, RADIUS, SSH, SSL, ACL, привязка MAC-адресов, изоляция портов и управление пользователями.
- Управление устройством: обновление программного обеспечения и передача файлов при помощи FTP/TFTP/SFTP, запись и загрузка журнала.
- Диагностика устройства: зеркалирование портов, LLDP, проверка соединения, обнаружение петель, защита CRC и цифровая диагностика
- Функция аварийной сигнализации: Сигнализация использования ЦП/памяти, сигнализация порта, сигнализация питания, сигнализация кольца, сигнализация высокой температуры, сигнализация низкой температуры, сигнализация трафика порта, сигнализация ошибки CRC/потери пакетов и сигнализация мощности SFP.
- Управление сетью: командная строка, Telnet, веб-интерфейс и ПО для управления сетью Kyvision, DHCP и SNMP v1/v2c/v3, мониторинг сети IEC61850.
- …

2. Доступ к коммутатору

Доступ к коммутатору осуществляется через:

- Порт консоли
- 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 представления или переключаться между представлениями с помощью следующих команд.

Таблица 1 Варианты представления

Приглашение	**Вариант представления**	**Функция**	**Команда для переключения представления**
Switch >	Общий режим	➢ Просмотр системной даты и времени. ➢ Просмотр версии программного обеспечения.	Введите **enable** для входа в привилегированный режим.
Switch#	Привилегированный режим	➢ Настройка системных часов и даты. ➢ Передача фала и обновление ПО. ➢ Удаление файла коммутатора. ➢ Настройка языка командной строки. ➢ Просмотр настроек коммутатора и информации о системе. ➢ Восстановление конфигурации по умолчанию. ➢ Сохранение текущей конфигурации. ➢ Перезагрузка коммутатора.	➢ Введите **config** 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** 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; <H.H.H.H> означает IP-адрес ; <H: H: H: H: H: H> означает MAC-адрес; word<1, 31> означает диапазон строк 1~31. Кроме того, символы ↑ и ↓ могут использоваться для просмотра недавно использованных команд.

2.2 Доступ к коммутатору через порт консоли

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.

Предупреждение:

Порты консоли поддерживают разъемы RJ45 и Mini USB. При необходимости можно выбрать любой из двух разъемов. Если выбрать разъем Mini USB для одного порта и разъем RJ45 для другого, при подключении обоих портов будет работать только консольный порт с разъемом Mini USB.

Разъем RJ45

1. Подключите 9-контактный последовательный порт ПК к консольному порту коммутатора с помощью консольного кабеля DB9-RJ45.

Разъем Mini-USB

1. Установите Mini USB_driver.exe. Программу можно найти в папке [Software download] на прилагаемом компакт-диске. Подключите USB-порт ПК к консольному порту коммутатора с помощью кабеля Mini USB.

2. Запустите HyperTerminal на рабочем столе Windows. Щелкните [Start] → [All Programs] → [Accessories] → [Communications] → [Hyper Terminal], как показано на рисунке 1.

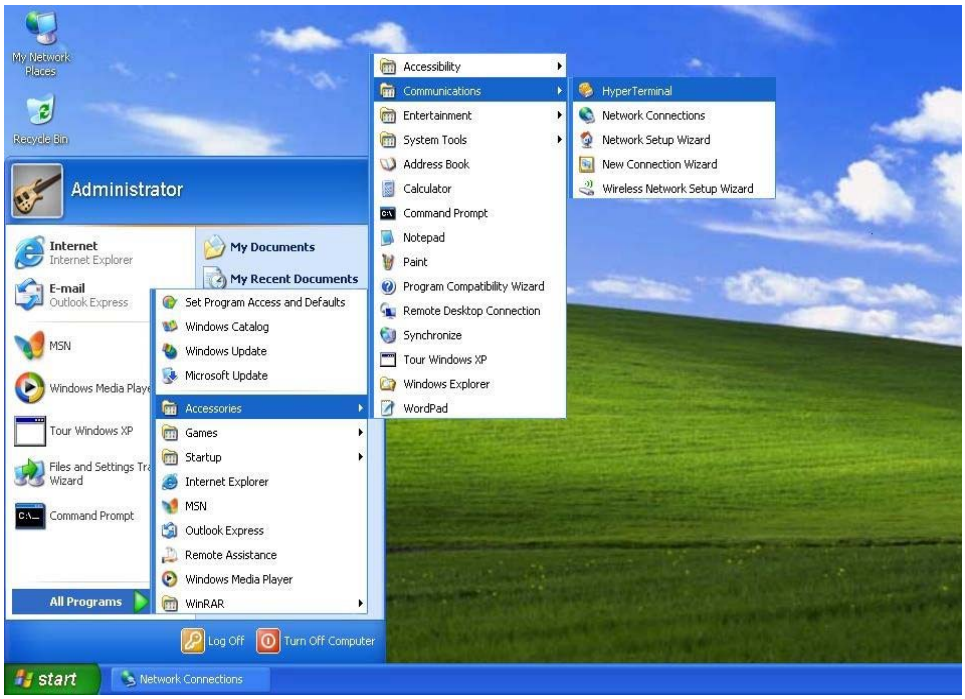


Рисунок 1 Запуск Hyper Terminal

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.

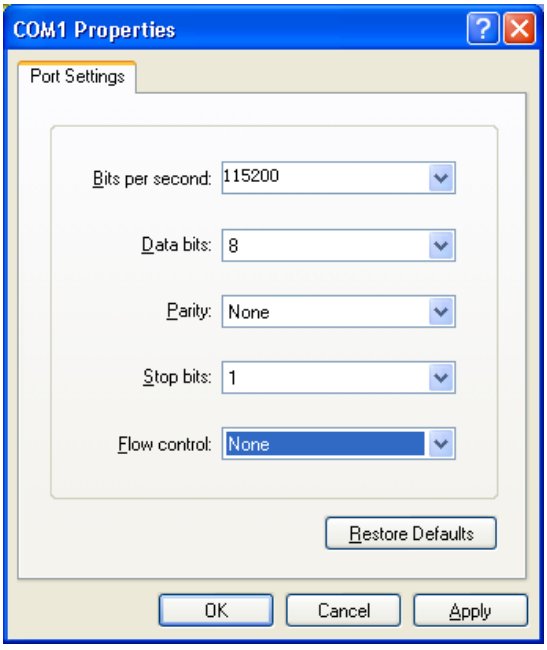


Рисунок 4 Настройка параметров порта

6. Щелкните кнопку <OK>, чтобы войти в интерфейс командной строки коммутатора. Введите пароль admin и нажмите <Enter>, чтобы войти в общий режим, как показано на рисунке 5.

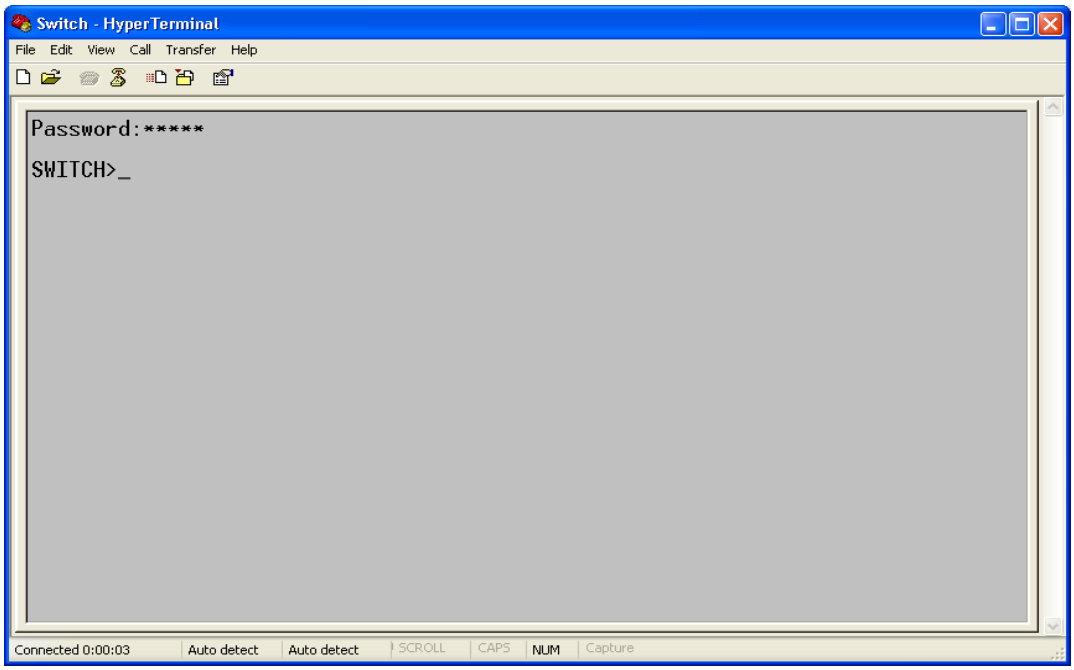


Рисунок 5 Интерфейс командной строки

7. Введите команду enable 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 6.

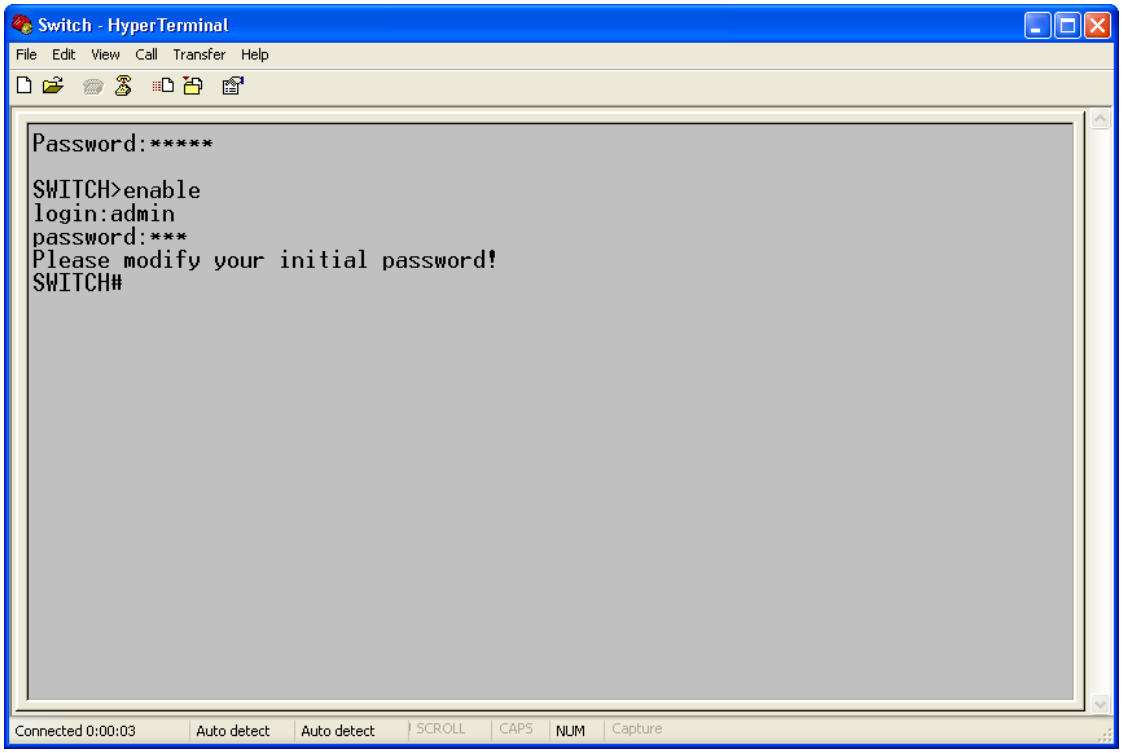


Рисунок 6 Привилегированный режим

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 7. IP-адрес коммутатора Kyland по умолчанию 192.168.0.2.

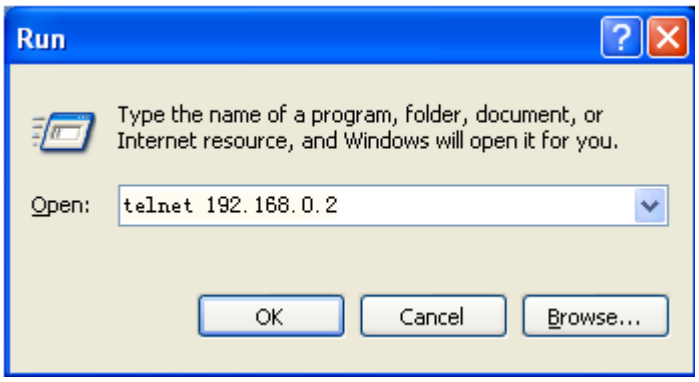


Рисунок 7 Доступ по Telnet

Примечание:

Для подтверждения IP-адреса обратитесь к разделу 6.2.1 IP-адрес коммутатора, 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 8.

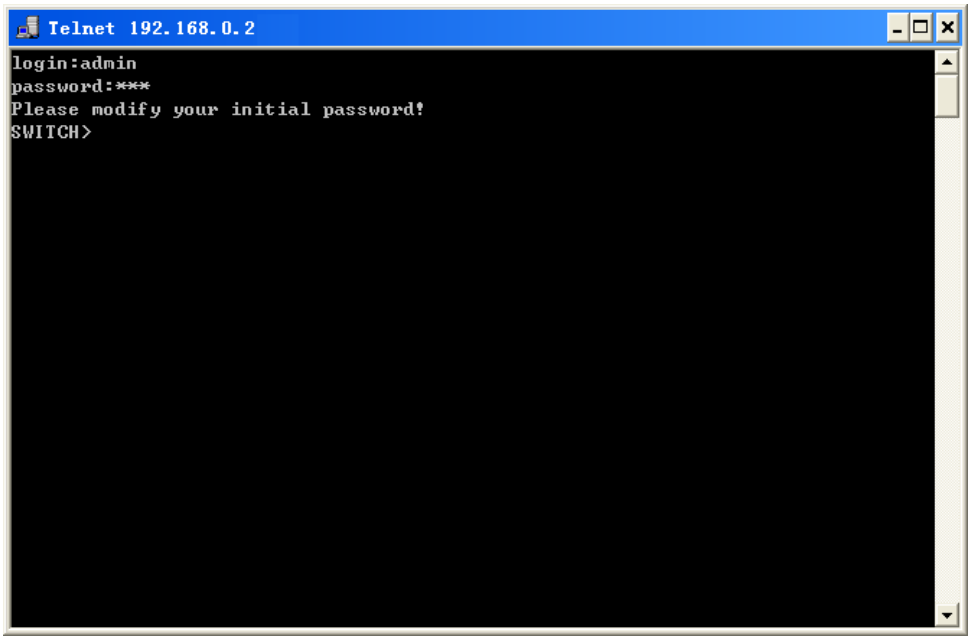


Рисунок 8 Интерфейс Telnet

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 9. 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 9 Вход через веб-интерфейс

По умолчанию отображается английский интерфейс. Можно выбрать <中文>, чтобы изменить язык интерфейса на китайский.

Примечание:

Для подтверждения IP-адреса обратитесь к разделу 6.2.1 IP-адрес коммутатора, чтобы узнать, как получить IP-адрес.

2. Появится приглашение изменить исходный пароль, щелкните кнопку <OK>.

3. После успешного входа слева в окне интерфейса появится дерево навигации, как показано на рисунке 10.

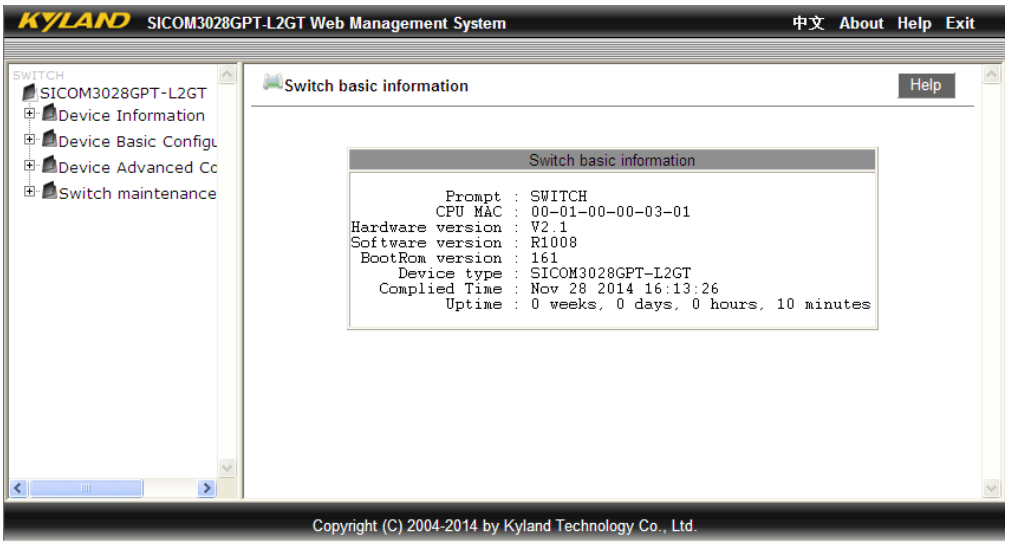


Рисунок 10 Веб-интерфейс

В правом верхнем углу можно щелкнуть <中文>, чтобы изменить язык на китайский, или <Exit> для выходат из веб-интерфейса.

3. Информация об устройстве

3.1 Основные сведения о коммутаторе

Основная информация о коммутаторе включает текст приглашения, MAC-адрес, версию оборудования, версию программного обеспечения, версию BootROM, тип устройства, дату компиляции и время работы. Щелкните [Device Information] → [Switch basic information] в дереве навигации, чтобы отобразить основную информацию о коммутаторе, как показано на рисунке 11.

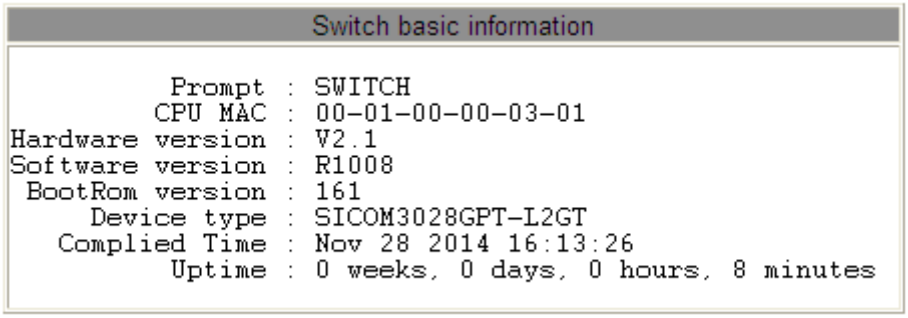


Рисунок 11 Основные сведения о коммутаторе

4. Обслуживание коммутатора

4.1 Сохранение текущей конфигурации

Щелкните [Switch maintenance] → [Save current running-config] в дереве навигации, чтобы сохранить текущую конфигурацию, как показано на рисунке 12.

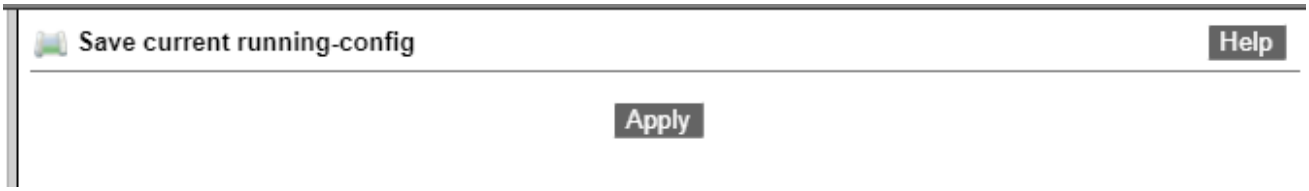


Рисунок 12 Сохранение текущей конфигурации

4.2 Загрузка настроек по умолчанию

Щелкните [Switch maintenance] → [Save current running-config] в дереве навигации, чтобы загрузить настройки по умолчанию, как показано на рисунке 13.

Рисунок 13 Загрузка настроек по умолчанию

4.3 Обновление программного обеспечения

Обновление программного обеспечения может помочь улучшить производительность коммутатора. Коммутаторам серии требуется обновить только один файл версии программного обеспечения. Он содержит не только версию системного программного обеспечения, но и версию программного обеспечения BootROM.

Для обновления версии программного обеспечения требуется использовать сервер FTP/TFTP/SFTP.

4.3.1 Обновление программного обеспечения 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 14.

Создайте имя пользователя и пароль, например, имя пользователя admin и пароль

123. Щелкните <OK>.

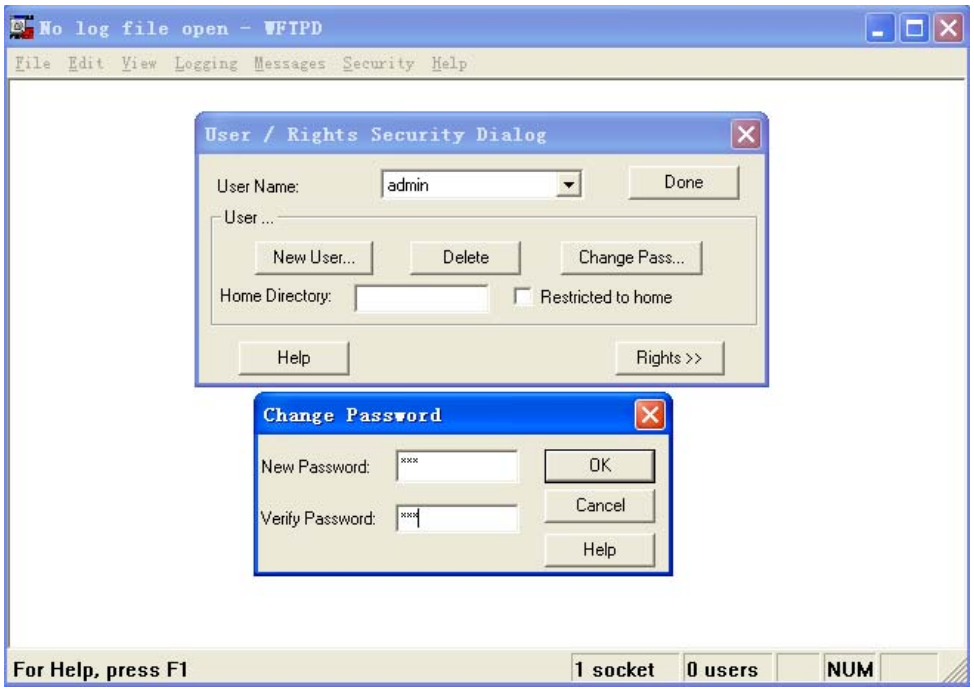


Рисунок 14 Создание нового пользователя FTP

2. Введите путь хранения файла обновления в Home Directory, как показано на рисунке 15. Щелкните <Done>.

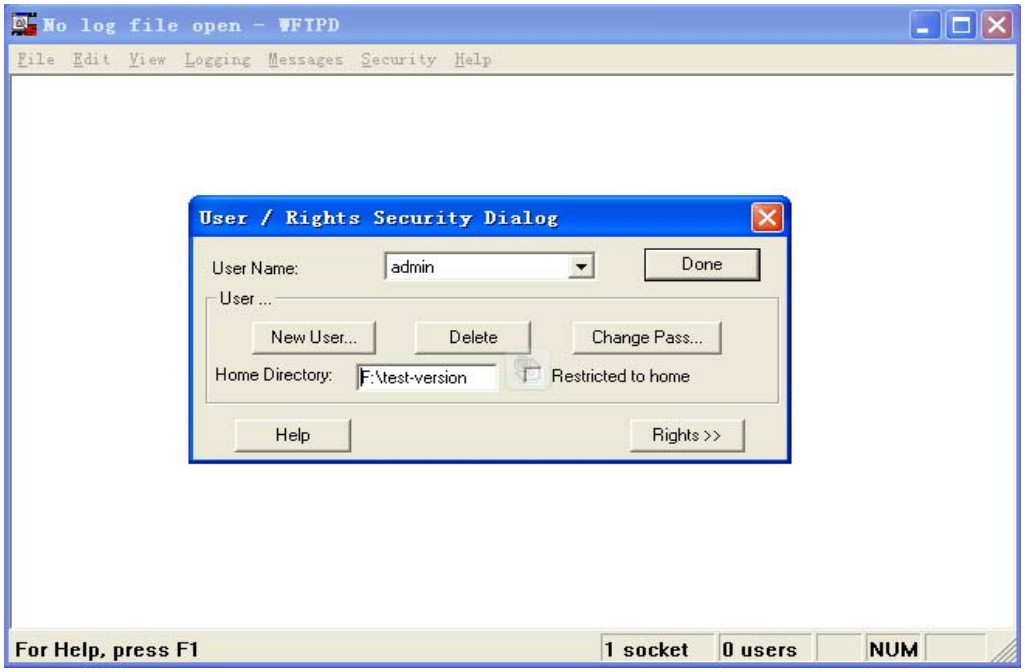


Рисунок 15 Местоположение файла

3. Щелкните [Switch maintenance] → [FTP software update] в дереве навигации, чтобы перейти на страницу обновления ПО по FTP, как показано на рисунке 16. Введите IP-адрес FTP-сервера, имя пользователя FTP, пароль и имя файла на сервере. Щелкните <Update>.

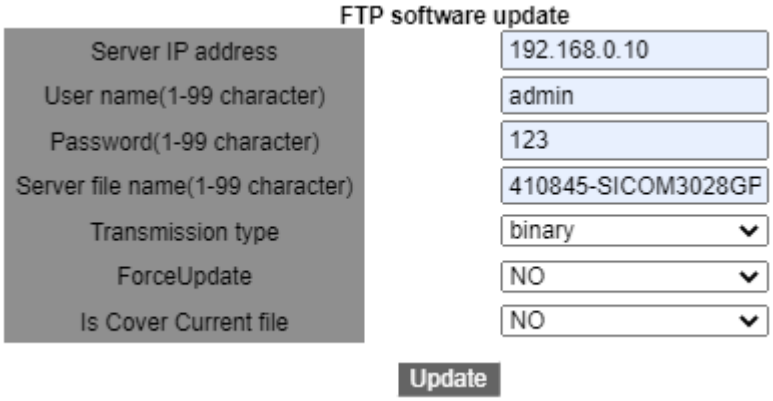


Рисунок 16 Обновление программного обеспечения по FTP

Transmission type

Варианты: **binary/ascii**

По умолчанию: **binary**

Функция: Выбор стандарта передачи.

Объяснение: **ascii** означает использование стандарта ASCII для передачи файла; **binary** означает использование двоичного стандарта для передачи файла.

ForceUpdate

Варианты: YES/NO

По умолчанию: NO

Функция: Выбор дейтсвия, если версия программного обеспечения не соответствует аппаратному обеспечению коммутатора.

Пояснение: NO означает отмену обновления программного обеспечения, если программное и аппаратное обеспечение не совпадают. YES означает продолжение обновления программного обеспечения, даже если программное и аппаратное обеспечение не совпадают. Однако это может привести к ненормальной работе системы или даже сбою загрузки.

Is Cover Current file

Варианты: YES/NO

По умолчанию: YES

Функция: перезаписывать ли напрямую текущую версию.

Описание: Если текущая версия перезаписывается, она начинает действовать после перезапуска устройства. Если текущая версия не перезаписывается, файл лишь загружается на устройство и используется в качестве резервного.

Внимание:

- Имя файла должно содержать расширение. В противном случае обновление может пройти неудачно.
- Файл версии программного обеспечения не является текстовым файлом, и для передачи нужно использовать двоичный стандарт.
- Чтобы гарантировать нормальную работу, выберите NO для ForceUpdate. То есть не обновляйте ПО, если версия ПО и оборудования не совпадают

4. Убедитесь в наличии нормальной связи между FTP-сервером и коммутатором, как показано на рисунке 17.

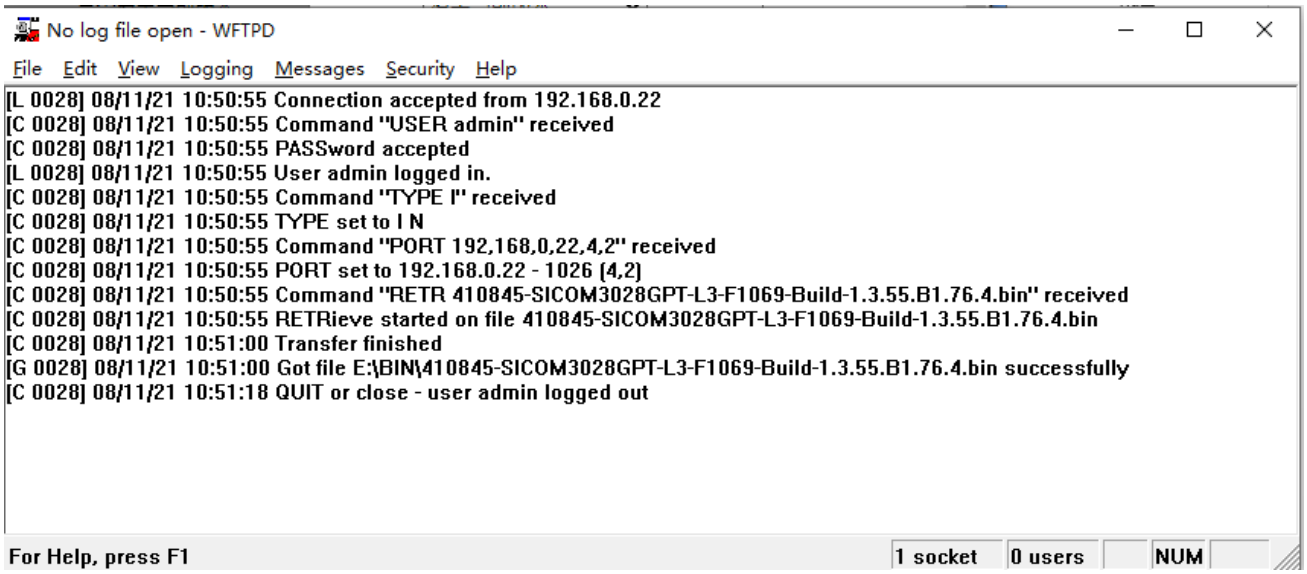


Рисунок 17 Нормальная связь между FTP-сервером и коммутатором

Предупреждение:

Чтобы отобразить информацию журнала обновлений, как показано на рисунке 17, нужно щелкнуть [Logging] → [Log

Options] in WFTPD в WFTPD и выбрать Enable Logging и информацию журнала для отображения.

5. Дождитесь завершения обновления, как показано на рисунке 18.

Рисунок 18 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:

- Во время обновления прошивки не выключайте FTP-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.

4.3.2 Обновление программного обеспечения по TFTP

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

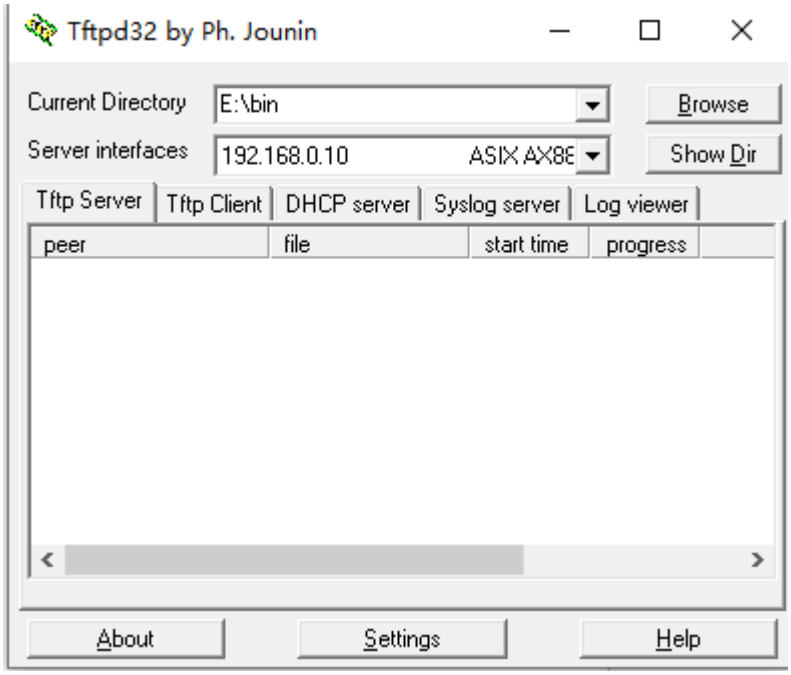


Рисунок 19 Конфигурация TFTP-сервера

1. В поле Current Directory выберите путь хранения файла обновления на сервере. Введите IP-адрес сервера в поле Server interface.

2. Щелкните [Switch maintenance] → [TFTP software update] в дереве навигации, чтобы перейти на страницу обновления ПО по TFTP, как показано на рисунке 20. Введите IP-адрес FTP-сервера, имя пользователя FTP и имя файла на сервере. Щелкните <Update> и дождитесь завершения обновления.

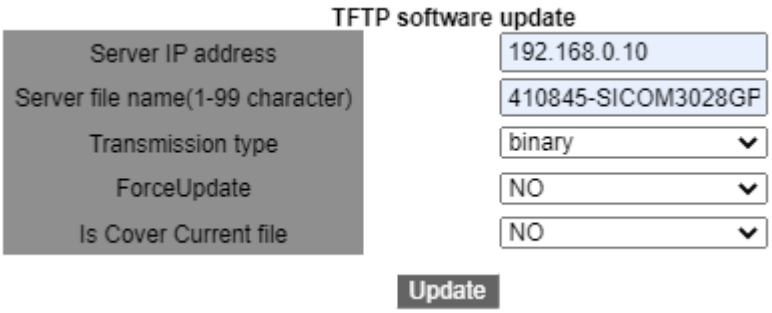


Рисунок 20 Обновление программного обеспечения по TFTP

Transmission type

Варианты: **binary/ascii**

По умолчанию: **binary**

Функция: Выбор стандарта передачи.

Объяснение: **ascii** означает использование стандарта ASCII для передачи файла; **binary** означает использование двоичного стандарта для передачи файла.

ForceUpdate

Варианты: YES/NO

По умолчанию: NO

Функция: Выбор дейтсвия, если версия программного обеспечения не соответствует аппаратному обеспечению коммутатора.

Пояснение: NO означает отмену обновления программного обеспечения, если программное и аппаратное обеспечение не совпадают. YES означает продолжение обновления программного обеспечения, даже если программное и аппаратное обеспечение не совпадают. Однако это может привести к ненормальной работе системы или даже сбою загрузки.

Is Cover Current file

Варианты: YES/NO

По умолчанию: YES

Функция: перезаписывать ли напрямую текущую версию.

Описание: Если текущая версия перезаписывается, она начинает действовать после перезапуска устройства. Если текущая версия не перезаписывается, файл лишь загружается на устройство и используется в качестве резервного.

Внимание:

- Имя файла должно содержать расширение. В противном случае обновление может пройти неудачно.
- Файл версии программного обеспечения не является текстовым файлом, и для передачи нужно использовать двоичный стандарт.
- Чтобы гарантировать нормальную работу, выберите NO для ForceUpdate. То есть не обновляйте ПО, если версия ПО и оборудования не совпадают

3. Убедитесь в наличии нормальной связи между TFTP-сервером и коммутатором, как показано на рисунке 21.

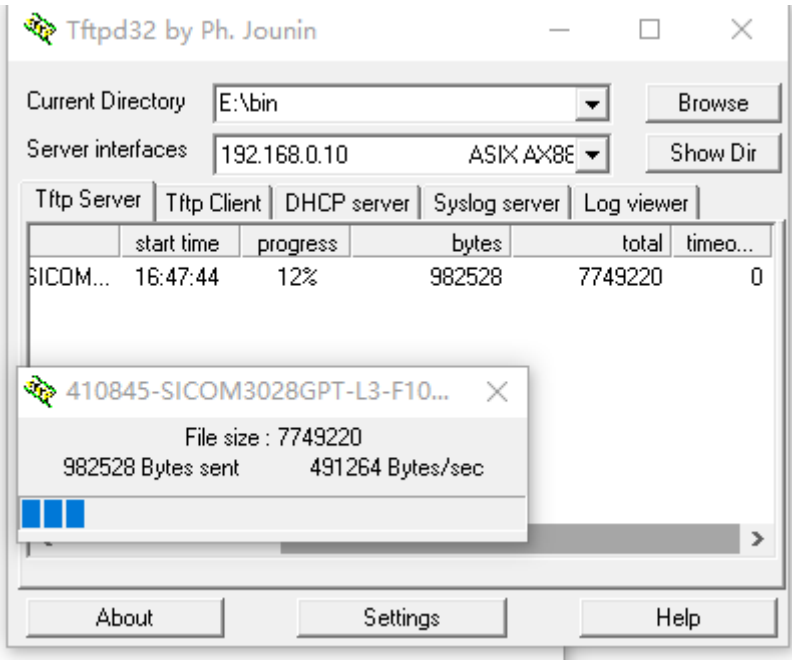


Рисунок 21 Нормальная связь между TFTP-сервером и коммутатором

4. Дождитесь завершения обновления, как показано на рисунке 22.

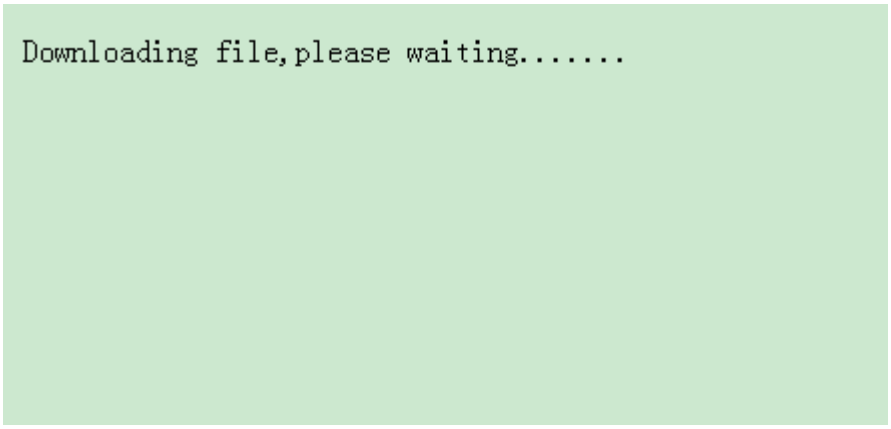


Рисунок 22 Ожидание завершения обновления

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.

4.3.3 Обновление программного обеспечения по SFTP

Протокол безопасной передачи файлов (SFTP) — это протокол передачи файлов на основе SSH. Он обеспечивает зашифрованную передачу файлов для гарантии безопасности.

В следующем примере MSFTP используется для описания конфигурации сервера SFTP и процесса обновления прошивки.

1. Добавьте пользователя SFTP, как показано на рисунке 23. Введите пользователя и пароль, например, admin и 123. Установите номер порта 22. Введите путь для сохранения файла версии прошивки в поле Root path.

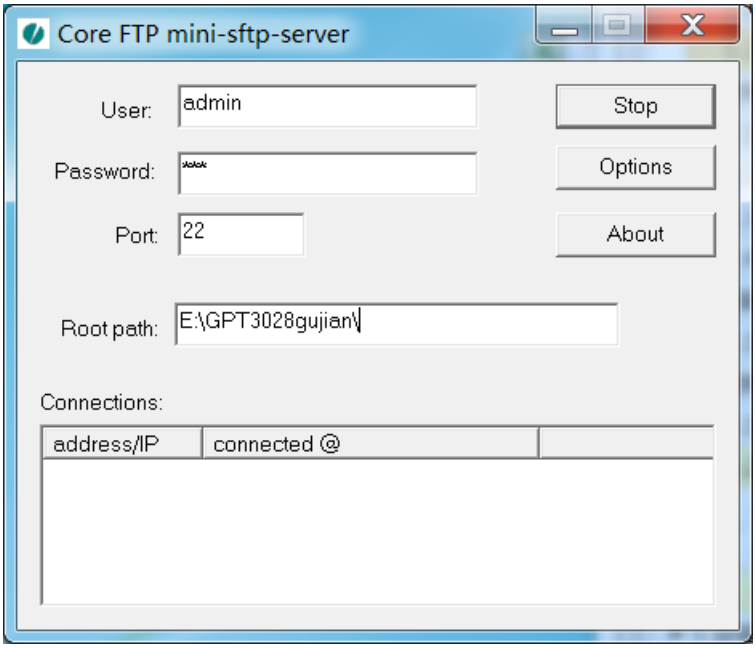


Рисунок 23 Добавление пользователя SFTP

2. Щелкните [Switch maintenance] → [SFTP software update] в дереве навигации, чтобы перейти на страницу обновления ПО по SFTP, как показано на рисунке 24.

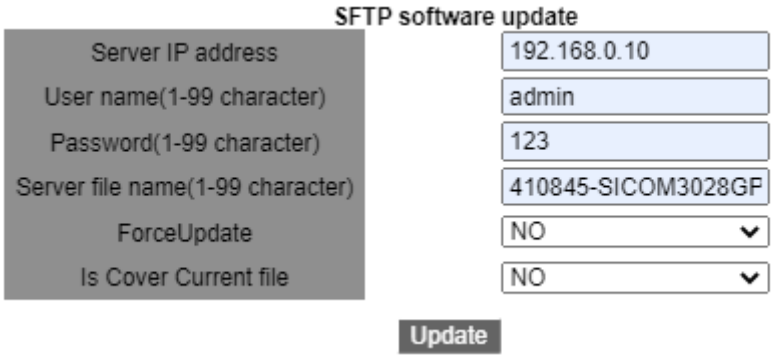


Рисунок 24 Обновление прошивки – SFTP

IP-адрес сервера

Формат: A.B.C.D

Описание: Настройте IP-адрес сервера SFTP.

{ User name, Password }

Диапазон: { 1~99 символов, 1~99 символов }

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

Имя файла на сервере

Диапазон: 1~99 символов

Описание: Укажите имя сохраненного на сервере SFTP файла прошивки.

ForceUpdate

Варианты: YES/NO

По умолчанию: NO

Функция: Выбор дейтсвия, если версия программного обеспечения не соответствует аппаратному обеспечению коммутатора.

Пояснение: NO означает отмену обновления программного обеспечения, если программное и аппаратное обеспечение не совпадают. YES означает продолжение обновления программного обеспечения, даже если программное и аппаратное обеспечение не совпадают. Однако это может привести к ненормальной работе системы или даже сбою загрузки.

Is Cover Current file

Варианты: YES/NO

По умолчанию: YES

Функция: перезаписывать ли напрямую текущую версию.

Описание: Если текущая версия перезаписывается, она начинает действовать после перезапуска устройства. Если текущая версия не перезаписывается, файл лишь загружается на устройство и используется в качестве резервного.

Внимание:

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

3. Когда обновление будет завершено, как показано на рисунке 25, активируйте версию программного обеспечения и перезагрузите устройство, откройте страницу System Information, чтобы проверить, успешно ли выполнено обновление и активна ли новая версия.

```
Write "SICOM3028G-R0001-Build.1.3.45.B3.1.4.bin" 70.7 %
Write "SICOM3028G-R0001-Build.1.3.45.B3.1.4.bin" 72.6 %
Write "SICOM3028G-R0001-Build.1.3.45.B3.1.4.bin" 74.4 %
Write "SICOM3028G-R0001-Build.1.3.45.B3.1.4.bin" 76.3 %
Write "SICOM3028G-R0001-Build.1.3.45.B3.1.4.bin" 78.2 %
Write "SICOM3028G-R0001-Build.1.3.45.B3.1.4.bin" 80.0 %
Write "SICOM3028G-R0001-Build.1.3.45.B3.1.4.bin" 82.9 %
Write "SICOM3028G-R0001-Build.1.3.45.B3.1.4.bin" 83.8 %
Write "SICOM3028G-R0001-Build.1.3.45.B3.1.4.bin" 85.6 %
Write "SICOM3028G-R0001-Build.1.3.45.B3.1.4.bin" 87.5 %
Write "SICOM3028G-R0001-Build.1.3.45.B3.1.4.bin" 89.4 %
Write "SICOM3028G-R0001-Build.1.3.45.B3.1.4.bin" 91.2 %
Write "SICOM3028G-R0001-Build.1.3.45.B3.1.4.bin" 93.1 %
Write "SICOM3028G-R0001-Build.1.3.45.B3.1.4.bin" 95.9 %
Write "SICOM3028G-R0001-Build.1.3.45.B3.1.4.bin" 96.8 %
Write "SICOM3028G-R0001-Build.1.3.45.B3.1.4.bin" 98.7 %
Write "SICOM3028G-R0001-Build.1.3.45.B3.1.4.bin" 100.0 %
write to flash success
```

Рисунок 25 Обновление выполнено успешно

Внимание:

- При обновлении прошивки сервер SFTP должен находиться в рабочем состоянии.
- 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 Выбор версии программного обеспечения

Щелкните [Switch maintenance] → [Software Version Select] в дереве навигации, чтобы перейти на страницу Software Version Select, как показано на рисунке 26.

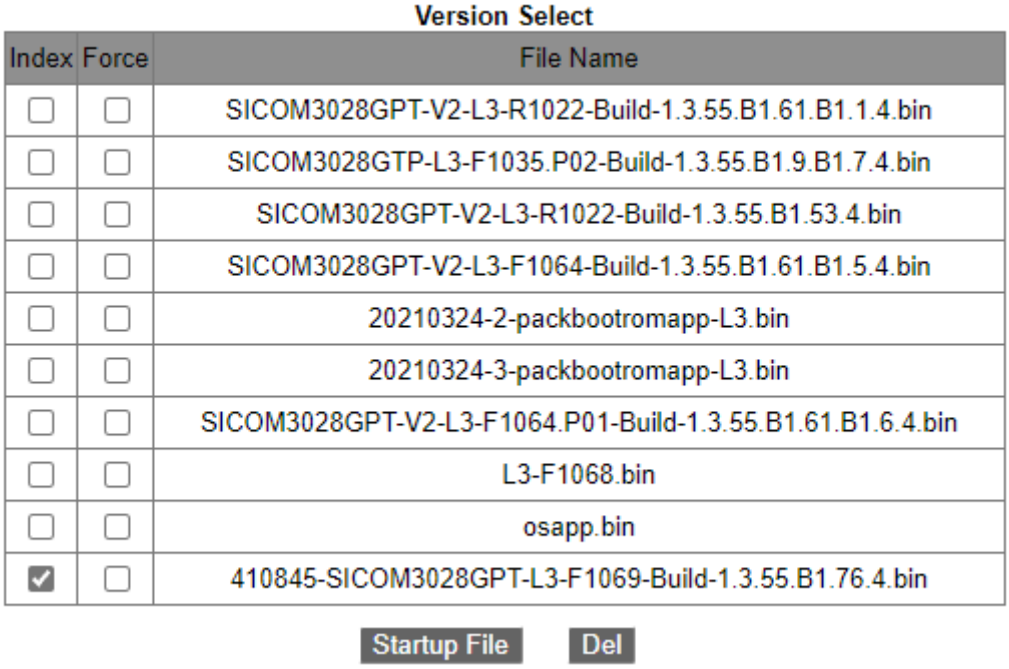


Рисунок 26 Выбор версии программного обеспечения

Index

Варианты: выбрать/отменить выбор

Функция: Выбор версии программного обеспечения.

Описание: Выберите одну версию и щелкните кнопку <Startup File>, настроив версию программного обеспечения, которая будет использована при следующем запуске. Если щелкнуть <Delete>, можно удалить выбранную версию.

Force

Варианты: выбрать/отменить выбор

Функция: При выборе принудительной установки проверка устройства не выполняется. Если принудительная установка не выбрана, файл будет проверен на совместимость и легальность. Если проверка не пройдена, установка не производится.

Предупреждение:

Если проверка легальности не выполнена, устройство может не запуститься.

4.5 Перезагрузка

Для перезагрузки устройства щелкните [Switch maintenance] → [Reboot] в дереве навигации, чтобы войти в интерфейс перезагрузки, как показано на рисунке 27.

Рисунок 27 Перезагрузка

Перед перезагрузкой подтвердите сохранение текущей конфигурации. Если выбрать "Yes", после перезагрузки коммутатор запустит текущую конфигурацию. Если выбрать «No", коммутатор запустит последнюю сохраненную конфигурацию. Если сохраненных конфигураций нет, после перезагрузки коммутатор восстановит конфигурацию по умолчанию.

5. Основная конфигурация устройства

5.1 Основная конфигурация коммутатора

Базовая конфигурация коммутатора включает имя хоста, сопоставление между хостом и IP-адресом и часы коммутатора.

5.1.1 Основные настройки

1. Задание имени хоста

Щелкните [Device Basic Configuration] → [Switch Basic Configuration] → [Basic Config], чтобы перейти на страницу основных настроек, как показано на рисунке 28.

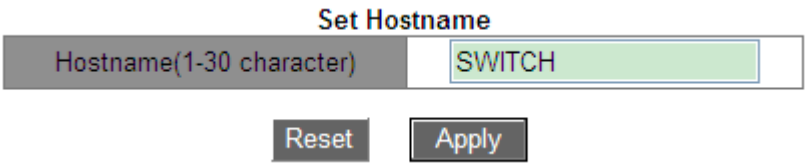


Рисунок 28 Задание имени хоста

Hostname

Диапазон: 0~30 символов

По умолчанию: SWITCH

Функция: Настройка приглашения в интерфейсе командной строки коммутатора.

Метод: Щелкните <Apply>, чтобы активировать новое имя хоста. Щелкните <Reset>, чтобы отменить текущую настройку и использовать предыдущее имя хоста.

2. Настройка соответствия между именем хоста и IP-адресом показана на рисунке 29.

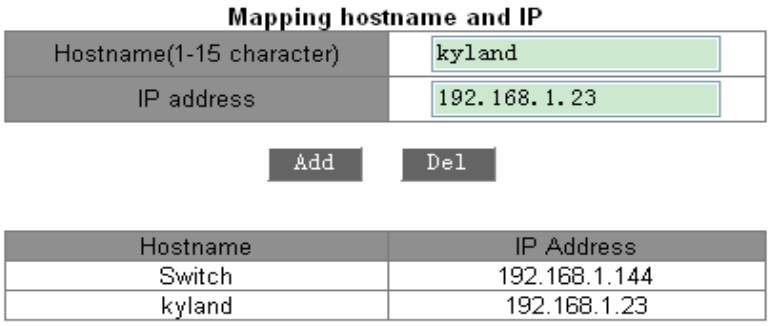


Рисунок 29 Настройка соответствия между именем хоста и IP-адресом

{Host name, IP address}

Формат: {1-15 символов, A.B.C.D}

Функция: Учитывая установленное соответствие, использовать имя хоста для доступа к соответствующему устройству. Метод: Введите допустимое имя хоста и IP-адрес. Щелкните <Add>, чтобы настроить запись сопоставления имени хоста и IP-адреса, или <Del>, чтобы удалить запись сопоставления.

Пример: После успешной установки сопоставления между именем хоста Switch и IP-адресом 192.168.0.4 можно пропинговать коммутатор с помощью команды **ping host Switch** вместо **ping 192.168.0.4**.

5.1.2 Настройка часов

Можно настроить системную дату и время. Коммутаторы серии поддерживают Real-Time Clock (RTC). Отсчет времени продолжается при отключении питания.

Чтобы в полной мере использовать время и экономить энергию, летом можно использовать летнее время (DST). Чтобы быть точным, переведите часы на час вперед летом.

Щелкните [Device Basic Configuration] →[Switch Basic Configuration]→[Clock configuration], чтобы перейти на страницу настройки часов, как показано на рисунке 30.

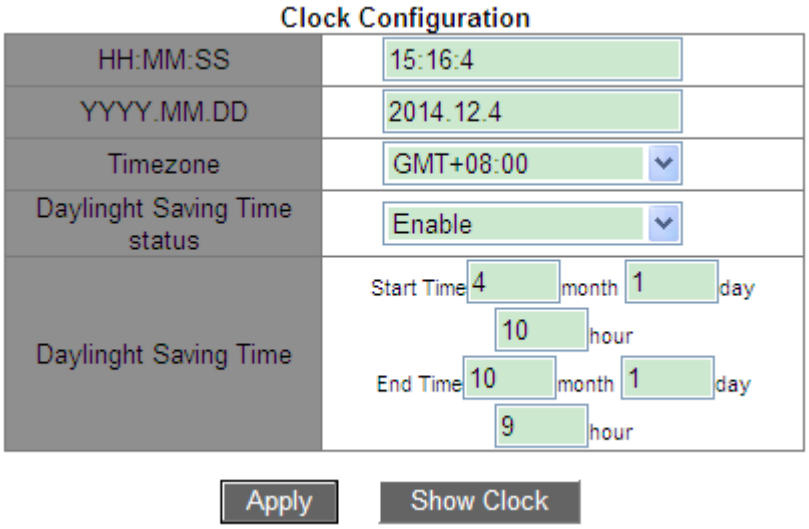


Рисунок 30 Настройка часов

HH:MM:SS

Диапазон: Значение HH находится в диапазоне от 0 до 23, а значения MM и SS — в диапазоне от 0 до 59.

YYYY.MM.DD

Диапазон: Значение YYYY находится в диапазоне от 1970 до 2099, значение MM — от 1 до 12, а значение DD — от 1 до 31.

Описание: Диапазон DD меняется в зависимости от месяца. Например, диапазон DD для марта — от 1 до 31, а для апреля — от 1 до 30. Вы можете настроить параметр в соответствии с реальной ситуацией.

Timezone

Функция: Выбор часового пояса.

Daylight Saving Time status

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение или выключение DST После включения DST часы будут переведены летом на один час вперед.

Daylight Saving Time

Настройка отрезка времени для перехода на летнее время.

Предупреждение:

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

Например, летнее время с 10:00:00 1 апреля до 9:00:00 1 октября.

Зимнее время идет до 10:00:00 1 апреля. Затем часы переводятся на 11:00:00, и начинается летнее время. Летнее время идет до 9:00:00 1 октября. Затем часы переводятся назад на 8:00:00 зимнего времени.

5.2 Настройка управления пользователями

Чтобы избежать проблем с безопасностью, вызванных незаконными пользователями, коммутаторы данной серии обеспечивают иерархическое управление пользователями. Коммутатор обеспечивает различные права работы в зависимости от уровня пользователя, удовлетворяя разнообразные требования к управлению доступом. Доступны три уровня пользователя, как показано в таблице 2.

Таблица 2 Уровень пользователей

Уровень пользователей	**Описание**
Guest	Самый низкий уровень, гостевые пользователи могут только просматривать конфигурацию коммутатора, но не могут проводить настройку или модификацию. Пользователи с уровнем Guest не могут получить доступ к следующим функциям: обновление программного обеспечения, управление пользователями, передача файлов, перезагрузка, сохранение текущей конфигурации и загрузка параметров по умолчанию.

System	Средний уровень, пользователи с уровнем System имеют определенные права для доступа и настройки. Пользователи с уровнем System не могут получить доступ к следующим функциям: обновление программного обеспечения, управление пользователями, передача файлов, перезагрузка и загрузка параметров по умолчанию. Примечание: Пользователь с уровнем System может изменить пароль текущего пользователя.
Admin	Самый высокий уровень, пользователи с уровнем Admin имеют права на выполнение всех функций.

5.2.1 Настройка через веб-интерфейс

1. Настройка пользователей

Щелкните [Device Basic Configuration] →[User Configuration]→[User Configuration], чтобы перейти на страницу настройки пользователей, как показано на рисунке 31.

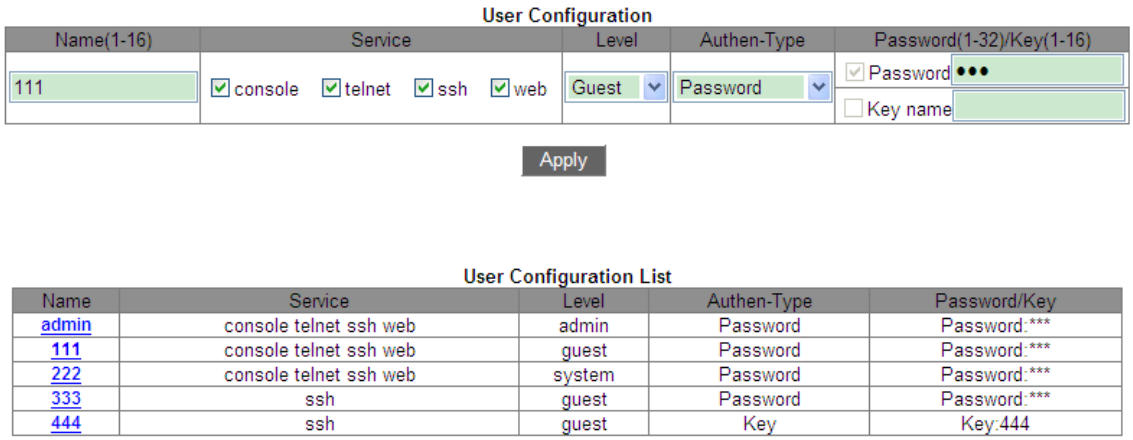


Рисунок 31 Настройка пользователей

Name

Диапазон: 1~16 символов

Service

Варианты: console/telnet/ssh/web

Функция: Выбор режима доступа к коммутатору для текущего пользователя. Можно выбрать один или несколько режимов доступа.

Level

Варианты: Guest/System/Admin

По умолчанию: Guest

Варианты: Выберите уровень пользователя, пользователи разных уровней имеют разные права.

Authen-Type

Варианты: Password/Key/Password or Key

По умолчанию: Password

Функция: Выбор типа аутентификации, который будет использоваться при доступе текущего пользователя к коммутатору. При выборе **Password** необходимо настроить опцию **Password**. При выборе **Key** необходимо настроить опцию **Key name**.

Password

Диапазон: 1~32 символа

Функция: Настройка пароля, который будет использоваться при доступе текущего пользователя к коммутатору.

Key name

Функция: Выбор имени ключа, которое будет использоваться при доступе текущего пользователя к коммутатору в режиме ssh.

Примечание:

- В настоящее время console/telnet/web не поддерживает режим аутентификации на основе ключа.

  Поэтому, когда тип подключения console/telnet/web, не выбирайте аутентификацию на основе ключа в качестве типа аутентификации.

- ssh поддерживает два режима аутентификации: аутентификацию на основе пароля и аутентификацию на основе ключа.
- Коммутатор поддерживает не более девяти пользователей.
- При наличии нескольких пользователей с правами администратора пользователь по умолчанию может быть удален, а последний пользователь с правами администратора не может быть удален.

  Пользователя по умолчанию admin удалить нельзя. Службу по умолчанию (console, telnet, ssh, web) и уровень (уровень администратора) этого пользователя изменить нельзя, но пароль по умолчанию (123) можно изменить.
- Сведения о режиме доступа console/telnet/web см. в разделе 2 Доступ к коммутатору.
- Сведения о режиме доступа ssh см. в разделе 5.12 Настройка сервера SSH.

2. Изменение и удаление информации пользователя

Щелкните запись пользователя в списке настроек пользователей на рисунке 31.

Можно изменить или удалить настройки пользователя, как показано на рисунке 32.

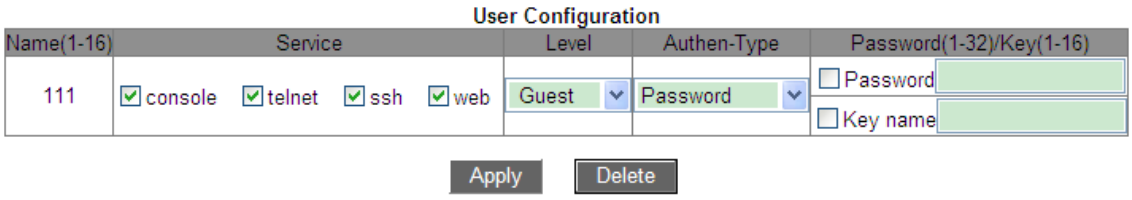


Рисунок 32 Изменение и удаление информации пользователя

3. Настройка ключа SSH

Щелкните [Device Basic Configuration] →[User Configuration]→[SSH Key Configuration], чтобы перейти на страницу настройки ключа SSH, как показано на рисунке 33.

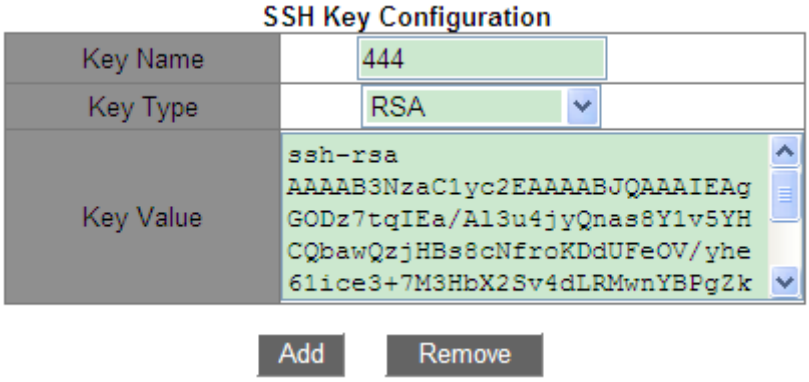


Рисунок 33 Настройка ключа SSH

Key name

Диапазон: 1~16 символов

Key Type

Обязательная настройка: RSA

Коммутаторы этой серии поддерживают только алгоритм RSA.

Key Value

Формат: {algorithm name, public key, key info}

Algorithm name: ssh-rsa | ssh-dsa

Public key: основан на 64 кодах и имеет длину менее 2048 байт Key

info: дополнительная информация о ключе

Функция: Настройка открытого ключа, соответствующего клиенту. Как правило, открытый ключ генерируется программным обеспечением Puttygen и копируется в значение ключа сервера, закрытый ключ сохраняется в клиенте.

4. Изменение пароля текущего пользователя

Щелкните [Device Basic Configuration] →[User Configuration]→[Modify Password], чтобы перейти на страницу изменения пароля, как показано на рисунке 34.

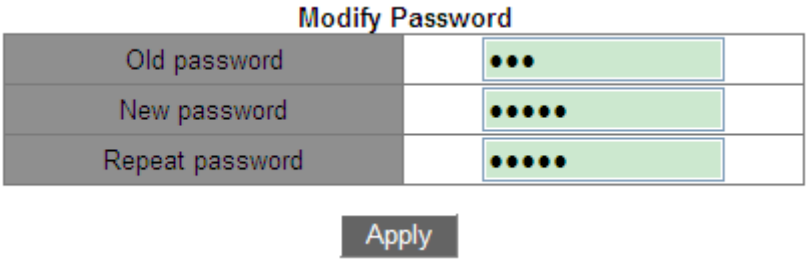


Рисунок 34 Изменение пароля

New password/Repeat password

Диапазон: 1~32 символа

5. Настройка таймаутов для режимов доступа к коммутатору

Щелкните [Device Basic Configuration] →[User Configuration]→[Timeouts Configuration], чтобы перейти на страницу настройки, как показано на рисунке 35.

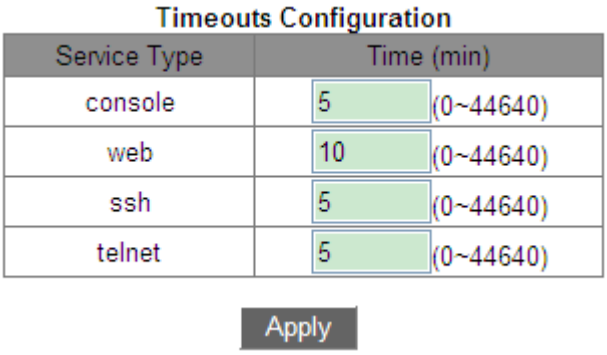


Рисунок 35 Настройка таймаутов

Time

Диапазон: 0~44640 мин

По умолчанию: 5 мин для командной строки/ssh/telnet, 10 мин для веб-интерфейса

Функция: Настройка времени ожидания входа пользователя и времени отключения. Отсчет времени начинается, когда пользователь завершит все настройки, и система автоматически выйдет из режима доступа, когда время истечет. Когда время установлено на 0, пользовательская функция тайм-аута и отключения выключена. В этом случае сервер не будет определять, истекло ли время входа пользователя в систему, и поэтому пользователь не выйдет из текущего режима входа.

6.WEB Server Security IP

Щелкните [Device Basic Configuration] →[User Configuration]→[WEB Server Security IP], чтобы перейти на страницу WEB Server Security IP, как показано на рисунке 36.

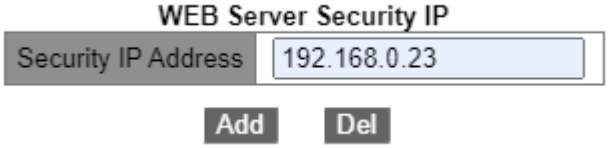


Рисунок 36 Страница WEB Server Security IP

Безопасный IP-адрес

Формат: A.B.C.D

Функция: Настройка безопасного IP-адреса для входа в систему через веб-интерфейс, когда коммутатор работает в качестве веб-сервера.

Описание: Если безопасный IP-адрес не установлен, ограничения на IP-адрес веб-клиента отсутствуют. После задания безопасных IP-адресов только клиент с безопасным IP-адресом может войти в систему и настроить коммутатор через веб-интерфейс.

Коммутатор поддерживает не более 10 безопасных IP-адресов. По умолчанию безопасные IP-адреса не настроены.

После завершения настройки в списке WEB server Security IP list отображаются IP-адреса клиентов, которые могут выполнить вход в коммутатор, как показано на рисунке 37.

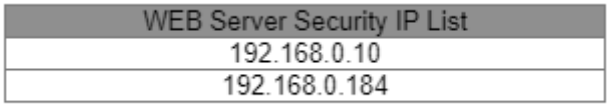


Рисунок 37 Список WEB Server Security IP List

5.3 Настройка порта

5.3.1 Настройка физического порта

5.3.1.1 Введение

В конфигурации физического порта вы можете настроить тип кабеля, состояние управления, скорость/режим и другую информацию.

5.3.1.2 Настройка через веб-интерфейс

Щелкните [Device Basic Configuration] → [Port configuration] → [Ethernet port configuration] → [Physical port configuration], чтобы перейти на страницу настройки порта, как показано на рисунке 38.

Port configuration

Port	Alias	Type	mdi	Status	Admin status	Speed/duplex status	Flow control	Linkup delay(unit,1/60 s)
1/1		GE	auto	down	no shutdown	auto	Invalid	0 (0-600)
1/2		GE	auto	down	no shutdown	auto	Invalid	0 (0-600)
1/3		GX	auto	down	no shutdown	auto	Invalid	0 (0-600)
1/4		GX	auto	down	no shutdown	auto	Invalid	0 (0-600)
2/1		GE	auto	down	no shutdown	auto	Invalid	0 (0-600)
2/2		GE	auto	down	no shutdown	auto	Invalid	0 (0-600)
2/3		GE	auto	down	no shutdown	auto	Invalid	0 (0-600)
2/4		GE	auto	down	no shutdown	auto	Invalid	0 (0-600)
3/1		GE	auto	down	no shutdown	auto	Invalid	0 (0-600)
3/2		GE	auto	down	no shutdown	auto	Invalid	0 (0-600)

Рисунок 38 Настройка физического порта

Port

Варианты: все порты коммутатора.

Описание: X/Y — формат имени порта; X — это номер слота для интерфейсного модуля, в котором находится порт, а Y — номер порта на интерфейсном модуле.

Alias

Диапазон: 1~64 символа

Функция: Настройка псевдонима для описания порта.

mdi

Варианты: auto/normal/across

По умолчанию: auto

Функция: Настройка типа кабеля для порта Ethernet.

Описание: auto означает автоматическое определение типа кабеля; across означает, что порт поддерживает только перекрестный кабель; normal означает, что порт поддерживает только прямой кабель.

Предупреждение:

Рекомендуется использовать вариант auto.

Admin Status

Варианты: shutdown/no shutdown

По умолчанию: no shutdown

Функция: Запрет/разрешение передачи данных через порт.

Описание: no shutdown означает, что порт включен и разрешает передачу данных; shutdown указывает на то, что порт отключен и запрещает передачу данных. Эта опция напрямую влияет на аппаратное состояние порта и запускает аварийные сигналы порта.

Speed/duplex status

Варианты: auto, 10M/Half, 10M/Full, 100M/Half, 100M/Full, 1000M/Half,1000M/Full

По умолчанию: auto

Функция: Настройка скорости связи и дуплексного режима порта.

Описание: Скорость порта и дуплексный режим поддерживают автосогласование и принудительную настройку. Если установлено значение auto, скорость порта и режим дуплекса будут автоматически согласовываться в соответствии со статусом подключения порта. Когда режим дуплекса порта изменяется с автоматического согласования на принудительный полный дуплекс или полудуплекс, скорость порта также будет изменена на принудительный режим. Рекомендуется установить для параметра значение auto, чтобы избежать проблем с подключением, вызванных несогласованной конфигурацией портов на обоих концах линии связи. Если для порта скорость или дуплекс установлены принудительно, убедитесь, что настройки скорости или режима дуплекса на обоих концах соединения одинаковы.

Предупреждение:

- Для порта 10/100Base-TX можно задать режим скорости/дуплекса auto, 10M/Half, 10M/Full,

  100M/Half или 100M/Full.

- Для порта 100Base-FX можно задать режим скорости/дуплекса только 100M/Full.
- Для порта 10/100/1000Base-TX можно задать режим скорости/дуплекса auto,

  10M/Half, 10M/Full, 100M/Half, 100M/Full, 1000M/Half или 1000M/Full.

- Режим скорости/дуплекса гигабитного оптоволоконного порта может быть установлен auto или 1000M/Full only.

Flow Control

Варианты конфигурации: Enable/disable

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.

Linkup delay

Диапазон: 0~600 (ед. изм: 1/60 с)

По умолчанию: 0 с

Функция: Настройка времени задержки подключения к порту. Оба конца соединения должны иметь одинаковую настройку параметра **Linkup delay.**

Можно просмотреть информацию о порте на основе конфигурации порта Ethernet и условий передачи данных, как показано на рисунке 39.

Port list

Port	Alias	Type	mdi	Status	Admin status	Speed	Mode	Flow control	Loopback	Linkup delay(unit,1/60 s)
1/1		GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	0
1/2		GE	auto	down	no shutdown	auto	auto	Invalid	no loopback	0
1/3		GX	auto	down	no shutdown	auto	auto	Invalid	no loopback	0
1/4		GX	auto	down	no shutdown	auto	auto	Invalid	no loopback	0
2/1	TCC	FE	auto	down	no shutdown	auto	auto	Invalid	no loopback	120
2/2		FE	auto	down	no shutdown	auto	auto	Invalid	no loopback	0
2/3		FE	auto	down	no shutdown	auto	auto	Invalid	no loopback	0
2/4		FE	auto	up	no shutdown	auto	auto	Invalid	no loopback	0
3/1		FX	auto	down	no shutdown	auto	auto	Invalid	no loopback	0
3/2		FX	auto	down	no shutdown	auto	auto	Invalid	no loopback	0
3/3		FX	auto	down	no shutdown	auto	auto	Invalid	no loopback	0
3/4		FX	auto	down	no shutdown	auto	auto	Invalid	no loopback	0
6/1		FE	auto	down	no shutdown	auto	auto	Invalid	no loopback	0
6/2		FE	auto	down	no shutdown	auto	auto	Invalid	no loopback	0
6/3		FE	auto	down	no shutdown	auto	auto	Invalid	no loopback	0
6/4		FE	auto	down	no shutdown	auto	auto	Invalid	no loopback	0

Рисунок 39 Список портов

5.3.2 Информация о порте

Щелкните [Device Basic Configuration] → [Port configuration] → [Port debug and maintenance]

→ [Show port information], чтобы перейти на страницу информации о порте. Она содержит состояние подключения порта, тип порта, статистику входных/выходных пакетов и другую информацию, как показано на рисунке 40.

Information Display

```
Ethernet2/3 is up, line protocol is up
Ethernet2/3 is layer 2 port, alias name is (null), index is 7
Hardware is Fast-Ethernet,  address is 00-01-00-00-03-09
PVID is 1
MTU 10240 bytes, BW 100000 Kbit
Encapsulation ARPA, Loopback  not set
Auto-duplex:  Negotiation  full-duplex,   Auto-speed:  Negotiation
100M bits
FlowControl is off,  MDI type is auto

Input and output rate statistics:
5 minute input rate 2935 bytes/sec, 29 packets/sec
5 minute output rate 4621 bytes/sec, 6 packets/sec
The last 5 second input rate 2701 bytes/sec, 29 packets/sec
The last 5 second output rate 698 bytes/sec, 5 packets/sec

Input packets statistics:
2162040 input packets, 217736548 bytes, 0 no buffer
80201 unicast packets, 116708 multicast packets, 1965131 broadcast packets
0 input errors, 0 CRC, 0 frame alignment, 0 overrun, 0 ignored,
0 abort, 0 length error , 0 pause frame

Output packets statistics:
136566 output packets, 93892260 bytes, 0 underruns
117989 unicast packets, 18527 multicast packets, 50 broadcast packets
0 output errors, 0 collisions , 0 pause frame

Input and output packets by length:
(64)          bytes:     818980, (65~127)      bytes:    1255746,
(128~255)     bytes:      81301,  (256~511)     bytes:      21617,
(512~1023)    bytes:      41904, (1024~10240) bytes:      79058
```

Рисунок 40 Информация о порте

5.4 Настройка VLAN

5.4.1 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.

5.4.2 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 3 показана структура кадра 802.1Q.

Таблица 3 Структура кадра 802.1Q

DA	SA	Заголовок 802.1Q				Длина/тип	Data	FCS
		Тип	PRI	CFI	VID			

4-байтовый заголовок 802.1Q в качестве тега VLAN добавляется к традиционному кадру данных Ethernet. Тип 16 бит. Используется для идентификации кадра данных, несущего тег VLAN. Значение равно 0x8100. PRI: три бита, определяющие приоритет пакета 802.1p.

CFI: один бит. 0 указывает на Ethernet, а 1 указывает на Token Ring.

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

Примечание:

- 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.

5.4.3 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. Тип порта

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

- Нетегированный порт VLAN: Пересылаемые нетегированным портом пакеты не имеют тегов VLAN. Нетегированные порты обычно используются для подключения к терминалам, не поддерживающим 802.1Q. По умолчанию все порты коммутатора являются нетегированным портами и принадлежат VLAN1.
- Тегированный порт Все пересылаемые тегированным портом пакеты имеют тег VLAN. Тегированные порты обычно используются для подключения сетевых передающих устройств.

2. Режим порта

- Access: В режиме access порт должен быть нетегированным и быть добавлен в одну VLAN; порт не может быть тегированным и добавленным в какую-либо VLAN.
- Trunk: В режиме trunk порт должен быть нетегированным и быть добавлен в VLAN PVID; порт может быть тегированным/нетегированным и добавленным в какую-либо другую VLAN.

3. PVID

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

PVID порта в режиме Access — это идентификатор VLAN, к которой принадлежит порт, и его нельзя настроить.

PVID порта в режиме Trunk может быть настроен как один из идентификаторов VLAN, разрешенных для порта.

Таблица 4 показывает, как коммутатор обрабатывает полученные и пересылаемые пакеты в зависимости от режима порта, типа порта и PVID.

Таблица 4 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>Тип порта</th><th>Обработка пакетов</th></tr>
<tr><td rowspan="2">Добавить теги PVID в пакеты:</td><td rowspan="2">➢ Если VLAN ID в пакете находится в списке разрешенных VLAN, принять пакет.
➢ Если VLAN ID в если VLAN ID в пакете не находится в списке разрешенных VLAN, отклонить пакет.</td><td>Нетегированный</td><td>Переслать пакет после удаления тега.</td></tr>
<tr><td>Тегированный</td><td>Сохранить тег и переслать пакет.</td></tr>
</table>

5.4.4 Настройка через веб-интерфейс

1. Создать или удалить VLAN.

Щелкните [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Create/Remove VLAN] → [VLAN ID allocation], чтобы перейти на страницу настройки VLAN, как показано на рисунке 41.

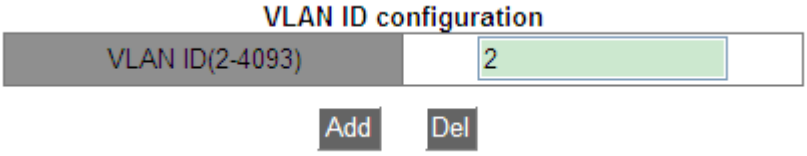


Рисунок 41 Создание/удаление VLAN

VLAN ID

Диапазон: 2~4093.

Функция: Разные идентификаторы VLAN используются, чтобы различать VLAN.

Описание: Коммутатор поддерживает не более 4093 VLAN.

Метод: Щелкните <Add>, чтобы создать VLAN; щелкните <Remove>, чтобы удалит указанную VLAN.

2. Настройте имя VLAN.

Щелкните [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Create/Remove VLAN] → [VLAN ID attribution configuration], чтобы перейти на страницу настройки имени VLAN, как показано на Figure 42.

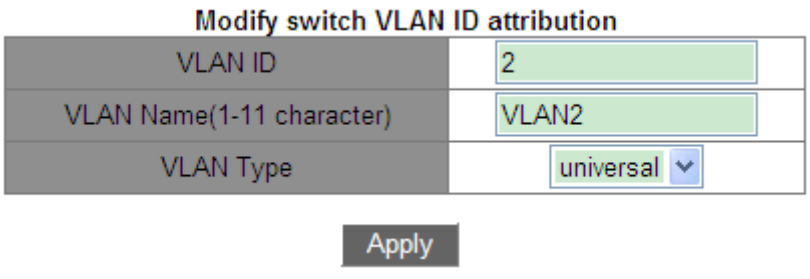


Рисунок 42 Настройка VLAN

VLAN ID

Варианты: все созданные VLAN

Функция: Ввод идентификатора VLAN, имя которой необходимо изменить.

VLAN Name

Диапазон: 1~11 символов

Функция: Ввод имени VLAN с указанным ID.

VLAN Type

Варианты: universal

По умолчанию: universal

После завершения настройки на странице VLAN ID Information отображается информация об атрибутах всех созданных VLAN, как показано на рисунке 43.

VLAN ID information

VLAN ID	VLAN Name	VLAN Type
1	default	universal
2	VLAN2	universal
100	VLAN100	universal
200	VLAN200	universal

Рисунок 43 Список VLAN

3. Настройка режима порта

Щелкните [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Port type configuration] → [Set port mode (Trunk/Access)], чтобы перейти на страницу настройки типа порта, как показано на рисунке 44.

Port mode configuration

Port	Type
2/1	access

Apply

Рисунок 44 Настройка типа порта

Port

Варианты: все порты коммутатора.

Type

Варианты: access/trunk

По умолчанию: access

Функция: Выбор режима для указанного порта. Каждый порт поддерживает только один режим.

После завершения настройки на странице Port mode configuration отображается информация о типах портов, как показано на рисунке 45.

Port mode configuration

Port	Type
1/1	access
1/2	access
1/3	access
1/4	access
2/1	access
2/2	access
2/3	access
2/4	access
4/1	access
4/2	access
4/3	access
4/4	trunk

Рисунок 45 Информация о типах портов

4. Назначение портов созданным VLAN.

Щелкните [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Allocate ports for VLAN] → [Allocate ports for VLAN], чтобы перейти на страницу настройки Access port VLAN, как показано на рисунке 46.

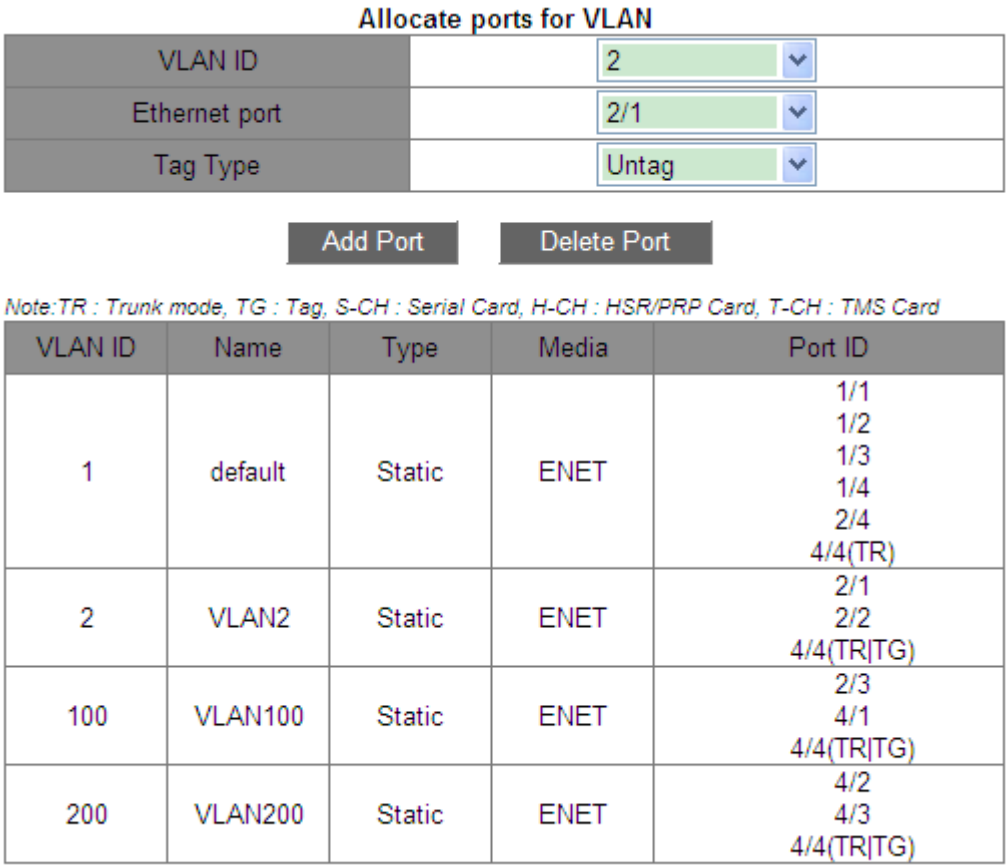


Рисунок 46 Назначение портов доступа для VLAN

Tag Type

Варианты: Tag/Untag

Функция: Выбор типа порта для добавления к VLAN.

Предупреждение:

- В режиме access порт должен быть нетегированным и быть добавлен в одну VLAN.
- В режиме trunk порт должен быть нетегированным и быть добавлен в VLAN PVID; порт может быть тегированным/нетегированным и добавленным в какую-либо другую VLAN.

5. Настройка PVID для порта Trunk.

Щелкните [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Trunk port configuration] → [VLAN setting for trunk port], чтобы перейти на страницу настройки Trunk port VLAN, как показано на рисунке 47.

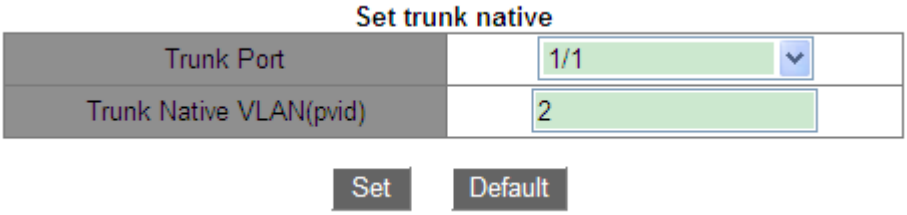


Figure 47 Настройка PVID порта Trunk

Trunk Port

Варианты: все порты Trunk

Trunk Native VLAN (pvid)

Варианты: все созданные VLAN

По умолчанию: 1

Функция: Настройка PVID для порта Trunk.

Описание: Независимо от того, существует ли порт в VLAN или существует в VLAN в виде нетегированного/тегированного, после указания PVID этот порт будет добавлен в VLAN в виде нетегированного.

Метод: Щелкните <Default>, чтобы восстановить значение PVID выбранного порта Trunk равным 1.

6. Настройте VLAN для порта, как показано на рисунке 48.

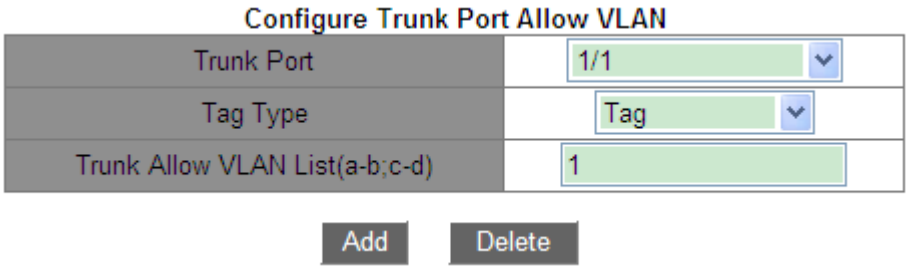


Рисунок 48 Настройка VLAN для порта Trunk

Trunk Port

Варианты: все порты Trunk

Tag Type

Варианты: Tag/Untag

Функция: Выбор типа порта Trunk для добавления к VLAN.

Trunk Allow VLAN List

Варианты: все созданные VLAN

По умолчанию: все созданные VLAN

Функция: Настройка VLAN для выбранного порта Trunk

После завершения настройки отображается информация VLAN всех портов Trunk, как показано на рисунке 49.

Trunk Port	Native VLAN	Allow VLAN List(Tag)	Allow VLAN List(Untag)
1/1	2	1	2;100
4/4	1	2;100;200	1

Рисунок 49 Настройка VLAN портов Trunk

7. Настройте правил обработки входящего трафика VLAN для порта.

Щелкните [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Enable/Disable VLAN ingress rule] → [Enable/Disable VLAN ingress rule], чтобы перейти на страницу настройки правил обработки входящего трафика VLAN, как показано на рисунке 50.

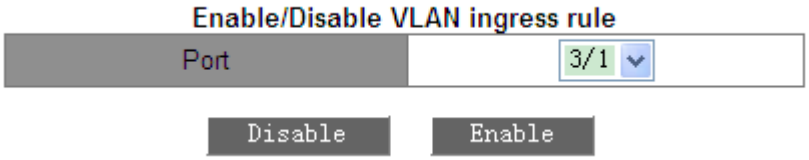


Рисунок 50 Настройка правил обработки входящего трафика VLAN

Варианты: Enable/Disable

По умолчанию: Enable

Функция: Включение/выключение правила обработки входящего трафика VLAN для порта.

Описание: Если эта функция включена, порт сверяет идентификатор VLAN пакета со своим списком разрешенных VLAN при получении пакета. Если совпадение найдено, порт пересылает пакет; в противном случае пакет отбрасывается. Если эта функция отключена, порт пересылает все пакеты без проверки их идентификаторов VLAN.

После завершения настройки отображается информация о правилах обработки входящего трафика VLAN, как показано на рисунке 51.

Port	Type	Ingress Rule
3/1	GX	Enable
3/2	GX	Disable
3/3	GX	Enable
3/4	GX	Enable
4/1	FE	Disable
4/2	FE	Enable
4/3	FE	Enable
4/4	FE	Enable

Рисунок 51 Информация о правилах обработки входящего трафика VLAN

8. Настройка VLAN-aware

Щелкните Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [VLAN-aware] → [VLAN-aware], чтобы перейти на страницу настройки правил обработки входящего трафика VLAN, как показано на рисунке 52.

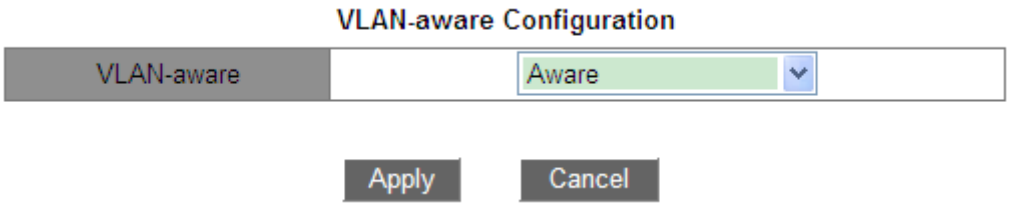


Рисунок 52 Настройка VLAN-aware

Варианты: Aware/Unaware

По умолчанию: Aware

Функция: Когда выбрано значение Aware, устройство идентифицирует и оценивает VLAN в соответствии с протоколом IEEE802.1Q и правильно пересылает пакеты. Если выбран параметр Unaware, устройство не оценивает идентификатор VLAN ID неизвестного одноадресного пакета и пересылает пакет на любой порт (широковещательно); устройство не оценивает идентификатор VLAN ID для известного одноадресного пакета и перенаправляет пакет на соответствующий порт в

соответствии с таблицей MAC-адресов.

9. Просмотр информации обо всех созданных VLAN.

Щелкните [Device Basic Configuration] → [VLAN configuration] → [VLAN debug and maintenance] → [Show VLAN], чтобы перейти на страницу информации о VLAN, как показано на рисунке 53.

VLAN ID	Name	Type	Media	Portid
1	default	Static	ENET	1/1(TR|TG) 1/2 1/3 1/4 2/4 4/4(TR)
2	VLAN2	Static	ENET	1/1(TR) 2/1 2/2 4/4(TR|TG)
100	VLAN100	Static	ENET	1/1(TR) 2/3 4/1 4/4(TR|TG)
200	VLAN200	Static	ENET	4/2 4/3 4/4(TR|TG)

Рисунок 53 Информация VLAN

5.4.5 Типовой пример конфигурации

Как показано на рисунке 54, 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 5 показана конкретная конфигурация.

Таблица 5 Конфигурация VLAN

VLAN	Конфигурация
VLAN2	Настройте порты 2/1 и 2/2 на коммутаторах A и B как нетегированные порты, а порт 4/4 как тегированный порт.
VLAN100	Настройте порты 2/3 и 4/1 на коммутаторах A и B как нетегированные порты, а порт 4/4 как тегированный порт.
VLAN200	Настройте порты 4/2 и 4/3 на коммутаторах A и B как нетегированные порты, а порт 4/4 как тегированный порт.

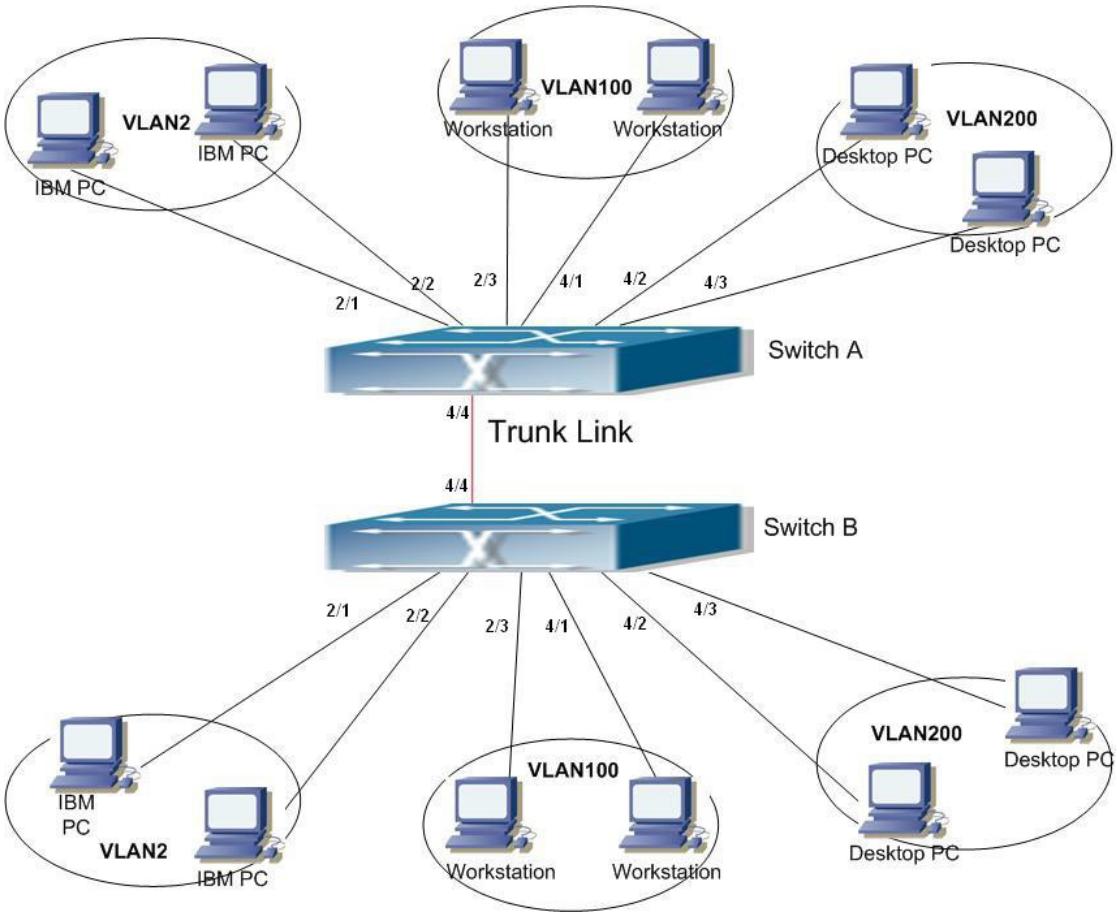


Рисунок 54 Использование VLAN

Конфигурация коммутатора A и коммутатора B:

1. Создайте VLAN2, VLAN100 и VLAN200, как показано на рисунке 41.

2. Настройте порты 2/1, 2/2, 2/3, 4/1, 4/2, 4/3 как порты Access, а порт 4/4 как порт Trunk, как показано на рисунке 44.

3. Добавьте порты 2/1 и 2/2 в VLAN2 как нетегированные порты; порты 2/3 и 4/1 в VLAN100 как нетегированные порты; порты 4/2 и 4/3 в VLAN200 как нетегированные порты; порт 4/4 в VLAN2, VLAN100, VLAN200 как тегированный порт, как показано на рисунке 46.

5.5 Настройка QinQ

5.5.1 Введение

Технология QinQ — это технология, которая расширяет пространство VLAN и реализует функцию расширения пространства VLAN за счет добавления еще одного уровня заголовка тега 802.1Q к сообщению тега 802.1Q, что может сделать прозрачной передачу трафика частной сети VLAN по общедоступной сети.

В режиме подключения к локальной сети, основанном на традиционном протоколе 802.1Q, когда двум пользовательским сетям необходимо получить доступ друг к другу через интернет-провайдера, интернет-провайдер должен назначить разные идентификаторы VLAN для разных VLAN для каждого имеющего доступ пользователя, как показано на рисунке 53. Предполагается, что сети пользователя 1 и 2 расположены в двух разных местах и имеют доступ к магистрали через PE1 и PE2 провайдера соответственно.

Если пользователю необходимо соединить VLAN100~VLAN200 сети 1 с VLAN100~VLAN200 сети 2, оба подключенных интерфейса узлов CE1, PE1, P и PE2, CE2 должны быть настроены в режиме trunk и разрешать прохождение трафика VLAN100~VLAN200.

Такой метод конфигурации делает VLAN пользователя видимой в магистральной сети, а не прозрачной передачей. Это не только расходует запас идентификаторов VLAN провайдера (обычно только 4094 идентификатора VLAN), но также требует, чтобы провайдер управлял номером VLAN пользователя. В этом случае структура сети слишком плотная, и изменения планирования сети провайдера или клиента повлияют на всю сеть, что ухудшает гибкость сети.

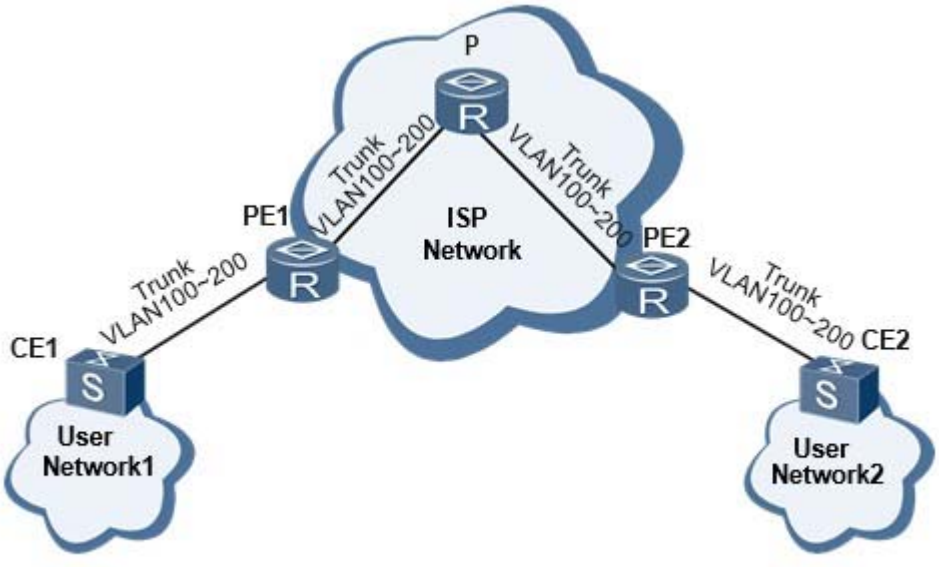


Рисунок 55. Традиционный режим подключения к локальной сети уровня 2 на основе протокола 802.1Q.

Технология QinQ добавляет еще один уровень тега 802.1Q в сообщение тега 802.1Q. Таким образом, сообщение, доставляемое в магистральной сети, имеет два уровня тегов 802.1Q (один тег общедоступной сети, один тег частной сети), и сеть провайдера должна предоставить только идентификатор VLAN для другого идентификатора VLAN из той же пользовательской сети, что экономит ресурс VLAN ID провайдера, решая проблему нехватки ресурсов VLAN ID. И это может обеспечить прозрачную передачу частной сети VLAN по общедоступной сети, а также предоставить простое решение VPN уровня 2 для небольших MAN (городских сетей) или LAN (локальных сетей).

5.5.2 Функции, поддерживаемые устройством

QinQ играет важную роль в различных решениях благодаря своим простым и гибким характеристикам.

Базовый QinQ: Базовый QinQ, также называемый туннелем QinQ уровня 2, реализуется на основе режима интерфейса. После того, как базовая функция QinQ интерфейса включена, когда интерфейс получает сообщение, устройство записывает тег VLAN, заданной по умолчанию для интерфейса, если полученное сообщение уже с

тегом VLAN, сообщение становится сообщением с двойным тегом, если принятое сообщение без тега VLAN, сообщение становится сообщением с тегом VLAN по умолчанию для интерфейса.

5.5.3 Значение TPID внешнего тега VLAN QinQ настраивается

Как показано на рисунке 54, это структура тегов VLAN кадров Ethernet, определенная протоколом IEEE802.1Q. Идентификация протокола метки TPID (идентификатор протокола тега) — это поле в теге VLAN, представляющее тип протокола для тега VLAN, а протокол IEEE 802.1Q определяет значение поля 0x8100.

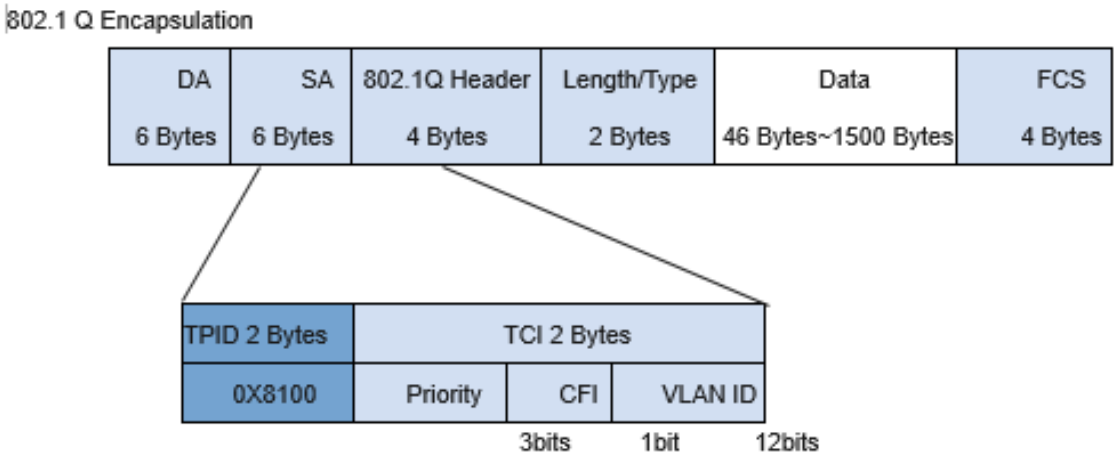


Рисунок 56 Инкапсуляция 802.1Q

Устройства разных производителей могут устанавливать в поле TPID тега внешней VLAN QinQ разные значения. Для обеспечения совместимости с устройствами других производителей устройство предоставляет функцию изменения значения TPID тега внешней VLAN QinQ. Путем настройки значения TPID, сообщение QinQ, отправляемое в общедоступную сеть, будет иметь то же значение TPID, что и у других производителей, чтобы устройства разных производителей могли взаимодействовать друг с другом.

Расположение TPID кадра Ethernet и типа протокола кадра без тега VLAN совпадают. Чтобы избежать проблем с пересылкой и обработкой пакетов в сети, TPID не может принимать ни одно из значений, указанных в следующей таблице:

Таблица 1 Тип протокола и соответствующие значения

Тип протокола	**Значение**
ARP	0x0806
RARP	0x8035
IP	0x0800
IPv6	0x86DD
PPPoE	0x8863/0x8864
MPLS	0x8847/0x8848
IPX/SPX	0x8137
LACP	0x8809
802.1x	0x888E
HGMP	0x88A7
Зарезервировано устройством	0xFFFD/0xFFFE/0xFFFF

5.5.4 Настройка через веб-интерфейс

Щелкните в дереве навигации [Device basic configuration] →[QinQ]→[QinQ configuration], чтобы войти в интерфейс настройки QinQ, как показано на рисунке 57:

Рисунок 57 Настройка QinQ

Port

Диапазон настройки: все порты коммутатора

Port status

Варианты настройки: флажок установлен/снят

Функция: включение QinQ для порта.

TPID (hex)

Диапазон настройки: 5dd-ffff

Функция: настройка **TPID (hex)**

Описание: Когда интерфейс получает сообщение, устройство записывает тег VLAN для VLAN по умолчанию.

5.6 Настройка PVLAN

5.6.1 Введение

PVLAN (частная VLAN) использует двухуровневые технологии изоляции для реализации сложной функции изоляции трафика портов, обеспечения сетевой безопасности и изоляции широковещательного домена.

Верхняя VLAN — это VLAN с общим доменом, в которой порты являются портами Uplink. Нижние VLAN являются изолированными доменами, в которых порты являются портами Downlink. Порты Downlink связи могут быть назначены разным доменам изоляции, и они могут одновременно взаимодействовать с портом Uplink. Изолированные домены не могут взаимодействовать друг с другом.

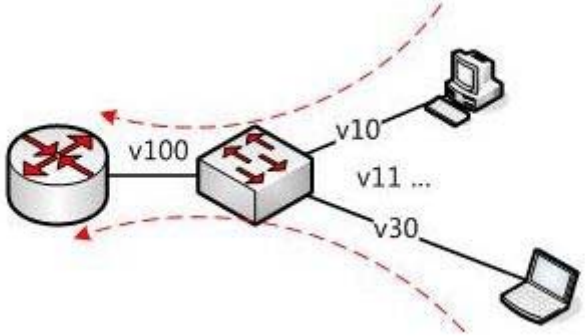


Рисунок 58 Использование PVLAN

Как показано на рисунке 58, общим доменом является VLAN100, а изолированными доменами являются VLAN 10 и VLAN 30; устройства в изолированных доменах могут взаимодействовать с устройством в совместно используемом домене, например, VLAN 10 может взаимодействовать с VLAN 100; VLAN 30 также может взаимодействовать с VLAN 100, но устройства в разных изолированных доменах не могут взаимодействовать друг с другом, например, VLAN 10 не может взаимодействовать с VLAN 30.

5.6.2 Пояснения

Функцию PVLAN можно реализовать с помощью специальной настройки портов.

- PVID портов Uplink совпадает с общим идентификатором VLAN домена; PVID портов Downlink совпадает с их собственным идентификатором VLAN домена изоляции.
- Порты Uplink настроены как нетегированные и назначены VLAN домена общего доступа и всем доменам изоляции; порты Downlink настроены как нетегированные и назначены VLAN с общим доменом и собственному изолированному домену.

5.6.3 Типовой пример конфигурации

Рисунок 59 показывает использование PVLAN. VLAN300 — это общий домен, а порты 1 и 2 — порты Uplink; VLAN100 и VLAN200 являются изолированными доменами, а порты 3, 4, 5 и 6 — портами Downlink.

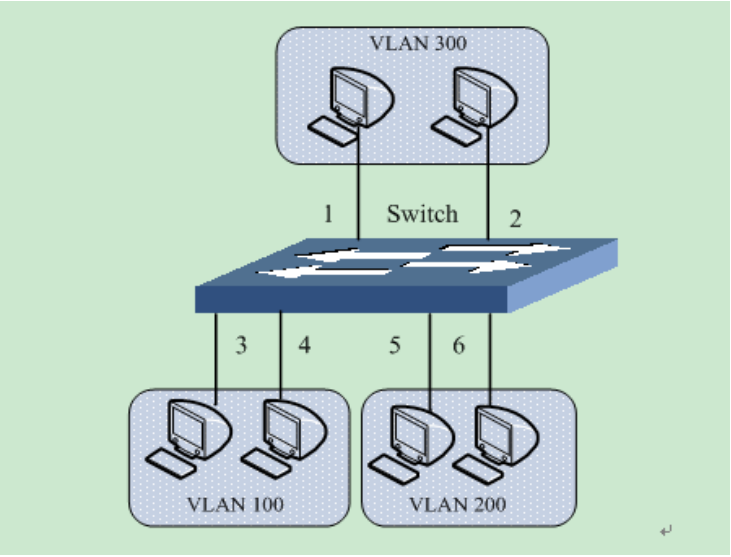


Рисунок 59 Пример настроек PVLAN

Настройка коммутатора:

1. Создайте VLAN300, VLAN 100, VLAN 200, как показано на рисунке 41.
2. Настройте порты 1, 2, 3, 4, 5, 6 как порты trunk как показано на рисунке 44.
3. Добавьте порты 1~6 к VLAN300 как нетегированные порты; порты 1~4 к VLAN100 как нетегированные порты; порты 1, 2, 5, 6 к VLAN200 как нетегированные порты, как показано на рисунке 46.
4. Настройте PVID портов 1 и 2 равным 300; PVID портов 3 и 4 равным 100; PVID портов 5 и 6 равным 200, как показано на рисунке 47.

5.7 Зеркалирование портов

5.7.1 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.

5.7.2 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:

Порт назначения зеркалирования и канал портов являются взаимоисключающими. Порт назначения

зеркалирования не может быть добавлен к каналу портов, а порт в канале портов не

может быть выбран в качестве порта назначения зеркалирования.

5.7.3 Настройка через веб-интерфейс

1. Выберите порт источника зеркалирования и режим зеркалирования.

Щелкните [Device Basic Configuration] → [Port mirroring configuration] → [Mirror configuration], чтобы перейти на страницу настройки порта источника зеркалирования, как показано нарисунке 60.

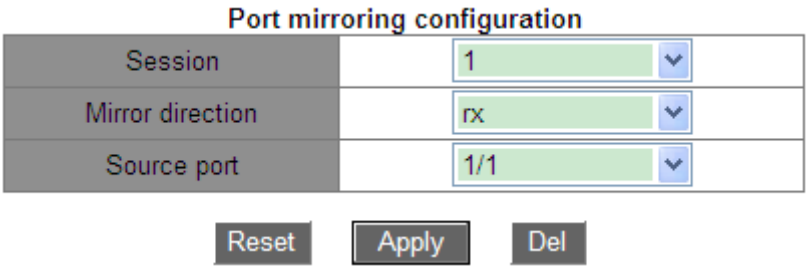


Рисунок 60 Настройка порта источника зеркалирования

Session

Варианты: 1~7

По умолчанию: 1

Функция: Выбор группы зеркалирования.

Mirror Direction

Варианты: rx/tx/both

По умолчанию: rx

Функция: Выбор данных для зеркалирования в исходном порту зеркалирования.

Описание: rx указывает, что в исходном порту зеркалируются только полученные пакеты. tx указывает, что в исходном порту зеркалируются только передаваемые пакеты.

Both: указывает, что в исходном порту зеркалируются полученные и отправленные пакеты.

Source port

Варианты: все порты коммутатора.

Функция: Выбор порта источника зеркалирования. Можно выбрать несколько исходных портов.

2. Выберите порт назначения зеркалирования, как показано на рисунке 61.

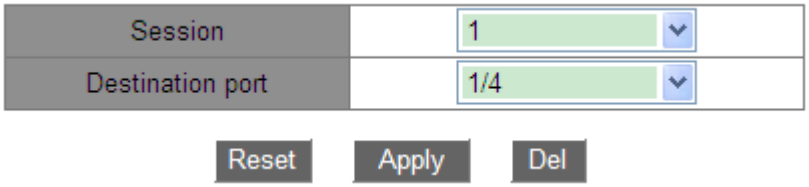


Рисунок 61 Настройка порта источника зеркалирования

Session

Варианты: 1~7

По умолчанию: 1

Функция: Выбор группы зеркалирования.

Destination port

Варианты: все порты, кроме исходного порта. Функция: Выбор порт назначения зеркалирования.

Описание: Выбор порта, который будет портом назначения зеркалирования. Существует только один порт назначения зеркалирования. Порт назначения зеркального отображения не может быть участником канала портов. Лучше, чтобы пропускная способность порта назначения была больше или равна общей пропускной способности портов-источников.

5.7.4 Типовой пример конфигурации

Как показано на рисунке 62, порт назначения зеркалирования — это порт 2, а порт источника зеркалирования — порт 1. Как переданные, так и полученные пакеты порта 1 зеркалируются на порт 2.

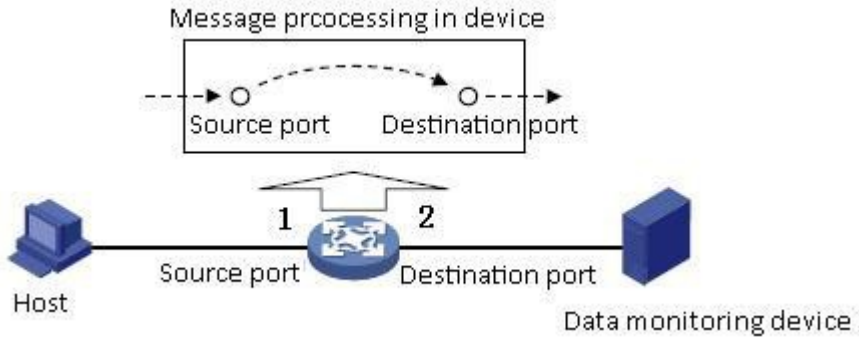


Рисунок 62 Пример зеркалирования порта

Процесс настройки:

1. Задайте порт 2 как порт назначения зеркалирования, как показано на рисунке 61.
2. Задайте порт 1 в качестве исходного порта зеркалирования и режим зеркалирования Both, как показано на рисунке 60.

5.8 Управление штормом порта

5.8.1 Введение

Управление штормом портов предназначено для ограничения принимаемых портом широковещательных/многоадресных/неизвестных одноадресных пакетов. Когда скорость широковещательных/многоадресных/неизвестных одноадресных пакетов, полученных через порт, превышает настроенный порог, система будет отбрасывать лишние широковещательные/многоадресные/неизвестные одноадресные пакеты, чтобы поддерживать широковещательный/многоадресный/неизвестный одноадресный трафик в пределах допустимого диапазона, обеспечивая нормальную работу сети.

5.8.2 Настройка через веб-интерфейс

1. Настройка порогового значения для подавления штормов.

Щелкните [Device Basic Configuration] → [Port Storm Suppression configuration] → [Port Storm Suppression configuration], чтобы перейти на страницу настройки, как показано на рисунке 63.

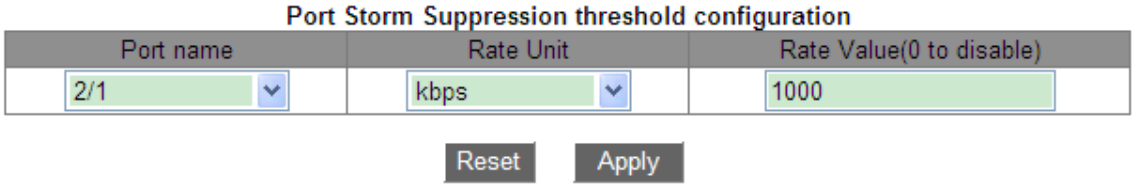


Рисунок 63 Настройка порогового значения для подавления штормов

Port name

Варианты: все порты коммутатора.

Функция: Выбор портов, для которых необходимо ограничить скорость.

Rate Unit:

Варианты: bps/kbps/percent

Функция: Выбор единицы измерения для порогового значения.

Rate Value:

Диапазон: 1~1000000kbps/1~1000000000bps/1~100 Percent

По умолчанию: 0, когда значение равно 0, подавление шторма отключено.

Функция: Настройка порогового значения для ограничения скорости порта. Пакеты, превышающие пороговое значение, будут отброшены. Диапазон значений зависит от фактической скорости порта. Подробности см. в таблице 6.

Описание: Пороговое значение порта Fast Ethernet находится в диапазоне 1~100000 кбит/с/1~100000000 бит/с; порог порта Gigabit Ethernet находится в диапазоне 1~1000000 кбит/с/1~1000000000 бит/с. Процент соответствует пропускной способности порта, например, если значение ограничения скорости для 100-мегабитного порта составляет 60 %, порт начинает отбрасывать данные после получения 60 мегабит трафика данных.

Таблица 6 Диапазон значений порога скорости порта

Скорость порта	Единица порогового значения	Шаг	Диапазон значений
10M	бит/с	512	512~10000000
	кбит/с	Не рекомендуется	Не рекомендуется
100M	бит/с	5120	5120~100000000
	кбит/с	5	5~100000
1000M	бит/с	51200	51200~1000000000
	кбит/с	50	50~1000000

2. Выберите тип контролируемых пакетов, как показано на рисунке 64.

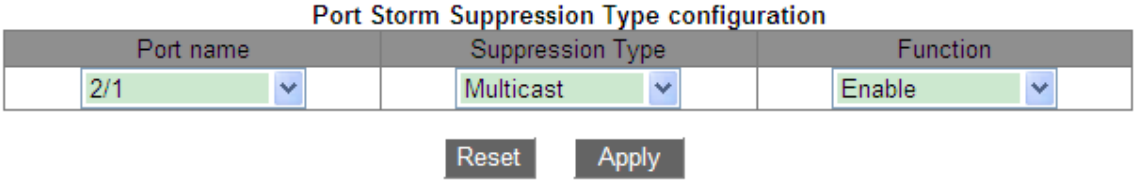


Рисунок 64 Настройка контролируемых пакетов

Port name

Варианты: все порты, на которых включена функция контроля шторма

Suppression Type

Варианты: Multicast/broadcast/dlf

Функция: Выбор типа контролируемых пакетов.

Function

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение или выключение контроля за выбранным типом пакетов.

Примечание:

Для каждого порта можно настроить только один порог. Порог влияет на настроенный тип пакетов.

5.8.3 Типовой пример конфигурации

Включение контроля неизвестного многоадресного шторма на порту 1/1 с порогом пропускной способности 1000 кбит/с.

Процесс настройки:

1. Выберите порт 1/1 и установите единицу скорости кбит/с и значение скорости 1000 кбит/с, как показано на рисунке 63.
2. Задайте тип пакетов multicast, как показано на рисунке 64.

5.9 Изоляция портов

5.9.1 Введение

Чтобы реализовать изоляцию пакетов на 2 уровне, можно добавить порты в разные VLAN. Однако этот метод приведет к расходованию ограниченных ресурсов VLAN. Используя функцию изоляции портов, можно изолировать порты в одной и той же VLAN друг от друга. Пользователю нужно только добавить порт в группу изоляции, и будет реализована изоляция данных на уровне 2 среди портов группы изоляции, поскольку порты в группе изоляции не будут пересылать пакеты на другие порты группы изоляции. Функция изоляции портов предоставляет пользователям более безопасное и гибкое сетевое решение.

Примечание:

- Порты группы изоляции могут быть только портами одного и того же коммутатора.
- Одно устройство поддерживает не более 14 групп изоляции, и количество портов Ethernet в каждой группе не ограничено.
- После настройки группы изоляции невозможен обмен пакетами только между портами группы изоляции, обмен данными между порами внутри группы изоляции и портами вне группы не затронут.
- Изолированный порт и канал портов являются взаимоисключающими. Порт из группы изоляции не может быть добавлен к каналу портов, а порт в канале портов не может быть добавлен в группу изоляции.

5.9.2 Настройка через веб-интерфейс

Щелкните [Device Basic Configuration] →[Port Isolate configuration] →[Port Isolate configuration], чтобы перейти на страницу настройки, как показано на рисунке 65.

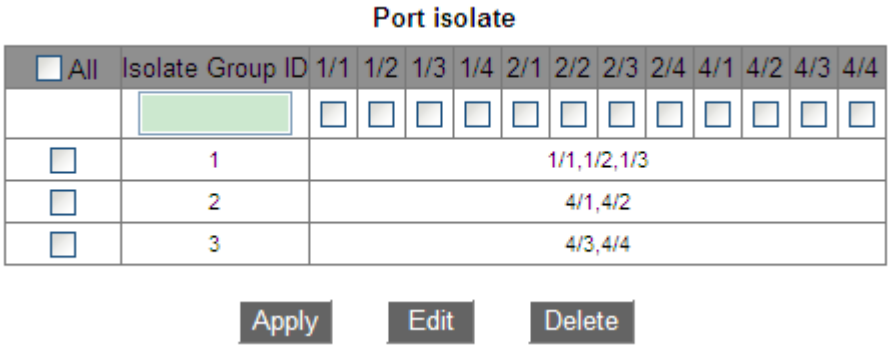


Рисунок 65 Настройка изоляции портов

Port isolate

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение или выключение изоляции портов.

Предупреждение:

Порт можно добавить только в одну группу изоляции.

5.9.3 Типовой пример конфигурации

Подключите ПК1, ПК2 и ПК3 к портам Ethernet 1, 2 и 3 коммутатора, а порт 4 подключите к внешней сети. Порты 1, 2, 3 и 4 находятся в VLAN 1. ПК1, ПК2 и ПК3 не могут обмениваться данными друг с другом, но имеют доступ к внешней сети, как показано на рисунке 66.

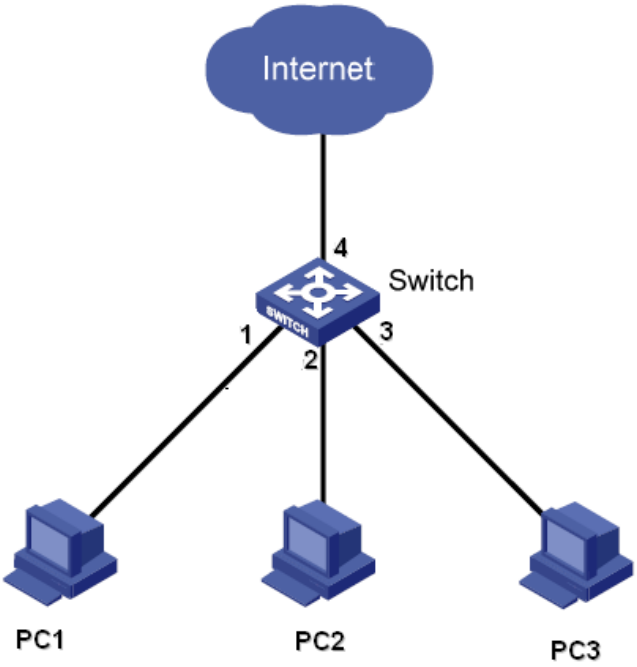


Рисунок 66 Экземпляр конфигурации изоляции портов

Добавьте порты 1, 2 и 3 в группу изоляции, чтобы изолировать ПК1, ПК2 и ПК3, как показано на рисунке 65.

5.10 Канал портов

5.10.1 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.

5.10.2 Реализация

Как показано на рисунке 67, три порта на коммутаторах A и B объединяются, образуя канал портов. Пропускная способность канала портов — это общая пропускная способность этих трех портов.

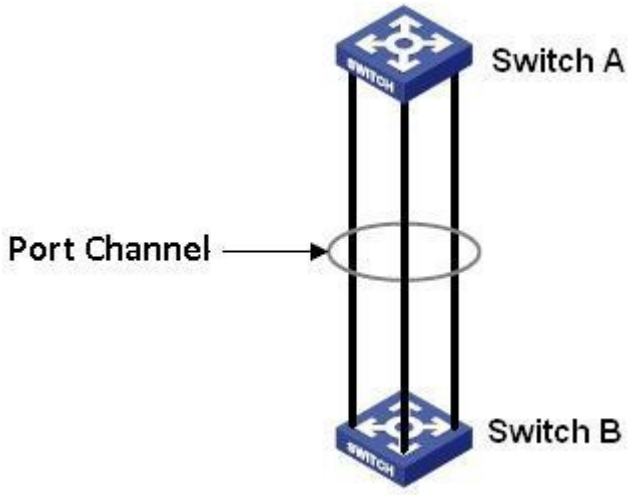


Рисунок 67 Канал портов

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.

5.10.3 5.10.3 Пояснения

Коммутаторы серии поддерживают не более 8 групп портов, и каждая группа содержит не более 8 портов.

Предупреждение:

- Порт можно добавить только в одну группу портов.
- Канал портов и изолированный порт являются взаимоисключающими. Порт из группы изоляции не может быть добавлен к каналу портов, а порт в канале портов не может быть добавлен в группу изоляции.
- Канал портов и порт назначения зеркалирования являются взаимоисключающими. Порты в канале портов нельзя настроить как порт назначения зеркалирования, а порт назначения зеркалирования нельзя добавить в канал портов.

5.10.4 Настройка через веб-интерфейс

1. Настройте режим распределения нагрузки канала портов.

Щелкните [Device Basic Configuration] → [Port channel configuration] → [port group configuration], чтобы перейти на страницу настройки, как показано на рисунке 68.

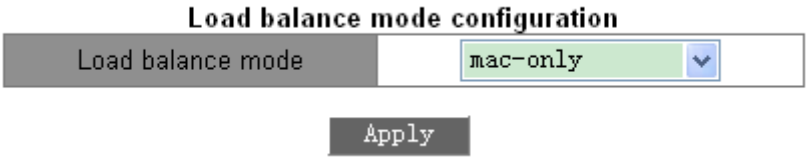


Рисунок 68 Настройка режима распределения нагрузки

Load balance mode

Варианты: mac-only/ip-only/mac-ip/ip-l4/mac-ip-l4

По умолчанию: mac-only

Функция: Задание режима распределения нагрузки канала портов.

Описание: mac-only указывает на распределение нагрузки на основе MAC-адреса. ip-only указывает на распределение нагрузки на основе IP-адреса.

mac-ip указывает распределение нагрузки на основе MAC-адреса и IP-адреса.

ip-l4 указывает на распределение нагрузки на основе IP-адреса и номера порта TCP/UDP.

mac-ip-14 указывает на распределение нагрузки на основе MAC-адреса, IP-адреса и номера порта TCP/UDP.

Пояснение: Если режим распределения нагрузки необходимо изменить после формирования канала порта, изменение вступит в силу после следующей агрегации.

2. Создайте или удалите группу портов, как показано на рисунке 69.

Рисунок 69 Настройка канала портов

group number

Диапазон: 1~8

Функция: Задание номера группы портов, не более 8 групп портов.

Operation type

Варианты: add port group/remove port group

По умолчанию: add port group

Функция: Создание или удаление группы портов.

После завершения настройки на странице port group table перечислены все созданные группы портов и режимы распределения нагрузки, как показано на рисунке 70.

port group table

port group	load balance
3	mac-only
2	mac-only
1	mac-only

Рисунок 70 Список групп портов

3. Настройка участника группы портов.

Щелкните [Device Basic Configuration] → [Port channel configuration] → [port configuration], чтобы перейти на страницу настройки, как показано на рисунке 71.

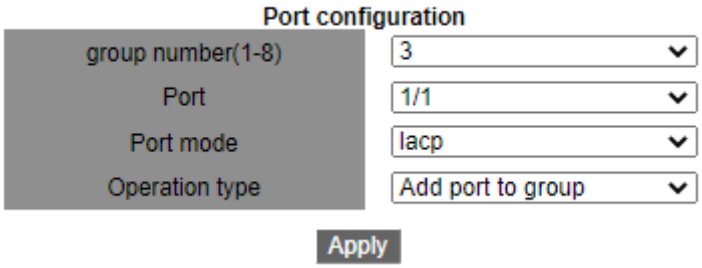


Рисунок 71 Настройка участника группы портов.

group number

Варианты: все созданные номера групп портов

Port

Варианты: все порты коммутатора.

Функция: Выбор порта для добавления в группу или удаления из группы.

Описание: Все порты в одной группе имеют одинаковые атрибуты.

Operation type

Варианты: Add port to group/Remove port from group

По умолчанию: Add port to group

Функция: Добавить порт в группу или удалить порт из группы.

5.10.5 Типовой пример конфигурации

Как показано на рисунке 67, 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 2. 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 группу портов 1 на коммутатор A, как показано на рисунке 69.
2. Добавьте порты 1, 2 и 3 в группу портов 1, как показано на рисунке 70.
3. Добавьте группу портов 2 на коммутатор B, как показано на рисунке 69.
4. Добавьте порты 1, 2 и 3 в группу портов 2, как показано на рисунке 70.

5.11 Настройка сервера Telnet

5.11.1 Введение

Telnet — это протокол для доступа с удаленных терминалов. Через Telnet можно войти на удаленный хост, используя IP-адрес или имя хоста. Telnet может передавать команды на удаленный хост и возвращать вывод удаленного устройства на дисплей через TCP.

Telnet работает в режиме клиент/сервер. Локальная система является клиентом, а удаленный хост — сервером. Коммутаторы этой серии могут служить в качестве сервера или клиента Telnet.

Когда коммутатор служит сервером Telnet, можно войти в коммутатор с помощью клиентского программного обеспечения Telnet в Windows или других ОС. Когда коммутатор служит сервером Telnet, он может устанавливать TCP-соединения максимум с 5 клиентами Telnet.

Когда коммутатор выступает в качестве клиента Telnet, можно использовать команды Telnet в общем виде для входа на другие удаленные хосты. При работе в качестве клиента Telnet коммутатор может устанавливать TCP-соединение только с одним удаленным хостом. Чтобы установить TCP-соединение с другим хостом, коммутатор должен сначала отключить подключенный хост.

5.11.2 Настройка через веб-интерфейс

1. Включите функцию сервера Telnet.

Щелкните [Device Basic Configuration] → [Telnet server configuration] → [Telnet server configuration], чтобы перейти на страницу настройки сервера telnet, как показано на рисунке 72.

Рисунок 72 Настройка сервера Telnet

Telnet server state

Элементы настройки: open/close

По умолчанию: open

Функция: Включение/выключение функции сервера Telnet.

Описание: Open означает, что клиенты Telnet могут войти в коммутатор. Close означает, что клиенты Telnet не могут войти в коммутатор.

Примечание:

Коммутатор может работать как клиент Telnet для входа на удаленный хост независимо от того,

включена ли эта функция.

2. Настройте безопасный IP-адрес для входа клиента Telnet.

Щелкните [Device Basic Configuration] → [Telnet server configuration] → [Telnet security IP], чтобы перейти на страницу настройки безопасного IP-адреса, как показано на рисунке 73.

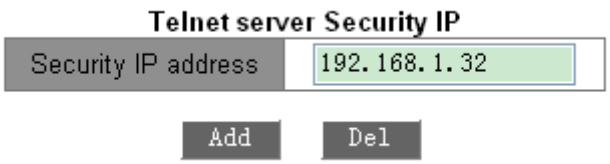


Рисунок 73 Безопасный IP-адрес сервера Telnet

Security IP address

Формат: A.B.C.D

Функция: Настройка безопасного IP-адреса для входа клиента Telnet, когда коммутатор работает в качестве сервера Telnet.

Описание: Если безопасный IP-адрес не установлен, ограничения на IP-адрес клиента Telnet отсутствуют.

После задания безопасных IP-адресов только клиент с безопасным IP-адресом может войти в систему и настроить коммутатор через Telnet.

Коммутатор поддерживает не более 32 безопасных IP-адресов. По умолчанию безопасные IP-адреса не настроены.

После завершения настройки в списке Telnet server Security IP list отображаются IP-адреса клиентов Telnet, которые могут выполнить вход в коммутатор, как показано на рисунке 74.

Telnet server Security IP list
192.168.1.30
192.168.1.31
192.168.1.32
192.168.1.33
192.168.1.34
192.168.1.35

Рисунок 74 Список безопасных IP-адресов

5.12 Настройка сервера SSH

5.12.1 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.

Серия коммутаторов поддерживает функцию SSH-сервера и позволяет подключаться нескольким пользователям SSH, которые удаленно входят в коммутатор через SSH, но не более двух пользователей могут подключиться к коммутатору одновременно.

5.12.2 Секретный ключ

Незашифрованное сообщение называется открытым текстом, а зашифрованное сообщение называется зашифрованным текстом. Шифрование или дешифрование находится под контролем секретного ключа. Секретный ключ представляет собой определенную строку символов и является единственным параметром, управляющим преобразованием между обычным текстом и зашифрованным текстом, работающим как ключ. Шифрование может превратить обычный текст в зашифрованный текст, а дешифрование может превратить зашифрованный текст в обычный текст.

Аутентификация на основе ключей требует секретных ключей, и каждый конец канала связи имеет пару секретных ключей, закрытый ключ и открытый ключ. Открытый ключ используется для шифрования данных, а законный владелец закрытого ключа может использовать закрытый ключ для расшифровки данных, чтобы гарантировать безопасность данных.

5.12.3 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.

5.12.4 Настройка через веб-интерфейс

➢ Этапы настройки сервера SSH:

Щелкните [Device Basic Configuration] → [SSH Server Configuration] → [SSH server configuration], чтобы перейти на страницу настройки сервера SSH.

1. Отключите SSH.
2. Щелкните <Destroy>, чтобы уничтожить старую пару ключей., как показано на рисунке 75.

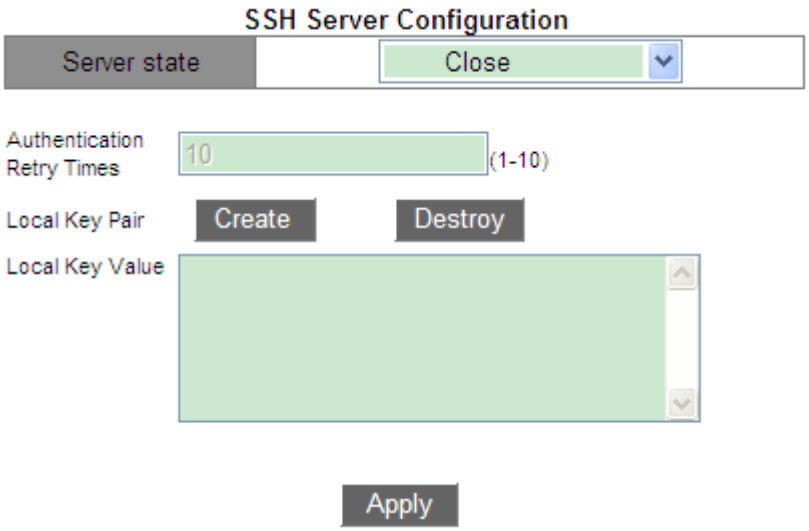


Рисунок 75 Уничтожение старой пары ключей

3. Щелкните <Create>, чтобы создать новую пару ключей.
4. Включите протокол SSH и настройте сервер SSH, как показано на рисунке 76.

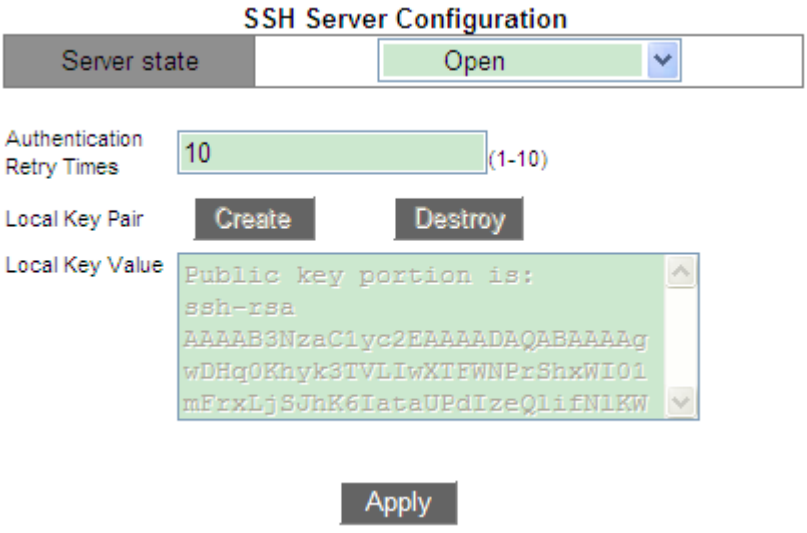


Рисунок 76 Конфигурация сервера SSH

Server state

Варианты: Open/Close

По умолчанию: Close

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

Authentication Retry Times

Диапазон настройки: 1~10

По умолчанию: 10

Функция: задание количества попыток входа на сервер SSH.

Local Key Pair

Варианты конфигурации: Create/Destroy

Функция: создать или уничтожить локальную пару ключей SSH-сервера. Перед включением SSH-сервера создайте локальную пару ключей; уничтожьте старую пару ключей перед созданием новой пары ключей.

Local Key Value

Функция: показать значение локального ключа. Щелкните <Create>, чтобы автоматически сгенерировать значение ключа.

- Настройте безопасный IP-адрес для входа клиента SSH.

Щелкните [Device Basic Configuration] → [SSH Server Configuration] → [SSH security IP], чтобы перейти на страницу настройки безопасного IP-адреса, как показано на рисунке 77.

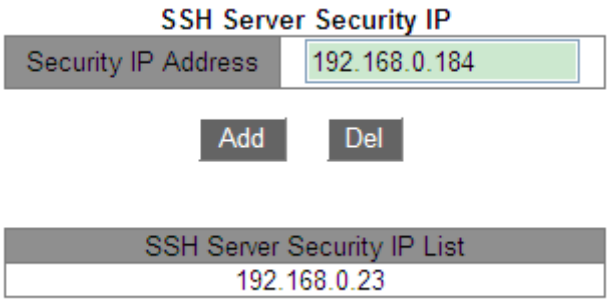


Рисунок 77 Настройка безопасного IP-адреса сервера SSH

Security IP address

Формат: A.B.C.D

Функция: Настройка безопасного IP-адреса для входа клиента SSH, когда коммутатор работает в качестве сервера SSH. Если безопасный IP-адрес не установлен, ограничения на IP-адрес клиента SSH отсутствуют. После задания безопасных IP-адресов только клиент с безопасным IP-адресом может войти в систему и настроить коммутатор через SSH.

Пояснение: Коммутатор поддерживает не более 6 безопасных IP-адресов. По умолчанию безопасные IP-адреса не настроены.

5.12.5 Типовой пример конфигурации

Хост работает как SSH-клиент для установления локального соединения с коммутатором, как показано на рисунке 78.

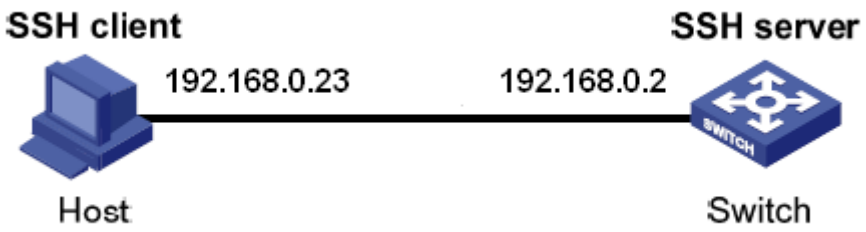


Рисунок 78 Пример настройки SSH

- Пользователь SSH выбирает тип аутентификации «пароль».

1. Уничтожьте старую пару ключей сервера, создайте новую пару ключей и запустите SSH-сервер, см.рисунок 75, рисунок 76.

2. Задайте имя пользователя SSH 333, службу SSH, тип аутентификации password, пароль 333, см. рисунок 31.

3. Установите соединение с сервером SSH. Сначала запустите программу PuTTY.exe, как показано на рисунке 79; введите IP-адрес SSH-сервера 192.168.0.2 в поле Host Name (или IP address).

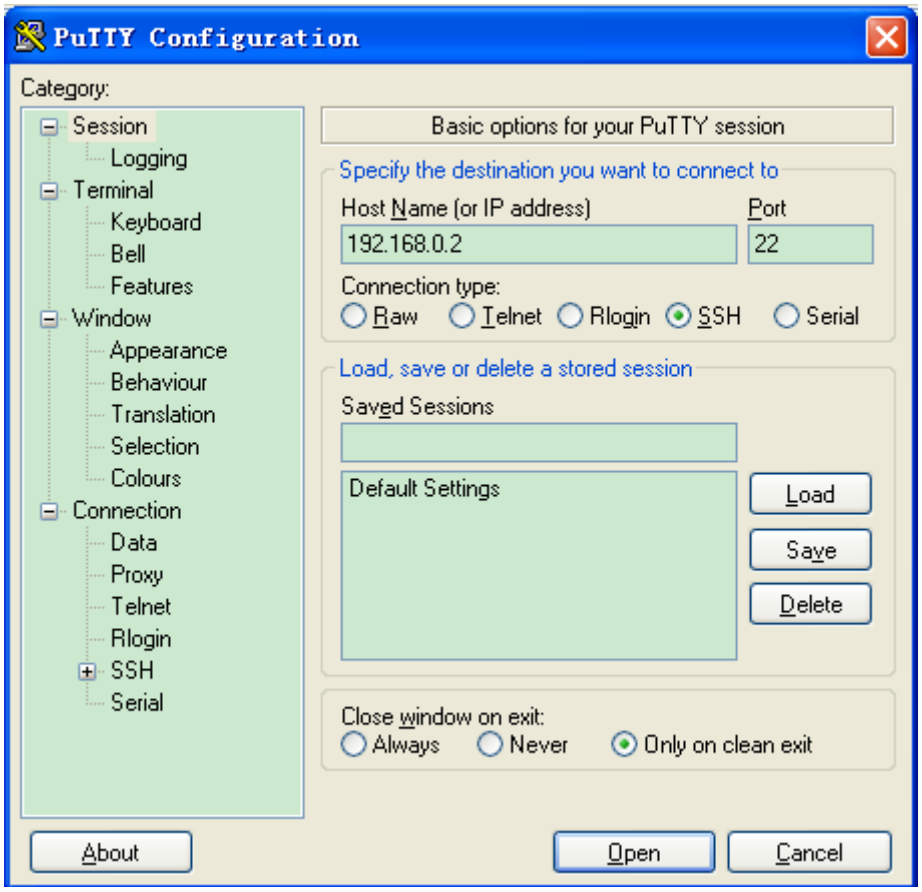


Рисунок 79 Настройка клиента SSH

4. Щелкните кнопку <Open>, появится предупреждающее сообщение, показанное на рисунке 80, щелкните кнопку <是(Y)>.

Рисунок 80 Предупреждающее сообщение

5. Введите имя пользователя 333 и пароль 333, чтобы войти в интерфейс настройки коммутатора, как показано на рисунке 81.

Рисунок 81 Интерфейс входа в SSH-аутентификацию по паролю

➢ Пользователь SSH выбирает тип аутентификации «ключ».

1. Уничтожьте старую пару ключей сервера, создайте новую пару ключей и запустите SSH-сервер, см.рисунок 75, рисунок 76.

2. Настройте клиента SSH, см. рисунок 33, запустите PuTTYGen.exe в клиенте, щелкните кнопку <Generate>, чтобы сгенерировать пару ключей клиента, как показано на рисунке 82.

Рисунок 82 Создание ключей клиента

3. В процессе генерации перемещайте мышь по экрану, в противном случае индикатор выполнения не будет двигаться вперед и генерация остановится, как показано на рисунке 83.

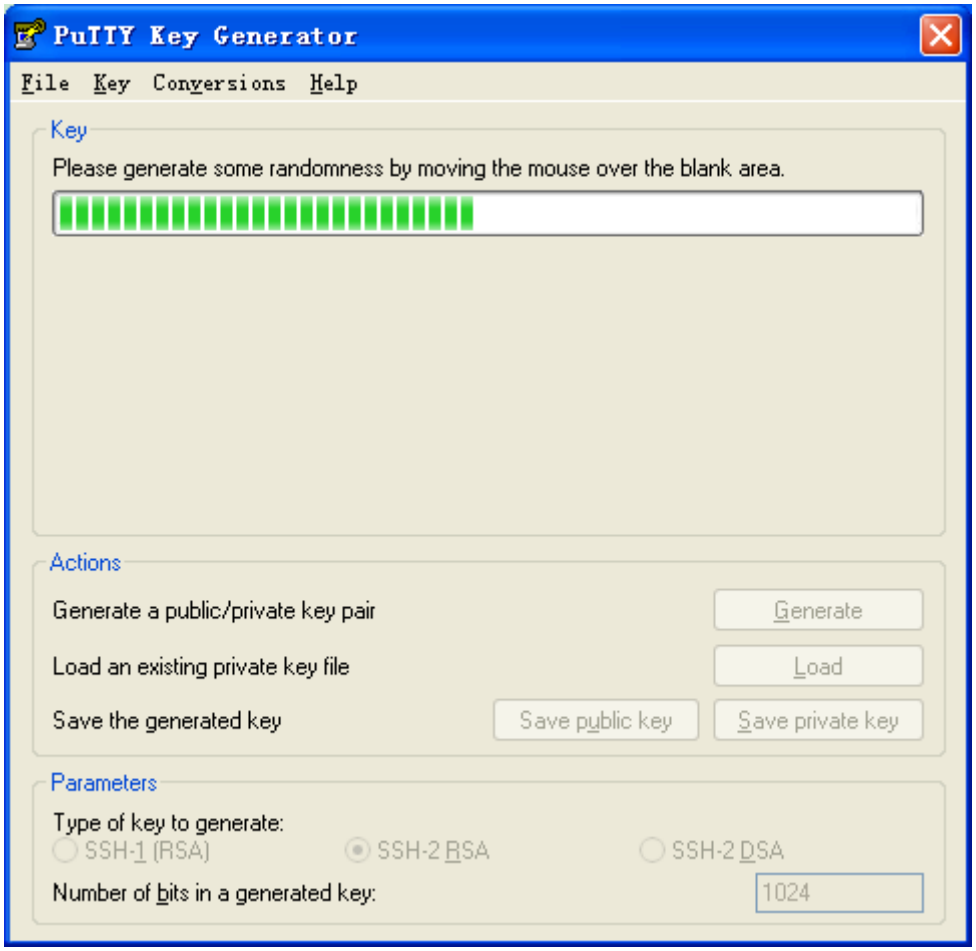


Рисунок 83 Генерация ключей

4. Как показано на рисунке 84, щелкните <Save private key>, чтобы сохранить закрытый ключ как 444.ppk. Скопируйте открытый ключ в область значения ключа в интерфейсе настройки ключа SSH и введите имя ключа 444, как показано на рисунке 33.

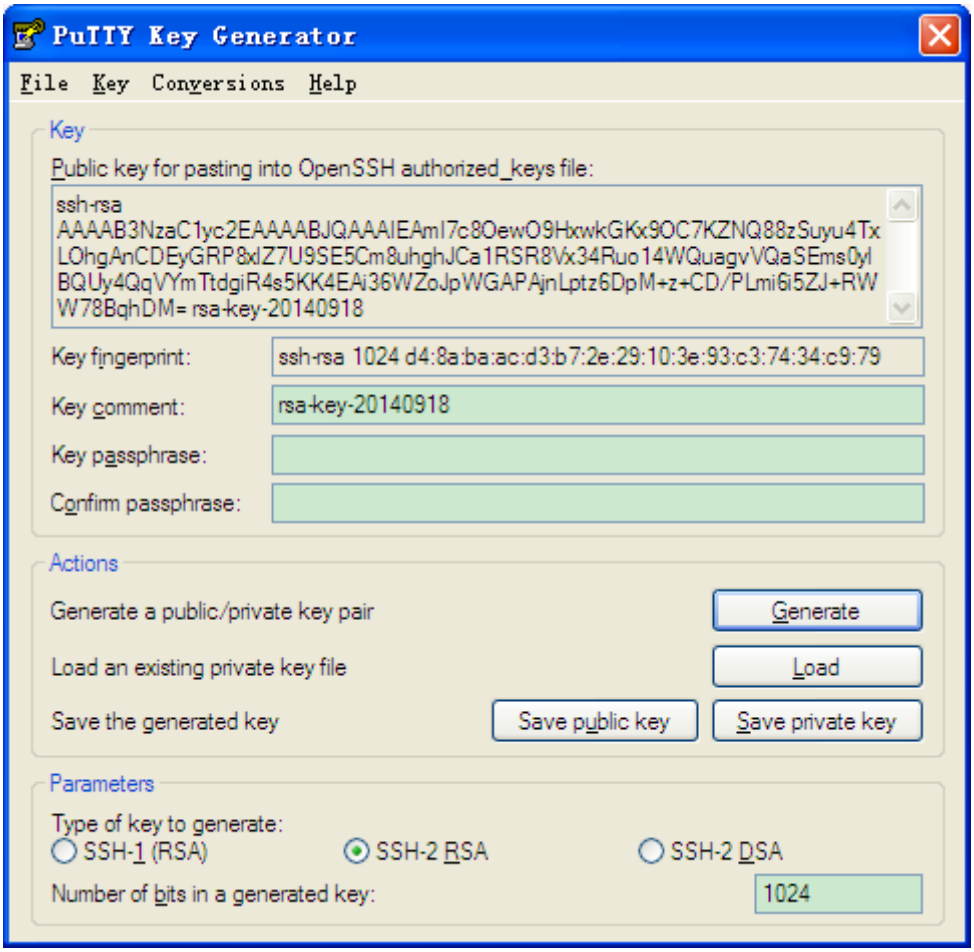


Рисунок 84 Создание значения ключа

5. Задайте имя пользователя SSH 444, службу SSH, тип аутентификации key, имя ключа 444, см. рисунок 31.

6. Установите соединение с сервером SSH. Сначала запустите программу PuTTY.exe, как показано на рисунке 85; введите IP-адрес SSH-сервера 192.168.0.2 в поле Host Name (или IP address).

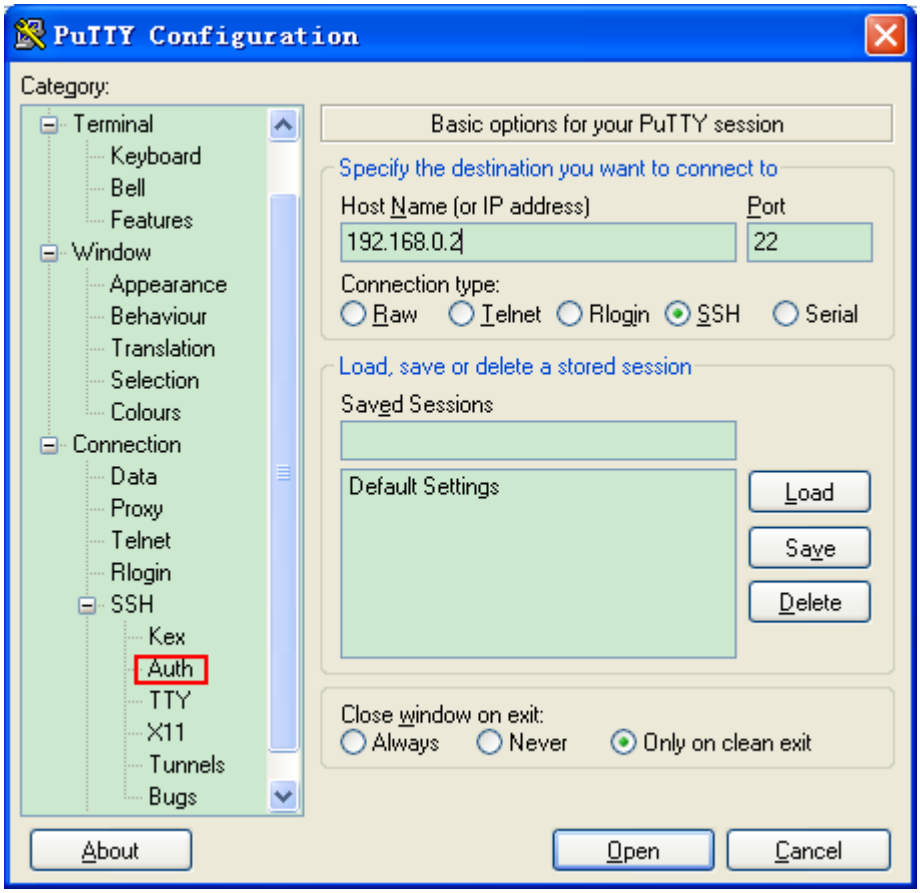


Рисунок 85 Настройка клиента SSH для аутентификации типа Key

7. Щелкните [SSH] →[Auth] в левой части рисунка 85, появится экран, показанный на рисунке 86, щелкните <Browse> и выберите файл, сохраненный на шаге 4.

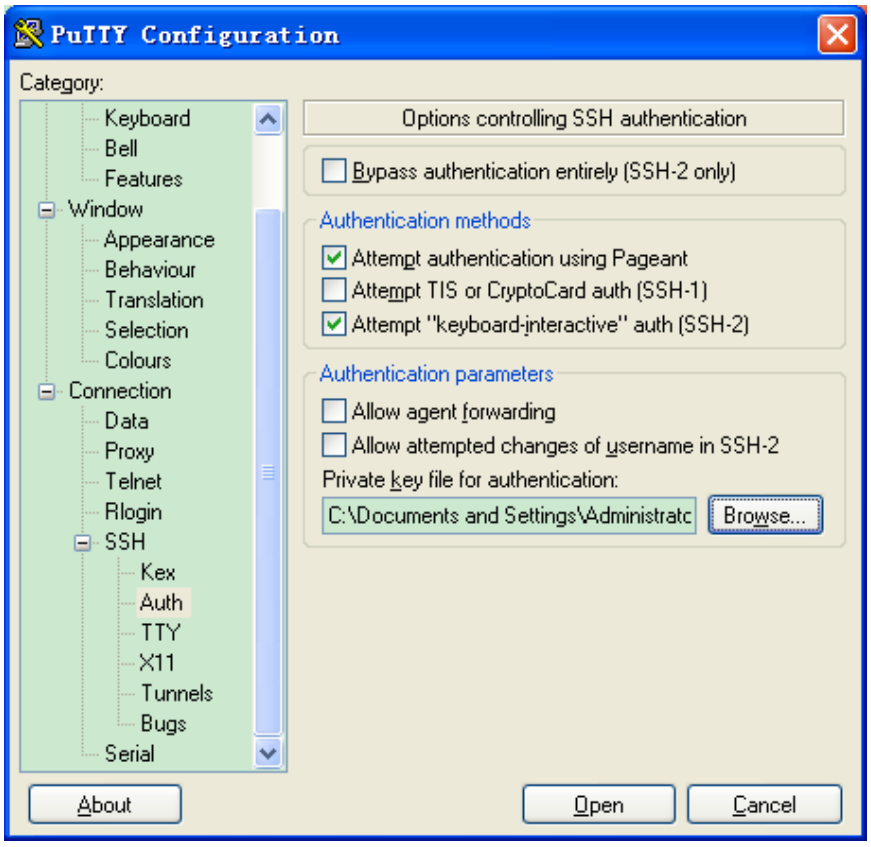


Рисунок 86 Выбор файла ключа

8. Щелкните кнопку <Open>; введите имя пользователя, чтобы войти в интерфейс настройки коммутатора, как показано на рисунке 87.

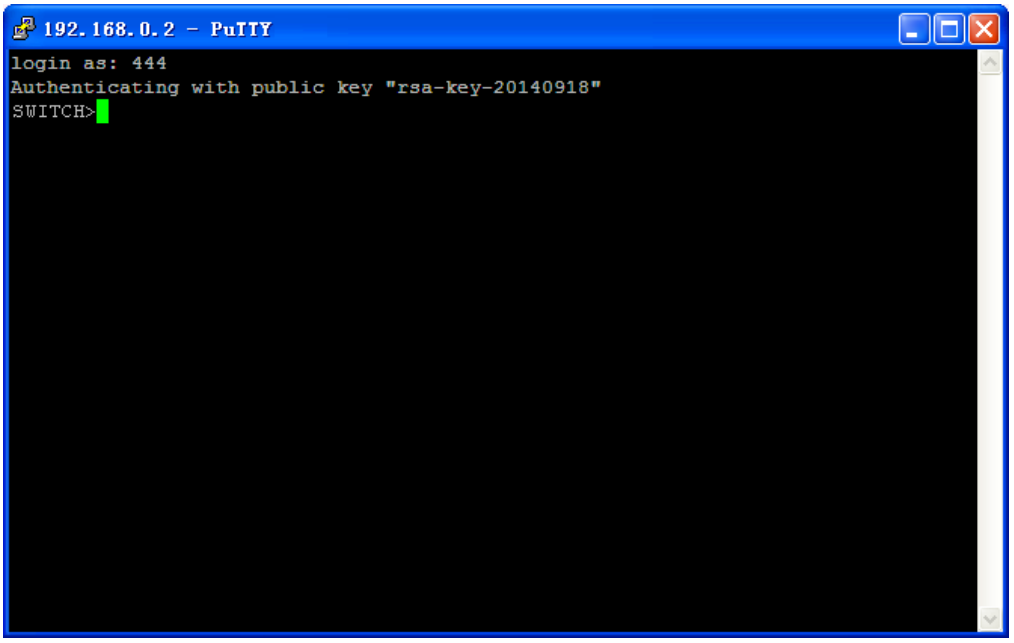


Рисунок 87 Интерфейс входа в SSH-аутентификацию по ключу

5.13 Настройка SSL

5.13.1 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.

После того, как коммутатор включит SSL, пользователи должны использовать безопасное подкючение https,например, https://192.168.0.2, для доступа к коммутатору

5.13.2 Настройка через веб-интерфейс

1. Включите протокол HTTPS

Щелкните [Device Basic Configuration] → [SSL Server configuration] → [SSL Server Configuration], чтобы перейти на страницу настройки сервера SSL, как показано на рисунке 88.

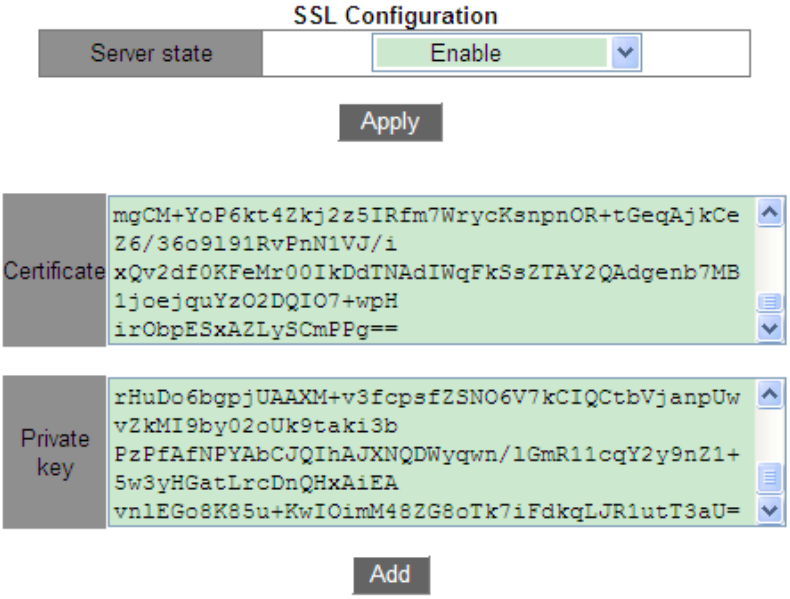


Рисунок 88 Включение протокола HTTPS

Server state

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение или выключение протокола SSL.

Пояснение: После включения SSL пользователи должны использовать безопасное подключение https://*ip-адрес* для доступа к коммутатору.

Certificate/Private key

Функция: Введите корректный сертификат и закрытый ключ, затем щелкните щелкните кнопку <Add>, чтобы импортировать их в коммутатор.

Предупреждение:

Сертификат по умолчанию и закрытый ключ, предоставленные компанией, уже импортированы в коммутатор. Пользователи могут напрямую включить протокол SSL и получить доступ к коммутатору в режиме HTTPS.

2. Введите имя пользователя и пароль для успешного входа в коммутатор через HTTPS.

5.14 Управление доступом

5.14.1 Настройка на веб-странице

Включить/выключить управление доступом, включить метод доступа через web/ftp/telnet, настроить идентификатор управления доступом, идентификатор Vlan, начальный IP-адрес, конечный IP-адрес, тип службы, удалить метод управления доступом можно настроить на странице управления доступом, как показано на рисунке. 89 错误!未找到引用源

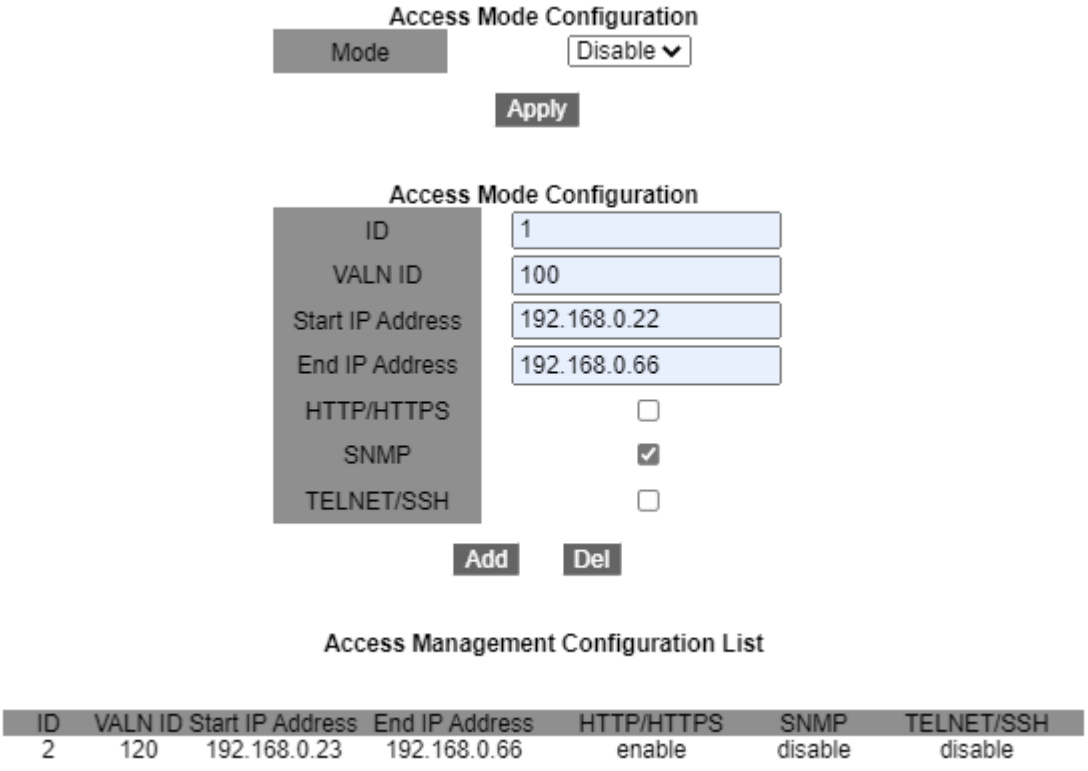


Рисунок 89 Страница настройки управления доступом

Access management status

Варианты: Enable/disable

По умолчанию: Disable

Функция: Если управление доступом включено, устройство будет управлять доступом к устройству.

ID

Диапазон настройки: 1~16

Функция: используется для обозначения условия управления доступом к устройству.

Vlan ID

Диапазон настройки: 1~4093

Функция: Настройка VLAN, для которых требуется управление доступом.

Start IP address

Формат: A.B.C.D

Функция: Настройка диапазона IP-адресов, которые позволяют войти в коммутатор; начальный IP-адрес не может быть пустым; после настройки начального IP-адреса только IP-адрес после начального IP-адреса может получить доступ к соответствующей VLAN.

End IP address

Формат: A.B.C.D

Функция: Настройка диапазона IP-адресов, которые позволяют войти в коммутатор; после настройки конечного IP-адреса только IP-адрес между начальным IP-адресом и конечным IP-адресом может получить доступ к соответствующей VLAN.

HTTP/HTTPS

Функция: При выборе HTTP/HTTPS, хост, который соответствует идентификатору VLAN и IP-адресу в записи доступа, может получить доступ к коммутатору через HTTP/HTTPS.

SNMP

Функция: При выборе SNMP, хост, который соответствует идентификатору VLAN и IP-адресу в записи доступа, может получить доступ к коммутатору через SNMP.

TELNET/SSH

Функция: При выборе TELNET/SSH, хост, который соответствует идентификатору VLAN и IP-адресу в записи доступа, может получить доступ к коммутатору через TELNET/SSH.

Щелкните <Add New Entry>, чтобы настроить запись управления доступом. Коммутатор поддерживает не более 16 записей управления доступом.

5.15 Служба передачи файлов

Служба передачи файлов обеспечивает взаимное резервное копирование файлов между сервером и клиентом. При изменении файла на сервере (или клиенте) можно получить файл резервной копии с клиента (или сервера) через FTP/TFTP/SFTP. Коммутатор может служить клиентом или сервером для загрузки и выгрузки файлов через FTP/TFTP/SFTP.

Примечание:

Для службы SFTP этот коммутатор поддерживает только службу клиента SFTP, что клиентом для загрузки и скачивания файлов через SFTP.

5.15.1 Служба TFTP

1. Коммутатор работает как сервер TFTP.

- Сначала установите TFTP-сервер, как показано на рисунке 90. В текущем каталоге выберите используемый путь к хранилищу файлов. Введите IP-адрес сервера в поле Server interface.

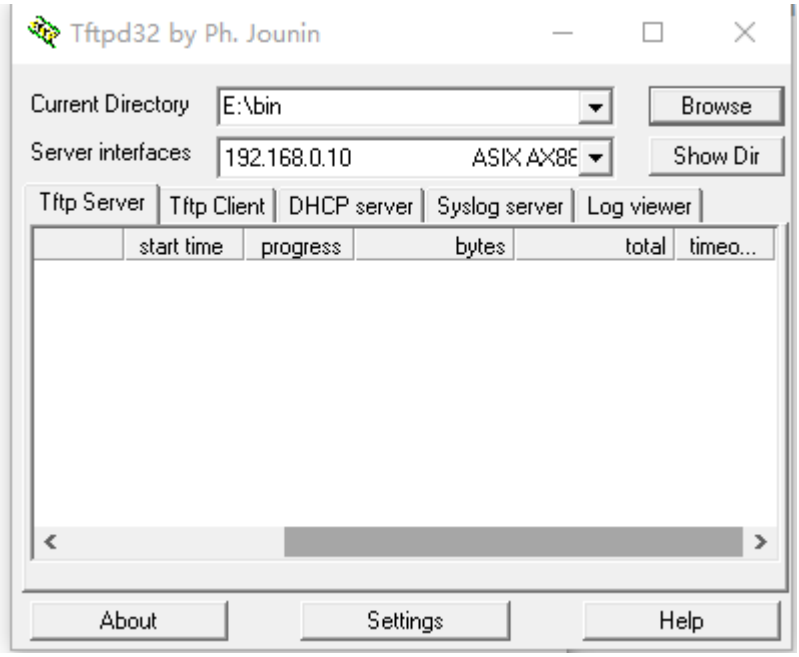


Рисунок 90 Конфигурация TFTP-сервера

- Щелкните [Device Basic Configuration] → [File transmit] → [TFTP Service] → [TFTP client service], чтобы перейти на страницу настройки клиента TFTP, как показано на рисунке 91.

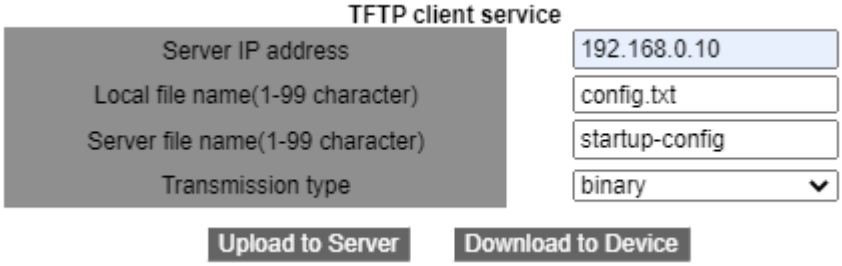


Рисунок 91 Служба клиента TFTP

IP-адрес сервера

Формат: A.B.C.D

Описание: Введите IP-адрес сервера.

Local file name

Диапазон: 1~99 символов

Описание: Введите имя файла коммутатора.

Server file name

Диапазон: 1~99 символов

Описание: Введите имя файла сервера.

Transmission type:

Варианты: binary/ascii

По умолчанию: binary

Функция: Выбор стандарта передачи.

Объяснение: ascii означает использование стандарта ASCII для передачи файла;

binary означает использование двоичного стандарта для передачи файла.

Метод: Щелкните <Upload to PC>, чтобы загрузить файл с коммутатора на сервер,

или <Download to Device>, чтобы загрузить файл с сервера на коммутатор.

- После успешной передачи файла в веб-интерфейсе появляется следующая информация, как показано на рисунке 92 и рисунке 93.

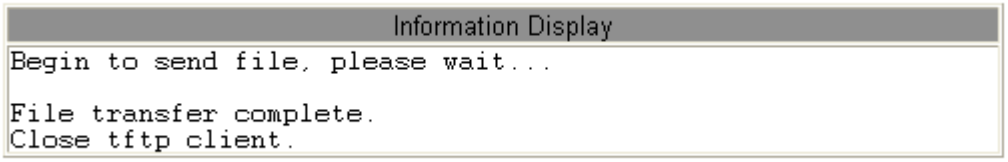


Рисунок 92 Успешная выгрузка файла по TFTP

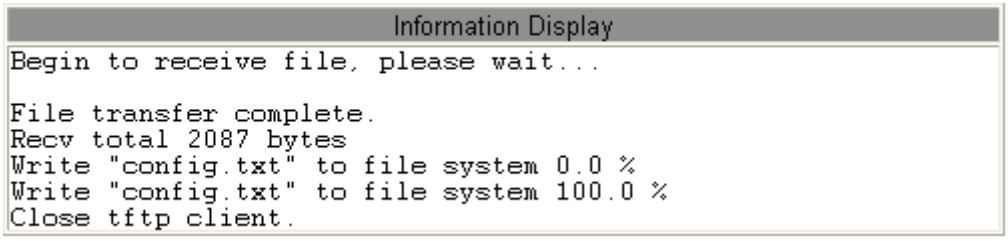


Рисунок 93 Успешная загрузка файла по TFTP

Предупреждение:

- При передаче файла сервер TFTP должен находиться в рабочем состоянии.
- Файл версии программного обеспечения не является текстовым файлом, и для передачи нужно использовать двоичный стандарт.

2. Коммутатор работает как сервер TFTP.

Щелкните [Device Basic Configuration] → [File transmit] → [TFTP Service] → [TFTP server service], чтобы перейти на страницу настройки сервера TFTP, как показано на рисунке 94.

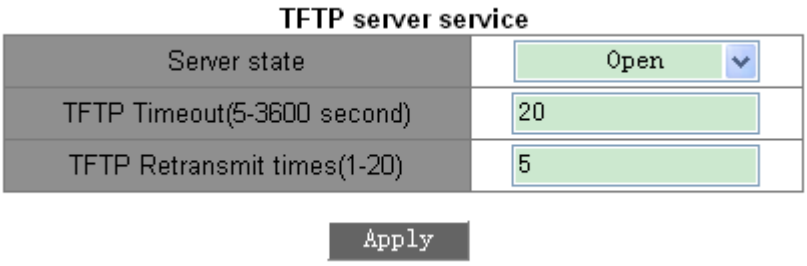


Рисунок 94 Служба сервера TFTP

Server state

Варианты: Close/Open

По умолчанию: Close

Функция: Включение/выключение функции сервера TFTP.

TFTP Timeout

Диапазон: 5~3600 с

По умолчанию: 20 с

Функция: Настройка времени ожидания для TFTP-соединения.

TFTP Retransmit times

Диапазон: 1~20

По умолчанию:5

Функция: Настройка количества попыток передачи данных по TFTP за период timeout.

- Установите ПО клиента TFTP, как показано на рисунке 95. Введите IP-адрес коммутатора в поле Host; выберите путь к хранилищу файлов клиента в поле Local File; введите имя файла, находящегося на коммутаторе в поле Remote File; щелкните <Get>, чтобы загрузить файл с коммутатора клиенту; щелкните <Put>, чтобы передать файл клиента на коммутатор.

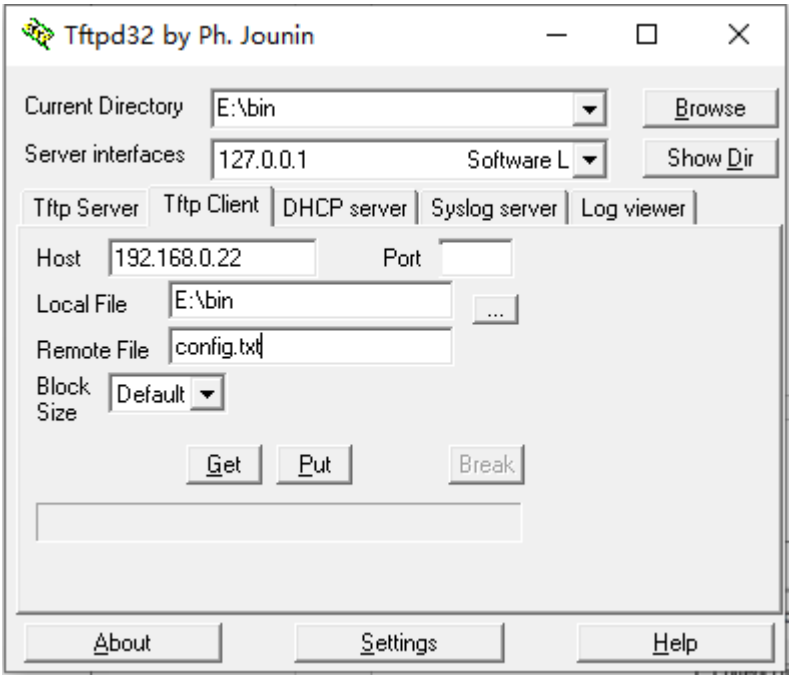


Рисунок 95 Настройка клиента TFTP

Предупреждение:

Во время передачи файлов не отключайте программное обеспечение клиента TFTP.

5.15.2 Служба FTP

1. Коммутатор работает как клиент FTP.

- Сначала установите FTP-сервер. Щелкните [Security] → [users/rights], чтобы открыть диалоговое окно. Щелкните

  <New User>, чтобы создать нового пользователя, как показано на рисунке 96. Введите имя пользователя и пароль, например, имя пользователя: admin, пароль: 123. Щелкните <OK>.

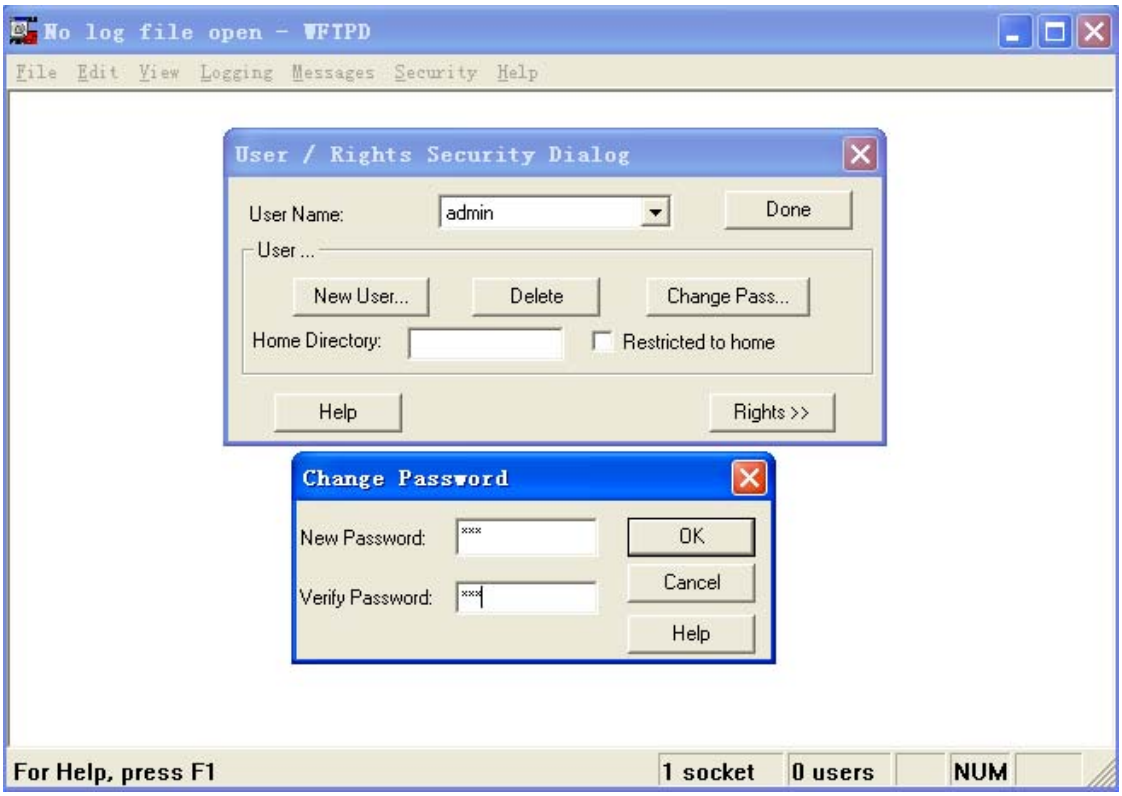


Рисунок 96 Создание нового пользователя FTP

- Введите путь хранения файла в Home Directory, как показано на рисунке 97. Щелкните <Done>.

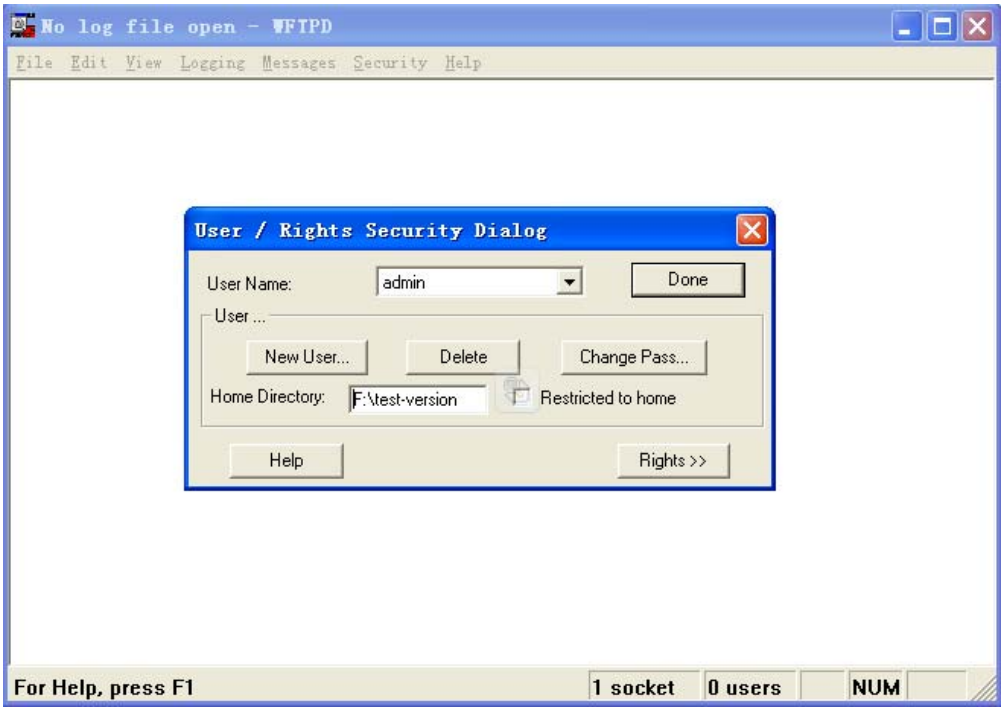


Рисунок 97 Местоположение файла

- Щелкните [Device Basic Configuration] → [File transmit] → [FTP Service] → [FTP client service], чтобы перейти на страницу настройки клиента FTP, как показано на рисунке 98.

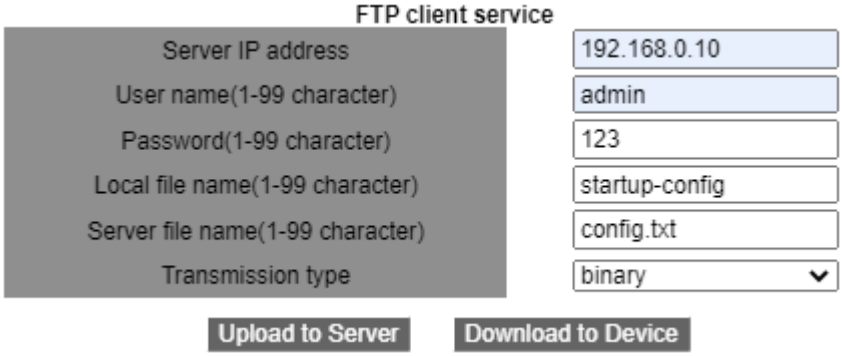


Рисунок 98 Служба клиента FTP

IP-адрес сервера

Формат: A.B.C.D

Описание: указывает IP-адрес сервера.

{User name, Password }

Диапазон: { 1~99 символов, 1~99 символов }

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

Local file name:

Диапазон: 1~99 символов

Описание: указывает имя файла на коммутаторе.

Server file name

Диапазон: 1~99 символов

Описание: указывает имя файла на сервере.

Transmission type:

Варианты: binary/ascii

По умолчанию: binary

Функция: Выбор стандарта передачи.

Объяснение: ascii означает использование стандарта ASCII для передачи файла; binary означает использование двоичного стандарта для передачи файла.

Метод: Щелкните <Upload to PC>, чтобы загрузить файл с коммутатора на сервер. Щелкните <Download to Device>, чтобы загрузить файл с сервера на коммутатор.

- После успешной передачи файла в веб-интерфейсе появляется следующая информация, как показано на рисунке 99 и рисунке 100.

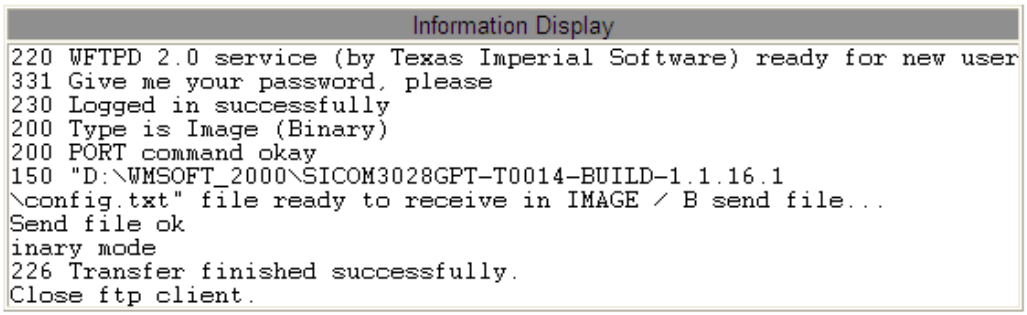


Рисунок 99 Успешная выгрузка файла по FTP

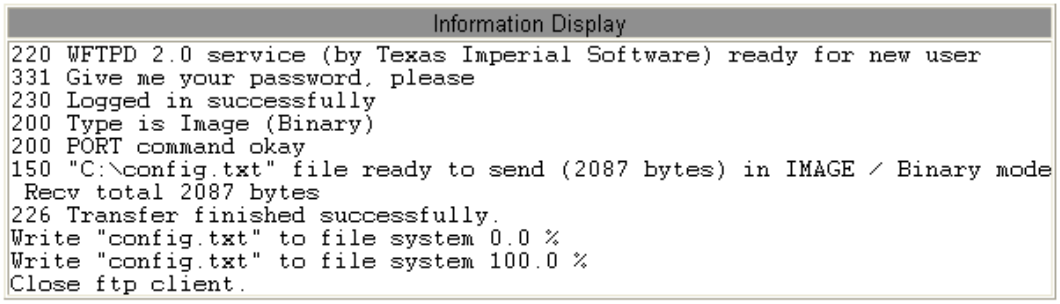


Рисунок 100 Успешная загрузка файла по FTP

Предупреждение:

- При передаче файла сервер FTP должен находиться в рабочем состоянии.
- Файл версии программного обеспечения не является текстовым файлом, и для передачи нужно использовать двоичный стандарт.

2. Коммутатор работает как сервер FTP.

- Щелкните [Device Basic Configuration] → [File transmit] → [FTP Service] → [FTP server service], чтобы перейти на страницу настройки сервера FTP, как показано на рисунке 101.

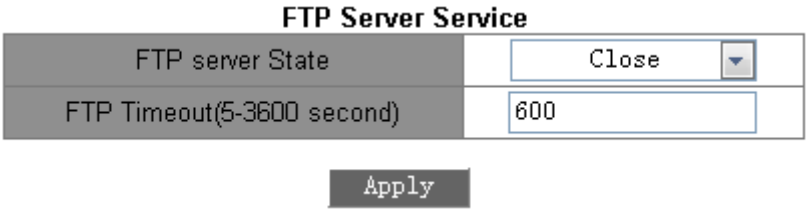


Рисунок 101 Служба сервера FTP

FTP Server state

Варианты: Close/Open

По умолчанию: close

Функция: Включение/выключение функции сервера FTP.

FTP Timeout

Диапазон: 5~3600 с

По умолчанию: 600 с

Функция: Настройка времени ожидания для FTP-соединения.

Описание: Если в течение периода timeout между FTP-сервером и клиентом не передаются данные, соединение между ними разрывается.

- Настройте имя пользователя и пароль, используемые для входа на FTP-сервер, как показано на рисунке 102.

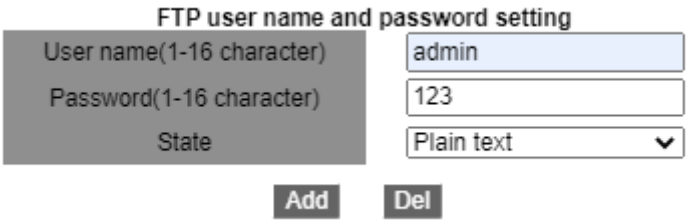


Рисунок 102 Настройка имени пользователя и пароля для FTP-сервера

{Username, Password}

Диапазон: {1~16 символов, 1~16 символов}

Функция: Настройка имени пользователя и пароля, используемых для входа на FTP-сервер. Описание: Когда коммутатор работает как FTP-сервер, он может быть подключен к нескольким FTP-клиентам одновременно.

State

Варианты: Plain text/Encrypted text

По умолчанию: Plain text

Функция: Выберите режим отображения пароля.

- Щелкните [Start] → [Run] в ОС Windows. Появится диалоговое окно Run. Введите cmd и нажмите Enter. Появится следующая страница.

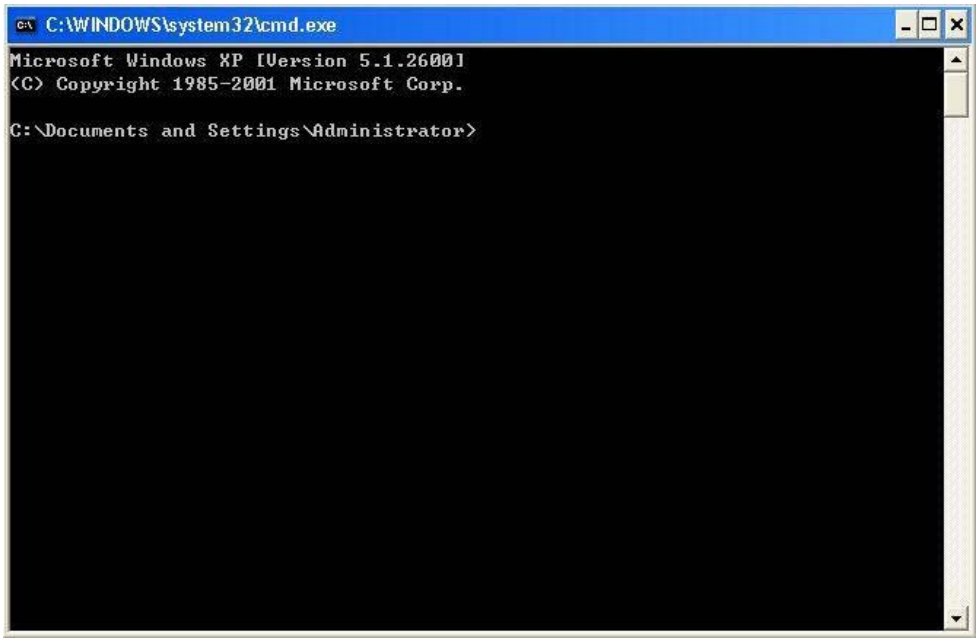


Рисунок 103 Интерфейс командной строки

- Путь передачи файла можно изменить. Выполните вход на FTP-сервер, как показано на рисунке 104.

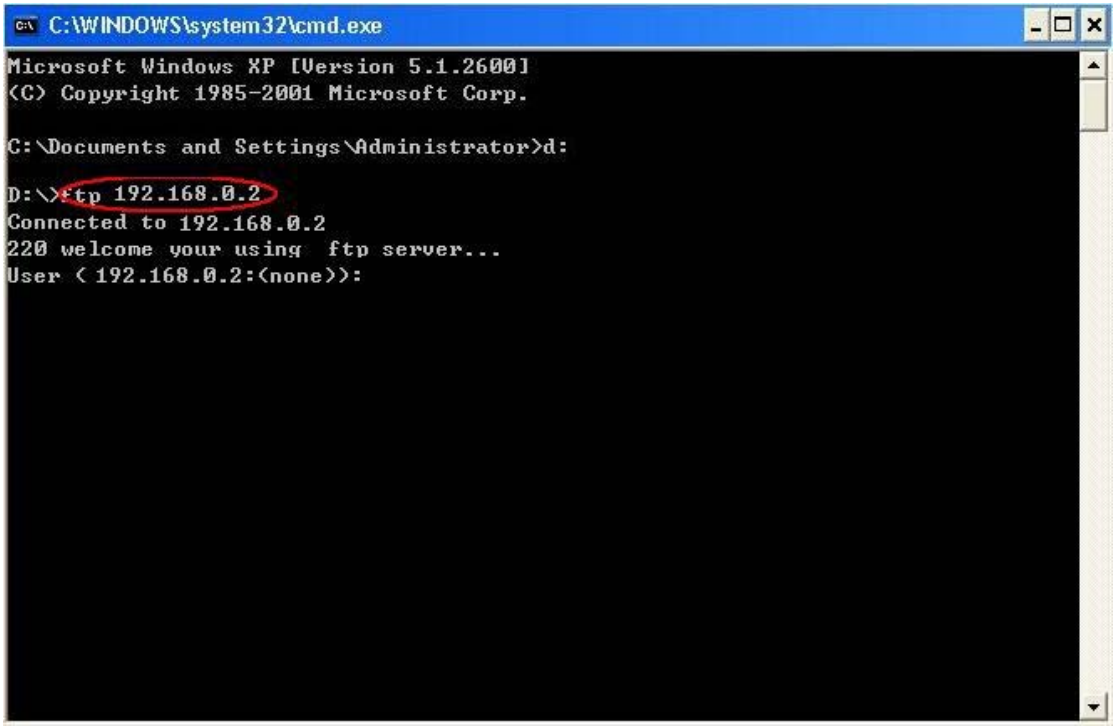


Рисунок 104 Подключение к серверу FTP

- Используйте настроенное имя пользователя admin и пароль 123 для входа на FTP-сервер, как показано на рисунке 105.

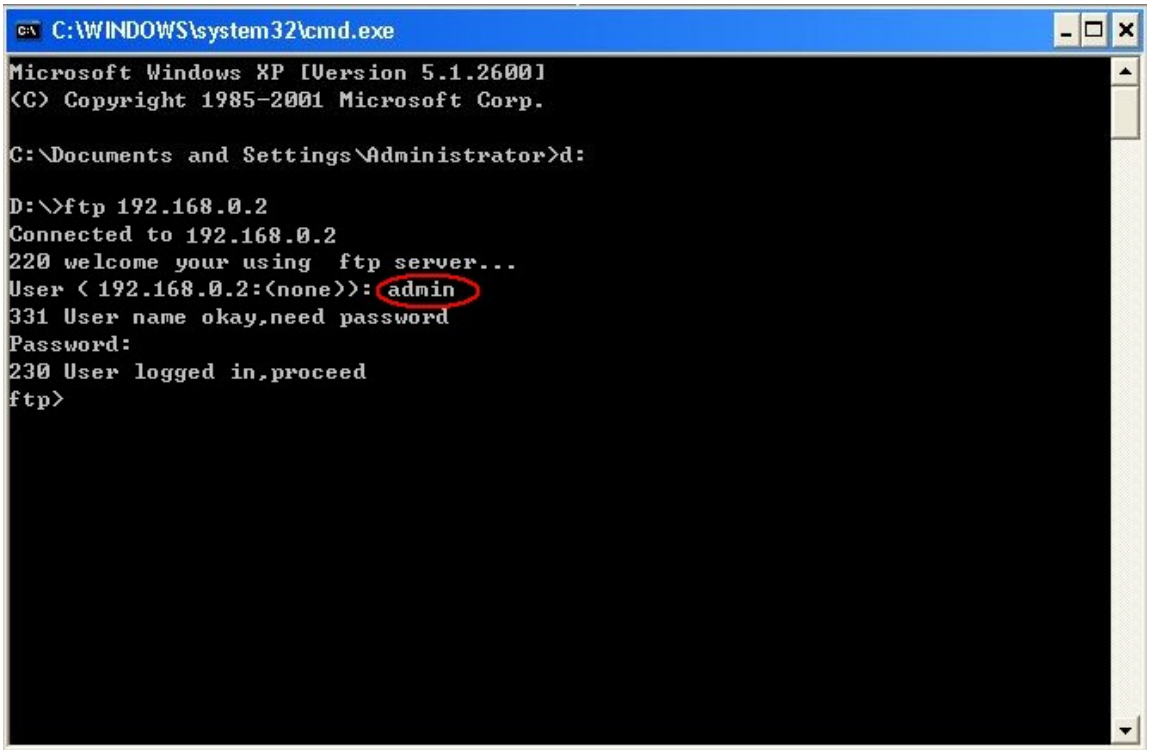


Рисунок 105 Вход на FTP-сервер

- Используйте команду get, чтобы загрузить файл по указанному пути на клиенте, как показано на рисунке 106. Введите команду get и нажмите Enter. В строке Remote file введите имя скачиваемого файла на коммутаторе. В строке Local file введите имя файла на клиенте.

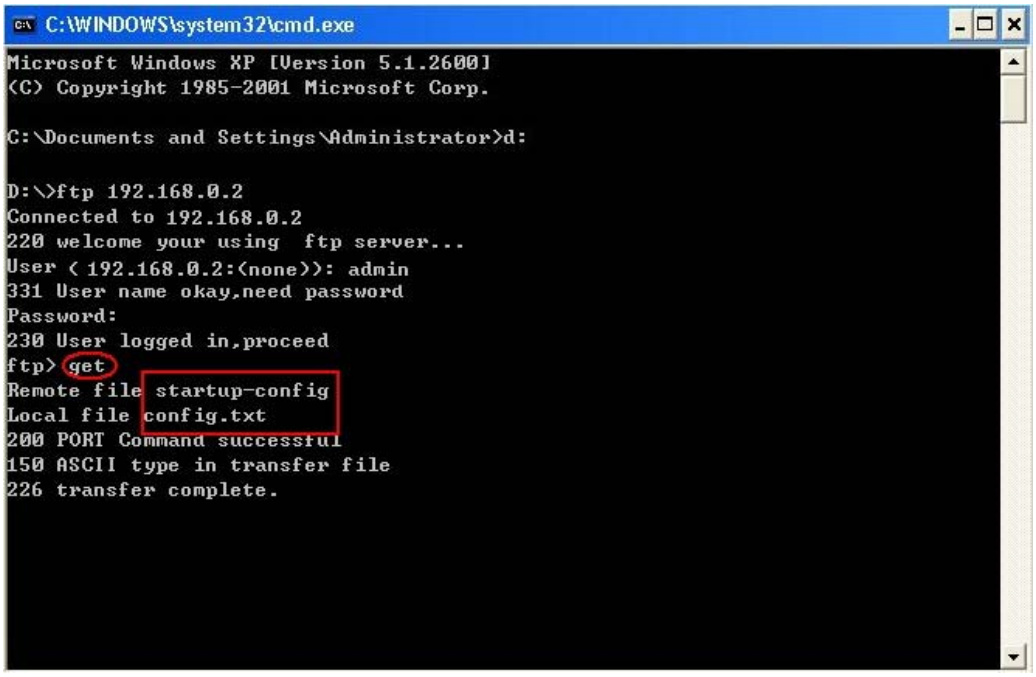


Рисунок 106 Загрузка файла с коммутатора на клиент

- Используйте команду put, чтобы выгрузить файл по указанному пути в клиенте на сервер,как показано на рисунке 107. Введите команду put и нажмите Enter. В строке Remote file введите имя файла на коммутаторе. В строке Local file введите имя файла, который будет выгружен на коммутатор.

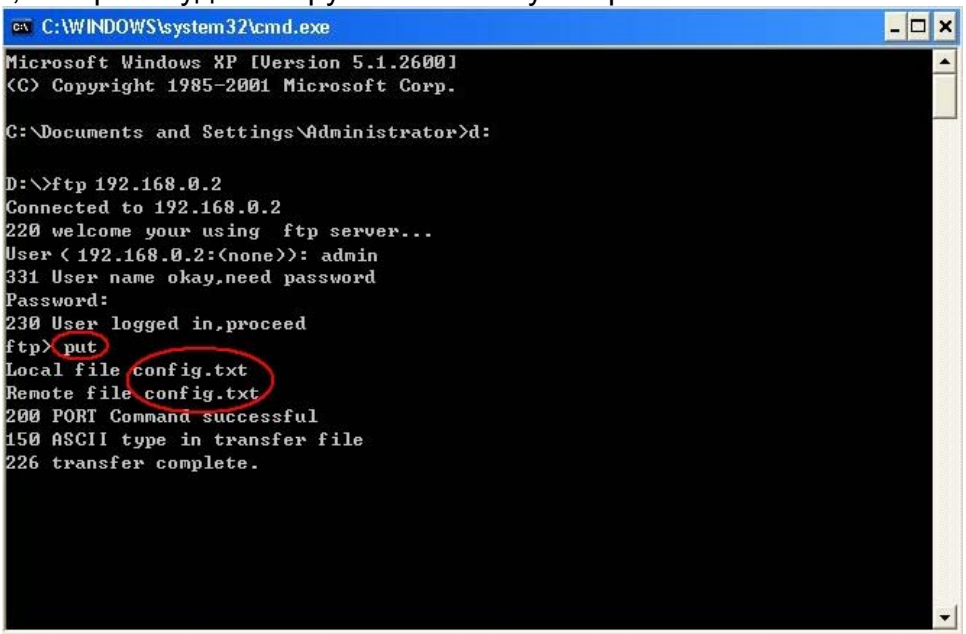


Рисунок 107 Выгрузка файла с клиента на коммутатор

5.15.3 Служба SFTP

Коммутатор работает как клиент SFTP.

- Сначала установите SFTP-сервер и добавьте пользователя SFTP, как показано на рисунке 108. Введите пользователя и пароль, например, admin и 123. Установите номер порта 22. Введите путь для сохранения файла версии прошивки в поле Root path.

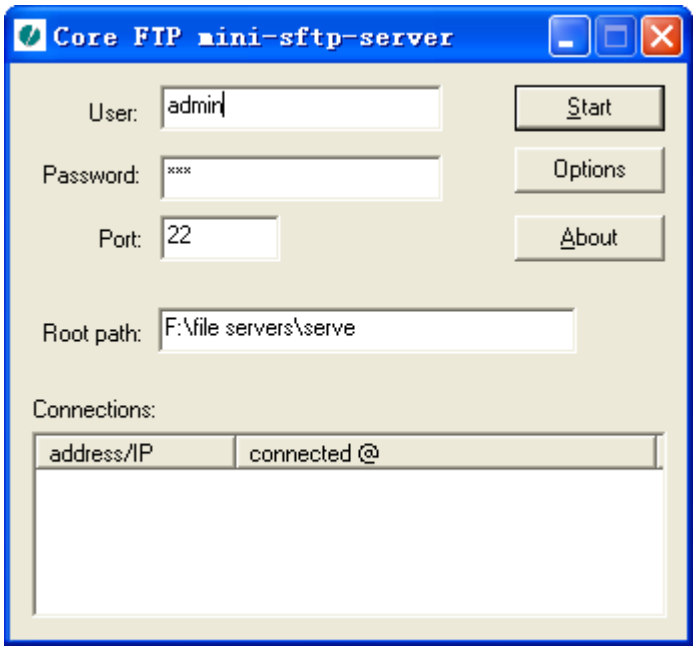


Рисунок 108 Добавление пользователя SFTP

- Щелкните [Device Basic Configuration] → [File transmit] → [SFTP Service] → [SFTP client service], чтобы перейти на страницу настройки клиента SFTP, как показано на рисунке 98.

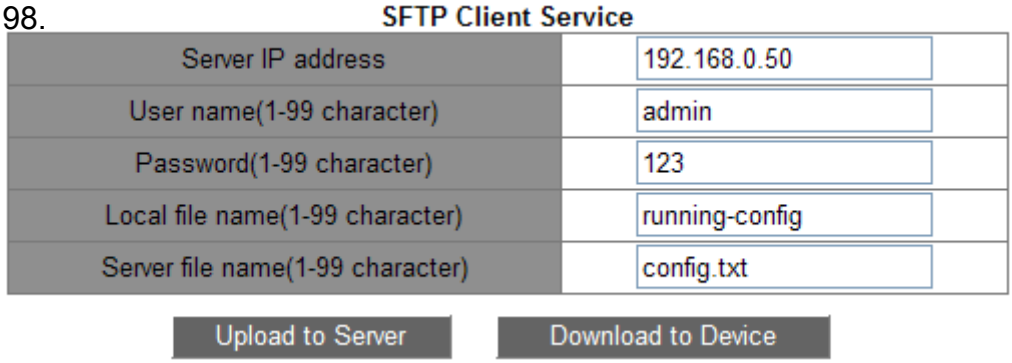


Рисунок 109 Клиент SFTP

IP-адрес сервера

Формат: A.B.C.D

Описание: Настройте IP-адрес сервера SFTP.

{ User name, Password }

Диапазон: { 1~99 символов, 1~99 символов }

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

Local file name:

Диапазон: 1~99 символов

Описание: указывает имя файла на коммутаторе.

Server file name

Диапазон: 1~99 символов

Описание: указывает имя файла на сервере.

Метод: Щелкните <Upload to Server>, чтобы выгрузить файл с коммутатора на сервер. Щелкните <Download to Device>, чтобы загрузить файл с сервера на коммутатор.

- После успешной передачи файла в веб-интерфейсе появляется следующая информация, как показано на рисунке 110 и рисунке 111.

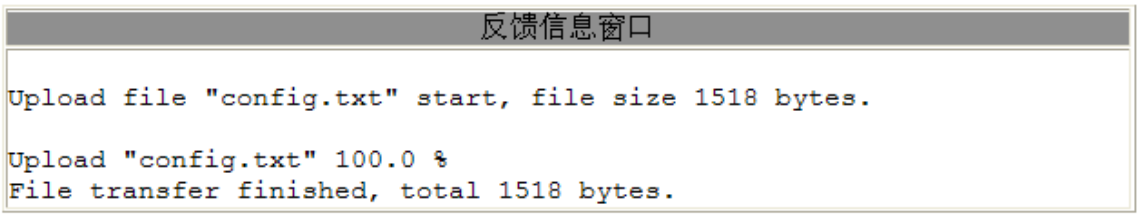


Рисунок 110 Успешная выгрузка файла по SFTP

Рисунок 111 Успешная загрузка файла по SFTP

Предупреждение:

- При передаче файла сервер SFTP должен находиться в рабочем состоянии.

5.16 Настройка MAC-адреса

5.16.1 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.

Коммутатор поддерживает не более 1024 статических одноадресных записей.

5.16.2 Настройка через веб-интерфейс

1. Настройка привязки по MAC-адресу.

Щелкните [Device Basic Configuration] → [MAC address table configuration] → [MAC bind Configuration], чтобы перейти на страницу настройки, как показано на рисунке 112.

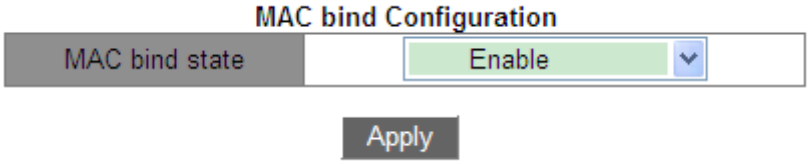


Рисунок 112 Настройка привязки по MAC-адресу.

MAC bind state

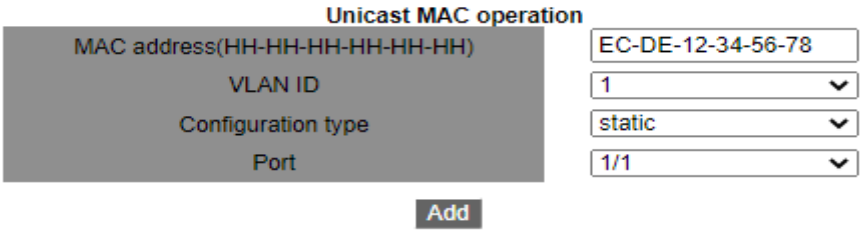
Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение или выключение функции привязки по MAC-адресу. Если выбрано значение Enable, для пакета, исходный MAC-адрес и VLAN ID которого соответствуют MAC-адресу и VLAN ID записи статического MAC-адреса Unicast, коммутатор проверяет, соответствует ли входной порт порту записи этого статического MAC-адреса Unicast. Если да, коммутатор получает и пересылает пакет. Если нет, коммутатор отбрасывает пакет. При выборе значения Disable эта проверка не выполняется.

2. Добавление статического MAC-адреса Unicast

Щелкните [Device Basic Configuration] → [MAC address configuration] → [Unicast address configuration], чтобы перейти на страницу настройки MAC-адреса Unicast, как показано на рисунке 113.



.

Рисунок 113 Добавление статической записи FDB

MAC address

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

Функция: Настройка статического MAC-адреса Unicast. Младший бит в первом байте равен 0.

VLAN ID

Варианты: все созданные VLAN ID

По умолчанию: VLAN1

Configuration type

Варианты: static/blackhole

По умолчанию: static

Функция: Выбор типа записи MAC-адреса.

Описание: Static означает установление соответствия между указанным MAC-адресом и номером порта или VLAN ID.

Blackhole означает отбрасывание пакета, исходный MAC-адрес которого или MAC-адрес назначения является указанным MAC-адресом.

Port

Варианты: все порты коммутатора.

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

Выбранный порт должен находиться в указанной VLAN.

3. Удаление адреса Unicast.

Щелкните [Device Basic Configuration] → [MAC address configuration] → [Delete unicast address], чтобы перейти на страницу настройки, как показано на рисунке 114.

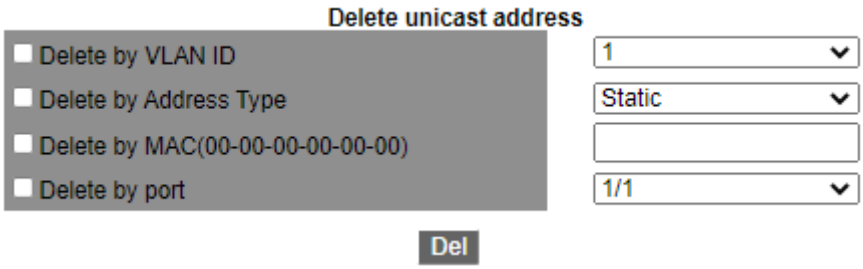


Рисунок 114 Удаление MAC-адреса Unicast.

Выберите критерий для удаления адреса Unicast. Если выбрано несколько критериев, они связаны логическим «И».

4. Настройка времени старения MAC-адреса.

Щелкните [Device Basic Configuration] → [MAC address configuration] → [MAC address aging time setting], чтобы перейти на страницу настройки времени старения, как показано на рисунке 115.

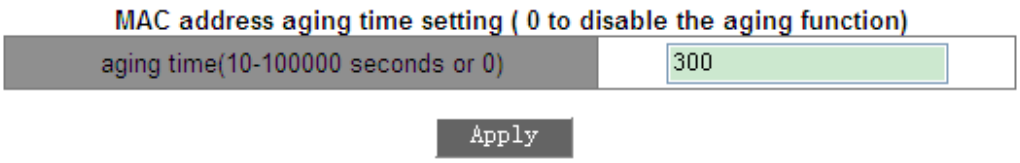


Рисунок 115 Настройка времени устаревания MAC-адреса

Aging Time

Диапазон: 10~100000 с

По умолчанию: 300 с

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

Описание: Если время старения установлено на 0, старение запрещено. В этом случае динамические адреса не устаревают со временем.

5. Запрос MAC-адресов Unicast.

Щелкните [Device Basic Configuration] → [MAC address configuration] → [MAC address query], чтобы перейти на страницу запроса MAC-адресов Unicast, как показано на рисунке 116.

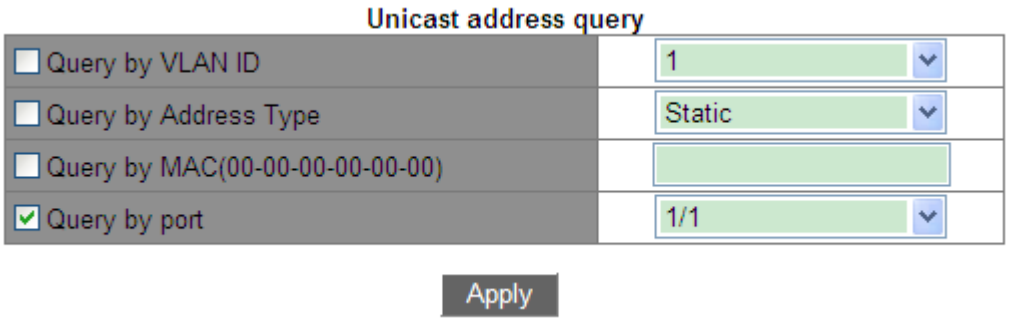


Рисунок 116 Запрос MAC-адресов Unicast

Выберите критерий для запроса MAC-адресов Unicast. Если выбрано несколько критериев, они связаны логическим «И». Например: Если запрошен адрес Unicast порта Ethernet 1/1, появится следующая страница.

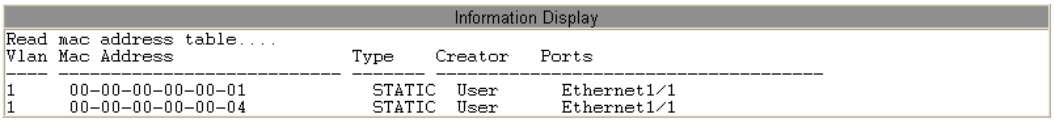


Рисунок 117 Список MAC-адресов Unicast

6. Просмотр записей адресов Unicast.

Щелкните [Device Basic Configuration] → [MAC address configuration] → [Show mac-address table], чтобы перейти на страницу запроса MAC-адресов Unicast. Отображаются все статические и динамические записи, как показано на рисунке 118.

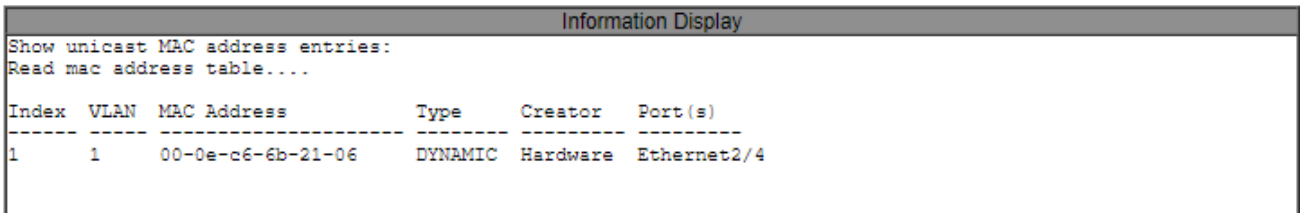


Рисунок 118 Запрос адресов Unicast

5.17 Основная информация по сопровождению конфигурации и отладке

При настройке коммутатора может потребоваться проверка правильности различных конфигураций для обеспечения нормальной работы. При возникновении определенных аномалий может потребоваться локализация неисправности. В этих случаях можно выполнить следующие операции для просмотра конфигурации системы и рабочего состояния.

1. Операция Ping.

Щелкните [Device Basic Configuration] → [Basic configuration debug] → [Ping and Traceroute], чтобы перейти на страницу Ping, как показано на рисунке 119.

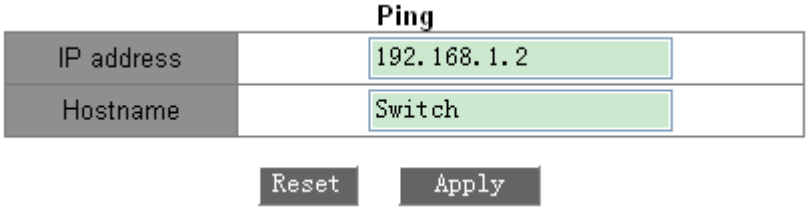


Рисунок 119 Операция Ping

IP Address

Формат: A.B.C.D

Описание: Ввод IP-адреса удаленного устройства.

Hostname

Диапазон: 1~30 символов

Функция: Если установлено сопоставление между удаленным хостом и IP-адресом, просто введите имя удаленного хоста и выполните операцию Ping.

Описание: Коммутатор отправляет пакеты запросов ICMP на удаленное устройство для обнаружения связи между коммутатором и удаленным устройством.

2. Настройте операцию Traceroute, как показано на рисунке 120.

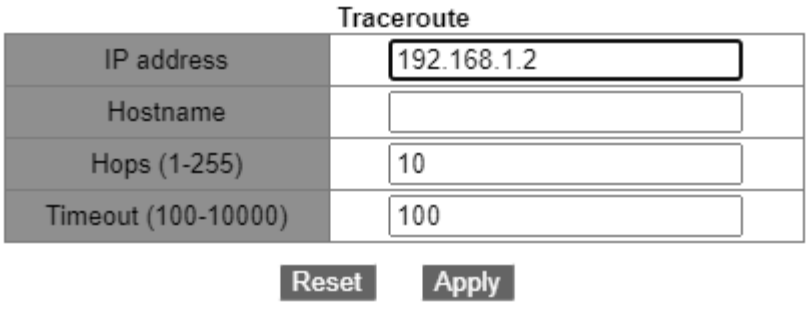


Рисунок 120 Операция Traceroute

IP Address

Формат: A.B.C.D

Описание: Ввод IP-адреса удаленного устройства.

Hostname

Диапазон: 1~30 символов

Функция: Если установлено сопоставление между удаленным хостом и IP-адресом, для выполнения операции Traceroute нужно просто ввести имя удаленного хоста.

Hops

Варианты: 1~255

Функция: Проверка количества шлюзов, которые проходят пакеты на пути между отправляющим и принимающим устройствами.

Timeout

Варианты: 100~10000 мс

Функция: Настройка времени ожидания. Если отправляющее устройство не получает ответный пакет от принимающего устройства в течение этого времени, считается, что соединения нет.

3. Просмотр системной даты и времени.

Коммутаторы этой серии поддерживают RTC. Отсчет времени продолжается даже при отключении питания.

Щелкните [Device Basic Configuration] → [Basic configuration debug] → [show clock], чтобы перейти на страницу информации часов, как показано на рисунке 121.

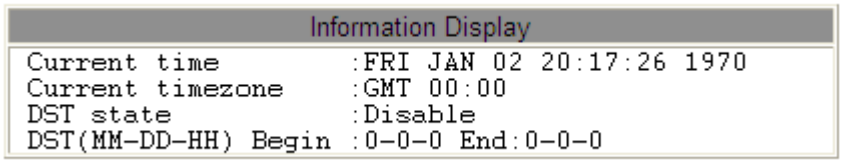


Рисунок 121 Информация часов

4. Просмотр информации во флэш-памяти.

Щелкните [Device Basic Configuration] → [Basic configuration debug] → [show flash], чтобы перейти на страницу информации, как показано на рисунке 122.

Information Display

```
Size(byte)   Last Modify          File Name
============ =================== ============================================
3210         2030-01-16 07:49:24  ssl.cky
427          2032-01-25 02:32:30  rsa_key
2048         2032-01-25 03:47:30  2222
2048         2032-01-26 01:49:36  kyland
7716778      2031-06-24 22:47:36  SICOM3028GPT-V2-L3-R1022-Build-1.3.55.B1.61.B1.1.4.bin
7524689      2031-06-29 03:08:48  SICOM3028GTP-L3-F1035.P02-Build-1.3.55.B1.9.B1.7.4.bin
5270         2031-06-29 08:11:16  c8888_SICOM6424SM_BSICOM3028GPT-L3G_V1.0.oem
159332       2031-07-01 08:16:05  Switch.cid
159332       2031-07-01 08:16:34  switch.cid
7708053      2031-07-01 08:32:05  SICOM3028GPT-V2-L3-R1022-Build-1.3.55.B1.53.4.bin
7719867      2030-01-17 11:12:50  SICOM3028GPT-V2-L3-F1064-Build-1.3.55.B1.61.B1.5.4.bin
168086       2030-01-21 04:49:53  autoerr.txt
7720948      2030-01-19 07:41:13  20210324-2-packbootromapp-L3.bin
7721239      2030-01-19 11:07:05  20210324-3-packbootromapp-L3.bin
7712236      2030-01-27 08:34:54  SICOM3028GPT-V2-L3-F1064.P01-Build-1.3.55.B1.61.B1.6.4.bin
3613         2030-10-11 05:11:02  SW5
7724791      2030-12-16 11:04:33  L3-F1068.bin
7708052      2020-07-15 00:00:17  osapp.bin
16           2030-01-16 08:39:17  11
7749220      2030-01-16 08:40:25  410845-SICOM3028GPT-L3-F1069-Build-1.3.55.B1.76.4.bin * #
24           2030-01-16 02:42:32  startup-config
--------------------------------------------------------------------------------
Total : 112852992
Free  : 35343713
--------------------------------------------------------------------------------
* : startup-file specified by user.
# : current startup-file.
================================================================================
```

Рисунок 122 Информация во флэш-памяти

5. Просмотрите информацию о конфигурации, то есть параметры после модификации.

Щелкните [Device Basic Configuration] → [Basic configuration debug] → [show running-config], чтобы перейти на страницу конфигурации, как показано на рисунке 123.

Information Display

```
Current configuration:
!
   hostname SICOM3028GPT
!
   port-group 1 load-balance src-mac
!
   telnet-user admin password 0 123
!
!
Vlan 1
   vlan 1
!
Vlan 2
   vlan 2
!
Vlan 3
   vlan 3
!
Interface Ethernet2/1
   rate-suppression bandwidth kbps 100000
   rate-suppression dlf
   port-group 1 mode on
!
Interface Ethernet2/2
   rate-suppression bandwidth kbps 500000
   rate-suppression dlf
   port-group 1 mode on
```

Рисунок 123 Информация о конфигурации

6. Просмотрите информацию о порте

Щелкните [Device Basic Configuration] → [Basic configuration debug] → [show switchport interface], чтобы перейти на страницу информации о порте, как показано на рисунке 124.

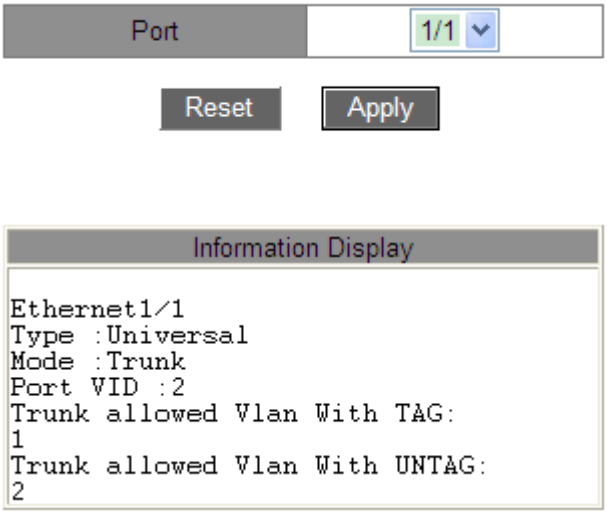


Рисунок 124 Информация о порте

Type

Описание: тип VLAN.

Mode

Описание: Режим порта

Port VID

Описание: PVID порта

Trunk allowed Vlan With TAG

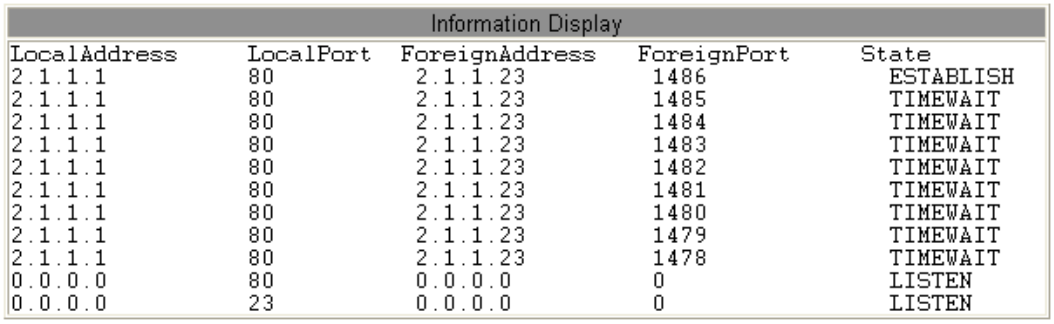
Описание: Указывает VLAN для выбранного порта Trunk как тегированные.

Trunk allowed Vlan With UNTAG

Описание: Указывает VLAN для выбранного порта Trunk как нетегированные.

7. Просмотр состояния подключения TCP.

Щелкните [Device Basic Configuration] → [Basic configuration debug] → [show tcp], чтобы перейти на страницу информации о подключении TCP, как показано на рисунке 125.



Information Display

LocalAddress	LocalPort	ForeignAddress	ForeignPort	State
2.1.1.1	80	2.1.1.23	1486	ESTABLISH
2.1.1.1	80	2.1.1.23	1485	TIMEWAIT
2.1.1.1	80	2.1.1.23	1484	TIMEWAIT
2.1.1.1	80	2.1.1.23	1483	TIMEWAIT
2.1.1.1	80	2.1.1.23	1482	TIMEWAIT
2.1.1.1	80	2.1.1.23	1481	TIMEWAIT
2.1.1.1	80	2.1.1.23	1480	TIMEWAIT
2.1.1.1	80	2.1.1.23	1479	TIMEWAIT
2.1.1.1	80	2.1.1.23	1478	TIMEWAIT
0.0.0.0	80	0.0.0.0	0	LISTEN
0.0.0.0	23	0.0.0.0	0	LISTEN

Рисунок 125 Подключение TCP

Local Address

Описание: указывает локальный адрес подключения TCP.

Local Port

Описание: указывает номер локального порта подключения TCP.

Foreign Address

Описание: указывает адрес на другом конце TCP-подключения.

Foreign Port

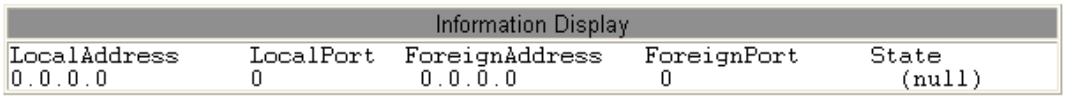
Описание: указывает номер порта на другом конце TCP-подключения.

State

Описание: указывает текущее состояние подключения TCP.

8. Просмотр состояния подключения UDP.

Щелкните [Device Basic Configuration] → [Basic configuration debug] → [show udp], чтобы перейти на страницу информации о подключении UDP, как показано на рисунке 126.



Information Display

LocalAddress	LocalPort	ForeignAddress	ForeignPort	State
0.0.0.0	0	0.0.0.0	0	(null)

Рисунок 126 Информация о подключении UDP

Local Address

Описание: указывает локальный адрес подключения UDP.

Local Port

Описание: указывает номер локального порта подключения UDP.

Foreign Address

Описание: указывает IP-адрес на другом конце UDP-подключения.

Foreign Port

Описание: указывает номер порта на другом конце UDP-подключения.

State

Описание: указывает текущее состояние подключения UDP.

9. Просмотр информации о пользователях, выполнивших вход.

Щелкните [Device Basic Configuration] → [Basic configuration debug] → [show login], чтобы перейти на страницу информации о пользователях, выполнивших вход, как показано на рисунке 127.

Information Display

No.	Name	Level	Login	Authen	IP Address	Time(min)
1	444	guest	ssh	local	192.168.0.184	0
2	333	guest	ssh	local	192.168.0.184	2
3	222	system	telnet	local	192.168.0.184	2
4	111	guest	telnet	local	192.168.0.184	3
5	admin	admin	web	local	192.168.0.184	3
6	111	guest	console	local	----	3

Рисунок 127 Пользователи, выполнившие вход

10. Просмотр информации модуля SFP

Щелкните [DeviceBasic Configuration]→[Basic configuration debug]→[showtransceiver information], чтобы перейти на страницу информации модуля SFP, как показано на рисунке 128.

Information Display

```
Vendor name          :OPWAY
Vendor PN            :OP3405DI
Vendor rev           :
Vendor SN            :1507310011
TransLen(MediaType):550m(MMF_62P5UM_OM1)
                     550m(MMF_50UM_OM2)
DDMI                 :Int_Calibrate
```

Рисунок 128 Просмотр информации модуля SFP

DDMI для SFP без цифровой диагностики недоступна.

6. Расширенная конфигурация устройства

6.1 Настройка ARP

6.1.1 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.

6.1.2 6.1.2 Пояснения

Записи ARP делятся на динамические и статические.

Динамические записи генерируются и поддерживаются на основе обмена пакетами ARP. Динамические записи могут устаревать, обновляться новым пакетом ARP или перезаписываться статической записью ARP.

Статические записи настраиваются и поддерживаются вручную. Они никогда не устаревают и не перезаписываются динамическими записями ARP.

Коммутатор поддерживает до 512 записей ARP (максимум 256 статических). Когда количество записей ARP превышает 512, новые записи автоматически перезаписывают старые динамические записи.

6.1.3 Прокси-ARP

Если запрос ARP отправляется с хоста на другой хост, который находится в том же сетевом сегменте, но в другой физической сети, шлюз, на котором реализована функция прокси-ARP, находящийся в прямом соединении с хостом-источником, может ответить на это сообщение запроса. Этот процесс называется прокси-ARP.

Процесс прокси-ARP выглядит так:

1. Хост-источник отправляет запрос ARP на другой хост в другой физической сети.
2. Функция proxy ARP на этом интерфейсе VLAN была включена на шлюзе, имеющем прямое соединение с исходным узлом. Если нормальный маршрут к целевому хосту существует, шлюз отвечает своим собственным MAC-адресом для хоста назначения.
3. IP-пакеты, отправляемые с исходного узла на узел назначения, отправляются на устройство с включенной функцией proxy ARP.
4. Шлюз выполняет обычную IP-маршрутизацию и пересылку пакетов.
5. IP-пакеты, которые должны быть отправлены на узел назначения, достигают узла назначения через сеть.

Предупреждение:

Прокси не используется для запросов ARP, соответствующих маршрутизации по умолчанию.

6.1.4 Настройка через веб-интерфейс

1. Добавьте или удалите статическую запись ARP.

Щелкните [Device Advanced Configuration] → [ARP configuration] → [ARP configuration], чтобы перейти на страницу настройки ARP, как показано на рисунке 129.

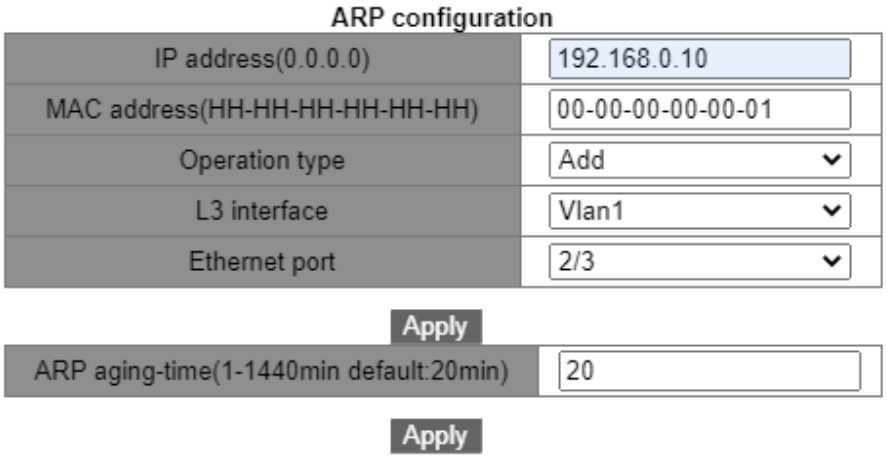


Рисунок 129 Настройка статической записи ARP.

IP Address

Формат: A.B.C.D

Функция: Настройка IP-адреса статической записи ARP.

MAC address

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

Функция: Настройка MAC-адреса статической записи ARP.

Operation type

Варианты: Add/Del

По умолчанию: Add

Функция: Добавление или удаление статической записи ARP.

L3 interface

Варианты: все созданные интерфейсы VLAN Layer-3

По умолчанию: VLAN1

Функция: Выбор интерфейса VLAN Layer-3 для текущей записи ARP.

Ethernet Port

Варианты: все порты выбранной VLAN

Функция: Выбор выходного порта для текущей записи ARP.

ARP Aging time

Диапазон：1 ~ 1440 мин

По умолчанию：20 мин

Функция：Настройка времени устаревания ARP.

Описание: Время старения ARP — это промежуток с момента добавления динамической записи ARP в таблицу до момента удаления записи из таблицы.

Предупреждение:

- IP-адрес, связанный со статической записью ARP, не может быть IP-адресом коммутатора.
- К одному MAC-адресу можно привязать разные IP-адреса.
- В VLAN запись ARP может соответствовать только одному порту пересылки.
- Как правило, коммутатор автоматически запоминает записи ARP без вмешательства администратора.

2. Просмотр записи адресов ARP.

Щелкните [Device Advanced Configuration] → [ARP configuration] → [Show ARP], чтобы перейти на страницу настройки ARP, как показано на рисунке 130.

ARP list

IP address	MAC address	L3 interface	Ethernet port	Type
192.168.0.120	90-b1-1c-23-71-12	Vlan1	2/3	dynamic
192.168.0.23	00-00-00-00-00-01	Vlan1	2/3	static
192.168.0.199	70-71-bc-95-cc-22	Vlan1	2/3	dynamic
192.168.0.192	78-2b-cb-2c-6b-87	Vlan1	2/3	dynamic
192.168.0.7	00-00-00-00-19-39	Vlan1	2/3	dynamic
192.168.0.223	00-1e-cd-11-01-b1	Vlan1	2/3	dynamic
192.168.0.2	00-00-00-00-00-02	Vlan1	2/3	dynamic
192.168.0.253	12-2a-bd-c3-44-55	Vlan1	2/3	dynamic
192.168.0.1	00-00-bb-bb-94-19	Vlan1	2/3	dynamic
192.168.0.184	44-37-e6-88-6e-90	Vlan1	2/3	dynamic
192.168.0.9	40-16-9f-f3-85-de	Vlan1	2/3	dynamic

Refresh

Рисунок 130 Список ARP

Список ARP

Состав: {IP address, MAC address, L3 interface, Ethernet port, Type}

Function: Просмотр записей ARP.

Описание: Список ARP показывает все записи ARP, соответствующие портам в состоянии LinkUp, включая статические записи и динамические записи.

3. Очистка кэша ARP.

Щелкните [Device Advanced Configuration] → [ARP configuration] → [Clear ARP cache], чтобы очистить кэш ARP, как показано на рисунке 131.

Рисунок 131 Очистка кэша ARP

Щелкните <Apply>, чтобы стереть динамические записи ARP в кэше.

4. Включение proxy ARP

Щелкните[Device Advanced Configuration] → [ARP configuration] → [Proxy ARP configuration], чтобы настроить proxy ARP, как показано на рисунке 132.

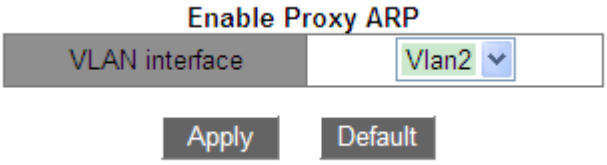


Рисунок 132 Настройка proxy ARP

Интерфейс VLAN

Функция: Выбор интерфейса VLAN 3-layer для включения прокси-ARP.

6.1.5 Типовой пример конфигурации

Как показано на рисунке 133, ПК1, ПК2 и ПК3 — это хосты в одном сегменте сети, принадлежащие к разным подсетям VLAN1, VLAN2 и VLAN4 соответственно.

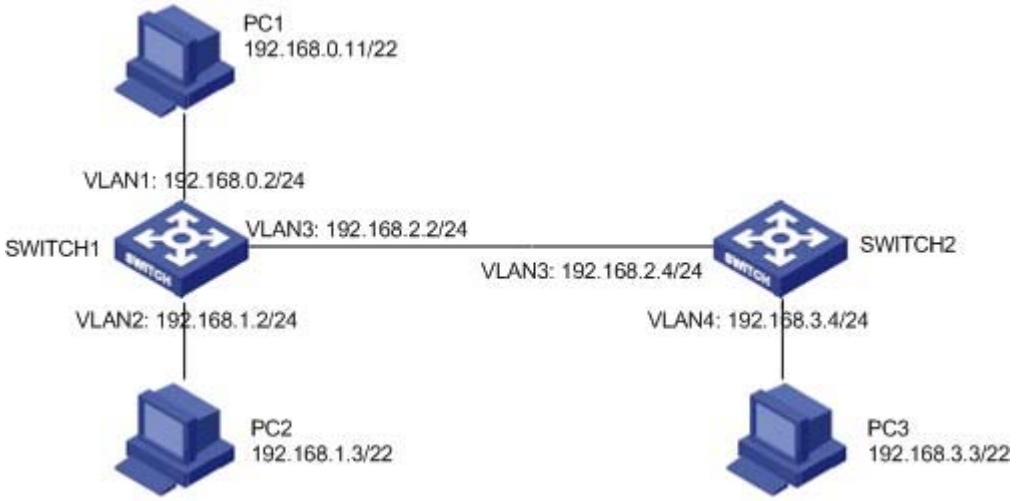


Рисунок 133 Пример настройки прокси-ARP

ПК1 посылает широковещательный запрос ARP, запрашивая MAC-адреса ПК2 и ПК3.

- Когда функция прокси-ARP в интерфейсе VLAN1 коммутатора SWITCH1 не включена, запрос ARP не может достичь ПК2 или ПК3, поскольку они находятся в разных с ПК1 VLAN, и связь между двумя сторонами невозможна.
- Когда функция прокси-ARP на интерфейсе VLAN1 коммутатора SWITCH1 включена, после получения запроса ARP через интерфейс VLAN1 коммутатор 1 проверяет таблицу маршрутизации и определяет маршруты к ПК2 и ПК3, а затем использует MAC-адрес интерфейса VLAN1 для отправки ответных ARP-сообщений (с исходными IP-адресами, являющимися IP-адресами ПК2 и ПК3). После получения ответного сообщения ПК1 создаёт запись в своей ARP-таблице для отправки последующих IP-пакетов в направлении ПК2 и ПК3 на интерфейс VLAN1 коммутатора 1, который затем выполняет переадресацию.

6.2 Настройка интерфейса Layer-3

6.2.1 IP Address коммутатора

Войдите в интерфейс командной строки коммутатора через порт консоли. Выполните команду **enable** в общем режиме, чтобы войти в привилегированный режим Выполните команду **show interface vlan 1**, чтобы увидеть IP-адрес коммутатора, как показано в красном круге на рисунке 134.

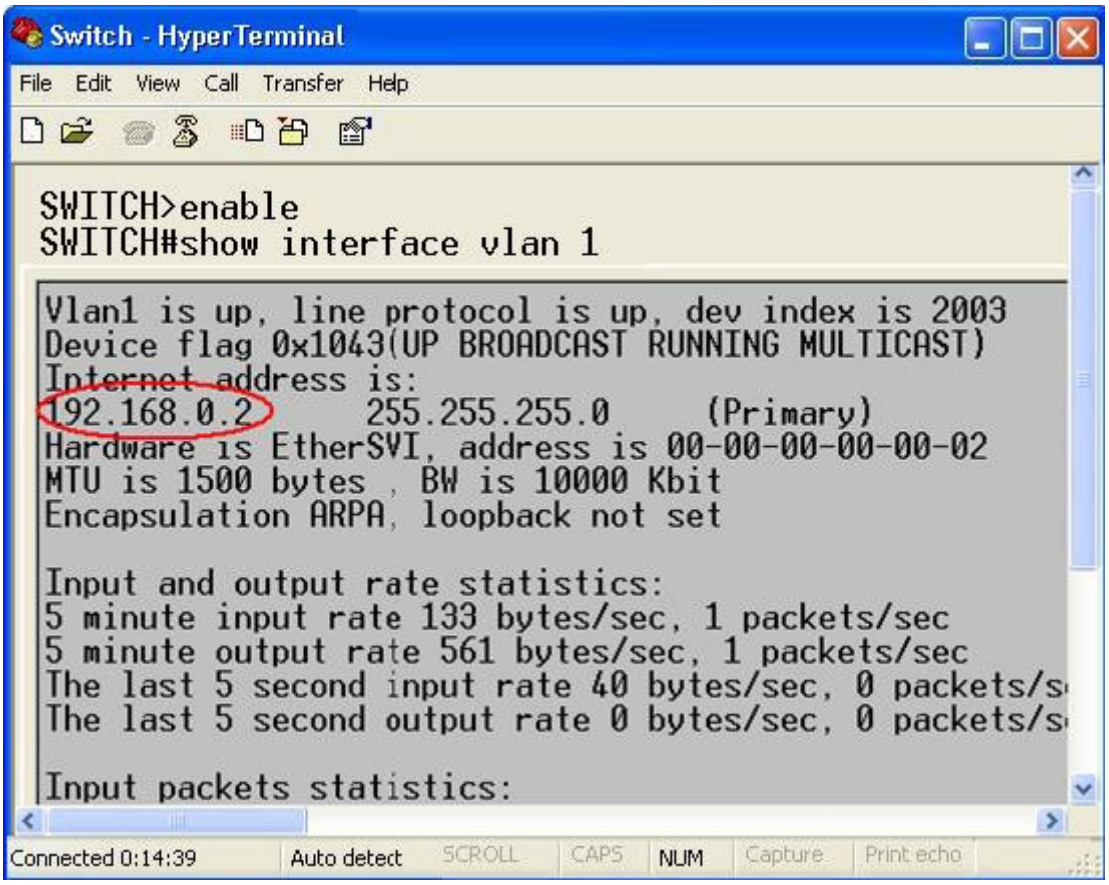


Рисунок 134 Отображение IP-адреса

6.2.2 Настройка IP-адреса

1. Создание интерфейса VLAN Layer-3.

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

Коммутаторы данной серии поддерживают VLAN-интерфейсы, которые представляют

собой виртуальные интерфейсы уровня 3, используемые для связи между VLAN. Для каждой VLAN можно создать один VLAN-интерфейс. Интерфейс используется для пересылки пакетов уровня 3 в VLAN.

Щелкните [Device Advanced Configuration] → [L3 interface configuration] → [Add interface VLAN], чтобы перейти на страницу настройки, как показано на рисунке 135.

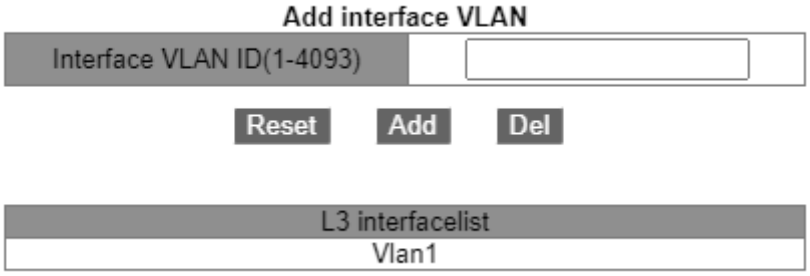


Рисунок 135 Создание интерфейса VLAN

Interface vlan ID

Варианты: все созданные номера VLAN

Функция: Создание интерфейса VLAN Layer-3.

Примечание:

- Коммутатор поддерживает не более 16 интерфейсов VLAN Layer-3.
- Перед созданием интерфейса VLAN убедитесь в наличии соответствующей VLAN. Если VLAN не существует, ее интерфейс VLAN не может быть создан.
- Нельзя удалить интерфейс VLAN, соответствующий IP-адрес которого используется для доступа к коммутатору через Интернет.

2. Получение IP-адреса

IP-адрес коммутатора можно настроить вручную или получить автоматически. Щелкните [Device Advanced Configuration] → [L3 interface configuration] → [L3 interface IP address mode configuration], чтобы перейти на страницу настройки IP-адреса интерфейса L3, как показано на рисунке 135.

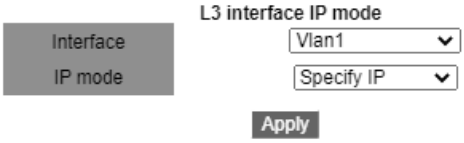


Рисунок 136 Получение IP-адреса

Интерфейс

Варианты: все созданные интерфейсы VLAN Layer-3

По умолчанию: VLAN1

IP Mode

Варианты: bootp-client/dhcp-client/Specify IP

По умолчанию: Specify IP

Функция: Выбор режима получения IP-адреса.

Описание: Specify IP – настроить IP-адрес вручную; bootp-client/dhcp-client – коммутатор автоматически получает IP-адрес через DHCP/BOOTP. В сети должен быть DHCP/BOOTP-сервер для назначения клиентам IP-адресов. О настройке сервера DHCP/BootP см. 6.14 Настройка DHCP.

3. Задание IP-адреса вручную.

Щелкните [Device Advanced Configuration] → [L3 interface configuration] → [Allocate IP address for L3 port], чтобы назначить IP-адрес, как показано на рисунке 137.

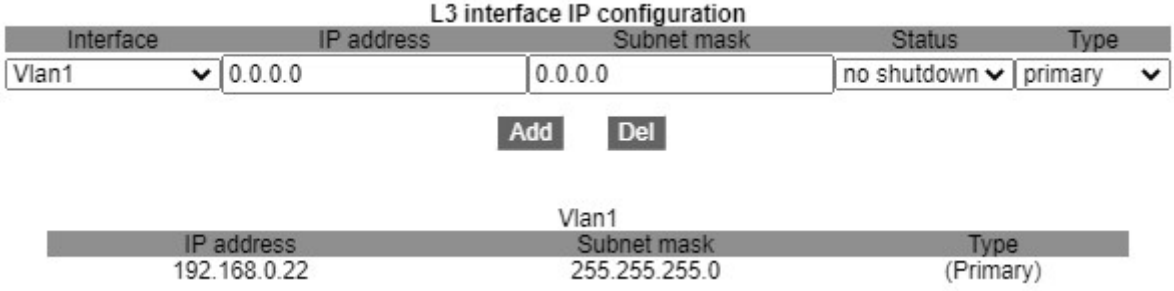


Рисунок 137 Настройка IP-адреса

IP Address

Формат: A.B.C.D

Функция: Настройка IP-адреса для указанного интерфейса VLAN Layer-3.

Маска 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.

Состояние

Варианты: shutdown/no shutdown

По умолчанию: no shutdown

Функция: Настройка состояния интерфейса VLAN Layer-3.

Описание: no shutdown: открывает интерфейс VLAN Layer-3. Shutdown: закрывает интерфейс VLAN Layer-3.

Type

Варианты: secondary/primary

По умолчанию: primary

Функция: На одном и том же порту можно установить более двух IP-адресов разных сетевых сегментов для реализации связи между разными сетевыми сегментами в одной и той же локальной сети. В целом, поскольку сегмента сети пользователю недостаточно, можно использовать этот метод.

Описание: вторичный IP-адрес может решить проблему агрегации маршрутизации в RIP v1. Его можно использовать для NAT, после преобразования он не является адресом прямого подключения маршрутизатора.

Щелкните <Add>, чтобы настроить IP-адрес для интерфейса VLAN; щелкните <Del>, чтобы удалить текущий IP-адрес, нужно сначала удалить вторичный IP-адрес, прежде чем удалять основной IP-адрес; нажмите <Update>, чтобы изменить основной IP-адрес интерфейса VLAN.

Примечание:

- Каждый интерфейс VLAN Layer-3 поддерживает не более 32 IP-адресов.
- Для каждого интерфейса VLAN можно настроить IP-адреса одного и того же сегмента сети или разных сегментов сети.
- IP-адреса разных сегментов сети должны быть настроены для разных интерфейсов VLAN.

6.3 SNMPv2c

6.3.1 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.

6.3.2 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.

6.3.3 Пояснения

Коммутаторы этой серии поддерживают SNMPv2 и SNMPv3. SNMPv2 совместим с SNMPv1. SNMPv1 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.

SNMPv2 также использует для аутентификации имя сообщества. Он совместим с SNMPv1 и расширяет функционал SNMPv1.

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.

6.3.4 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 138 показаны взаимоотношения между NMS, агентом и MIB.

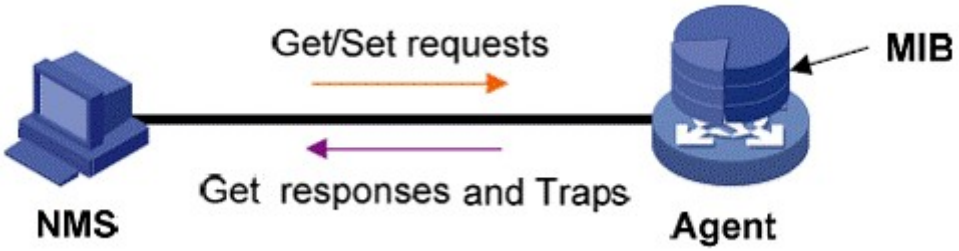


Рисунок 138 Взаимоотношения между NMS, агентом и MIB

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 139, OID объекта A – 1.2.1.1.

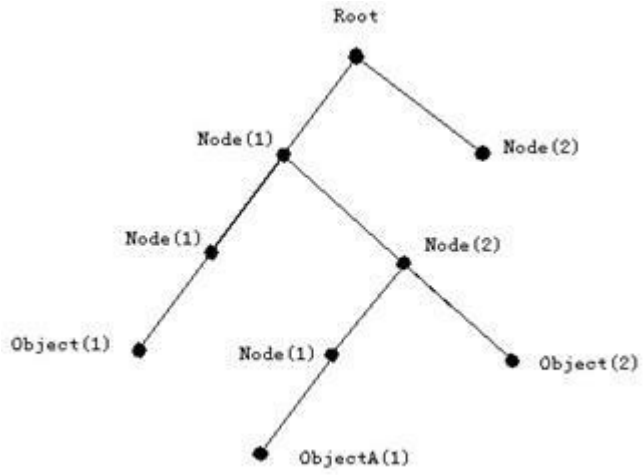


Рисунок 139 Структура MIB

6.3.5 Настройка через веб-интерфейс

1. Настройка SNMPv2

Щелкните [Device Advanced Configuration] → [SNMP Configuration] → [SNMP Base Configuration] чтобы настроить SNMPv2, как показано на рисунке 140.

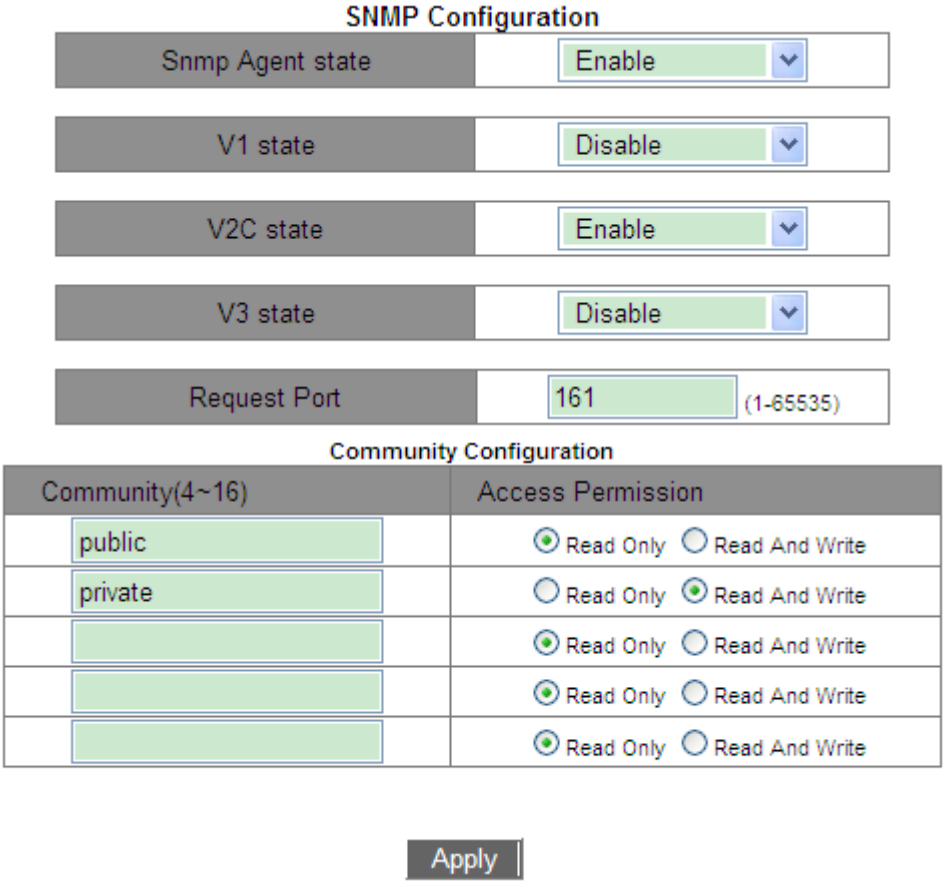


Рисунок 140 Настройка SNMPv2

Snmp Agent state

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение SNMP.

V1/V2C/V3 state

Варианты: Enable/Disable

Функция: Выбор версии SNMP.

Request Port

Диапазон: 1~65535

По умолчанию: 161

Функция: Настройка номера порта для получения запросов SNMP.

Сообщество

Диапазон: 4~16 символов

Функция: Настройка соодбщества коммутатора.

Описание: Пакет может получить доступ к MIB коммутатора, только если имя сообщества, передаваемое в пакете SNMP, совпадает с этой строкой community.

Пояснение: Можно настроить не более 5 строк community.

Access Permission

Варианты: Read Only/Read And Write

По умолчанию: Read Only

Функция: Настройка режима доступа MIB.

Описание: Read only: только чтение информации MIB. Read and write: чтение и запись информации MIB.

2. Настройка безопасного IP-адреса.

Щелкните [Device Advanced Configuration] → [SNMP Configuration] → [IP Address of SNMP Manager], чтобы перейти на страницу настройки безопасного IP-адреса, как показано на рисунке 141.

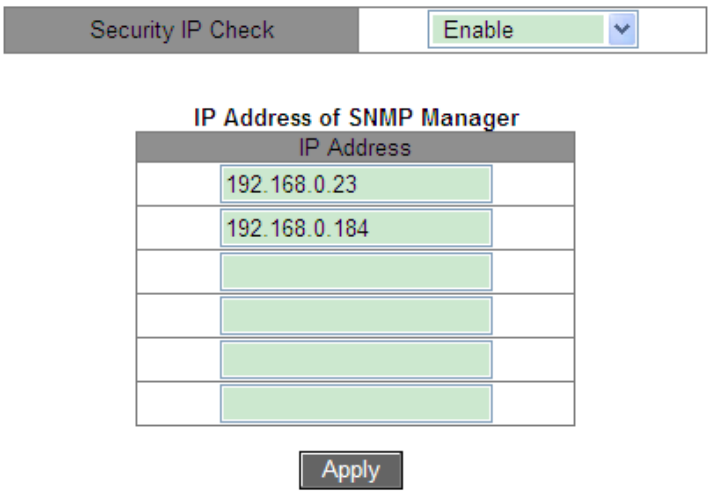


Рисунок 141 Настройка безопасного IP-адреса

Security IP Check

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение проверки безопасного IP. Если проверка безопасности IP отключена, нет ограничений на IP-адрес NMS, любая NMS, подключенная к коммутатору, может получить доступ к информации MIB коммутатора. После того, как проверка IP-адреса безопасности включена, необходимо задать безопасный установить IP-адрес, и только NMS с безопасным IP-адресом может получить доступ к информации MIB коммутатора.

IP Address

Формат: A.B.C.D

Функция: Настройка безопасного IP-адрес NMS.

Описание: Только NMS, адрес которой совпадает с безопасным IP-адресом может получить доступ к информации MIB коммутатора. Коммутатор поддерживает не более 6 безопасных IP-адресов NMS.

3. Настройка Trap.

Щелкните [Device Advanced Configuration] →[SNMP Configuration]→[TRAP Configuration], чтобы настроить trap, как показано на рисунке 142.

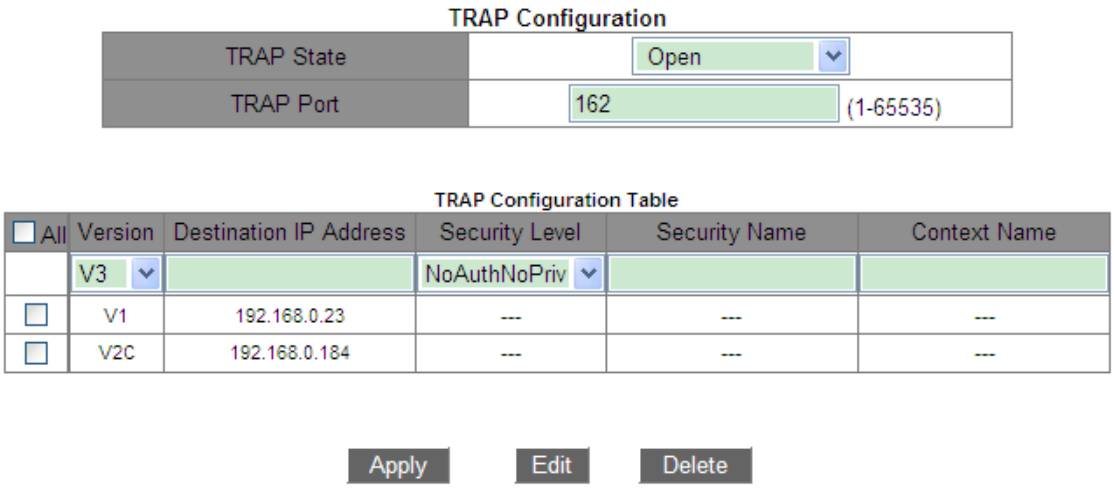


Рисунок 142 Включение Trap

TRAP State

Варианты: Open/Close

По умолчанию: Close

Функция: разрешение/запрет отправки сообщений Trap.

TRAP Port

Варианты: 1~65535

По умолчанию: 162

Функция: Настройка номера порта для отправки сообщений Trap.

Version

Варианты: V1/V2C/V3

Функция: V1/V2C указывает, что коммутатор отправляет сообщения trap версии 1/версии 2C на сервер. V3 указывает, что коммутатор отправляет сообщения trap версии 3 на сервер. При выборе V1/V2C необходимо настроить только IP-адрес назначения.

Destination IP Address

Формат: A.B.C.D

Функция: Настройка адреса сервера для приема сообщений Trap. Вы можете настроить не более 8 серверов, то есть 8 записей trap.

4. Просмотр статистики SNMP.

Щелкните [Device Advanced Configuration] → [SNMP Configuration] → [SNMP Statistics], чтобы перейти на страницу статистики SNMP, как показано на рисунке 143.

SNMP Statistics	number
Incoming Snmp Packet	37
Version Error Snmp Packet	0
Received Snmp GetNext Packet	4
Received SET Request Packet	2
Outgoing Snmp Packet	20
Too_big Error Snmp Packet	0
Max-Length of Snmp Datagram	1500
Snmp Request for Inexistent MIB Object	0
Bad_value Error Snmp Packet	0
General_error Snmp Packet	0
Transmitting Response Packet	12
Transmitting TRAP Packet	8
Nms SET Request Packet	2
Communitry String Error Snmp Packet	0
Communitry String Priority Error	6
Coding Error Snmp Packet	0

Show

Рисунок 143 Статистика SNMP

6.3.6 Типовой пример конфигурации

Управляющий сервер SNMP подключается к коммутатору через Ethernet. IP-адрес сервера управления — 192.168.0.23, а коммутатора — 192.168.0.2. NMS отслеживает и управляет агентом через SNMPv2c, а также считывает и записывает информацию узла MIB агента. Когда агент неисправен, он упреждающе отправляет пакеты Trap в NMS, как показано на рисунке 144.

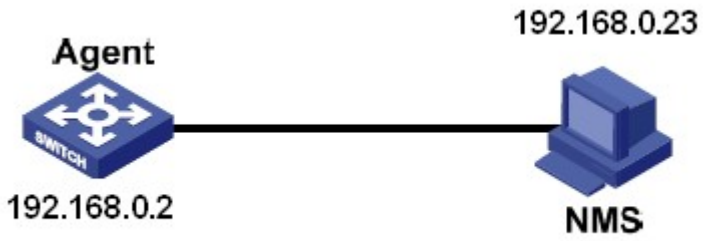


Рисунок 144 Пример настройки SNMPv2

Настройка агента:

1. Включите SNMP и V2C; настройте права доступа сообщества Read only – public и сообщества Read and write – private, как показано на рисунке 140.

2. Задайте IP-адрес 192.168.0.23, как показано на рисунке 141.

3. Включить состояние trap; установите версию trap V2C, IP-адрес назначения 192.168.0.23, как показано на рисунке 142.

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*.

6.4 SNMPv3

6.4.1 Введение

SNMPv3 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.

6.4.2 Реализация

SNMPv3 предоставляет пять таблиц 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 контекста идентифицирует строки, которые могут быть прочитаны пользователями, независимо от моделей безопасности.

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, названию контекста, модели безопасности и уровню безопасности.

6.4.3 Настройка через веб-интерфейс

1. Настройка таблицы пользователей

Щелкните [Device Advanced Configuration] → [SNMP Configuration] → [V3 User Table], чтобы перейти на страницу настройки таблицы пользователей V3, как показано на рисунке 145.

V3 User Table

Number	State	User Name	Authentication protocol	Authentication password	Privacy protocol	Privacy password
1	active	1111	HMAC-MD5	••••	HMAC-DES	••••
2	active	2222	HMAC-SHA	••••	HMAC-DES	••••
3	----		NONE		NONE	
4	----		NONE		NONE	
5	----		NONE		NONE	
6	----		NONE		NONE	
7	----		NONE		NONE	
8	----		NONE		NONE	
9	----		NONE		NONE	
10	----		NONE		NONE	
11	----		NONE		NONE	
12	----		NONE		NONE	
13	----		NONE		NONE	
14	----		NONE		NONE	
15	----		NONE		NONE	
16	----		NONE		NONE	

Apply

Рисунок 145 Настройка таблицы пользователей SNMPv3

User Name

Диапазон: 1~16 символов

Функция: Создание имени пользователя.

Authentication protocol

Варианты: NONE/HMAC-MD5/HMAC-SHA

По умолчанию: NONE

Функция: Выбор алгоритма аутентификации.

Authentication password

Диапазон: 4~16 символов

Функция: Создание пароля аутентификации

Privacy Protocol

Варианты: NONE/CBC-DES

По умолчанию: NONE

Функция: Выбор протокола шифрования пакета.

Privacy Password

Диапазон: 4~16 символов

Функция: Создание пароля шифрования пакета.

2. Настройка таблицы групп

Щелкните [Device Advanced Configuration] → [SNMP Configuration] → [V3 Group Table], чтобы перейти на страницу настройки таблицы групп V3, как показано на рисунке 146.

V3 Group Table

Number	GroupName	SecurityName	SecurityModel
1	group	1111	SNMP V3
2	group	2222	SNMP V3
3			SNMP V3
4			SNMP V3
5			SNMP V3
6			SNMP V3
7			SNMP V3
8			SNMP V3
9			SNMP V3
10			SNMP V3
11			SNMP V3
12			SNMP V3
13			SNMP V3
14			SNMP V3
15			SNMP V3
16			SNMP V3

Apply

Рисунок 146 Настройка таблицы групп SNMPv3

Group Name

Диапазон: 4~16 символов

Функция: Настройка имени таблицы групп.

Security Name

Диапазон: все существующие имена пользователей, 4~16 символов

Функция: Настройка имени безопасного пользователя. Имя должно совпадать с именем пользователя в таблице пользователей. Пользователи с одинаковым именем группы принадлежат к одной группе.

Security Model

По умолчанию: SNMPv3

Описание: SNMPv3 указывает на использование модели безопасности на основе пользователей (USM). Сейчас значение должно быть SNMPv3.

3. Настройка таблицы контекста

Щелкните Click [Device Advanced Configuration] → [SNMP Configuration] → [V3 Context Table], чтобы перейти на страницу настройки таблицы контекста V3, как показано на рисунке 147.

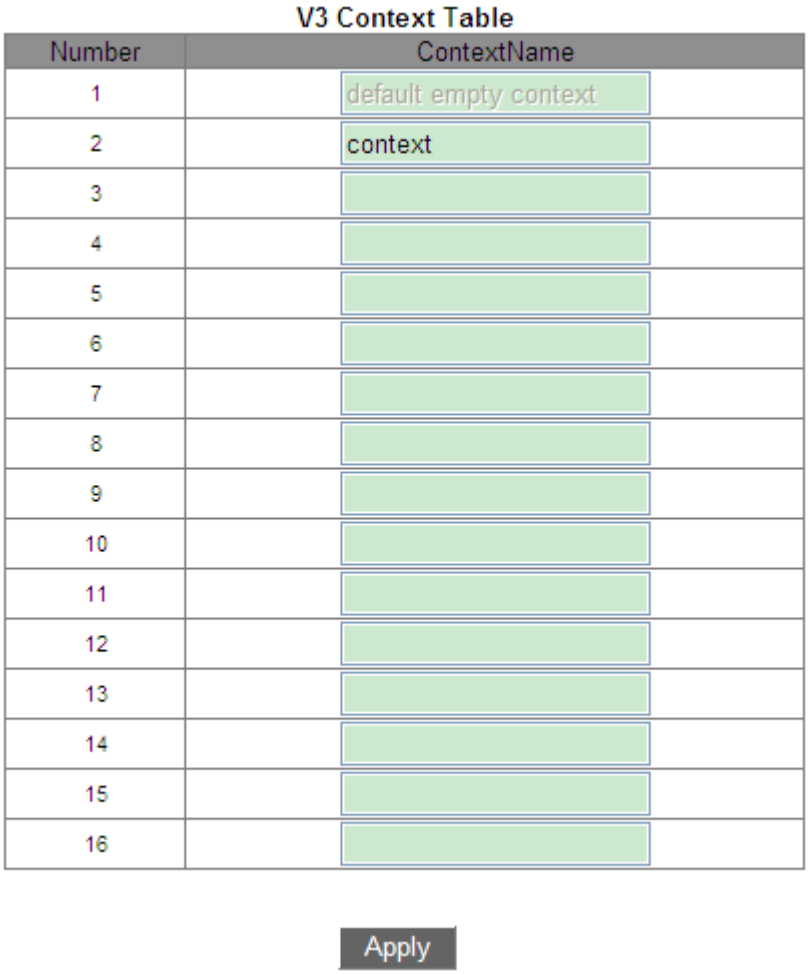


Рисунок 147 Настройка таблицы контекста SNMPv3

Context Name

Диапазон: 4~16 символов

Функция: Настройка имени контекста

Описание: Первое контекстное имя должно быть пустым.

4. Настройка таблицы представлений

Щелкните [Device Advanced Configuration] → [SNMP Configuration] → [V3 View Table], чтобы перейти на страницу настройки таблицы представлений V3, как показано на рисунке 148.

V3 View Table

Index	View Name	Type	oid-tree	mask
1	view1	included	1.3.6.1.2.1.1.1	0xfd,0xff,0xff,0xff
2	view2	excluded	1.3.6.1.2.1.1.1	0xff,0xff,0xff,0xff
3	view-no	excluded	1	0xff,0xff,0xff,0xff
4	view-all	included	1	0xff,0xff,0xff,0xff
5		included		
6		included		
7		included		
8		included		
9		included		
10		included		
11		included		
12		included		
13		included		
14		included		
15		included		
16		included		

Apply

Рисунок 148 Настройка таблицы представлений SNMPv3

View Name

Диапазон: 4~16 символов

Функция: Настройка имени представления

Type

Варианты: included/excluded

По умолчанию: included

Функция: Included указывает, что текущее представление включает все узлы дерева MIB. Excluded указывает, что текущее представление не включает узлы дерева MIB. **oid-tree**

Функция: Дерево MIB, указанное OID корневого узла дерева.

Mask

Функция: Маска дерева MIB. Параметры oid-tree и mask вместе определяют вместе определяют информацию об узле MIB текущего представления.

Например, на рисунке 148 представление view1 может получить доступ только к информации узла 1.3.6.1.2.1.1.1, 1.3.6.1.2.1.2.1, 1.3.6.1.2.1.3.1 и 1.3.6.1.2.1.4.1… 1.3.6.1.2.1.n.1.

5. Настройка таблицы доступа

Щелкните [Device Advanced Configuration] → [SNMP Configuration] → [V3 Access Table], чтобы перейти на страницу настройки таблицы доступа V3, как показано на рисунке 149.

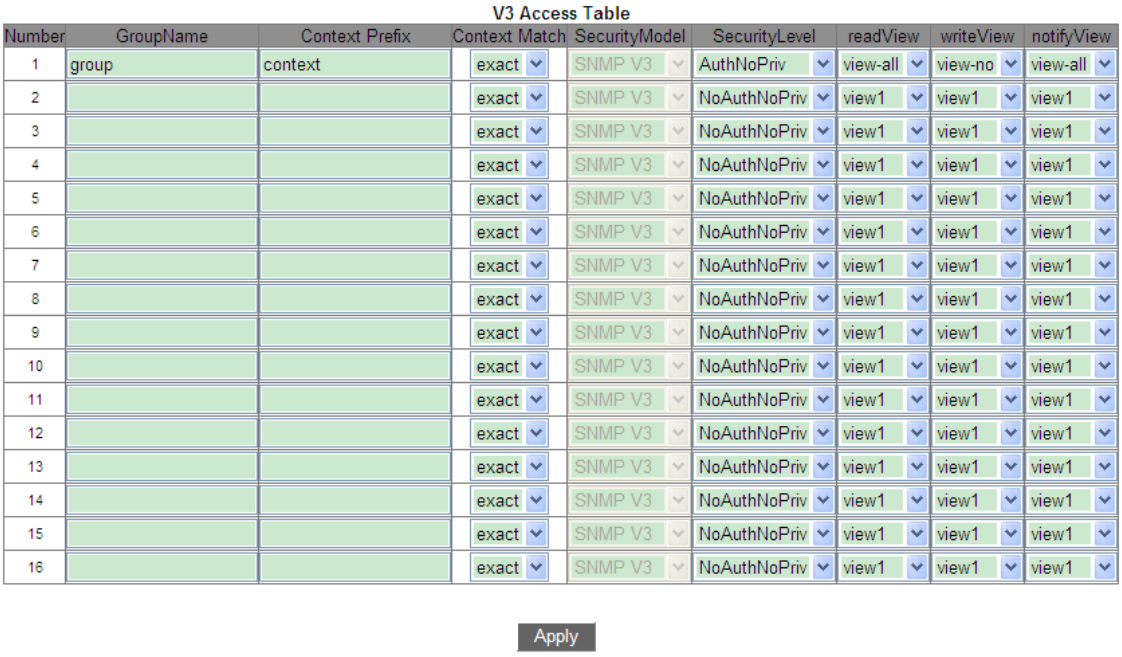


Рисунок 149 Настройка таблицы доступа SNMPv3

Group Name

Диапазон: все существующие имена групп, 4~16 символов

Функция: Пользователи в группе имеют одинаковые права доступа.

Context Prefix

Диапазон: все существующие имена контекста, 4~16 символов

Функция: Настройка имени контекста. Имя группы и имя контекста вместе определяют права доступа группы. Поскольку первое имя контекста в таблице контекстов должно быть пустым, префикс контекста может быть пустым.

Context Match

Варианты: exact/prefix

По умолчанию: exact

Функция: Выбор режима соответствия имени контекста. Exact указывает, что значение префикса контекста должно совпадать с именем контекста. Prefix указывает, что значение префикса контекста должно совпадать с первыми 4–16 символами имени контекста. В этом случае имена контекстов с одинаковым префиксом имеют одинаковые права доступа.

Security Model

По умолчанию: SNMP V3

Описание: SNMPv3 указывает на использование модели безопасности на основе пользователей (USM). Сейчас значение должно быть SNMPv3.

Security Level

Варианты: NoAuthNoPriv/AuthNoPriv/AuthPriv

По умолчанию: NoAuthNoPriv

Функция: Выбор прав доступа для информации MIB.

Описание: NoAuthNoPriv указывает, что ни аутентификация, ни шифрование пакета не требуются. AuthNoPriv указывает, что требуется аутентификация, но не требуется шифрование пакета. AuthPriv указывает, что требуется и аутентификация, и шифрование пакета. Когда требуется шифрование, пользователь может получить доступ к указанной информации MIB только в том случае, если алгоритм шифрования и пароль идентичны настроенным в пользовательской таблице.

read View

Варианты: все существующие имена представлений

Функция: Задание имени представления read-only.

write View

Варианты: все существующие имена представлений

Функция: Задание имени представления write.

notify View

Варианты: все существующие имена представлений

Функция: Задание имени представления, которое может отправлять сообщения trap.

6. Настройка безопасного IP-адреса.

Щелкните [Device Advanced Configuration] → [SNMP Configuration] → [IP Address of SNMP Manager], чтобы перейти на страницу настройки безопасного IP-адреса, как показано на рисунке 150.

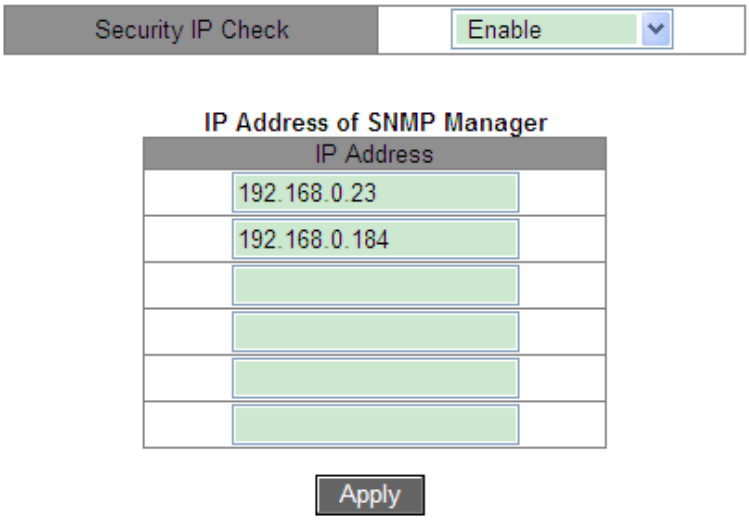


Рисунок 150 Настройка безопасного IP-адреса

Security IP Check

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение проверки безопасного IP. Если проверка безопасности IP отключена, нет ограничений на IP-адрес NMS, любая NMS, подключенная к коммутатору, может получить доступ к информации MIB коммутатора. После того, как проверка IP-адреса безопасности включена, необходимо задать безопасный установить IP-адрес, и только NMS с безопасным IP-адресом может получить доступ к информации MIB коммутатора.

IP Address

Формат: A.B.C.D

Функция: Настройка безопасного IP-адрес NMS.

Описание: Только NMS, адрес которой совпадает с безопасным IP-адресом может получить доступ к информации MIB коммутатора. Коммутатор поддерживает не более 6 безопасных IP-адресов NMS.

7. Настройка Trap.

Щелкните [Device Advanced Configuration] →[SNMP Configuration]→[TRAP Configuration], чтобы настроить trap, как показано на рисунке 151.

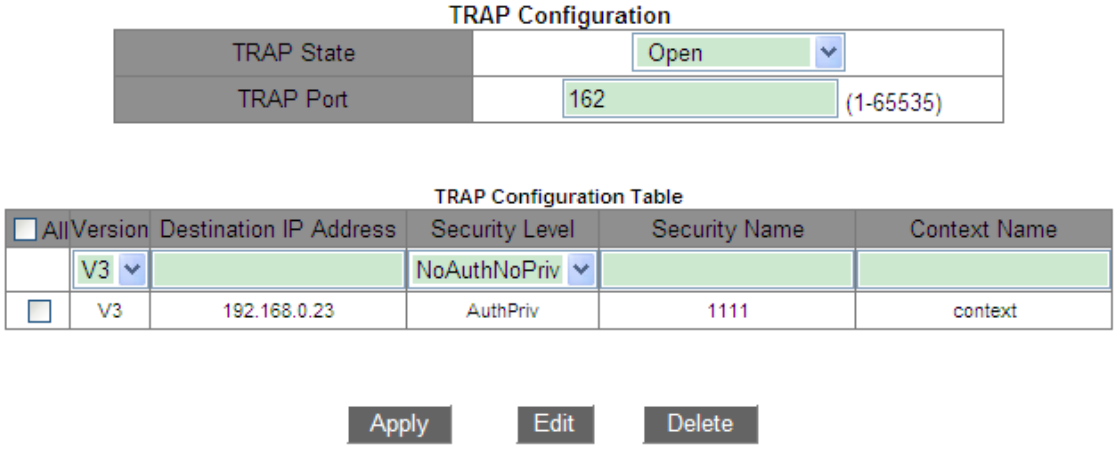


Рисунок 151 Настройка Trap SNMP v3

TRAP State

Варианты: Open/Close

По умолчанию: Close

Функция: Разрешение/запрет отправки сообщений Trap.

TRAP Port

Варианты: 1~65535

По умолчанию: 162

Функция: Настройка номера порта для отправки сообщений Trap.

Version

Варианты: V1/V2C/V3

Функция: V1/V2C указывает, что коммутатор отправляет сообщения trap версии 1/версии 2C на сервер. V3 указывает, что коммутатор отправляет сообщения trap версии 3 на сервер.

Destination IP Address

Формат: A.B.C.D

Функция: Настройка адреса сервера для приема сообщений Trap. Вы можете настроить не более 8 серверов, то есть 8 записей trap.

{Security Level, Security Name, Context Name}

Варианты: {NoAuthNoPriv/AuthNoPriv/AuthPriv, 4~16 символов, 4~16 символов}

Функция: Эти три параметра необходимо настраивать только при выборе V3. Эти настройки должны соответствовать настройкам в таблице доступа. Значение Security Level может быть равным или выше, чем в таблице доступа. Например, когда право доступа пользователя 1111 установлено как AuthNoPriv, коммутатор может отправлять сообщения trap на сервер только в том случае, если уровень безопасности доверенного имени 1111 — AuthNoPriv или AuthPriv. Имя контекста должно совпадать с Context Prefix в таблице доступа.

6.4.4 Типовой пример 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 SNMPv3. Уровень безопасности установлен как AuthNoPriv, и коммутатор может выполнять операцию «только чтение» для всей информации узла Агента. При возникновении тревоги агент заранее отправляет сообщения trap v3 в NMS, как показано на рисунке 152.

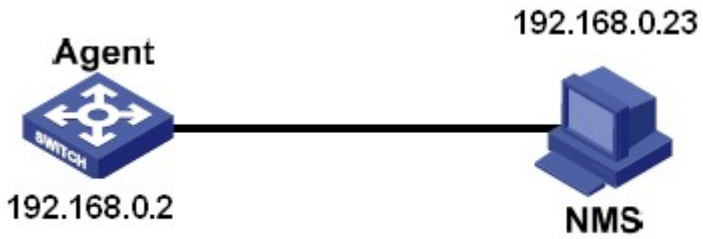


Рисунок 152 Пример настройки SNMPv3

Настройка агента:

1. Настройте таблицу пользователей SNMPv3. Задайте имя пользователя 1111, протокол аутентификации HMAC-MD5, пароль аутентификации aaaa, протокол конфиденциальности HMAC-DES и пароль конфиденциальности xxxx. Задайте имя другого пользователя 2222, протокол аутентификации HMAC-SHA, пароль аутентификации bbbb, протокол конфиденциальности HMAC-DES и пароль конфиденциальности yyyy, как показано на рисунке 145.

2. Создайте группу и добавьте пользователей 1111 и 2222 в группу, как показано на рисунке 146.

3. Создайте имя контекста, то есть контекст, как показано на рисунке 147.

4. Создайте таблицу представлений. view-all включает все узлы дерева MIB 1, view-no не включает ни один узел дерева MIB 1, как показано на рисунке 148.

5. Настройте таблицу доступа SNMPv3. Задайте значения параметров: group name – group; context name – context; context match – exact; security level – AuthNoPriv; readView – view-all; writeView – view-no; notifyView – view-all, как показано на рисунке 149.

6. Включите функцию trap и установите номер порта 162. Настройте запись Trap. Установите для Trap версию V3, IP-адрес назначения — 192.168.0.23, уровень безопасности — AuthPriv, доверенное имя — 1111, контекстное имя — context, как показано на рисунке 150.

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

6.5 DT-Ring

6.5.1 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.

6.5.2 Основные концепции

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.

Другой кольцевой порт находится 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.

6.5.3 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 на рисунке 153.

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.

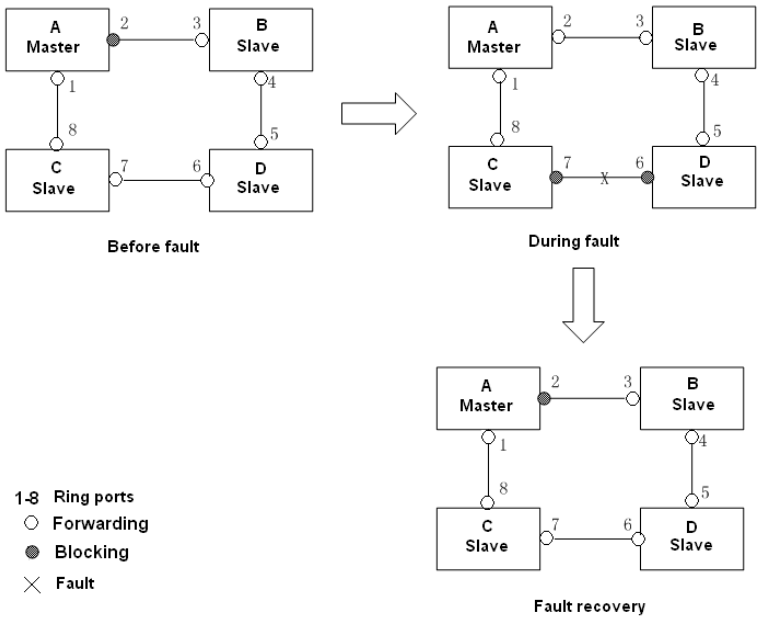


Figure 153 Отказ линии CD

4. Если линия связи AC неисправна, как показано на рисунке 154.

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.

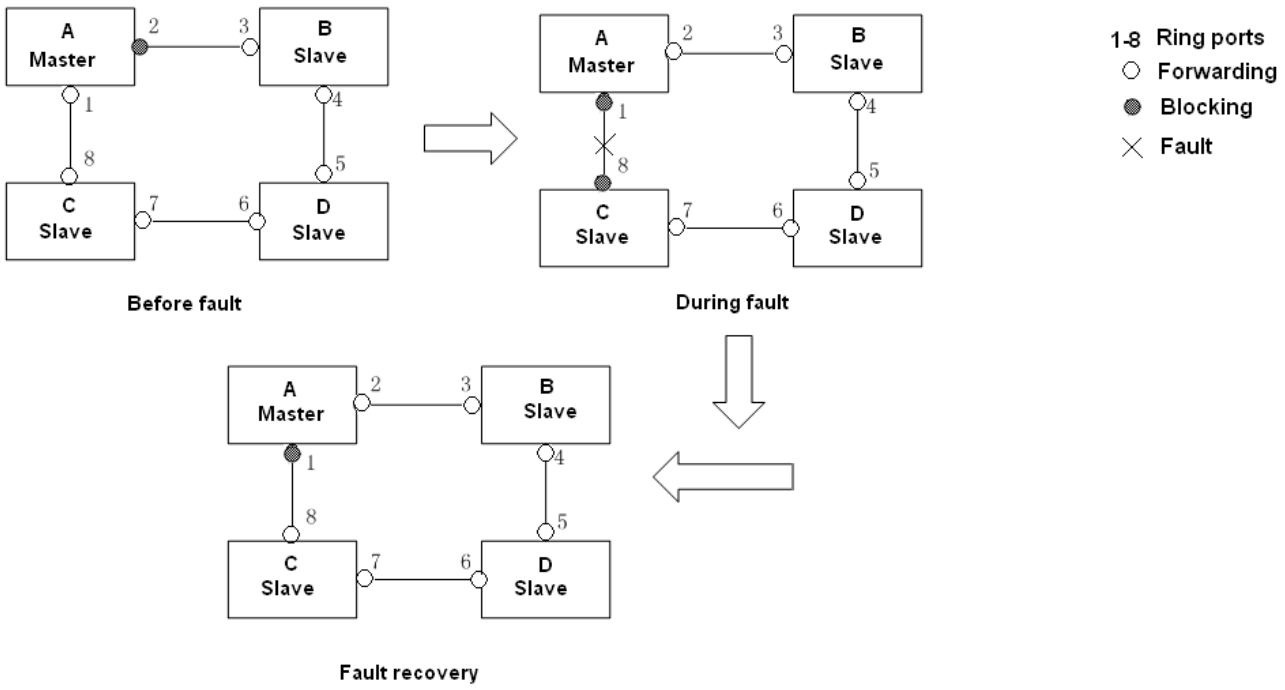


Рисунок 154 Отказ линии DT-Ring

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 155, 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.

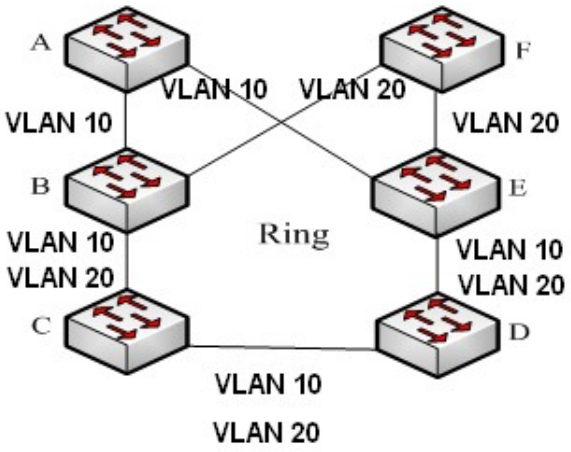


Рисунок 155 DT-Ring-VLAN

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 на рисунке 156. 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, для пересылки данных будет выбран резервный порт Slave, предотвращая образования петель и обеспечивая нормальную связь между резервными кольцами.

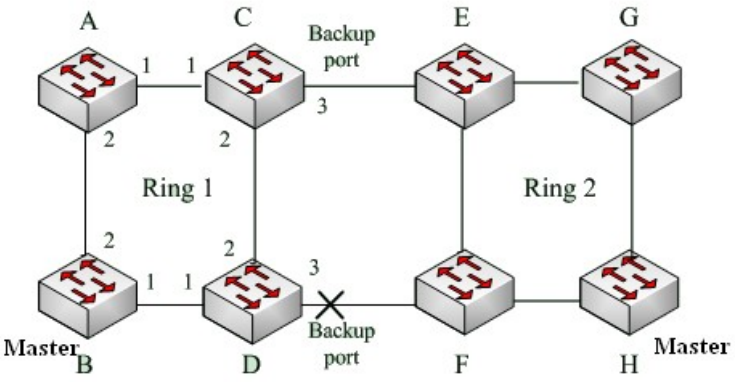


Рисунок 156 Топология DT-Ring+

Предупреждение:

Изменение статуса соединения влияет на статус резервных портов.

6.5.4 6.5.4 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.

6.5.5 Настройка через веб-интерфейс

1. Настройка режима резервирования.

Щелкните [Device Advanced Configuration] → [DT-Ring Configuration] → [DT-Ring Mode], чтобы перейти на страницу настройки режима кольца, как показано на рисунке 157.

Рисунок 157 Настройка режима резервного кольца

Redundancy Mode Set

Варианты: DT-PORT/DT-VLAN

По умолчанию: DT-PORT

Функция: Включение протокола DT-Ring и выбор режима резервного кольца.

Предупреждение:

- К кольцевым протоколам на основе портов относятся RSTP, DT-Ring-Port и DRP-Port, 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. Создайте DT-Ring.

Щелкните [Device Advanced Configuration] → [DT-Ring Configuration] → [DT-Ring Configuration], чтобы создать DT-Ring, как показано на рисунке 158.

Рисунок 158 Создание DT-Ring

Щелкните <Add> чтобы создать DT-Ring.

3. Настройте DT-Ring и DT-VLAN-Ring, как показано на рисунке 159 и рисунке 160.

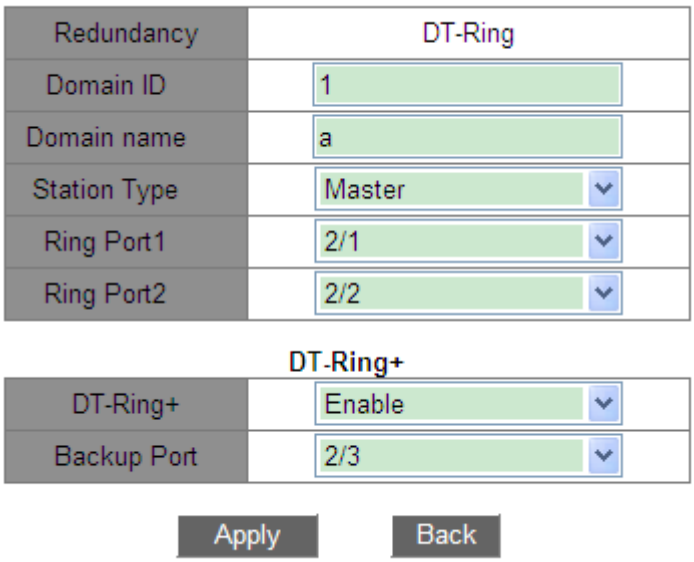


Рисунок 159 Конфигурация DT-Ring

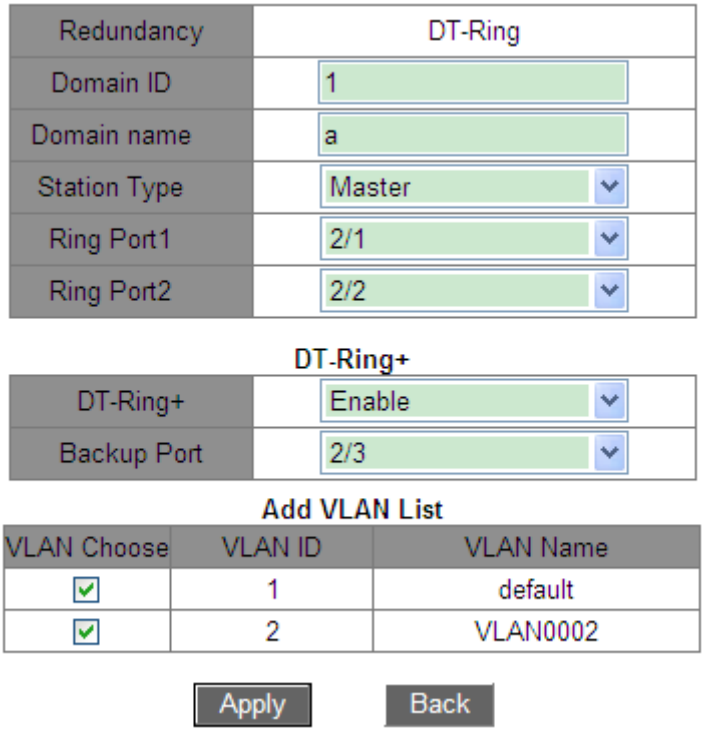


Рисунок 160 Конфигурация DT-VLAN-Ring

Резервирование

Принудительная конфигурация: DT-Ring

Domain ID

Диапазон настройки: 1~32

Функция: Идентификатор домена используется, чтобы различать разные кольца.

Один коммутатор поддерживает максимум 16 колец на основе портов или 8 колец на основе VLAN.

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.

- Кольцевой порт DT-Ring или резервный порт и назначение зеркалирования являются взаимоисключающими. Кольцевой порт DT-Ring или резервный порт не могут быть настроены как порт назначения зеркалирования; порт назначения зеркалирования 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, порты DT-Ring и резервные порты нельзя добавлять в изолированную группу.

DT-Ring+

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение DT-Ring+.

Backup port

Варианты: все порты коммутатора.

Функция: Настройка порта как резервного.

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

Add VLAN list

Варианты: все созданные VLAN

Функция: Выбор VLAN для кольцевого порта.

После завершения настройки DT-Ring List показывает все созданные кольца, как показано на рисунке 161.

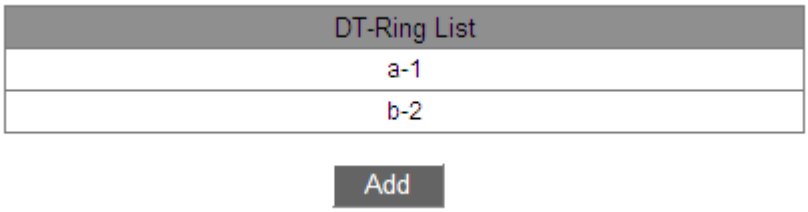


Рисунок 161 Список DT-Ring List

4. Просмотр и изменение конфигурации DT-Ring.

Щелкните запись DT-Ring на рисунке 161, чтобы отобразить конфигурацию кольца и изменить ее, как показано на рисунке 162.

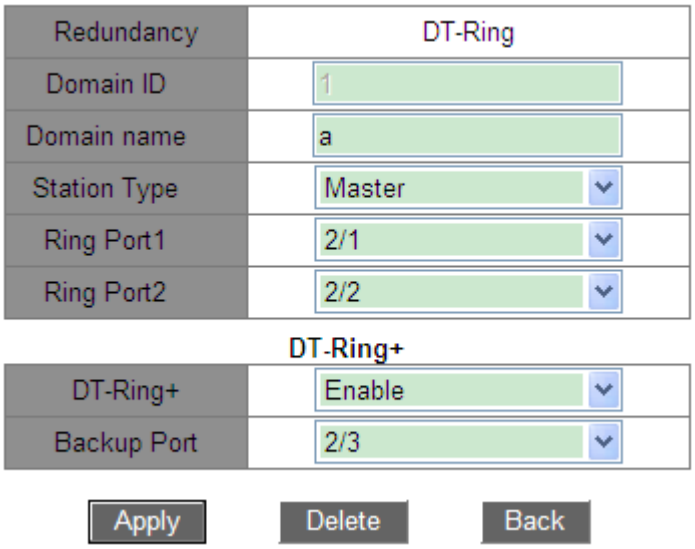


Рисунок 162 Конфигурация DT-Ring

Щелкните <Apply>, чтобы внесенные изменения вступили в силу. Щелкните <Delete>, чтобы удалить запись конфигурации DT-Ring.

5. Просмотрите статус DT-Ring и порта, как показано на рисунке 163.

DT-Ring State List

Redundancy	DT-Ring
Ring Port1	forwarding
Ring Port2	blocking
Ring State	RING-CLOSE

Redundancy	DT-Ring+
Equipment IP	192.168.0.4
Equipment MAC	00-00-00-00-00-01
BackupPort Status	blocking

Рисунок 163 Состояние DT-Ring

6.5.6 Типовой пример конфигурации

Как показано на рисунке 156, 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. Domain ID: 1; Domain name: Ring; Ring port: port 1 and port2; Station type: Slave; DT-Ring+: Disable; резервные порты не назначены, как показано на рисунке 159.

Конфигурация коммутатора B:

2. Domain ID: 1; Domain name: Ring; Ring port: port 1 and port 2; Station type: Master; DT-Ring+: Disable; резервные порты не назначены, как показано на рисунке 159.

Конфигурация коммутатора C:

3. Domain ID: 1; Domain name: Ring; Ring port: port 1 and port2; Station type: Slave; DT-Ring+: Enable; Backup port: port 3, как показано на рисунке 159.

Конфигурация коммутатора E, коммутатора F и коммутатора G:

4. Domain ID: 2; Domain name: Ring; Ring port: port 1 and port2; Station type: Slave; DT-Ring+: Disable; резервные порты не назначены, как показано на рисунке 159.

Конфигурация коммутатора H:

5. Domain ID: 2; Domain name: Ring; Ring port: port 1 and port2; Station type: Master; DT-Ring+: Disable; резервные порты не назначены, как показано на рисунке 159.

6.6 STP/RSTP

6.6.1 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.

6.6.2 Основные концепции

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.

6.6.3 6.6.3 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 7 показана структура данных BPDU.

Таблица 7 BPDU

…	ID корн. моста	Стоим. корн. пути	ID назн. моста	ID назн. порта	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--пересылка).

6.6.4 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.

6.6.5 Настройка через веб-интерфейс

1. Включите RSTP.

Щелкните [Device Advanced Configuration] → [RSTP configuration] → [RSTP configuration], чтобы перейти на страницу настройки RSTP, как показано на рисунке 164.

Рисунок 164 Включение RSTP/STP

Protocol Status

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включить или выключить RSTP или STP.

Предупреждение:

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

2. Задайте параметры времени сетевого моста, как показано на рисунке 165.

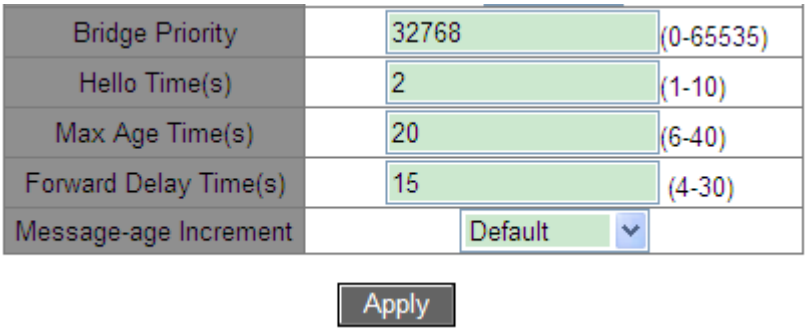


Рисунок 165 Задание параметров времени сетевого моста

Bridge Priority

Диапазон: 0~65535 Шаг составляет 4096.

По умолчанию: 32768

Функция: Настройка приоритета сетевого моста.

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

Hello Time

Диапазон: 1~10 с

По умолчанию: 2 с

Функция: Настройка интервала времени для отправки BPDU.

Max Age Time

Диапазон: 6~40 с

По умолчанию: 20 с

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

Forward Delay Time

Диапазон: 4~30 с

По умолчанию: 15 с

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

Message-age Increment

Варианты: Compulsion/Default

По умолчанию: Default

Функция: Настройка значения, которое будет добавляться к возрасту сообщения, когда BPDU проходит через сетевой мост.

Описание: В режиме Compulsion значение равно 1.

В режиме Default значение равно макс. из (max age time/16, 1).

Значения Forward Delay Time, Max Age Time и Hello Time должны соответствовать следующим требованиям: 2 x (Forward Delay Time – 1,0 с) ≥ Max Age Time;

Max Age Time ≥ 2 x (Hello Time + 1,0 с).

3. Включите RSTP на портах, как показано на рисунке 135.

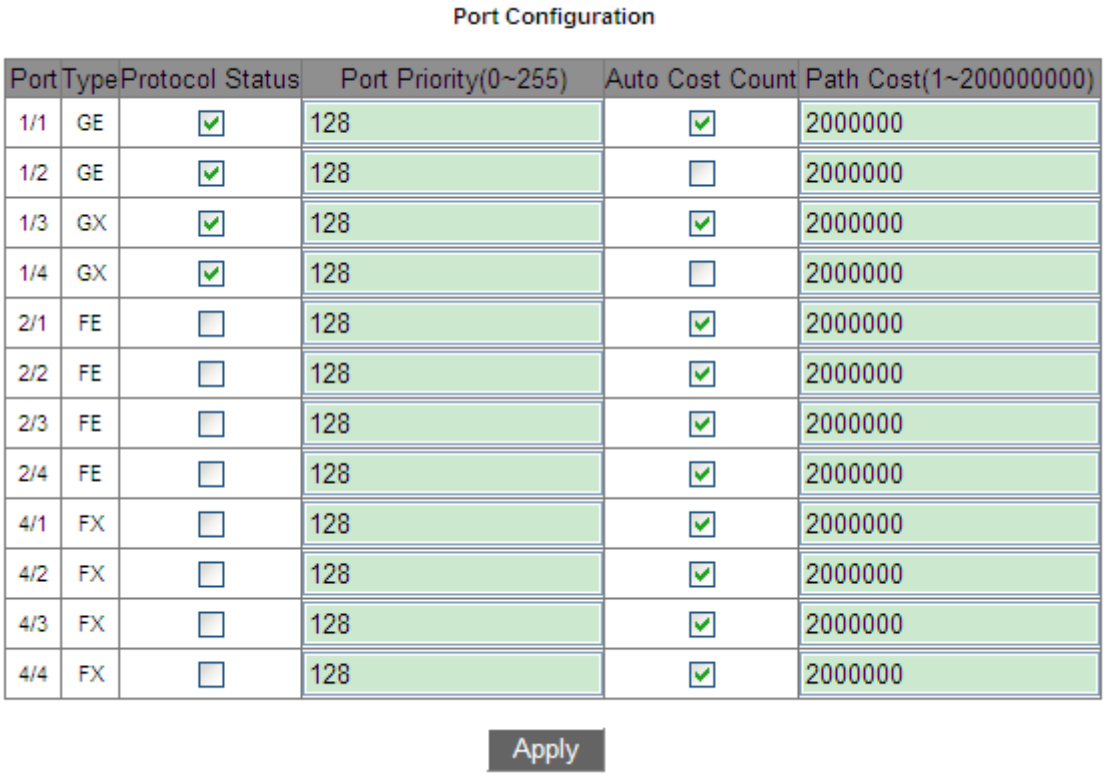


Рисунок 166 Настройки портов

Protocol Status

Варианты: Enable/Disable

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.
- Порт RSTP и назначение зеркалирования являются взаимоисключающими. Порт RSTP нельзя настроить как порт назначения зеркалирования; порт назначения зеркалирования не может быть настроен как порт RSTP.
- 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.
- Не рекомендуется одновременно настраивать порты в изолированной группе как порты RSTP, а порты RSTP нельзя добавлять в изолированную группу.

Port Priority

Диапазон: 0~255 Шаг составляет 16.

По умолчанию: 128

Функция: Настройка приоритета порта, определяющего роли портов.

Path Cost

Диапазон: 1~200000000

По умолчанию: 2000000 (10M порт), 200000 (100M port), 20000 (1000M port)

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.

Auto Cost Count

Диапазон: Yes/No

По умолчанию: Yes

Описание: Yes указывает, что стоимость пути порта принимает значение по умолчанию. No означает, что можно настроить стоимость пути.

4. Просмотрите статус RSTP, как показано на рисунке 167.

Root Info

Root MAC	00:1e:cd:11:01:b1
Root Priority	0x8000
Root Path Cost	200000
Root Port	1/3
Max Age(s)	20
Hello Time(s)	2
Forward Delay(s)	15

Bridge Info

Bridge MAC	08:00:3e:32:53:22
Bridge Priority	0x8000
Bridge Version	2
Max Age(s)	20
Hello Time(s)	2
Forward Delay(s)	15

Port Info

Port	Priority	Path Cost	Role	State	Link State
1/1	0x80	200000	Root	Forwarding	Up
1/2	0x80	2000000	Alternate	Discarding	Up
1/3	0x80	200000	Disabled	Discarding	Down
1/4	0x80	2000000	Disabled	Discarding	Down

Рисунок 167 Информация о статусе RSTP

6.6.6 Типовой пример конфигурации

Приоритеты коммутаторов A, B и C: 0, 4096 и 8192. Стоимость пути для соединений составляет 4, 5 и 10, как показано на рисунке 168.

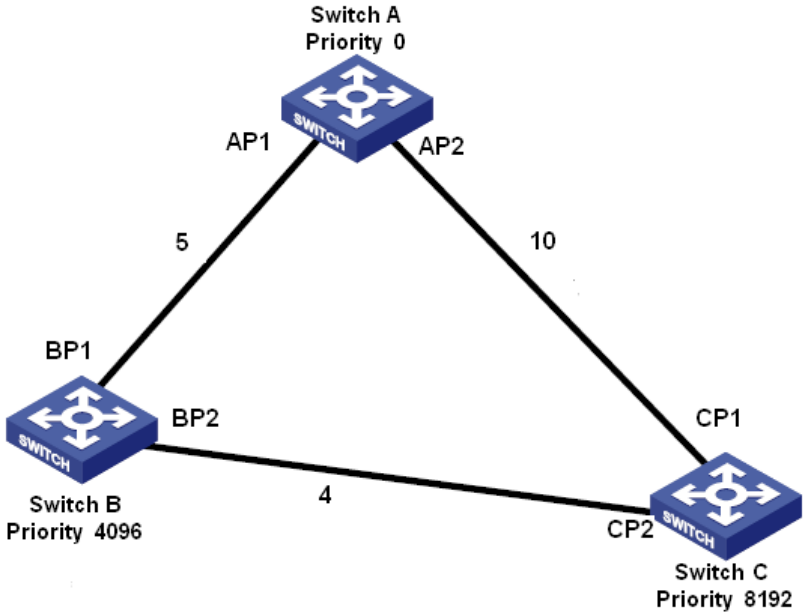


Рисунок 168 Пример настроек RSTP

Конфигурация коммутатора A:

1. Установите приоритет 0 и значения по умолчанию для временных параметров, как показано на рисунке 165.

2. Установите стоимость пути для порта 1 – 5 и для порта 2 – 10, как показано нарисунке 166. Конфигурация коммутатора B:

1. Установите приоритет 4096 и значения по умолчанию для временных параметров, как показано на рисунке 165.

2. Установите стоимость пути для порта 1 – 5 и для порта 2 – 4, как показано нарисунке 166. Конфигурация коммутатора C:

1. Установите приоритет 8192 и значения по умолчанию для временных параметров, как показано на рисунке 165.

2. Установите стоимость пути для порта 1 – 10 и для порта 2 – 4, как показано нарисунке 166.

- 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.

6.7 DRP

6.7.1 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 касательные 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.

6.7.2 Основные концепции

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, на «работает» (когда кольцо замкнуто), и он будет состоянии пересылки. Другой кольцевой порт находится 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.

6.7.3 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 8 Вектор пакета Announce

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

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 8 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. 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 следующая:

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.

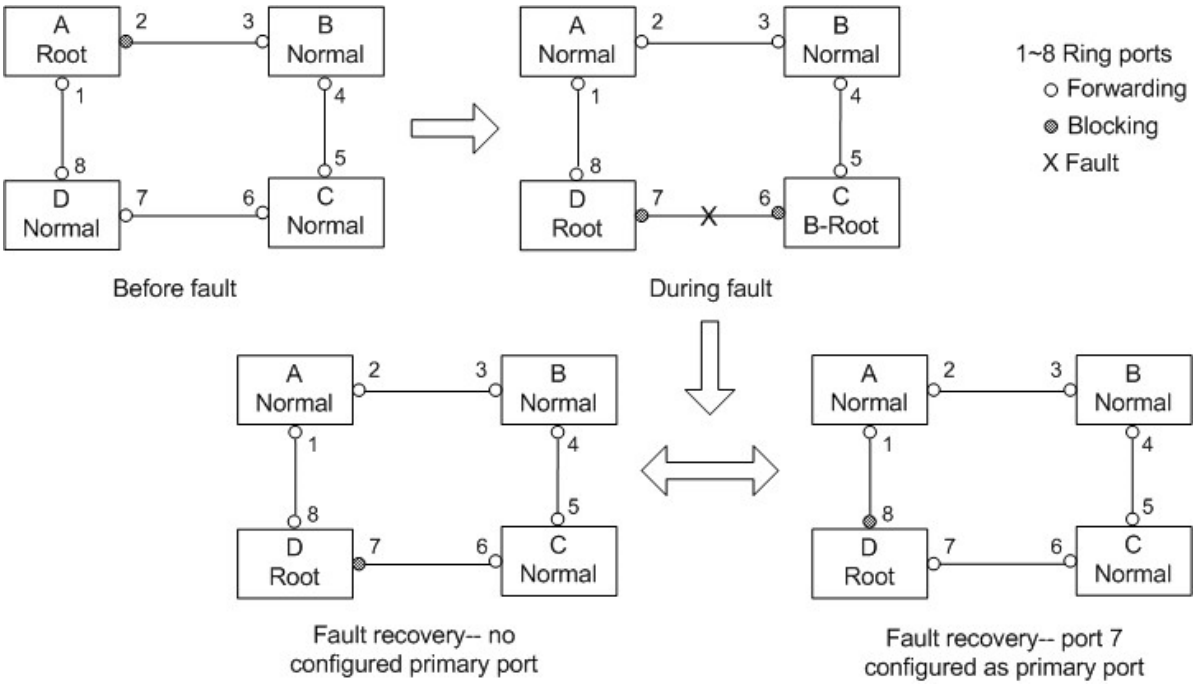


Рисунок 169 Отказ канала DRP

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

DRP-VLAN-Based устанавливает сопоставление между VLAN и экземпляром STG. Одна или несколько сетей VLAN могут быть сопоставлены с одним экземпляром STG. Экземпляр STG: Каждый экземпляр STG соответствует одному кольцу DRP-VLAN-Based. С помощью DRP экземпляр STG записывает роли устройств и состояние порта. После получения пакета коммутатор определяет сопоставленный экземпляр STG на основе атрибута VLAN пакета. Коммутатор обрабатывает пакет в соответствии с ролями устройства и статусом порта экземпляра.

При настройке кольца DRP-VLAN-Based пакеты из разных VLAN могут пересылаться по разным путям. Как показано на рисунке 170, сопоставление между экземплярами STG и VLAN одинаково для всех устройств.Кольцо на основе STG1: AB-BC-CD-DE-EA. Пакеты VLAN10 и VLAN20 пересылаются по каналу. A является корнем.

Кольцо на основе STG2: FB-BC-CD-DE-EF. Пакеты VLAN30 пересылаются по каналу. F является корнем.

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.

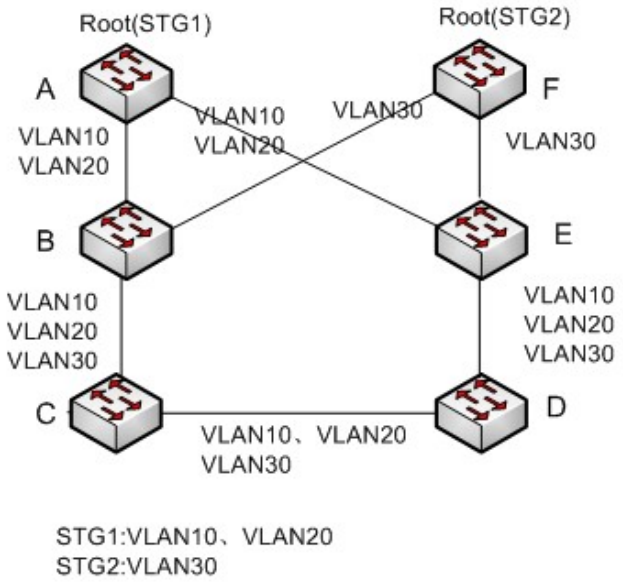


Рисунок 170 DRP-VLAN-Based

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 следующем рисунке, 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.

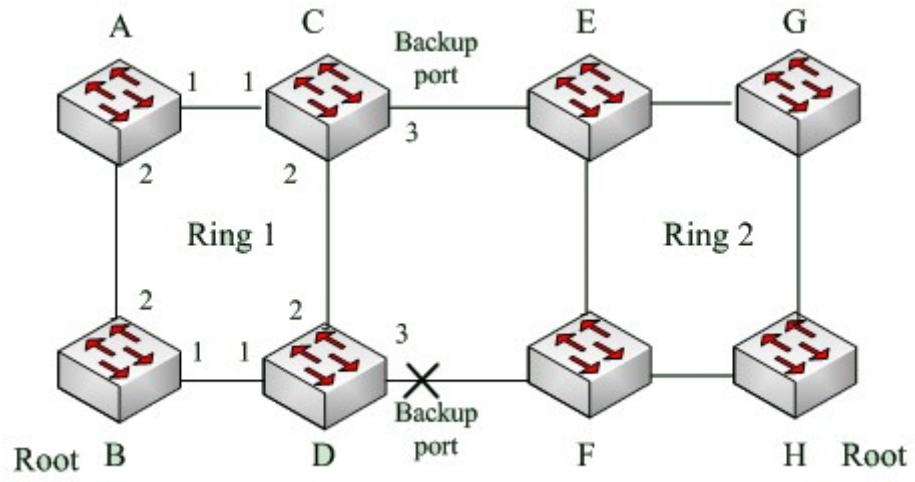


Рисунок 171 Резервирование DRP

Предупреждение:

Изменение статуса соединения влияет на статус резервных портов.

6.8 DHP

6.8.1 Обзор

Как показано на следующем рисунке, 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.

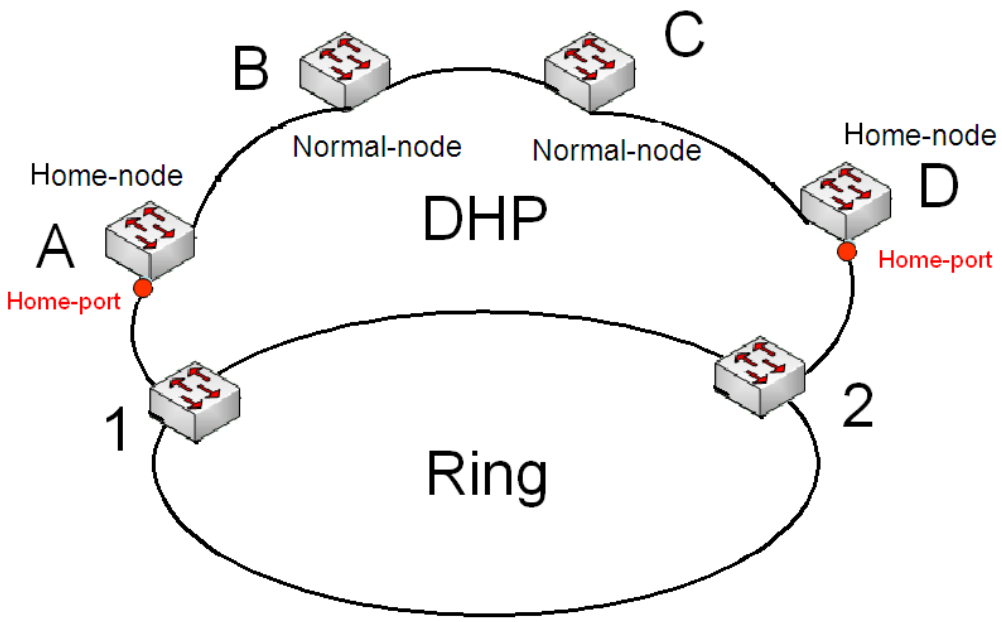


Рисунок 172 Использование DHP

6.8.2 Основные концепции

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.

6.8.3 Реализация

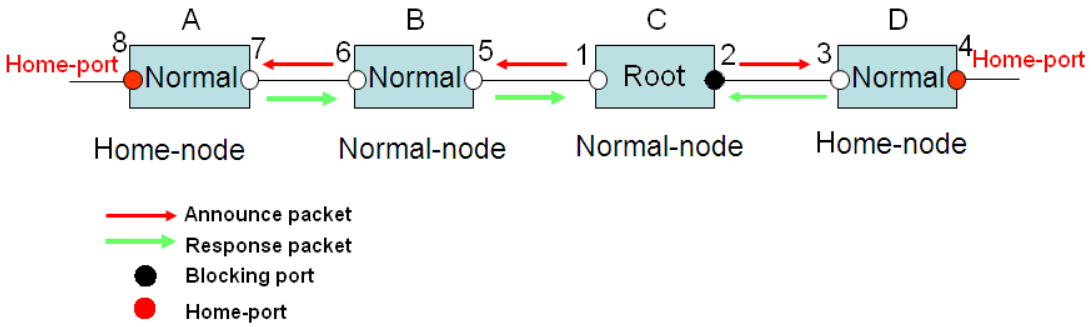


Рисунок 173 Конфигурация DHP

Как показано на предыдущем рисунке, конфигурации A, B, C и D на рисунке 6 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.

- В 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 следующем рисунке.

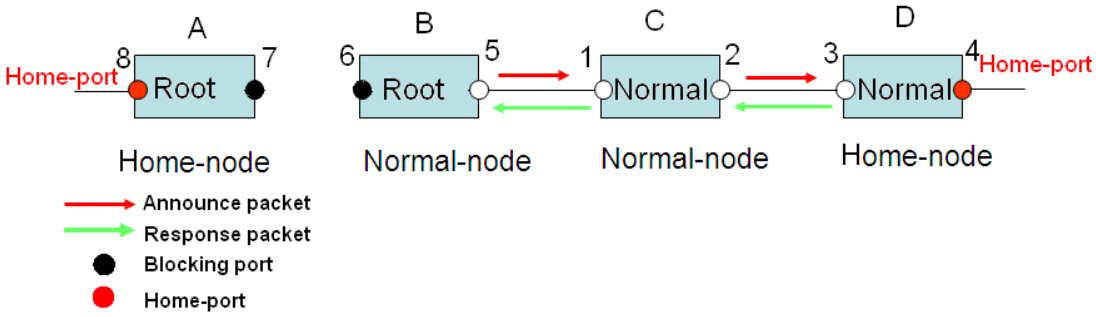


Рисунок 174 Устранение отказа DHP

6.8.4 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.

6.8.5 Настройка через веб-интерфейс

1. Настройка режима DRP

Щелкните [Device Advanced Configuration] → [DRP configuration] → [DRP Mode], чтобы перейти на страницу настройки режима DRP, как показано на следующем рисунке.

Рисунок 175 Режим DRP

DRP Mode

Варианты: Port Based/VLAN Based

По умолчанию: Port Based

Функция: Настройка режима DRP

Предупреждение:

- К кольцевым протоколам на основе портов относятся RSTP, DT-Ring-Port и DRP-Port, 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. Создайте запись DRP-Port-Based.

Щелкните [Device Advanced Configuration] → [DRP configuration] → [Port-Based DRP Configuration], чтобы перейти на страницу создания записи DRP, как показано на следующем рисунке.

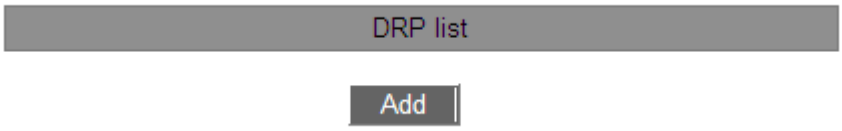


Рисунок 176 Создание записи DRP-Port-Based

Щелкните <Add> чтобы создать запись DRP.

- Задайте параметры записи DRP-Port-Based, как показано на следующем рисунке.

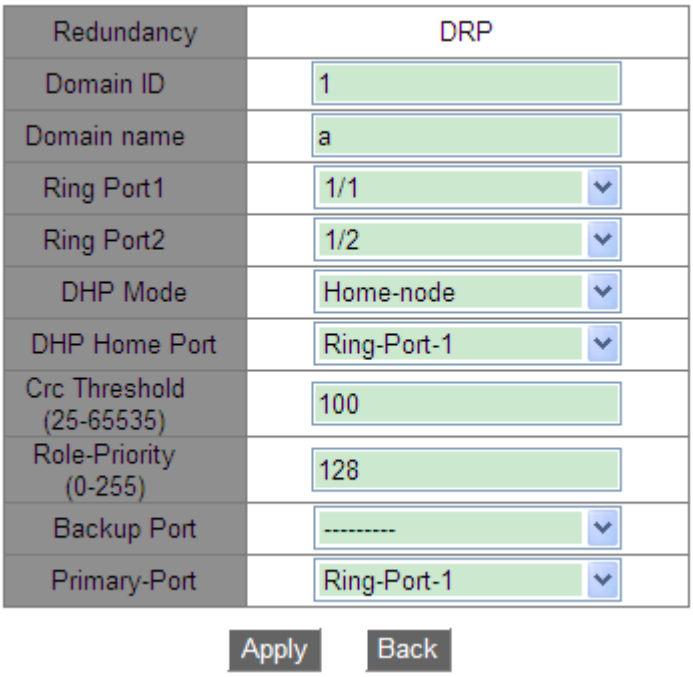


Рисунок 177 Настройка записи DRP-Port-Based

Резервирование

Обязательная настройка: DRP

Domain ID

Диапазон: 1~32

Описание: Каждое кольцо имеет уникальный идентификатор домена. На одном коммутаторе можно настроить не более 16 колец DRP.

Domain Name

Диапазон: 1~31 символ

Функция: Задание доменного имени.

Ring port 1/Ring port 2

Варианты: все порты коммутатора

Функция: Выбор двух кольцевых портов.

Режим DHP

Варианты: Disable/Normal-Node/Home-Node

По умолчанию: Disable

Функция: Отключение DHP или настройка режима DHP.

DHP Home Port

Варианты: 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: 25~65535

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.

Role-Priority

Диапазон: 0~255

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.

Primary-Port

Варианты: --/Ring-Port-1/Ring-Port-2

По умолчанию: --

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

После завершения настройки параметров созданная запись будет отображаться в списке DRP List, как показано на следующем рисунке.

Рисунок 178 Список DRP-Port-Based List

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.

- Кольцевой порт DRP или резервный порт и назначение зеркалирования являются взаимоисключающими. Кольцевой порт DRP или резервный порт не могут быть настроены как порт назначения зеркалирования; порт назначения зеркалирования 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, DRP-Port. кольцевой порт DT-Ring-Port или резервный порт DT-Ring-Port; Порт RSTP, кольцевой порт DT-Ring-Port и резервный порт DT-Ring-Port нельзя настроить как кольцевой порт DRP-Port или резервный порт.
- Не рекомендуется одновременно настраивать порты в изолированной группе как порты DRP и резервные порты, а порты DRP и резервные порты нельзя добавлять в изолированную группу.

- Просмотр настроек параметров записи DRP-Port-Based.

Щелкните запись DRP на рисунке 178. Можно просматривать и изменять настройки параметров записи, как показано на следующем рисунке.

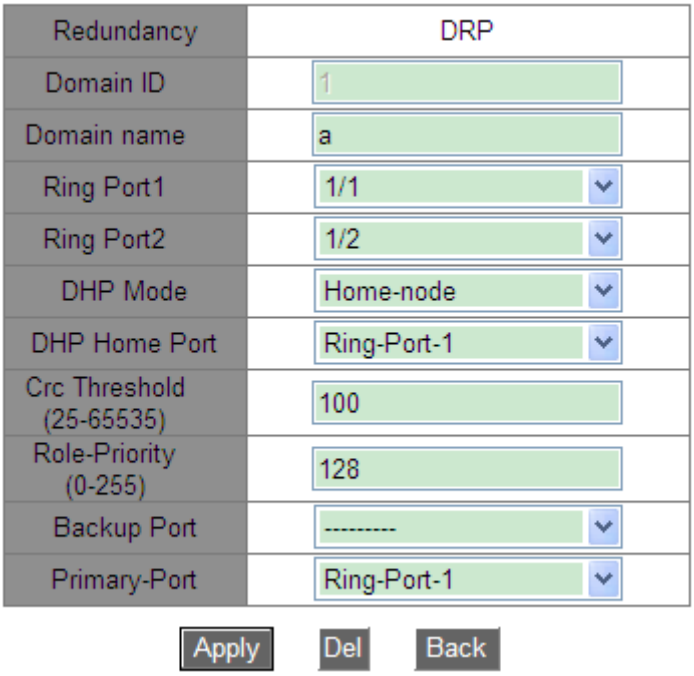


Рисунок 179 Запрос и изменение записи DRP-Port-Based.

После внесения изменений щелкните <Apply>, чтобы внесенные изменения вступили в силу. Можно удалить запись DRP, щелкнув <Delete>.

- Просмотрите роли и статус порта кольца DRP, как показано на следующем рисунке.

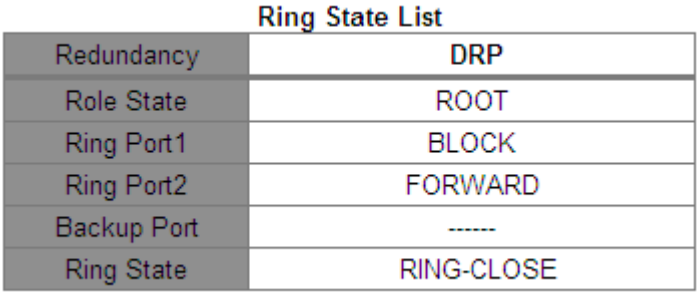


Рисунок 180 Запрос статуса DRP-Port-Based

3. Настройте запись DRP-VLAN-Based.

Щелкните [Device Advanced Configuration] → [DRP configuration] → [DRP Mode], чтобы перейти на страницу настройки режима DRP. Выберите VLAN Based.

➢ Настройка экземпляра DRP

Щелкните Click [Device Advanced Configuration] → [DRP configuration] → [VLAN-Based DRP Configuration] → [DRP STG Instance], чтобы перейти на страницу настройки экземпляра DRP STG, как показано на следующем рисунке.

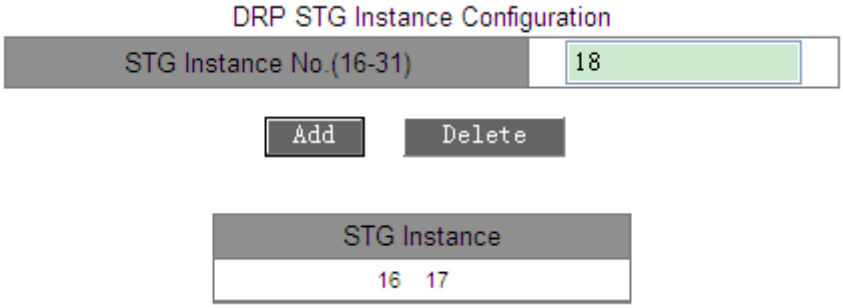


Рисунок 181 Настройка экземпляра DRP

STG Instance No. (16-31)

Диапазон: 16~31

Функция: Настройка ID экземпляра DRP.

➢ Настройка VLAN в экземпляре DRP

Щелкните [Device Advanced Configuration] → [DRP configuration] → [VLAN-Based DRP Configuration] → [STG Instance Protocol VLAN Configuration], чтобы перейти на страницу настройки VLAN экземпляра DRP, как показано на следующем рисунке.

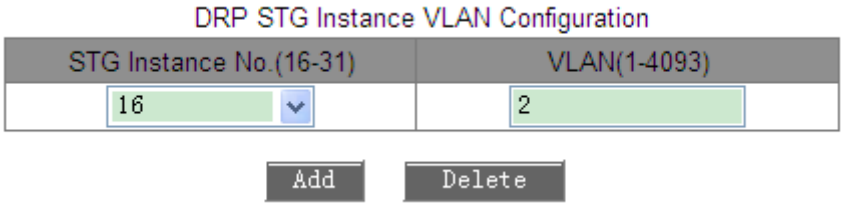


Рисунок 182 Настройка VLAN для экземпляра DRP

DRP STG Instance VLAN Configuration

Состав: {STG instance ID, VLAN ID}

Range: {16~31, 1~4093}

Функция: Настройка VLAN ID для экземпляра DRP.

Описание: Один экземпляр может соответствовать нескольким идентификаторам VLAN ID, но один идентификатор VLAN ID может соответствовать только одному экземпляру.

➢ Просмотр информации об экземплярах DRP.

Щелкните [Device Advanced Configuration] → [DRP configuration] → [VLAN-Based DRP Configuration] → [STG Instance Information], чтобы перейти на страницу информации экземпляра DRP, как показано на следующем рисунке.

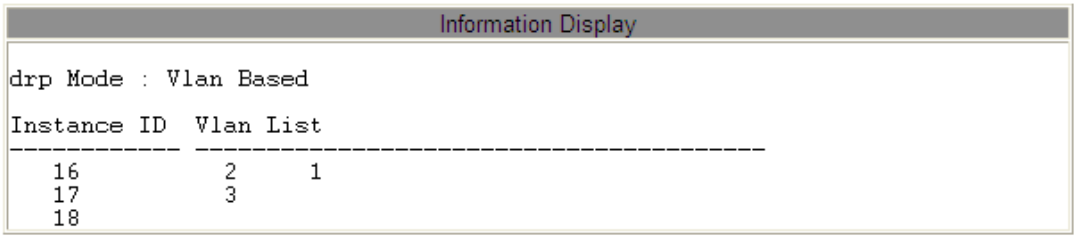


Рисунок 183 Информация экземпляра DRP

➢ Настройка DRP-VLAN-Based

Щелкните [Device Advanced Configuration] → [DRP configuration] → [VLAN-Based DRP Configuration] → [Ring Configuration], чтобы перейти на страницу создания DRP-VLAN-Based, как показано на следующем рисунке.

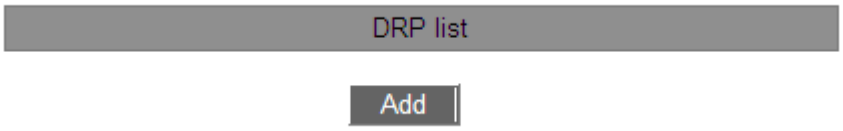


Рисунок 184 Создание записи DRP-VLAN-Based

Щелкните <Add> чтобы создать запись DRP. Задайте параметры записи, как показано на следующем рисунке.

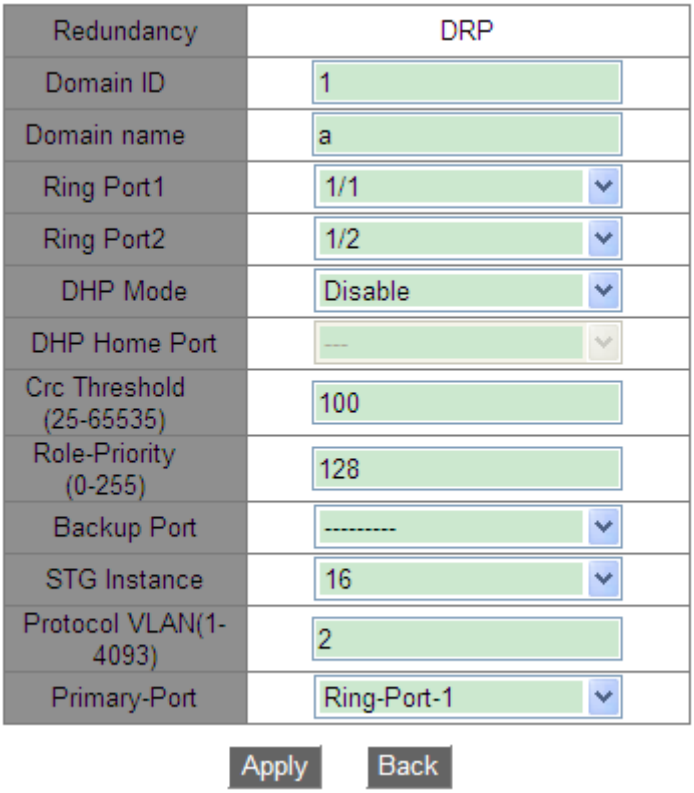


Рисунок 185 Настройка записи DRP-VLAN-Based

Резервирование

Обязательная настройка: DRP

Domain ID

Диапазон: 1~32

Функция: Каждое кольцо имеет уникальный идентификатор домена. На одном коммутаторе можно настроить не более 8 колец DRP.

Domain Name

Диапазон: 1~31 символ

Функция: Задание доменного имени.

Ring Port 1/Ring Port 2

Варианты: все порты коммутатора.

Функция: Выбор двух кольцевых портов.

Режим DHP

Варианты: Disable/Normal-Node/Home-Node

По умолчанию: Disable

Функция: Отключение DHP или настройка режима DHP.

DHP Home Port

Варианты: 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: 25~65535

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.

Role-Priority

Диапазон: 0~255

По умолчанию: 128

Функция: Настройка приоритета коммутатора.

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.

- Кольцевой порт DRP или резервный порт и назначение зеркалирования являются взаимоисключающими. Кольцевой порт DRP или резервный порт не могут быть настроены как порт назначения зеркалирования; порт назначения зеркалирования не может быть настроен в качестве кольцевого порта DRP или резервного порта.
- Не рекомендуется одновременно настраивать порты в изолированной группе как порты DRP и резервные порты, а порты DRP и резервные порты нельзя добавлять в изолированную группу.

Резервный порт

Варианты: все порты коммутатора.

Функция: Настройка резервного порта.

Предупреждение:

Не следует настраивать кольцевой порт в качестве резервного.

STG Instance

Варианты: созданные экземпляры DRP

Функция: Настройка экземпляра для кольца.

Описание: Блокирующий порт в кольце будет блокировать пакеты данных всех VLAN, соответствующих экземпляру.

Protocol Vlan (1~4093)

Диапазон: 1~4093

Описание: VLAN ID должен быть Одним из соответствующих экземпляру STG.

Функция: Пакеты DRP с VLAN ID служат основой для диагностики и обслуживания

кольца DRP-VLAN-Based.

Primary-Port

Варианты: --/Ring-Port-1/Ring-Port-2

По умолчанию: --

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

После завершения настройки созданные кольца будут отображаться в списке DRP List, как показано на следующем рисунке.

Рисунок 186 Список DRP-Port-Based List

Щелкните запись DRP. Можно просматривать и изменять настройки параметров, как показано на следующем рисунке.

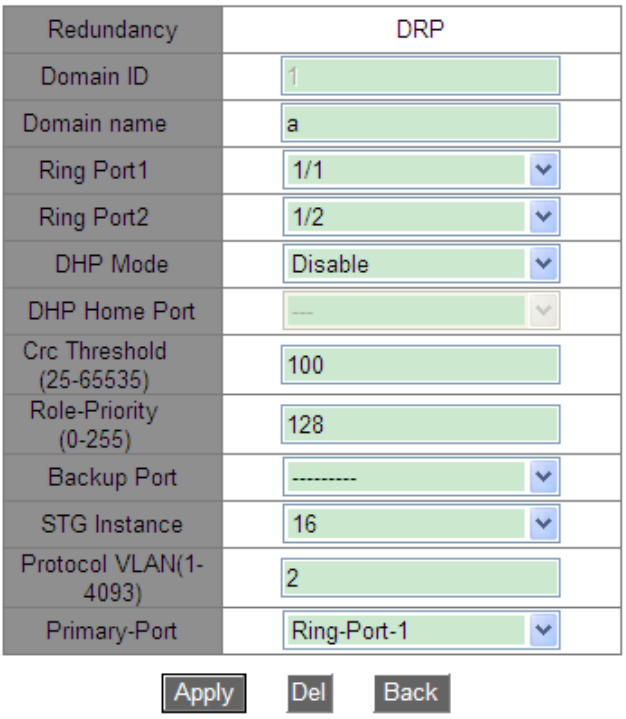


Рисунок 187 Просмотр и изменение записи DRP-VLAN-Based.

После внесения изменений щелкните <Apply>, чтобы внесенные изменения вступили в силу. Можно удалить запись DRP, щелкнув <Delete>.

Просмотрите роли и статус порта кольца DRP, как показано на следующем рисунке.

Ring State List

Redundancy	DRP
Role State	ROOT
Ring Port1	FORWARD
Ring Port2	BLOCK
Backup Port	------
Ring State	RING-OPEN

Рисунок 188 Запрос записи DRP-VLAN-Based

6.8.6 Типовой пример конфигурации

Как показано на рисунке 171, 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 Ring. Выберите кольцевой порт 1 и кольцевой порт 2. Сохраните значения по умолчанию для приоритета роли и резервного порта, как показано на рисунке 177.

Конфигурация коммутатора C и коммутатора D:

2. Установите Domain ID 1, Domain name Ring, резервный порт 3. Выберите кольцевой порт 1 и кольцевой порт 2. Сохраните значения по умолчанию для приоритета роли, как показано на рисунке 177.

Конфигурация коммутаторов E, F, G и H:

3. Установите Domain ID 2 и Domain name Ring. Выберите кольцевой порт 1 и кольцевой порт 2. Сохраните значения по умолчанию для приоритета роли и резервного порта, как показано на рисунке 177.

6.9 Настройка MSTP

6.9.1 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 189, 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.

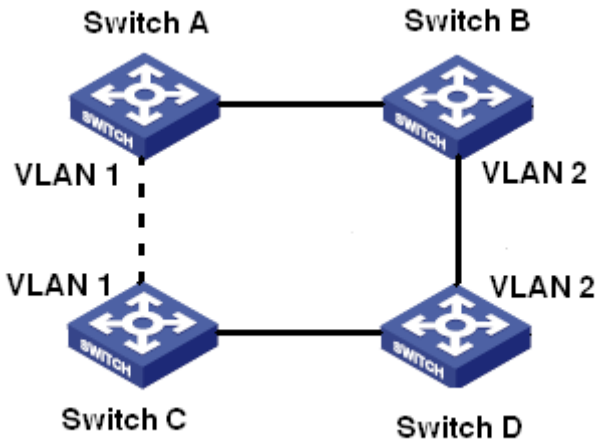


Рисунок 189 Недостатки RSTP

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

189 формирует топологию, показанную на рисунке 190. 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.

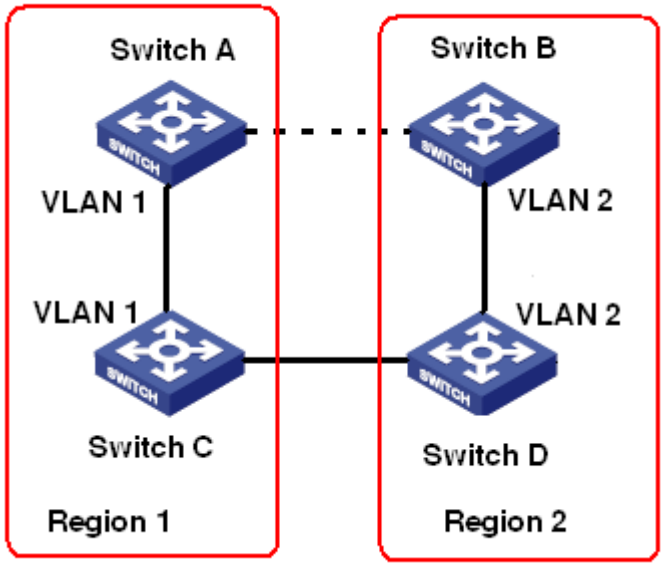


Рисунок 190 Топология MSTP

6.9.2 Основная концепция

Ознакомьтесь с концепцией MSTP, показанной на рисунке 191 и рисунке 194.

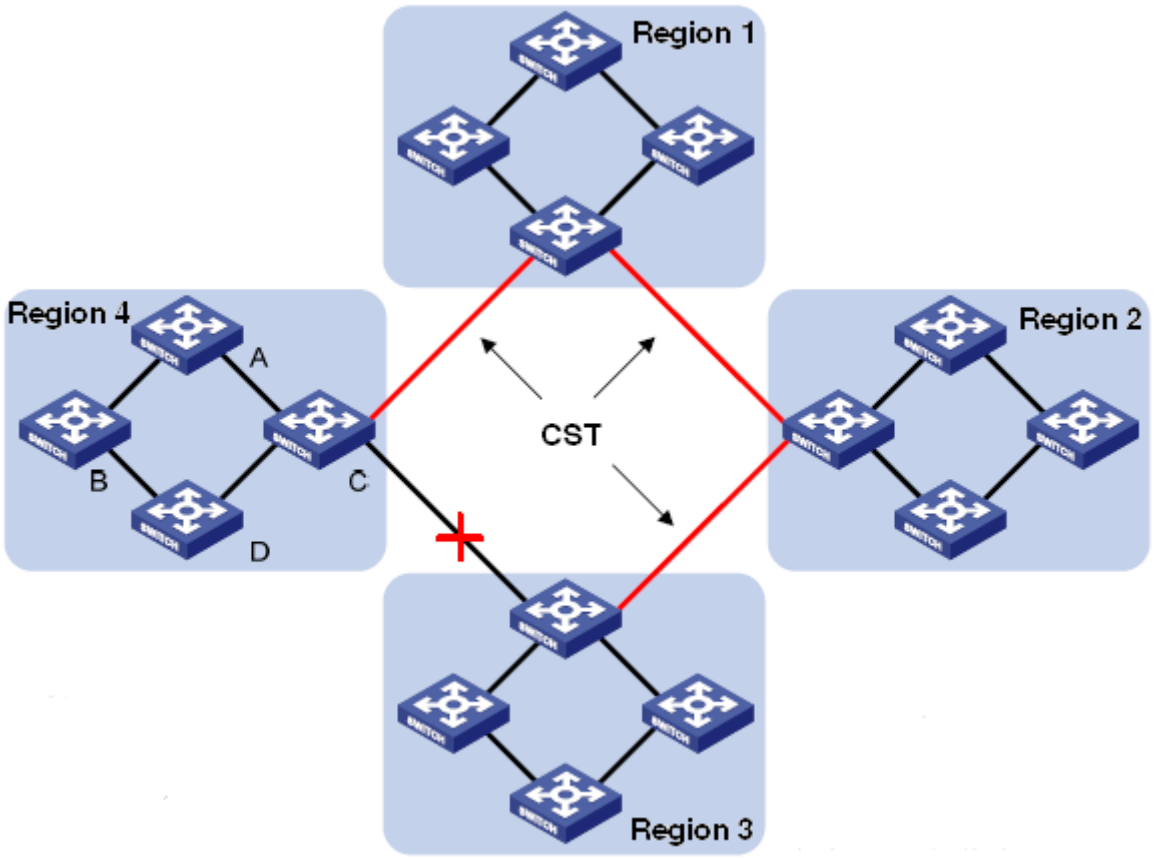


Рисунок 191 Концепция MSTP

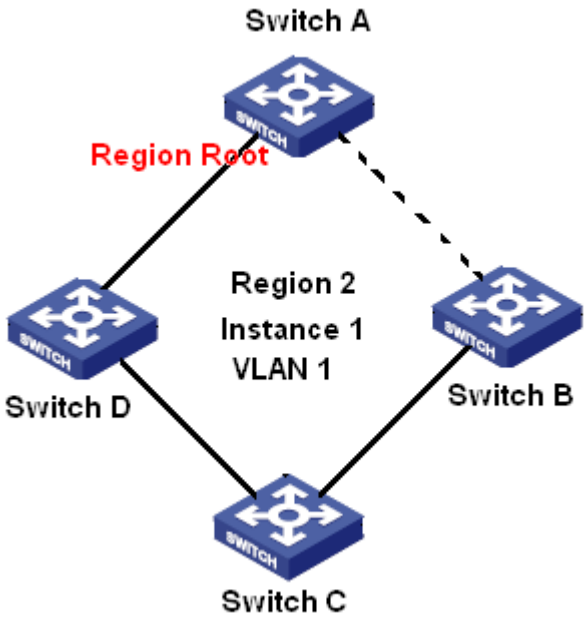


Рисунок 192 Сопоставление VLAN 1 с экземпляром 1

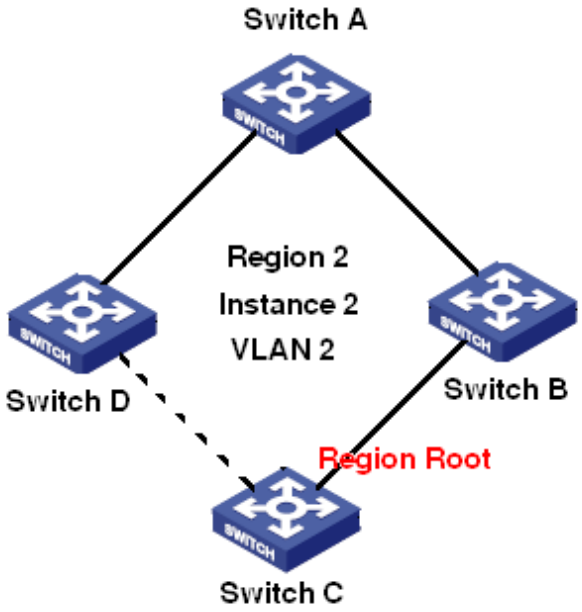


Рисунок 193 Сопоставление VLAN 2 с экземпляром 2

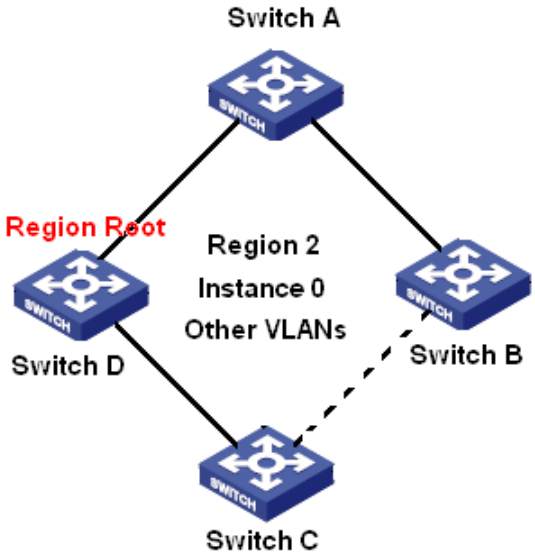


Рисунок 194 Сопоставление другой VLAN с экземпляром 0

Экземпляр: набор из нескольких VLAN. Одна VLAN (как показано на рисунке 192 и рисунке 193) или несколько VLAN с одинаковой топологией (как показано на рисунке 194) 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 191, 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 191 , таблица сопоставления VLAN региона 2 – это сопоставление VLAN 1 и экземпляра 1, как показано на рисунке 192; VLAN 2 сопоставляется с экземпляром 2, как показано на рисунке 193.. Другие VLAN сопоставляются с экземпляром 0, как показано на рисунке 194.

Общее и внутреннее связующее дерево (CIST): указывает экземпляр 0, то есть связующее дерево, охватывающее все устройства в коммутируемой сети. Как показано на рисунке 191, 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 194.

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 191, красные линии обозначают связующее дерево.

MST (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 192 и рисунке 193. 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 192, рисунке 193 и рисунке 194, 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.

6.9.3 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.

6.9.4 Настройка через веб-интерфейс

1. Включите протокол MSTP

Щелкните [Device Advanced Configuration] → [MSTP configuration] → [Enable MSTP], чтобы перейти на страницу настройки MSTP, как показано на рисунке 195.

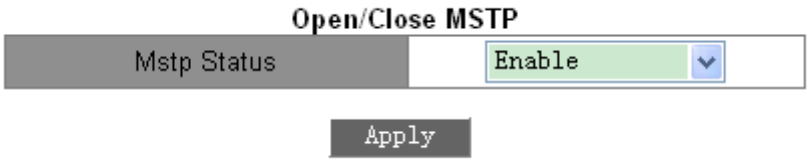


Рисунок 195 Включение RSTP/STP

Состояние MSTP

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение MSTP.

Предупреждение:

- К кольцевым протоколам на основе портов относятся RSTP, DT-Ring-Port и DRP-Port, 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. Принудительно переведите порт в режим MSTP, как показано на рисунке 196.

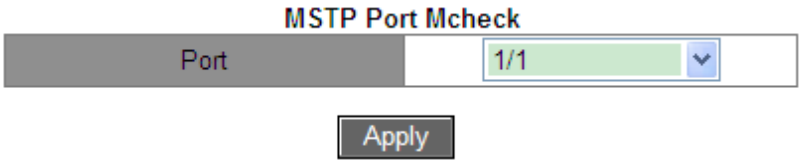


Рисунок 196 Принудительный перевод порта в режим MSTP

Port

Варианты: все порты коммутатора.

Функция: Когда порт с поддержкой MSTP подключен к устройству с поддержкой STP, этот порт будет автоматически изменен для работы в режиме STP. Если устройство с поддержкой STP будет удалено, этот порт не вернется автоматически к работе в режиме MSTP. При желании вернуться к работе в режиме MSTP в этом состоянии, установите эту функцию для порта. Как только порт снова получит STP-сообщение, он автоматически переключится на работу в режиме STP.

Предупреждение:

Эта конфигурация вступит в силу, только если коммутатор работает в режиме MSTP; иначе это бесполезно.

3. Настройте состояние MSTP порта.

Щелкните[Device Advanced Configuration] → [MSTP configuration] → [Enable Port MSTP], чтобы перейти на страницу настройки протокола MSTP, как показано на рисунке 197.

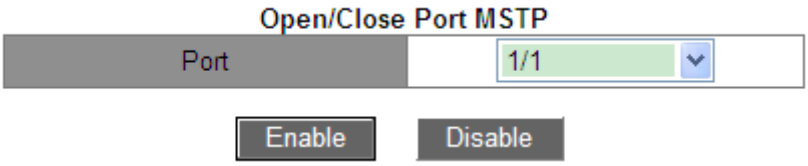


Рисунок 197 Настройка MSTP для порта

Port

Варианты: все порты коммутатора.

По умолчанию: Если на включен глобальный протокол MSTP, функция MSTP на всех портах открыта. Функция: Включение/выключение MSTP для порта.

4. Настройте параметр региона MST.

Щелкните [Device Advanced Configuration] → [MSTP configuration] → [MSTP Region Config], чтобы перейти на страницу параметров региона MST, как показано на рисунке 198.

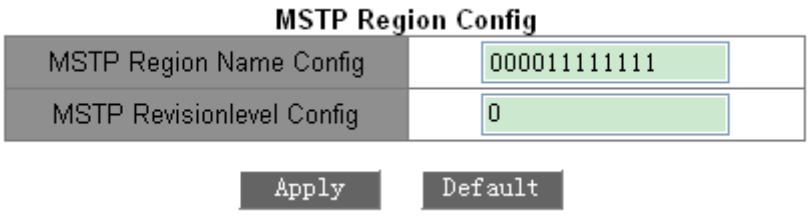


Рисунок 198 Настройка параметров региона MST

MSTP Region Name config

Диапазон: 1-32 символа

По умолчанию: MAC-адрес устройства

Функция: Задание имени региона MST.

MSTP Revision level config

Варианты: 0~65535

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.

5. Настройте таблицу сопоставления VLAN, как показано на рисунке 199.

Рисунок 199 Настройка таблицы сопоставления VLAN

{MSTP Instance ID, VLAN list}

Диапазон: {0~16, 1~4094}

По умолчанию: {0, 1~4094}

Функция: Настройка таблицы сопоставления VLAN в регионе MST.

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.

Предупреждение:

<Del> не может удалить список VLAN экземпляра 0.

После завершения настройки Instance List покажет сопоставление между VLAN и экземпляром.

6. Настройка приоритета моста коммутатора в назначенном экземпляре.

Щелкните [Device Advanced Configuration] → [MSTP configuration] → [MSTP Instance Config], чтобы перейти на страницу параметров региона MST, как показано на рисунке 200.

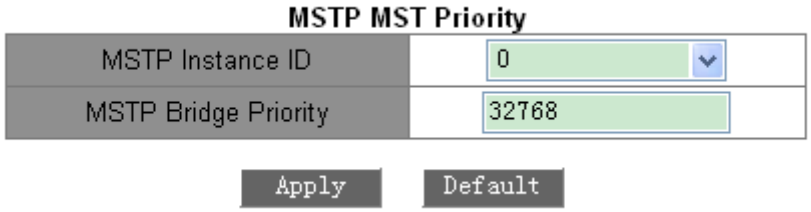


Рисунок 200 Настройка приоритета моста коммутатора в назначенном экземпляре

MSTP Instance ID

Варианты: все созданные экземпляры

MSTP Bridge Priority

Диапазон: 0~61440 с шагом 4096

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.

7. Настройте приоритет порта и стоимость пути в назначенном экземпляре, как показано на рисунке 201.

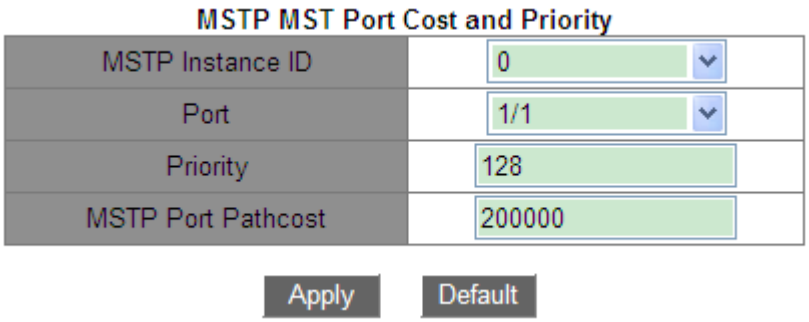


Рисунок 201 Настройка приоритета порта и стоимости пути в назначенном экземпляре

MSTP Instance ID

Варианты: все созданные экземпляры

Port

Варианты: все порты коммутатора.

Priority

Диапазон: 0~240 с шагом 16

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.

MSTP Port Path cost

Диапазон: 1~200000000

По умолчанию: как указано в таблице 9 и таблице 10.

Таблица 9 Стоимость пути для общего порта по умолчанию

Тип порта	**Стоимость пути по умолчанию**	**Рекомендуемый диапазон**
10 Мбит/с	2000000	2000000~20000000
100 Мбит/с	200000	200000~2000000
1 Гбит/с	20000	20000~200000

Таблица 10 Стоимость пути по умолчанию для порта агрегации

Тип порта	**Количество портов агрегации (в разрешенном диапазоне агрегации)**	**Рекомендуемый диапазон**
10 Мбит/с	N	2000000/N
100 Мбит/с	N	200000/N
1 Гбит/с	N	20000/N

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.

8. Настройте параметр времени MSTP.

Щелкните [Device Advanced Configuration] → [MSTP configuration] → [MSTP Time Config], чтобы перейти на страницу параметров времени MST, как показано на рисунке 202.

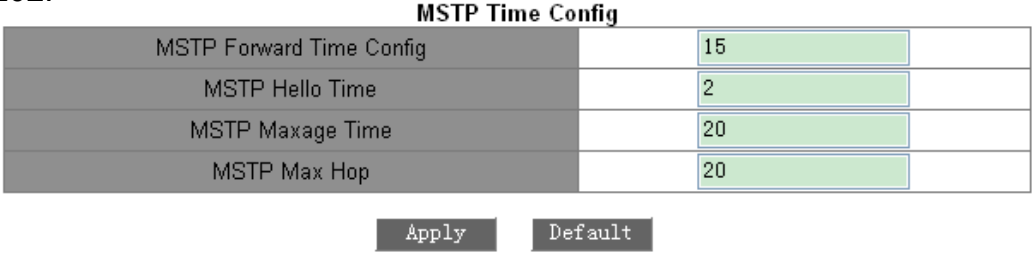


Рисунок 202 Настройка параметров времени MSTP.

MSTP Forward Time Config

Варианты: 4~30 с

По умолчанию: 15 с

Функция: Настройка временного интервала для смены состояния порта (Discarding – Learning или Learning – Forwarding). **MSTP Hello Time** Диапазон: 1~10 с

По умолчанию: 2 с

Функция: Настройка интервала времени для отправки BPDU.

MSTP Max Age Time

Диапазон: 6~40 с

По умолчанию: 20 с

Функция: Задание максимального возраста пакетов BPDU.

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.

MSTP Max Hop

Диапазон: 1~40

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.

9. Настройте функцию быстрого переключения состояний MSTP.

Щелкните [Device Advanced Configuration] → [MSTP configuration] → [MSTP Fast Transfer Config], чтобы перейти на страницу настройки, как показано на рисунке 203.

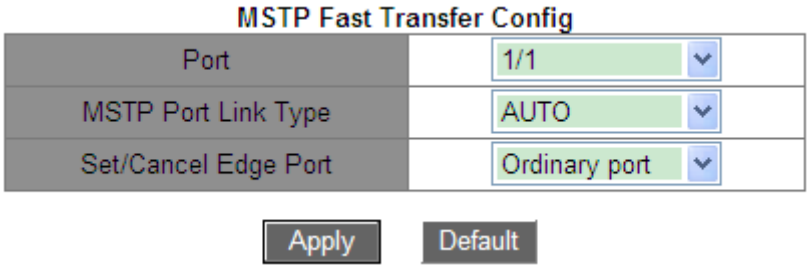


Рисунок 203 Настройка функции быстрого переключения состояний MSTP

MSTP Port Link Type

Варианты: AUTO/Forced True/Forced False

По умолчанию: AUTO

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

Описание: **AUTO** означает, что коммутатор автоматически определяет тип соединения в соответствии с состоянием дуплекса порта. Когда порт работает в полнодуплексном режиме, протокол MSTP автоматически предполагает, что канал, подключенный к порту, является каналом «точка-точка». Когда порт работает в полудуплексном режиме, протокол MSTP автоматически предполагает, что канал, подключенный к порту, является общим каналом. **Force True** предполагает, что канал, подключенный к локальному порту, является каналом «точка-точка». **Force False** предполагает, что канал, подключенный к локальному порту, является общим каналом.

Set/Cancel Edge Port

Варианты: Edge port/Ordinary port

По умолчанию: Ordinary port

Функция: Настроить порт как граничный порт или обычный порт.

Описание: Когда порт напрямую подключен к оконечным устройствам и не подключен к другим устройствам или общему сегменту сети, этот порт считается граничным портом. Граничный порт может быстро перейти от блокировки к пересылке без задержки. Как только пограничный порт получит сообщение BPDU, этот порт снова меняет состояние на обычный порт.

10. Просмотрите настройки MSTP.

Щелкните [Device Advanced Configuration] → [MSTP configuration] → [MSTP Information], чтобы просмотреть настройки MSTP, как показано на рисунке 204.

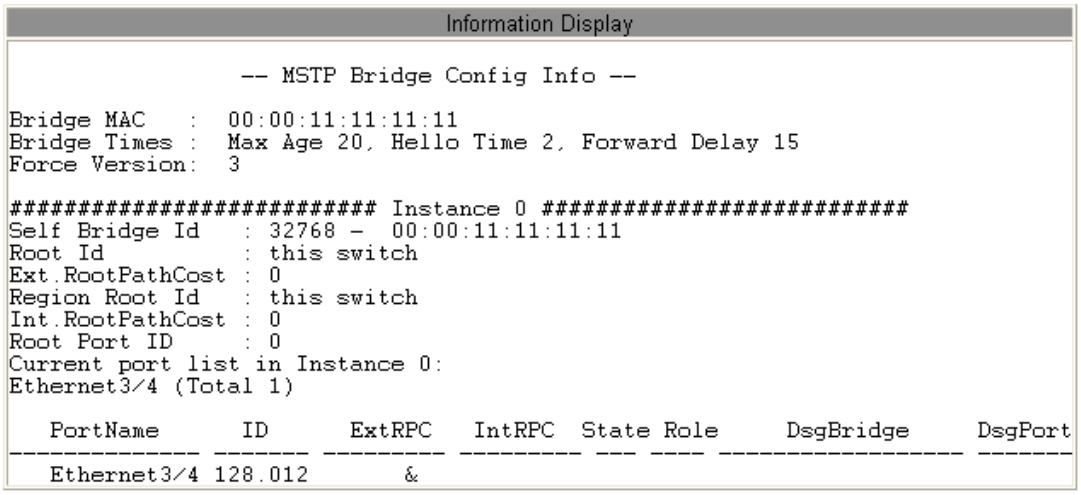


Рисунок 204 Настройки MSTP

6.9.5 Типовой пример конфигурации

Как показано на рисунке 205, 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.

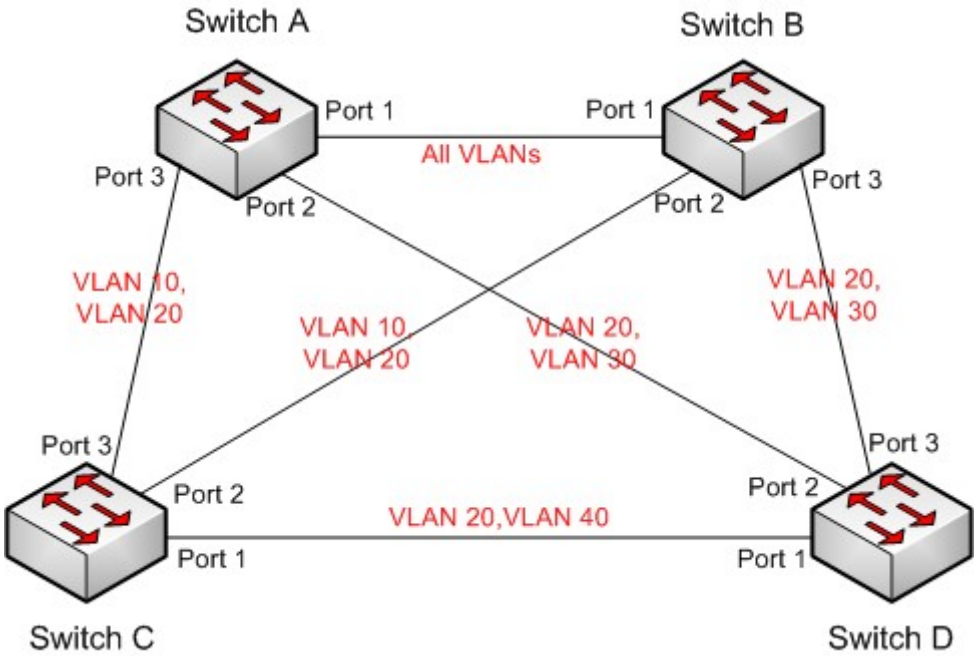


Рисунок 205 Пример типовой конфигурации MSTP

Конфигурация коммутатора A:

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

2. Включите глобальный протокол MSTP, как показано на рисунке 195.

3. Установите имя региона MST Region, а параметр версии 0, как показано на рисунке 198.

4. Создайте экземпляры 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с экземплярами 1, 3 и 4 соответственно, как показано на рисунке 199.

5. Установите приоритет моста коммутатора в экземпляре 1 равным 4096 и сохраните приоритет по умолчанию в других экземплярах, как показано на рисунке 200.

Конфигурация коммутатора B:

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

7. Включите глобальный протокол MSTP, как показано на рисунке 195.

8. Установите имя региона MST Region, а параметр версии 0, как показано на рисунке 198.

9. Создайте экземпляры 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с экземплярами 1, 3 и 4 соответственно, как показано на рисунке 199.

10. Установите приоритет моста коммутатора в экземпляре 3 и в экземпляре 0 равным 4096 и сохраните приоритет по умолчанию в других экземплярах, как показано на рисунке 200.

Конфигурация коммутатора C:

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

12. Включите глобальный протокол MSTP, как показано на рисунке 195.

13. Установите имя региона MST Region, а параметр версии 0, как показано на рисунке 198.

14. Создайте экземпляры 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с экземплярами 1, 3 и 4 соответственно, как показано на рисунке 199.

14. Установите приоритет моста коммутатора в экземпляре 4 равным 4096 и сохраните приоритет по умолчанию в других экземплярах, как показано на рисунке 200.

Конфигурация коммутатора B:

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

17. Включите глобальный протокол MSTP, как показано на рисунке 195.

18. Установите имя региона MST Region, а параметр версии 0, как показано на рисунке 198.

19. Создайте экземпляры 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с экземплярами 1, 3 и 4 соответственно, как показано на рисунке 199.

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

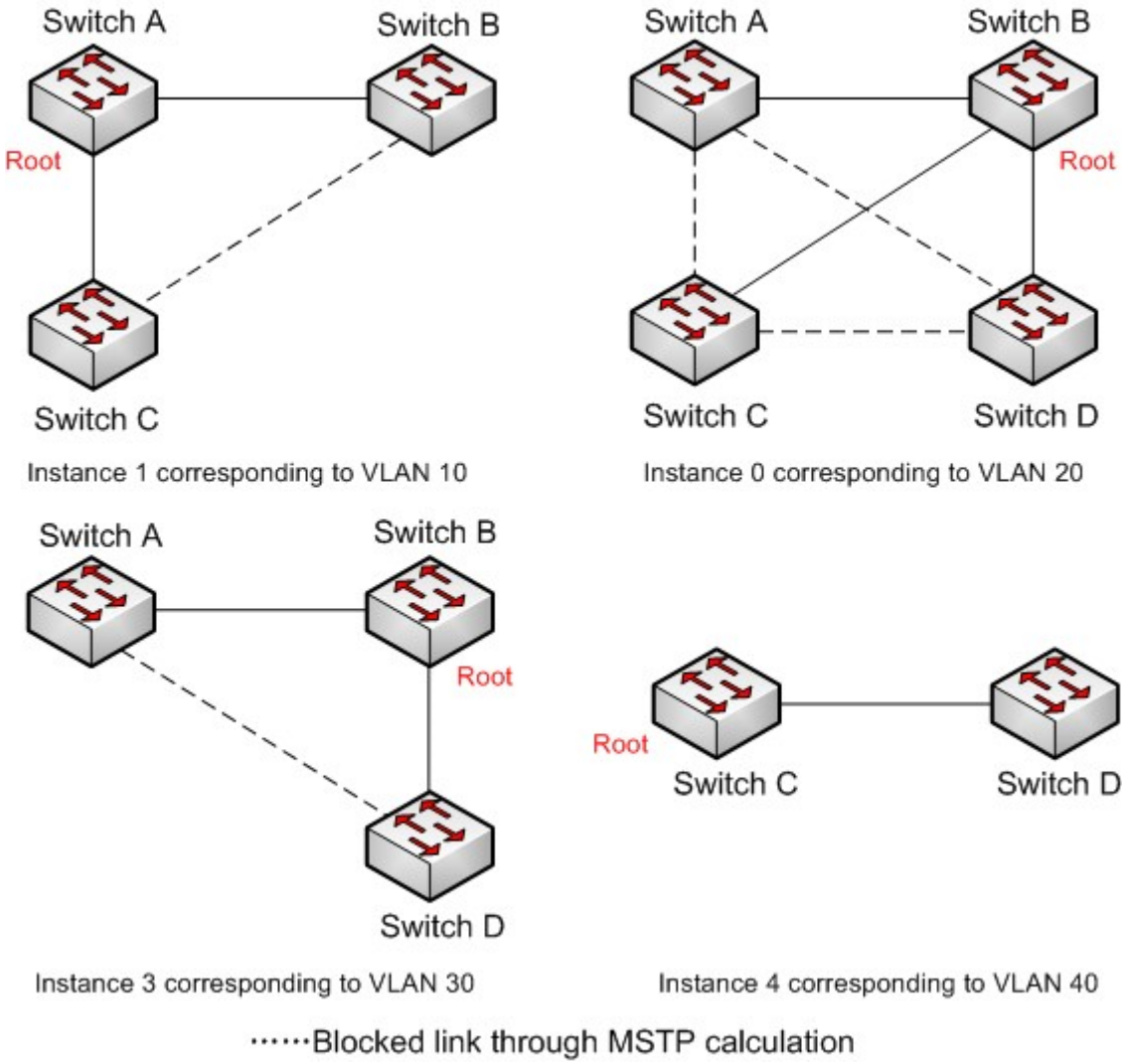


Рисунок 206 Экземпляры связующего дерева для каждой VLAN

6.10 Аварийная сигнализация

6.10.1 Введение

Коммутаторы этой серии поддерживают следующие типы аварийной сигнализации:

- Аварийная сигнализация по конфликту IP/MAC Если включено, аварийная сигнализация возникает при конфликте 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 электропитанию: Это применимо к изделиям с двумя источниками питания. Если эта функция включена, аварийный сигнал генерируется при отключении или нарушении питания.

- Аварийная сигнализация по кольцу: Если эта функция включена, аварийный сигнал генерируется, когда кольцо разомкнуто.
- Аварийная сигнализация высокой температуры: Если эта функция включена, аварийный сигнал генерируется, когда температура коммутатора превышает порог высокой температуры.

  Диапазон общего порога высокой температуры (T-high) составляет от 85° C до 94° C при

  настройке по умолчанию 85° C.

  Диапазон опасного порога высокой температуры (T-Max) составляет от 95° C до 100° C при настройке по умолчанию 95° C.

  Общий аварийный сигнал высокой температуры срабатывает, когда температура коммутатора (T-cur) выше порогового значения T-high и ниже порогового значения T-Max (T-high <T-cur<T-max).

  Аварийный сигнал опасной высокой температуры срабатывает, когда температура коммутатора равна или превышает пороговое значение T-Max (T-cur>=T-max).
- Аварийная сигнализация низкой температуры: Если эта функция включена, аварийный сигнал генерируется, когда температура коммутатора ниже порога низкой температуры.

  Диапазон порога низкой температуры (T-low) составляет от -40° C до 10° C при настройке по умолчанию -40° C.

  Аварийный сигнал низкой температуры срабатывает, когда температура коммутатора (T-cur) ниже порогового значения T-low (T-cur<T-low).
- Аварийная сигнализация по трафику порта: Если эта функция включена, аварийный сигнал генерируется, когда скорость входящего/исходящего трафика порта превышает указанный порог.

- Аварийная сигнализация по CRC и потере пакетов: Если эта функция включена, аварийный сигнал генерируется, когда число ошибок CRC/потерь пакетов превышает указанный порог.

Когда функция аварийной сигнализации активна, режимы тревоги включают запись в журнал, мигание тревожного светодиода на передней панели, срабатывание клеммного блока тревоги и отправку сообщений trap SNMP.

Предупреждение:

Только главное устройство станция кольца DT и корень DRP поддерживают функцию аварийной сигнализации кольца.

6.10.2 Настройка через веб-интерфейс

1. Настройте и отобразите аварийную сигнализацию по использованию памяти/ЦП. Щелкните [Device Advanced Configuration] → [Alarm] → [Basic Alarm], чтобы перейти на страницу настройки аварийной сигнализации по использованию памяти/ЦП, как показано на рисунке 207.

Mem and CPU Usage Alarm

Enable	☐ Mem Usage Alarm	☐ CPU Usage Alarm
Threshold	85 (50~100)	85 (50~100)
Margin Value	5 (1~20)	5 (1~20)
Alarm Status	Disable	Disable

Apply

Рисунок 207 Аварийная сигнализация по использованию памяти/ЦП

Mem Usage Alarm/CPU Usage Alarm

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение аварийной сигнализации по использованию памяти/ЦП.

Threshold (%)

Диапазон: 50~100

По умолчанию: 85
Функция: Задание порога использования памяти/ЦП. Когда использование памяти/ЦП коммутатора превышает пороговое значение, генерируется аварийный сигнал.

Margin Value (%)

Диапазон: 1~20

По умолчанию: 5

Функция: Задание значения допуска для порога использования памяти/ЦП.

Описание: Если использование памяти/ЦП 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 памяти/ЦП 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%.

Alarm Status

Варианты: Disable / Disable:

Функция: Отображение состояния использования памяти/ЦП коммутатора. Alarm означает, что использование памяти/ЦП превышает пороговое значение и вызывает сигнал тревоги.

Предупреждение:

Загрузка ЦП в этом документе относится к средней загрузке ЦП за пять минут.

2. Настройте и отобразите аварийную сигнализацию по питанию и температуре, как показано на рисунке 208.

Power and Temperature Alarm

Enable	Alarm Status
☐ Power Alarm	Disable
☐ High-Temperature Alarm	Disable
☐ Low-Temperature Alarm	Disable

Apply

Рисунок 208 Настройка аварийной сигнализации по питанию и температуре

Power Alarm/High-Temperature Alarm/Low-Temperature Alarm

Варианты: Disable/Enable

По умолчанию: Disable

Функция: Включение/выключение аварийной сигнализации по питанию, высокой температуре и низкой температуре.

Power Alarm Status

Варианты: 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. **High-Temperature Alarm Status / Low-Temperature Alarm Status**

Варианты: Normal/Alarm

Функция: Просмотр рабочей температуры коммутатора. Alarm означает, что температура коммутатора превышает пороговое значение высокой/низкой температуры и вызывает сигнал тревоги. Normal означает, что рабочая температура коммутатора в норме.

3. Настройте и отобразите аварийную сигнализацию по конфликту IP/MAC, как показано на рисунке 209.

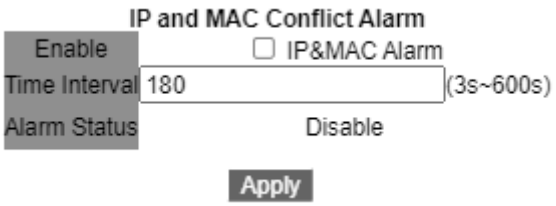


Рисунок 209 Аварийная сигнализация при конфликте IP/MAC.

Варианты конфигурации: Enable/disable

По умолчанию: disable

Функция: Включение/выключение аварийной сигнализации по конфликту адресов.

Time Interval

Диапазон настройки: 3~600 с

По умолчанию: 180 с

Функция: Настройка интервала времени для обнаружения конфликта адресов.

3. Настройте и отобразите аварийную сигнализацию по порту.

Щелкните [Device Advanced Configuration] → [Alarm] → [Port LinkDown Alarm], чтобы перейти на страницу настройки аварийной сигнализации по порту, как показано на рисунке 210.

Port LinkDown Alarm

Enable(Port)	Alarm Status	Enable(Port)	Alarm Status
☐ 1/1	Disable	☐ 1/2	Disable
☐ 1/3	Disable	☐ 1/4	Disable
☑ 2/1	LinkDown	☑ 2/2	LinkDown
☑ 2/3	LinkUp	☑ 2/4	LinkDown
☐ 3/1	Disable	☐ 3/2	Disable
☐ 3/3	Disable	☐ 3/4	Disable
☐ 4/1	Disable	☐ 4/2	Disable
☐ 4/3	Disable	☐ 4/4	Disable
☐ 5/1	Disable	☐ 5/2	Disable
☐ 5/3	Disable	☐ 5/4	Disable

Apply

Рисунок 210 Настройка аварийной сигнализация по порту

Port

Варианты: Disable/Enable

По умолчанию: Disable

Функция: Включение/выключение аварийной сигнализации по порту.

Alarm Status

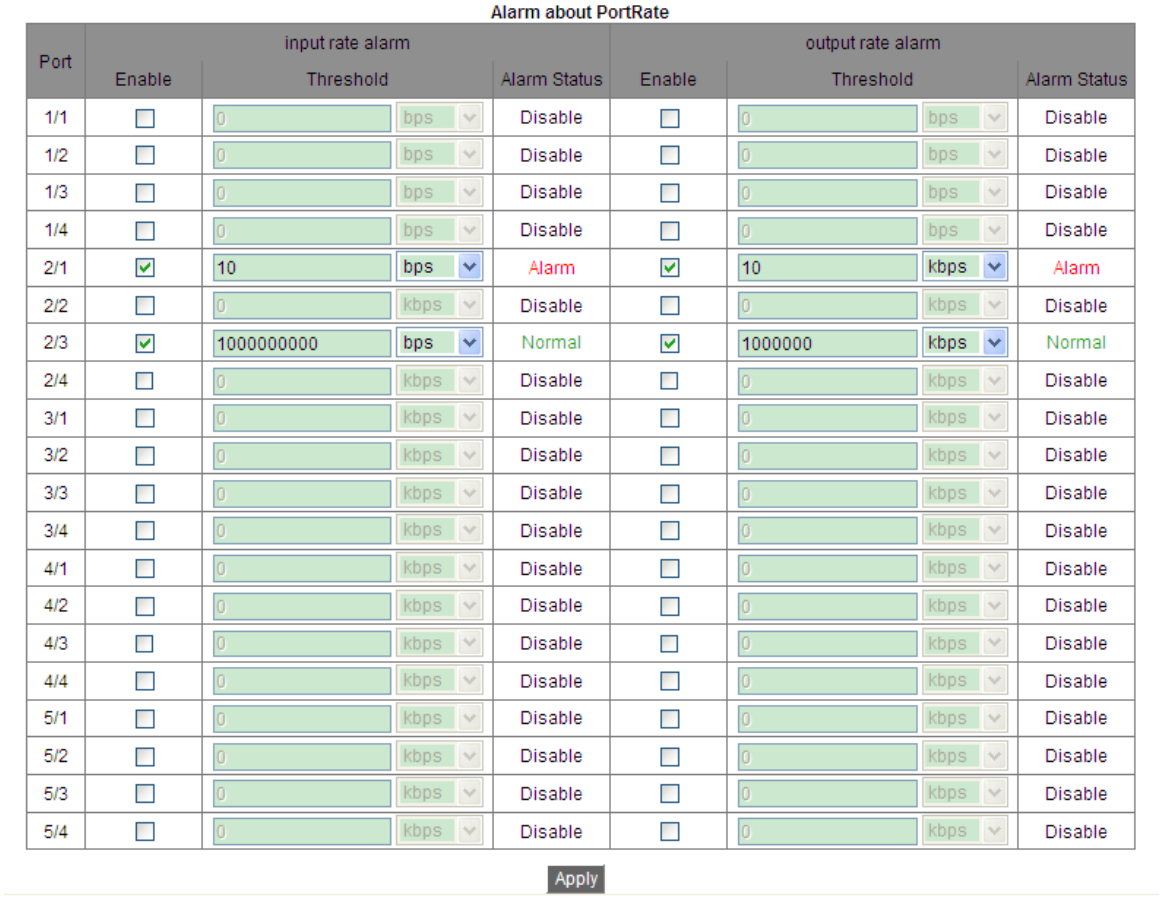
Варианты: LinkDown/LinkUp

Функция: Просмотр состояния подключения порта. LinkUp означает, что порт находится в состоянии подключения и поддерживает нормальный обмен данными. LinkDown означает, что порт отключен или находится в ненормальном состоянии (сбой обмена данными).

4. Настройте и отобразите аварийную сигнализацию по трафику порта.

Щелкните [Device Advanced Configuration] → [Alarm] → [Alarm about PortRate], чтобы

перейти на страницу настройки аварийной сигнализации по трафику порта, как показано на рисунке 211.



Port	input rate alarm			output rate alarm		
	Enable	Threshold	Alarm Status	Enable	Threshold	Alarm Status
1/1	☐	0 bps	Disable	☐	0 bps	Disable
1/2	☐	0 bps	Disable	☐	0 bps	Disable
1/3	☐	0 bps	Disable	☐	0 bps	Disable
1/4	☐	0 bps	Disable	☐	0 bps	Disable
2/1	☑	10 bps	Alarm	☑	10 kbps	Alarm
2/2	☐	0 kbps	Disable	☐	0 kbps	Disable
2/3	☑	1000000000 bps	Normal	☑	1000000 kbps	Normal
2/4	☐	0 kbps	Disable	☐	0 kbps	Disable
3/1	☐	0 kbps	Disable	☐	0 kbps	Disable
3/2	☐	0 kbps	Disable	☐	0 kbps	Disable
3/3	☐	0 kbps	Disable	☐	0 kbps	Disable
3/4	☐	0 kbps	Disable	☐	0 kbps	Disable
4/1	☐	0 kbps	Disable	☐	0 kbps	Disable
4/2	☐	0 kbps	Disable	☐	0 kbps	Disable
4/3	☐	0 kbps	Disable	☐	0 kbps	Disable
4/4	☐	0 kbps	Disable	☐	0 kbps	Disable
5/1	☐	0 kbps	Disable	☐	0 kbps	Disable
5/2	☐	0 kbps	Disable	☐	0 kbps	Disable
5/3	☐	0 kbps	Disable	☐	0 kbps	Disable
5/4	☐	0 kbps	Disable	☐	0 kbps	Disable

Apply

Рисунок 211 Настройка аварийной сигнализация по трафику порта

input rate alarm/output rate alarm

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение аварийной сигнализации по трафику порта.

Threshold

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

Функция: Задание порогового значения для трафика порта.

Alarm Status

Варианты: Alarm/ Normal

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

5. Настройте и отобразите аварийную сигнализацию по CRC и потере пакетов.

Щелкните [Device Advanced Configuration] → [Alarm] → [Alarm about CRC/ Pkt Loss], чтобы перейти на страницу настройки аварийной сигнализации по CRC и потере пакетов, как показано на рисунке 211.

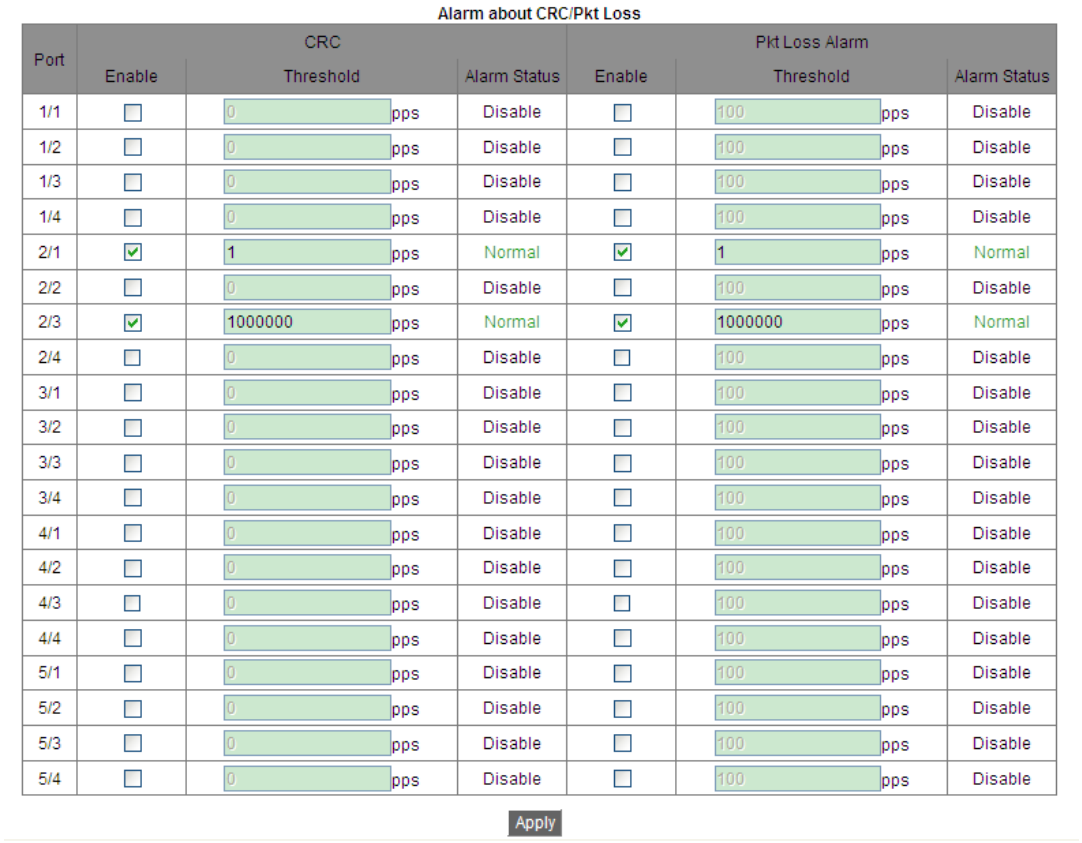


Рисунок 212 Настройка аварийной сигнализации по CRC и потере пакетов

CRC/Pkt Loss Alarm

Варианты: Enable/Disable

По умолчанию: Disable

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

Threshold

Диапазон: от 1 до 1000000 pps.

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

Alarm Status

Варианты: 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 DT-Ring.

Щелкните [Device Advanced Configuration] → [Alarm] → [Alarm about Ring], чтобы перейти на страницу настройки аварийной сигнализации DT-Ring, как показано на рисунке 213.

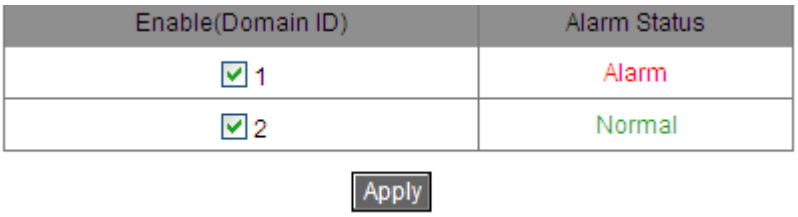


Рисунок 213 Настройка аварийной сигнализации DT-Ring

Alarm About DT-Ring

Варианты: Disable/Enable

По умолчанию: Disable

Функция: Включение/выключение аварийной сигнализации DT-Ring.

Alarm Status

Варианты: Alarm/Normal

Функция: Просмотр состояния DR-Ring. Normal означает, что DT-Ring замкнуто. Alarm означает, что DT-Ring разомкнуто или находится в ненормальном состоянии.

7. Настройте и отобразите аварийную сигнализацию DRP, как показано на рисунке 214.

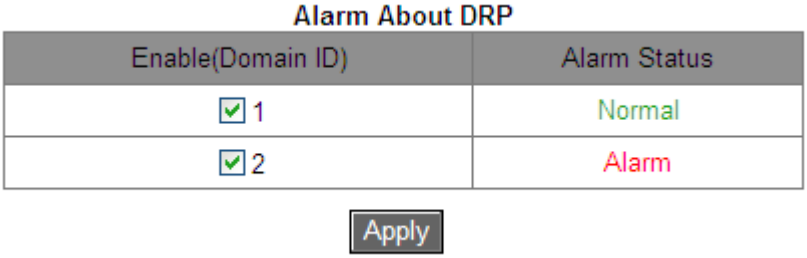


Рисунок 214 Настройка аварийной сигнализация DRP

Alarm About DRP

Варианты: Disable/Enable

По умолчанию: Disable

Функция: Включение/выключение аварийной сигнализации DRP.

Alarm Status

Варианты: Alarm/Normal

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

6.11 Цифровая диагностика

6.11.1 Введение

Цифровая диагностика является эффективным методом контроля важных рабочих параметров оптических приемопередатчиков. Параметры, подлежащие контролю, включают оптическую мощность передачи, оптическую мощность приема, температуру, рабочее напряжение, ток смещения и аварийные сигналы. Функция цифровой диагностики оптических трансиверов позволяет блоку NMS через двухлинейные последовательные шины получать доступ к оптическим трансиверам и контролировать их температуру, рабочее напряжение, ток смещения, передавать и получать оптическую мощность в режиме реального времени. Измеряя эти параметры, блок управления способен быстро определить конкретное место, где возникает ошибка в оптоволоконной линии связи, тем самым упрощая техническое обслуживание и повышая надежность системы.

6.11.2 Настройка через веб-интерфейс

1. Настройте и отобразите аварийную сигнализацию по мощности порта RX Sfp.

Щелкните [Device Advanced Configuration] → [Alarm] → [Sfp Port Rx Power Alarm], чтобы перейти на страницу настройки аварийной сигнализации по мощности порта RX Sfp, как показано на рисунке 215.

Sfp Port Rx Power Alarm

Enable(Port)	Threshold(unit:0.1dBm)	Alarm Status
☑ 1/3	-220 (-400~82)	Normal
☐ 1/4	-220 (-400~82)	Disable
☑ 3/1	-220 (-400~82)	Normal
☐ 3/2	-220 (-400~82)	Disable
☐ 3/3	-220 (-400~82)	Disable
☐ 3/4	-220 (-400~82)	Disable
☑ 4/1	-220 (-400~82)	Alarm
☑ 4/2	-220 (-400~82)	Alarm
☑ 4/3	-220 (-400~82)	Normal
☑ 4/4	-220 (-400~82)	Alarm

Apply

Рисунок 215 Аварийная сигнализация по мощности порта RX SFP

Sfp Port Rx Power Alarm

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение аварийной сигнализации по мощности порта RX Sfp.

Threshold

Диапазон: -400~82 (ед. изм: 0,1dBm)

По умолчанию: -220 (-22,0 dBm)

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

Alarm Status

Варианты: Alarm/ Normal

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

2. Настройте и отобразите аварийную сигнализацию приемопередатчика.

Щелкните [Device Advanced Configuration] → [Alarm] → [Alarm about transceiver], чтобы перейти на страницу настройки аварийной сигнализации приемопередатчика, как показано на рисунке 216.

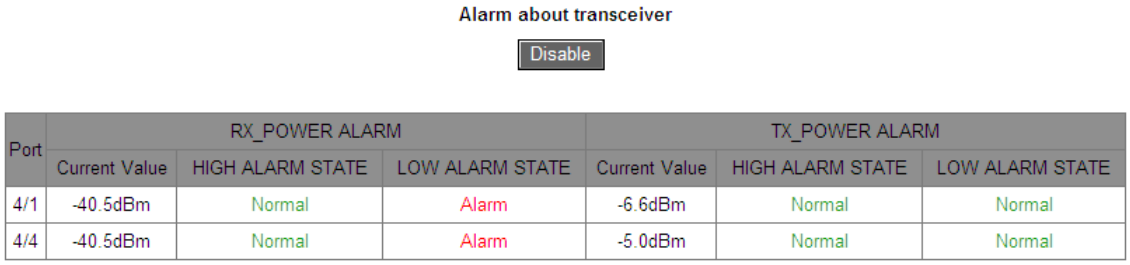


Рисунок 216 Настройка аварийной сигнализации приемопередатчика

Alarm about transceiver

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.

6.12 Настройка журнала

6.12.1 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.

Журналы делятся на 4 уровня в зависимости от их важности и важности от Критического, Предупреждения, Информации до Отладки в порядке убывания. Чем меньше значение, тем более актуальной является информация.

Таблица 11 Уровни информации

Уровень информации	**Значение**	**Описание**
Critical	2	Серьезная проблема в системе
Warning	4	Предупреждение
Information	6	Уведомление, которое должно быть зафиксировано
Debugging	7	Информация, созданная в процессе отладки

6.12.2 Настройка через веб-интерфейс

1. Настройте функцию журнала

Щелкните [Device Advanced Configuration] → [Log Configuration] → [Log Configuration] , чтобы перейти на страницу настройки журнала, как показано на рисунке 217.

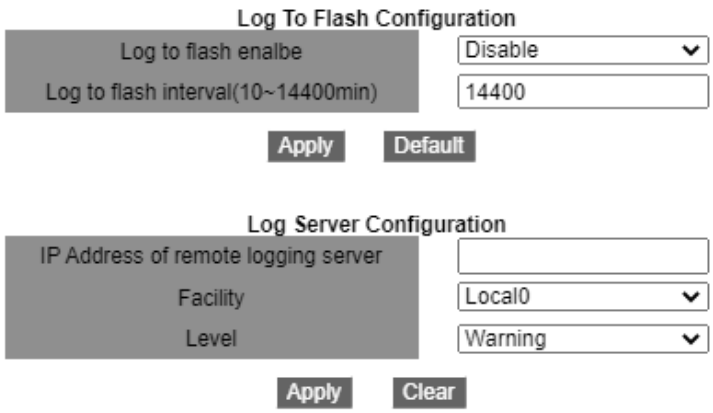


Рисунок 217 Настройка журнала

Log to flash enable

Варианты: Enable/Disable

По умолчанию: disable

Функция: Сохранение журнала во флэш-памяти.

Log to flash interval

Варианты: 10~14400 мин

По умолчанию: 14400

Функция: Настройка интервала времени для сохранения журнала во флэш-памяти.

IP Address of remote logging server

Настройка IP-адреса сервера для выгрузки информации журнала.

Facility

Варианты: Local0-Local7

По умолчанию: Local0

Описание: Параметр Facility используется для идентификации различных источников журналов на сервере.

Level

Варианты: Critical/Warning/Information/Debugging

По умолчанию: Warning

Функция: Выбор уровня регистрируемой отображаемой информации журнала.

Описание: Информацию журнала можно отфильтровать по уровням. Правило фильтрации заключается в том, что запрещается вывод информации, значение уровня которой больше значения выбранного уровня. Например, если выбран уровень информации Warning и соответствующее ему значение равно 4, система выводит только информацию Critical со значением 2 и информацию Warning со значением 4.

Можно установить программное обеспечение Syslog Server, например, Tftp32, на ПК для создания Syslog Server.

Информация журнала может отображаться в режиме реального времени на сервере Syslog, как показано на рисунке 218.

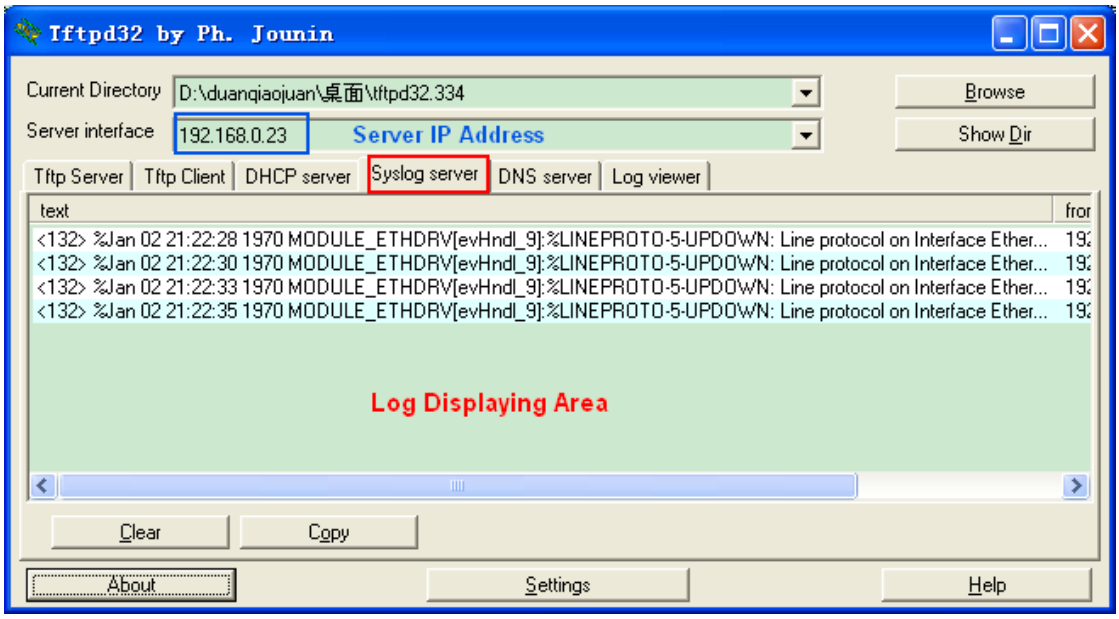


Рисунок 218 Выгрузка информации журнала в реальном времени

2. Просмотрите настройки журнала.

Щелкните [Device Advanced Configuration] → [Log Configuration] → [Show Log], чтобы просмотреть журнал, как показано на рисунке 219.

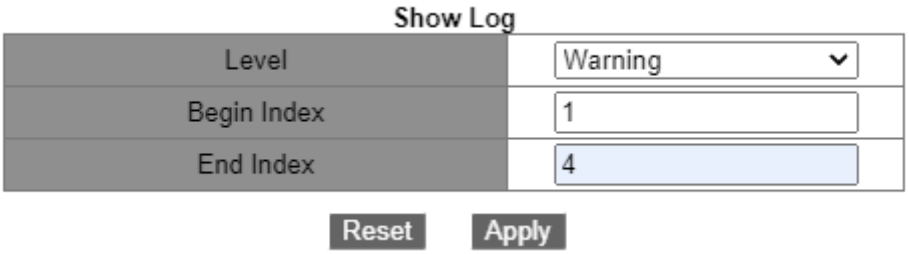


Рисунок 219 Настройка журнала

Level

Варианты: Warning/Critical

По умолчанию: Warning

Функция: Выбор нижнего уровня отображаемой информации журнала.

Begin Index/End Index

Диапазон: 1~65535

Функция: Просмотр выбранной информации журнала в буфере, где одна строка соответствует одной записи.Рисунок 220 показывает выбранную информацию журнала в буфере.

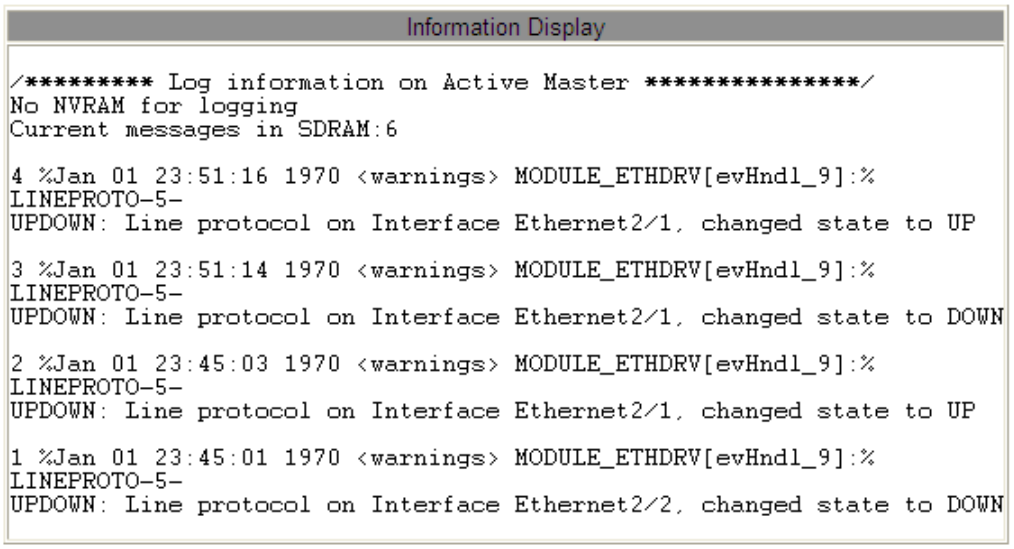


Рисунок 220 Информация журнала

Предупреждение:

В буфере сохраняется только информация уровня Critical и Warning, без информации уровня Information и Debugging.

3. Выгрузка журнала

Щелкните [Device Advanced Configuration] → [Log Configuration] → [Log Transmit], чтобы перейти на страницу выгрузки журнала, как показано на рисунке 221.

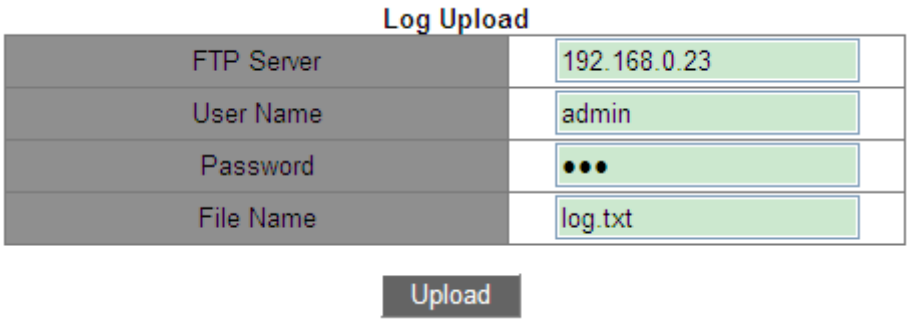


Рисунок 221 Выгрузка журналов

FTP Server

Формат: A.B.C.D

Функция: Настройка IP-адреса сервера FTP.

User Name

Функция: Настройка имени пользователя сервера FTP.

Password

Функция: Настройка пароля пользователя сервера FTP.

File Name

Диапазон: 1~32 символа

Функция: задание имени файла на сервере.

Предупреждение:

FTP-сервер должен оставаться в рабочем состоянии во время выгрузки журналов.

4. Стирание информации журнала в буфере

Щелкните [Device Advanced Configuration] → [Log Configuration] → [Clear Log] , чтобы очистить журнал, как показано на рисунке 222.

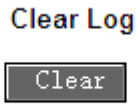


Рисунок 222 Очистка журнала

6.13 Настройка маршрутизации

Чтобы получить доступ к удаленному узлу в Интернете, узел должен выбрать соответствующий маршрут с помощью маршрутизаторов или коммутаторов уровня Layer-3. В процессе выбора пути каждый коммутатор уровня Layer-3 выбирает путь к следующему коммутатору уровня Layer-3 в соответствии с адресом получателя полученного пакета до тех пор, пока последний коммутатор уровня Layer-3 не отправит пакет хосту-получателю. Путь, который выбирает каждый коммутатор

уровня Layer-3, называется маршрутом. Маршруты делятся на следующие типы:

Прямой маршрут: указывает маршрут, обнаруженный протоколом канального уровня.

Статический маршрут: указывает маршрут, настроенный сетевым администратором вручную. Динамический маршрут: указывает маршрут, обнаруженный протоколом маршрутизации.

Примечание: В коммутаторах этой серии протоколы маршрутизации поддерживают только SICOM3028GPT-L3GT, SICOM3028GPT-L3FT, SICOM3028GPT-L3G и SICOM3028GPT-L3F уровня Layer-3.

6.13.1 Настройка статического маршрута

6.13.1.1 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.

6.13.1.2 Таблица маршрутизации

Каждый коммутатор уровня Layer-3 поддерживает таблицу маршрутизации, в которой записываются все маршруты, используемые коммутатором. Каждая запись в таблице указывает, через какой интерфейс VLAN должен пройти пакет, предназначенный для определенной подсети или хоста, чтобы достичь следующего маршрутизатора или пункта назначения, подключенного напрямую.

Запись маршрута включает следующие элементы:

Пункт назначения: указывает IP-адрес или сеть назначения.

Маска подсети: вместе с адресом назначения указывает сеть, в которой находится хост

назначения или коммутатор уровня Layer-3. Логическая операция И между адресом назначения и маской подсети дает адрес сети назначения. Например, если адрес назначения — 129.102.8.10, а маска — 255.255.0.0, адрес сети назначения — 129.102.0.0. Маска состоит из определенного количества последовательных единиц. Она может быть выражен в десятичном формате с точками или количеством единиц.

Выход: указывает интерфейс, через который должен быть перенаправлен соответствующий IP-пакет.

IP-адрес следующего коммутатора уровня Layer-3 (следующий переход): указывает новый коммутатор уровня Layer-3, через который будет проходить IP-пакет.

Приоритет: Маршруты к одному и тому же месту назначения, но с разными следующими переходами, могут иметь разные приоритеты и обнаруживаться с помощью различных протоколов маршрутизации или настраиваться вручную. Оптимальный маршрут — маршрут, который имеет наивысший приоритет.

6.13.1.3 Маршрут по умолчанию

Чтобы избежать слишком большого числа записей в таблице маршрутизации, можно настроить маршрут по умолчанию. Маршрут по умолчанию является статическим маршрутом. Если пакету данных не удается найти соответствие в таблице маршрутизации, он пересылается по маршруту по умолчанию. В таблице маршрутизации маршрутом по умолчанию является маршрут, в котором пункт назначения и маска равны 0.0.0.0. Если пакет не соответствует ни одной записи в таблице маршрутизации и маршрут по умолчанию не настроен, коммутатор отбрасывает пакет и возвращает пакет ICMP, указывающий, что адрес назначения или сеть недоступны.

6.13.1.4 Настройка через веб-интерфейс

1. Настройте статический маршрут.

Щелкните [Device Advanced Configuration] → [Route configuration] → [Static route configuration]

→ [Static route configuration], чтобы перейти на страницу настройки статического маршрута, как показано на рисунке 223.

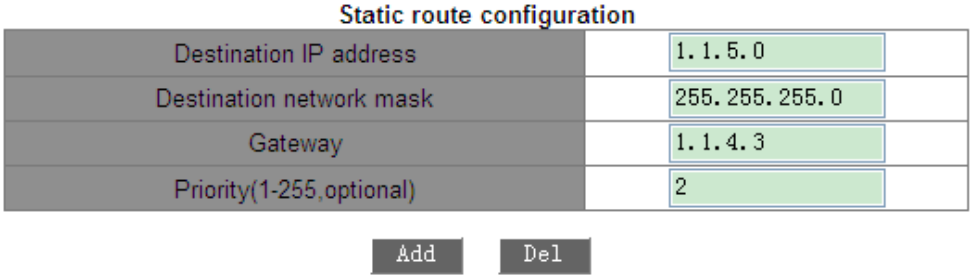


Рисунок 223 Настройка статического маршрута

Destination IP Address

Формат: A.B.C.D

Функция: Задание IP-адреса сети назначения.

Destination network mask

Функция: Задание маски подсети, в которой находится хост назначения или коммутатор уровня Layer-3.

Gateway

Формат: A.B.C.D

Функция: Задание IP-адреса следующего перехода.

Priority

Диапазон: 1~255

По умолчанию: 1

Функция: Настройка приоритета текущего маршрута. Маршрут с наименьшим значением приоритета выбирается как лучший маршрут для пересылки пакетов.

Чтобы удалить запись маршрута, необходимо настроить все параметры так, чтобы они соответствовали параметрам маршрута; в противном случае маршрут не может быть удален из-за сбоя сопоставления.

После настройки маршрута он отображается в списке статических маршрутов, как показано на рисунке 224.

Static ip route list

Destination IP address	Destination network mask	Gateway	Priority
1.1.1.0	255.255.255.0	1.1.2.3	1
1.1.5.0	255.255.255.0	1.1.4.3	2

Рисунок 224 Список статических маршрутов

6.13.1.5 Типовой пример конфигурации

Как показано на рисунке 225, 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.

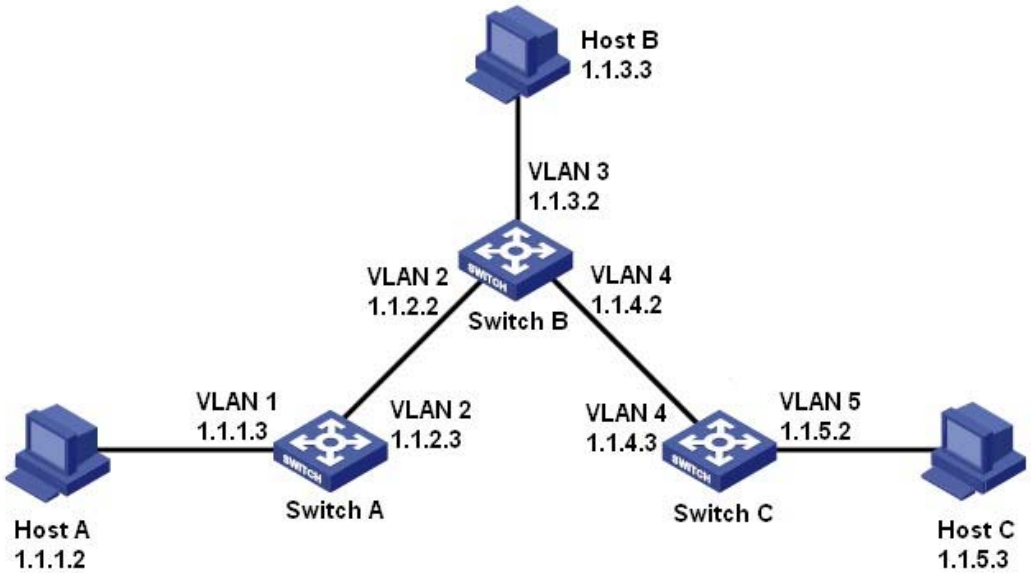


Рисунок 225 Пример настройки статических маршрутов

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 223.

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 223.

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 223.

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 223.

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 223.

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.

6.13.2 Настройка RIP

6.13.2.1 Введение

Примечание:

В этой главе под маршрутизаторами понимаются коммутаторы уровня Layer-3.

Протокол Routing Information Protocol (RIP) — это протокол внутреннего шлюза с вектором расстояния, использующий пакеты UDP для обмена информацией через порт 520. Каждый коммутатор L3, на котором работает протокол RIP, имеет базу данных маршрутизации. База данных маршрутизации содержит записи маршрутизации ко всем доступным пунктам назначения этого коммутатора L3, на

основе которых создается таблица маршрутизации. Когда коммутатор L3, использующий RIP, отправляет пакеты обновления маршрута своим соседним устройствам, этот пакет содержит всю таблицу маршрутизации, установленную этим коммутатором L3 на основе базы данных маршрутизации. Следовательно, в крупномасштабной сети каждый коммутатор L3 должен передавать и обрабатывать большой объем данных маршрутизации, что снижает производительность сети. RIP позволяет вносить информацию о маршрутизации, обнаруженную другими протоколами маршрутизации, в таблицу маршрутизации.

RIP имеет две версии, RIP-1 и RIP-2. RIP-1 поддерживает объявление сообщений только через широковещательную рассылку, не поддерживает маску подсети и аутентификацию. Некоторые поля в сообщении RIP-1 должны быть нулевыми. Эти поля называются нулевыми полями, которые следует проверять при получении сообщения RIP-1. Если такое поле содержит ненулевое значение, сообщение RIP-1 не будет обработано. RIP-2 – это усовершенствованная версия на основе RIP-1. В RIP-2 пакеты протокола отправляются в многоадресном режиме, а адрес назначения — 224.0.0.9. Кроме того, в RIP-2 добавлены домен маски подсети и домен проверки RIP (поддерживается простой текстовый пароль и проверка пароля MD5), а также поддерживаются маски подсети переменной длины (VLSM). RIP-2 сохраняет часть нулевых доменов в RIP-1, и поэтому нет необходимости проверять все нулевые домены. По умолчанию коммутатор уровня L3 передает сообщение RIP-2 в многоадресном режиме, принимает сообщения RIP-1 и RIP-2.

RIP использует количество переходов для измерения расстояния до пункта назначения. Количество переходов от маршрутизатора к сети с непосредственным подключением равно 0. Количество переходов от маршрутизатора к непосредственно подключенному маршрутизатору равно 1. Чтобы ограничить время конвергенции, диапазон значений метрики RIP составляет от 0 до 15. Значение метрики 16 (или выше) считается бесконечным, что означает, что сеть назначения недоступна. Поэтому RIP подходит для сетей небольшого размера.

6.13.2.2 Предотвращение петель маршрутизации

В сети, использующей RIP, когда маршрут RIP становится недоступным, коммутатор RIP L3 не будет отправлять пакет обновления маршрута немедленно, пока не истечет интервал обновления маршрута (30 с). Если соседний коммутатор L3 отправляет пакет, содержащий информацию о его собственной таблице маршрутизации, на коммутатор L3 до того, как будет получен пакет обновления маршрута, произойдет бесконечный подсчет. То есть метрика выбора маршрута к недостижимому коммутатору L3 увеличивается постепенно. Это значимо влияет на время маршрутизации и время агрегации маршрутов.

Чтобы избежать бесконечного подсчета, RIP предоставляет механизмы расщепления горизонта и триггерного обновления для решения проблемы петли маршрутизации. Расщепление горизонта направлено на то, чтобы избежать отправки маршрутов на шлюз, из которого они были получены. Технология включает в себя простое расщепление горизонта и расщепление горизонта с отравлением обратного маршрута. Простое расщепление горизонта удаляет маршруты, которые должны быть отправлены на соседний шлюз, от которого эти маршруты были получены. Расщепление горизонта с отравлением обратного маршрута удаляет предыдущие маршруты из пакета обновления и устанавливает метрики этих маршрутов на 16. В механизме триггерного обновления всякий раз, когда шлюз изменяет метрику маршрута, пакет обновления маршрута будет передан немедленно, без учета состояния 30-секундного таймера обновления.

6.13.2.3 6.13.2.3 Принцип работы

1. После включения RIP маршрутизатор отправляет сообщения-запросы соседним маршрутизаторам. Соседние маршрутизаторы возвращают ответные сообщения, включая информацию о своих таблицах маршрутизации.

2. Получив такую информацию, маршрутизатор обновляет свою локальную таблицу маршрутизации и отправляет инициированные сообщения об обновлении своим соседям. Все маршрутизаторы в сети делают то же самое для сохранения самой последней информации о маршрутизации.

3. По умолчанию локальная таблица маршрутизации отправляется на соседние маршрутизаторы с интервалом в 30 секунд. После получения пакета, содержащего эту таблицу маршрутизации, соседние маршрутизаторы, использующие протокол RIP, будут поддерживать свои собственные локальные маршруты, выбирать оптимальный маршрут и отправлять сообщение об обновлении своим соответствующим соседям, чтобы обновленный маршрут стал действовать глобально. Кроме того, RIP использует механизм истечения срока действия для обработки устаревших маршрутов. В частности, если коммутатор L3 не получает информацию об обновлении маршрута от соседа в течение указанного интервала времени (значение параметра invalid timer), все маршруты от этого соседа будут считаться недопустимыми маршрутами, и маршрут переходит в состояние подавления. Такие маршруты имеет срок действия (значение таймера удержания) в таблице маршрутизации. Если в течение этого периода от соседнего узла не будет получена информация об обновлении, эти маршруты удаляются из таблицы маршрутизации.

6.13.2.4 Настройка через веб-интерфейс

Базовая настройка работы RIP в коммутаторе уровня L3 проста. Как правило, необходимо включить RIP и разрешить порту передавать и получать пакеты RIP, что означает передачу и получение пакетов RIP в соответствии с настройкой RIP по умолчанию (по умолчанию коммутатор уровня L3 передает RIP-2, принимает RIP-1 и RIP-2).

1. Включите RIP

Щелкните [Device Advanced Configuration] →[Route configuration]→[RIP configuration]→[Enable RIP]→[Enable RIP], чтобы включить RIP, как показано на рисунке 226.

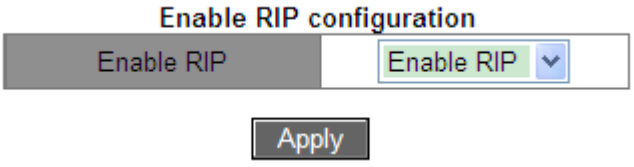


Рисунок 226 Включение RIP

Enable RIP

Варианты: Enable RIP/Disable RIP

По умолчанию: Disable RIP

Функция: Включение/выключение RIP.

2. Включите RIP на интерфейсе

Щелкните [Device Advanced Configuration] →[Route configuration]→[RIP configuration]→[Enable RIP]→[Enable port to receive/transmit RIP packet], чтобы включить RIP на интерфейсе, как показано на рисунке 227.

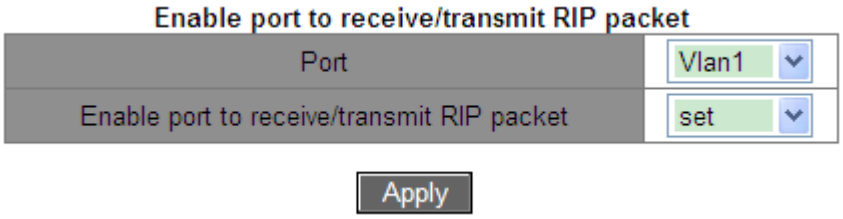


Рисунок 227 Включение RIP на интерфейсе

Enable port to receive/transmit RIP packet

Варианты: set/cancel

По умолчанию: set

Функция: Включение/выключение RIP на интерфейсе.

3. Настройка импортированного маршрута

Щелкните [Device Advanced Configuration] →[Route configuration]→[RIP configuration]→[RIP parameter configuration]→[Enable imported route], чтобы перейти на страницу настройки импортированного маршрута, как показано на рисунке 228.

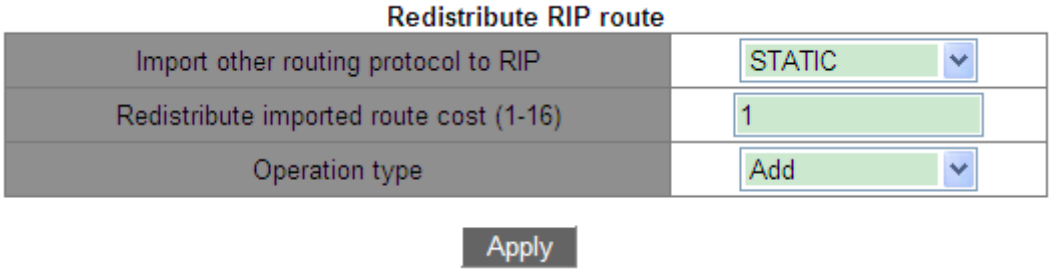


Рисунок 227 Настройка импортированного маршрута

Import other routing protocol to RIP

Варианты: STATIC/OSPF

Функция: Импорт другого протокола маршрутизации в RIP. Можно импортировать только активные маршруты.

Redistribute imported route cost

Диапазон: 1~16

Функция: Перераспределение значения метрики импортированного маршрута. Это дополнительный параметр. Если параметр не настроен, перераспределение будет в соответствии со значением метрики по умолчанию.

Operation type

Варианты: Add/Del

Функция: Ддобавление/отмена импорта другого протокола маршрутизации в RIP. По умолчанию никакие другие протоколы маршрутизации в RIP не импортируются.

4. Настройте дополнительную метрику маршрутизации

Щелкните [Device Advanced Configuration] →[Route configuration]→[RIP configuration]→[RIP parameter configuration]→[Metricin/out configuration], чтобы перейти на страницу настройки дополнительной метрики маршрутизации, как показано на рисунке 229.

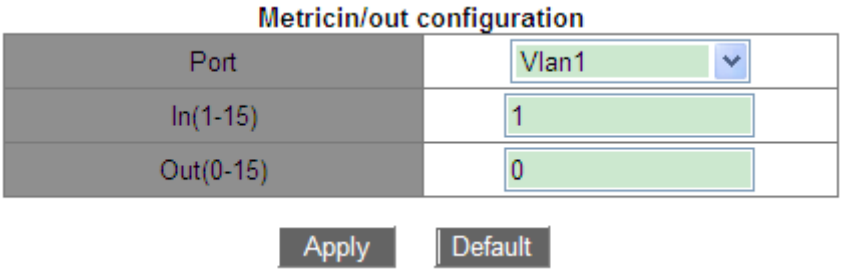


Рисунок 229 Настройка дополнительной метрики маршрутизации

In

Диапазон: 1~15

По умолчанию: 1

Функция: Настройка входящей дополнительной метрики маршрутизации. Входящая дополнительная метрика добавляется к метрике полученного маршрута перед добавлением маршрута в таблицу маршрутизации, и метрика маршрута изменяется. Если сумма дополнительной метрики и исходной метрики больше 16, метрика маршрута будет равна 16.

Out

Диапазон: 0~15

По умолчанию: 0

Функция: Настройка исходящей дополнительной метрики маршрутизации. Исходящая дополнительная метрика добавляется к метрике отправленного маршрута, и метрика маршрута в таблице маршрутизации не изменяется.

5. Настройка порта RIP

Щелкните [Device Advanced Configuration] →[Route configuration]→[RIP configuration]→[RIP parameter configuration]→[RIP port configuration], чтобы перейти на страницу настройки порта RIP, как показано на рисунке 230.

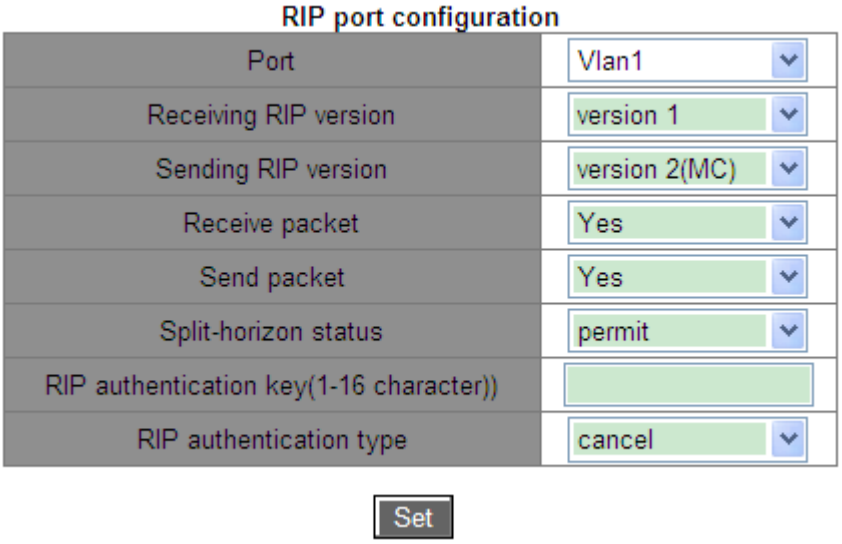


Рисунок 230 Настройка порта RIP

Receiving RIP version

Варианты: version 1/version 2/version 1 and 2

По умолчанию: version 1 and 2

Функция: Задать версию сообщения RIP, полученного интерфейсом. Version 1 означает сообщение RIP-1, полученное интерфейсом, version 2 означает RIP-2, а version 1 и 2 означают RIP-1 и RIP-2.

Sending RIP version

Варианты: version 1/version 2 (BC)/version 2 (MC)

По умолчанию: version 2 (MC)

Функция: Задать версию сообщения RIP, переданного интерфейсом. Version 1 означает сообщение RIP-1, version 2 (BC) – сообщение RIP-2, передаваемое интерфейсом в широковещательном режиме, version 2 (MC) означает сообщение RIP-2, передаваемое в многоадресном режиме.

Receive packet

Варианты: Yes/No

По умолчанию: Yes

Функция: Разрешить/запретить интерфейсу принимать сообщения RIP.

Send packet

Варианты: Yes/No

По умолчанию: Yes

Функция: Разрешить/запретить интерфейсу отправлять сообщения RIP.

Split-horizon status

Варианты: permit/forbid

По умолчанию: permit

Функция: Разрешить/запретить расщепление горизонта. Расщепление горизонта позволяет предотвратить образование петель маршрутизации, то есть избежать отправки маршрута обратно на узел, от которого его получил данный интерфейс.

RIP authentication key

Диапазон: 1~16 символов

Функция: Задать ключ аутентификации RIP.

RIP authentication type

Варианты: text /Cisco MD5/MD5/cancel

По умолчанию: cancel

Функция: Задать тип аутентификации RIP. text означает текстовую аутентификацию; MD5 означает общую аутентификацию MD5; Cisco MD5 означает аутентификацию Cisco MD5; cancel означает восстановление аутентификации по умолчанию: текстовая

аутентификация. RIP-1 не поддерживает аутентификацию.

6. Настройка режима RIP

Щелкните [Device Advanced Configuration] →[Route configuration]→[RIP configuration]→[RIP parameter configuration]→[RIP mode configuration], чтобы перейти на страницу настройки режима RIP, как показано на рисунке 231.

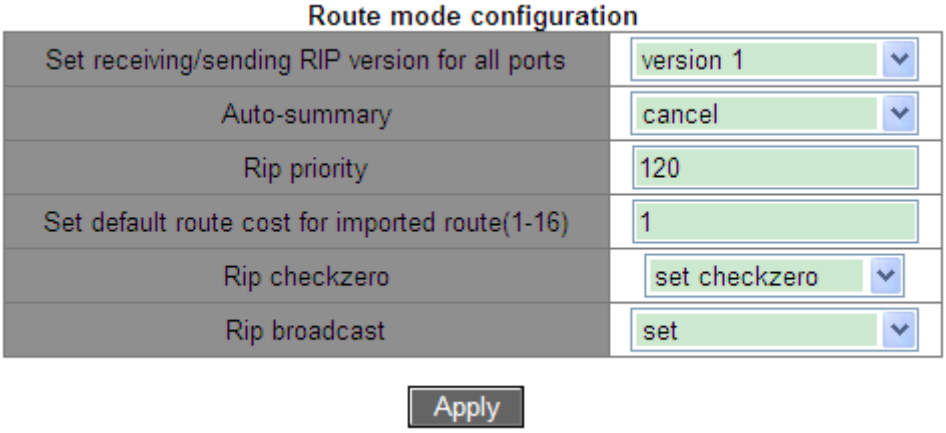


Рисунок 231 Настройка режима RIP

Set receiving/sending RIP version for all ports

Варианты: version 1/version 2/cancel

По умолчанию: передача сообщения RIP-2, получение сообщения RIP 1 и RIP 2.

Функция: Настройка версии сообщения RIP, передаваемого и принимаемого всеми интерфейсами маршрутизации. version 1 означает, что сообщение RIP-1 передается и принимается всеми интерфейсами маршрутизации, version 2 означает RIP-2, cancel означает восстановление конфигурации по умолчанию.

Auto-summary

Варианты: cancel/set

По умолчанию: cancel

Функция: Задать/отменить агрегацию маршрутов. Агрегация маршрутов означает, что подсети в естественной сети объединяются в естественную сеть, которая отправляется в другие сети. Эта функция может уменьшить объем информации о маршрутизации в таблице маршрутизации и объем информации о коммутации. RIP-1

не поддерживает маску подсети, если переадресация маршрута подсети может вызвать неоднозначность, поэтому RIP-1 всегда включает функцию агрегации маршрутизации. Для RIP-2, если вы хотите транслировать маршруты подсети, отключите функцию агрегирования маршрутов.

Rip Priority

Диапазон: 0~255

По умолчанию: 120

Функция: Настройка приоритета RIP. Чем меньше значение, тем выше приоритет. Приоритет определяет маршруты в базовой таблице маршрутизации, выбирая, какой алгоритм будет использоваться для получения наилучшей маршрутизации.

Set default route cost for imported route

Диапазон: 1~16

По умолчанию: 1

Функция: Настройка значения по умолчанию для метрики импортированного маршрута.

Rip checkzero

Варианты: set checkzero/cancel checkzero

По умолчанию: set checkzero

Функция: Проверять/не проверять нулевое поле сообщения RIP-1. Некоторые поля в сообщении RIP-1 должны быть нулевыми. Эти поля называются нулевыми полями. Можно включить проверку нулевого поля в полученном сообщении RIP-1. Если такое поле содержит ненулевое значение, сообщение RIP-1 не будет обработано. Поскольку в сообщении RIP-2 нет нулевого поля, эта функция не работает для RIP-2.

Rip broadcast

Варианты: set/cancel

По умолчанию: set

Функция: значение set разрешает всем интерфейсам коммутатора уровня 3 передавать широковещательные пакеты RIP или многоадресные пакеты; cancel — запретить всем интерфейсам коммутатора 3-го уровня передавать широковещательные или многоадресные пакеты RIP, а лишь передавать пакеты данных RIP между соседними коммутаторами 3-го уровня.

7. Настройка таймеров RIP

Щелкните [Device Advanced Configuration] →[Route configuration]→[RIP configuration]→[RIP parameter configuration]→[RIP timer configuration], чтобы перейти на страницу настройки таймеров RIP, как показано на рисунке 232.

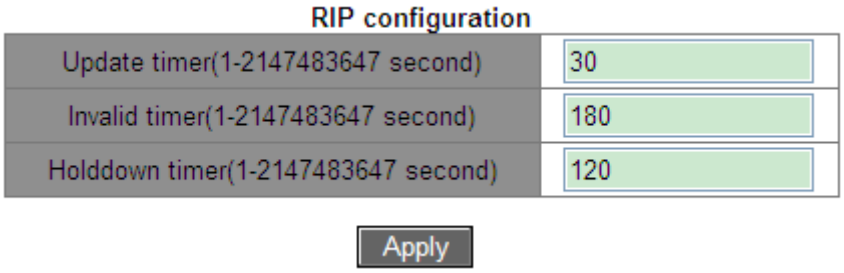


Рисунок 232 Настройка таймеров RIP

Update timer

Диапазон: 1～2147483647

По умолчанию: 30

Функция: Настройка интервала между обновлениями маршрутизации.

Invalid timer

Диапазон: 1～2147483647

По умолчанию: 180

Функция: Настройка интервала времени, после которого маршрутизация RIP объявляется недействительной. В частности, если коммутатор L3 не получает информацию об обновлении маршрута от соседа в течение указанного интервала времени (значение параметра invalid timer), все маршруты от этого соседа будут считаться недопустимыми маршрутами, и маршрут переходит в состояние подавления. Invalid timer >Update timer.

Holddown timer

Диапазон: 1～2147483647

По умолчанию: 120

Функция: Настройка времени, в течение которого маршрут RIP остается в подавленном состоянии. Если в течение этого периода (значение параметра holddown timer) от соседнего узла не будет получена информация об обновлении, эти маршруты удаляются из таблицы маршрутизации. Holddown timer >Update timer.

6.13.2.5 Типовой пример конфигурации

Как показано на рисунке 233, коммутатор B подключен к коммутатору A через интерфейс VLAN 2 и к коммутатору C через интерфейс VLAN 4, все три коммутатора работают по протоколу маршрутизации RIP. Маски подсети всех коммутаторов в сети имеют вид 255.255.255.0.

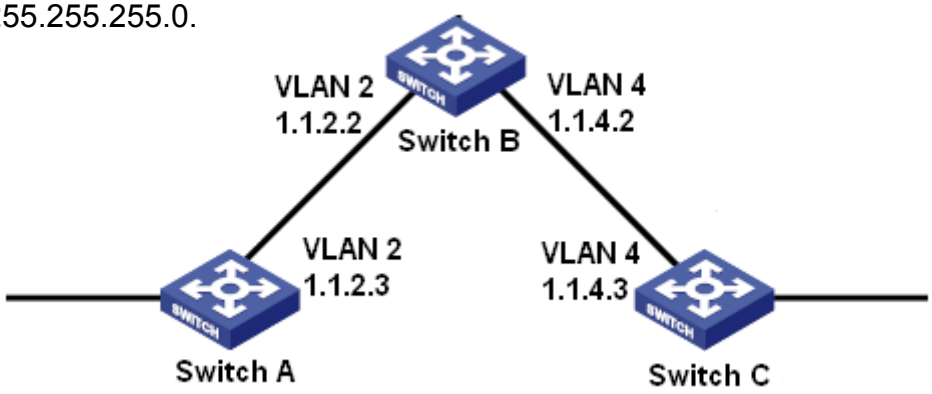


Рисунок 233 Пример настроек RIP

Конфигурация коммутатора A:

1. Задайте IP-адрес для интерфейса VLAN 2.
2. Включите протокол RIP, как показано на рисунке 226.
3. Включите интерфейс VLAN 2 для передачи/получения сообщения RIP, как показано на рисунке 227.

Конфигурация коммутатора B:

1. Задайте IP-адреса для интерфейсов VLAN 2 и VLAN 4.
2. Включите протокол RIP, как показано на рисунке 226.
3. Включите интерфейсы VLAN 2 и VLAN 4 для передачи/получения сообщения RIP, как показано на рисунке 227.

Конфигурация коммутатора C:

1. Задайте IP-адрес для интерфейса VLAN 4.

2. Включите протокол RIP, как показано на рисунке 226.

3. Включите интерфейс VLAN 4 для передачи/получения сообщения RIP, как показано на рисунке 227.

6.13.3 Настройка OSPF

6.13.3.1 Введение

Open Shortest Path Первое (OSPF) – это протокол маршрутизации на основе отслеживания состояния канала. Коммутаторы уровня Layer-3 обмениваются информацией о состоянии канала для создания базы данных состояния канала (LSDB). Затем каждый из маршрутизаторов использует алгоритм SPF (Shortest Path First), базирующийся на LSDB, для генерации таблицы маршрутизации. Коммутаторы этой серии поддерживают OSPF версии 2.

Примечание:

В этой главе под маршрутизаторами понимаются коммутаторы уровня Layer-3.

6.13.3.2 Основная концепция

1. AS

Автономная система (AS) включает в себя группу маршрутизаторов, которые работают, используя один и тот же протокол маршрутизации.

2. Router ID

Router ID (RID): Маршрутизатор с поддержкой OSPF должен иметь собственный идентификатор маршрутизатора, который является уникальным идентификатором маршрутизатора в AS. RID можно настроить вручную или сгенерировать автоматически. Автоматически сгенерированный RID — это основной IP-адрес интерфейса VLAN с наименьшим идентификатором на коммутаторе.

3. Пакеты OSPF

Hello: Периодически отправляется для поиска и обслуживания соседей, содержит значения некоторых таймеров, информацию о DR, BDR и известных соседях.

Database description (DD): Описывает дайджест каждого объявления о состоянии канала (LSA) в LSDB, которым обмениваются два маршрутизатора для

синхронизации данных.

Link state request (LSR): После обмена пакетами DD два маршрутизатора узнают, какие LSA соседа отсутствуют в их LSDB. Затем они отправляют друг другу пакет LSR, запрашивая недостающие LSA. Пакет LSA содержит дайджест отсутствующих LSA.

Link state update (LSU): Передает LSA для обновления соседнему узлу. Каждый пакет LSU может содержать несколько LSA.

Link state acknowledgment (LSAck): Подтверждает полученные пакеты LSU. Он содержит заголовки полученных LSA (пакет LSAck может подтверждать несколько LSA).

4. Соседние и смежные узлы

Соседний: Когда маршрутизатор OSPF запускается, он отправляет пакет hello через интерфейс OSPF, а маршрутизатор, получивший пакет hello, проверяет параметры, содержащиеся в пакете. Если параметры двух маршрутизаторов совпадают, они становятся соседями.

Смежный: Два соседа OSPF устанавливают отношения смежности для синхронизации своих LSDB. Следовательно, любые два соседа без обмена информацией о маршруте не устанавливают смежность.

5. Типы LSA

Обмен LSA возможен только между смежными маршрутизаторами. Различные типы LSA описывают топологию сети OSPF. Все LSA сохраняются в LSDB. Информация в LSDB используется для вычисления наилучшего маршрута с помощью алгоритма SPF.

Router LSA (тип 1): создается каждым маршрутизатором в сети OSPF и рассылается по сгенерированной области. LSA описывает состояние канала и стоимость маршрутизатора.

Network LSA (тип 2): исходит от назначенного маршрутизатора (DR) и рассылается по сгенерированной области. Этот LSA содержит состояние каналов всех маршрутизаторов в сегменте сети.

Network Summary LSA (Type 3): создается Area Border Routers (ABR) и распространяется в других зонах. LSA описывает информацию о маршрутизации в зоне.

ASBR Summary LSA (Type 4): создается ABR и распространяется в смежных зонах. LSA типа 4 описывают маршруты к граничному маршрутизатору автономной системы (ASBR).

AS External LSA (Type5): исходят от ASBR и рассылаются по всей AS (кроме тупиковых областей). Каждый LSA типа 5 описывает маршрут к другой AS.

6.13.3.3 Зона и маршрутизатор

1. Разделение зон

OSPF разбивает AS на несколько зон, которые идентифицируются идентификаторами зон. Зоны классифицируют маршрутизаторы в сети по различным логическим группам, как показано на рисунке 234. Зоны обмениваются сводной информацией о маршрутизации.

Зона 0, магистральная зона, является основной зоной всей сети OSPF. Все немагистральные зоны должны быть напрямую связаны с магистральной зоной. Информация о маршрутизации немагистральных зон должна пересылаться магистральной зоной.

Чтобы уменьшить размер базы данных топологии, OSPF может разделить определенные зоны на тупиковые зоны. LSA типа 4 и типа 5 не могут входить в тупиковые зоны. Чтобы гарантировать, что маршруты к другим областям в AS или к другим AS по-прежнему доступны, ABR генерирует маршрут по умолчанию и объявляет его другим маршрутизаторам в этой зоне.

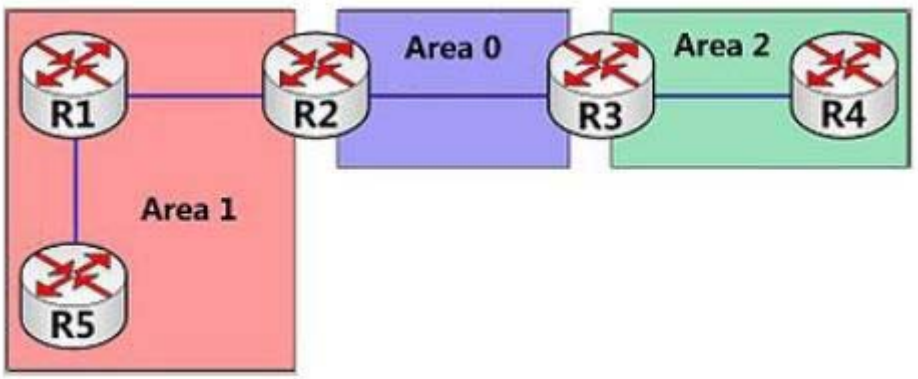


Рисунок 234 Разделение зон

Разделение области основано на интерфейсах. Следовательно, маршрутизатор с несколькими интерфейсами может принадлежать нескольким зонам, но каждый интерфейс принадлежит только одной зоне. Все маршрутизаторы в одной зоне поддерживают одну и ту же LSDB. Если маршрутизатор принадлежит нескольким зонам, он поддерживает LSDB для каждой зоны. Разделение сети имеет следующие преимущества:

- Маршрутизаторы в каждой зоне поддерживают только LSDB зоны, но не всю сеть OSPF.
- Если топология сети ограничена областью, это не влияет на всю сеть OSPF, что снижает частоту вычислений SPF.
- Ограничение передачи LSA одной зоной может уменьшить объем данных OSPF.

2. Типы маршрутизаторов

В зависимости от положения коммутатора уровня Layer-3 в AS он может выполнять роль внутреннего маршрутизатора, ABR, магистрального маршрутизатором или ASBR, как показано на рисунке 235.

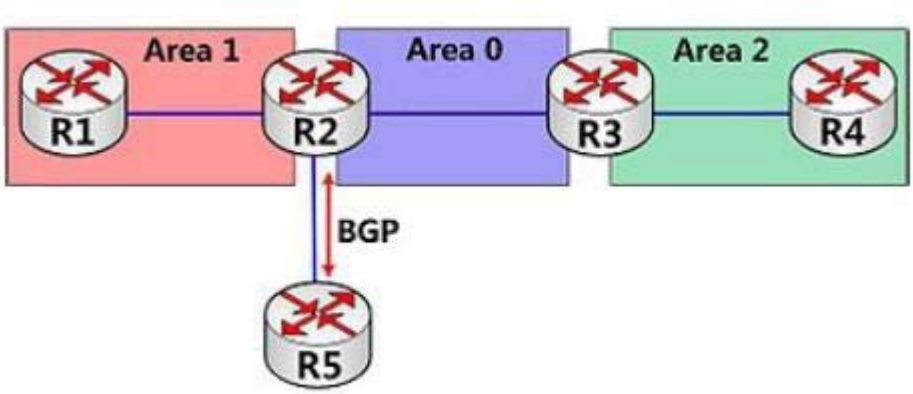


Рисунок 235 Типы маршрутизаторов OSPF

Внутренний маршрутизатор: Все интерфейсы внутреннего маршрутизатора принадлежат одной зоне OSPF. Например, R1 и R4 на рисунке 235.

ABR: ABR соединяет одну или несколько зон с магистральной зоной. В ABR хотя бы один интерфейс должен принадлежать магистральной зоне. Например, R2 и R3 на рисунке 235.

Магистральный маршрутизатор: По крайней мере, один интерфейс магистрального маршрутизатора должен находиться в магистральной зоне. Все ABR и внутренние

маршрутизаторы в зоне 0 являются магистральными маршрутизаторами. Например, R2 и R3 на рисунке 235.

ASBR: Маршрутизатор, обменивающийся информацией маршрутизации с другой AS, является ASBR. Например, R2 на рисунке 235.

Один маршрутизатор может относится к нескольким типам. Например, R2 на рисунке 235 является магистральным маршрутизатором, ABR и ASBR.

3. Виртуальный канал

Если немагистральные зоны не могут обмениваться данными с магистральной зоной из-за определенных ограничений, виртуальные каналы OSPF можно настроить для создания логических соединений между ними.

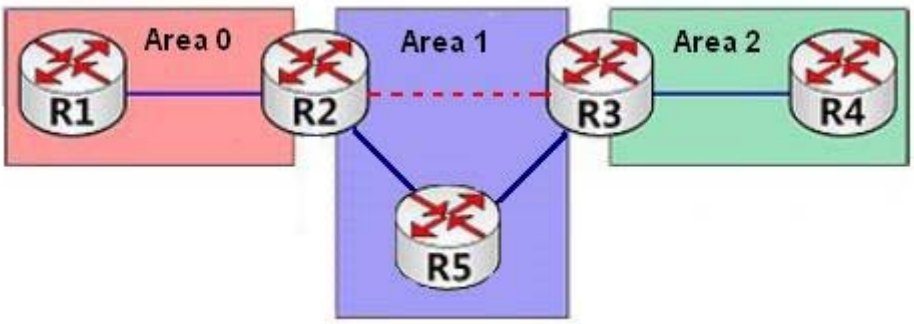


Рисунок 236 Виртуальный канал

Виртуальный канал — это логическое соединение, установленное между двумя ABR через немагистральную зону и настроенное на обоих ABR. Немагистральная зона называется транзитной зоной. Например, красная пунктирная линия на рисунке 236 — это виртуальный канал, а область 1 — транзитная зона для виртуального канала.

4. Типы маршрутов

OSPF распределяет маршруты по четырем уровням приоритета: маршруты зоны, маршруты между зонами, внешние маршруты типа 1 и внешние маршруты типа 2 в порядке убывания. Маршруты внутри и между зонами описывают топологию сети AS. Внешние маршруты описывают маршруты к внешним AS.

6.13.3.4 DR и BDR

В сетях NBMA любые два маршрутизатора обмениваются друг с другом маршрутной информацией. В результате генерируется много ненужных LSA. Для решения этой

проблемы был введен выделенный маршрутизатор (DR). Все остальные маршрутизаторы устанавливают отношения смежности и обмениваются маршрутной информацией с DR. DR извещает о состоянии каналов сети другие маршрутизаторы. Чтобы предотвратить одноточечные сбои, вызванные сбоем DR, OSPF определяет резервный выделенный маршрутизатор (BDR). BDR также устанавливают отношения смежности с другими маршрутизаторами. BDR является резервным DR. Когда DR выходит из строя, BRD становится DR. Поскольку были установлены отношения смежности с другими маршрутизаторами, сбой DR оказывает незначительное влияние на сеть.

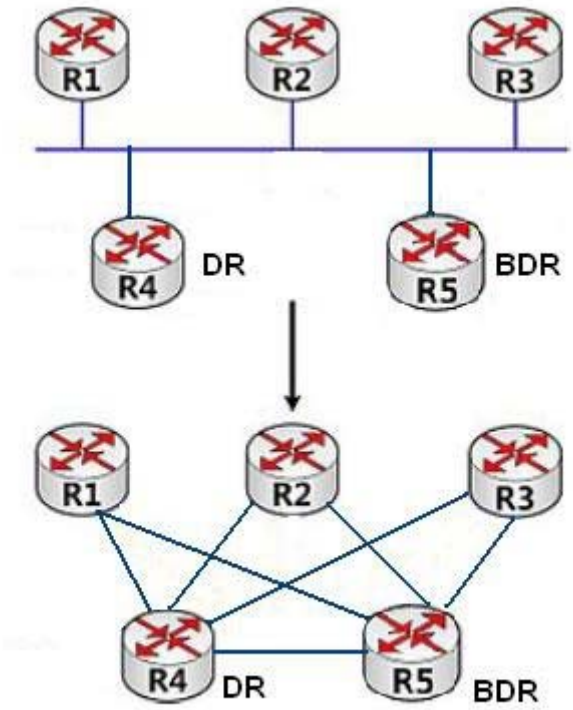


Рисунок 237 DR и DBR

Как показано на рисунке 237, на первом рисунке показаны физические соединения Ethernet, а на втором рисунке показаны установленные отношения смежности. После реализации DR/BDR для пяти маршрутизаторов требуется только семь смежных связей.

Правила выбора DR/BDR следующие:

- Маршрутизатор с приоритетом маршрутизатора 0 не может стать DR или BDR.
- Маршрутизатор с наивысшим приоритетом в сегменте сети выбирается в качестве

DR, а маршрутизатор со вторым по величине приоритетом — в качестве BDR.

- Если несколько маршрутизаторов имеют одинаковый приоритет, маршрутизатор с большим RID выбирается в качестве DR.
- Когда DR выходит из строя, BDR становится DR, а другой маршрутизатор выбирается BDR.
- Концепция DR основана на интерфейсах. Маршрутизатор может быть DR с точки зрения одного интерфейса и BDR или обычным маршрутизатором с точки зрения другого интерфейса.
- Если маршрутизатор с наивысшим приоритетом добавляется в сеть после выбора DR/BDR, маршрутизатор не заменит существующий DR или BDR, чтобы стать новым DR или BDR.

6.13.3.5 Настройка через веб-интерфейс

1. Включите OSPF.

Щелкните [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF process configuration] → [OSPF Enable/Disable], чтобы перейти на страницу включения OSPF, как показано на рисунке 238.

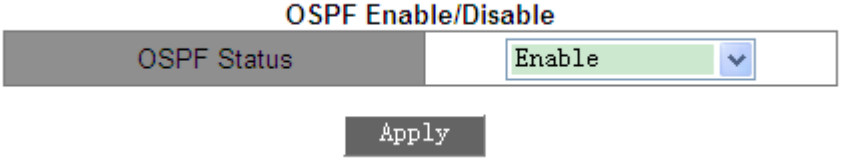


Рисунок 238 Включение OSPF

OSPF Status

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение или выключение OSPF

2. Задайте RID.

Щелкните [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF process configuration] → [Router-ID configuration], чтобы перейти на страницу настройки RID, как показано на рисунке 239.

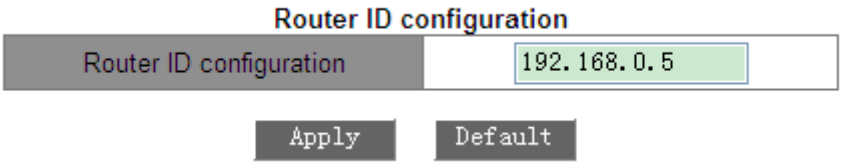


Рисунок 239 Настройка RID

Router ID configuration (IP address)

Формат: A.B.C.D

По умолчанию: основной IP-адрес интерфейса VLAN с наименьшим идентификатором на коммутаторе. Функция: Настройка RID для коммутаторов с включенным OSPF. Каждый коммутатор с OSPF имеет уникальный RID в AS.

Предупреждение:

Изменение RID вступает в силу только после повторного включения OSPF.

3. Настройте сетевой диапазон OSPF.

Щелкните [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF process configuration] → [OSPF network range configuration], чтобы перейти на страницу настройки сетевого диапазона OSPF, как показано на рисунке 240.

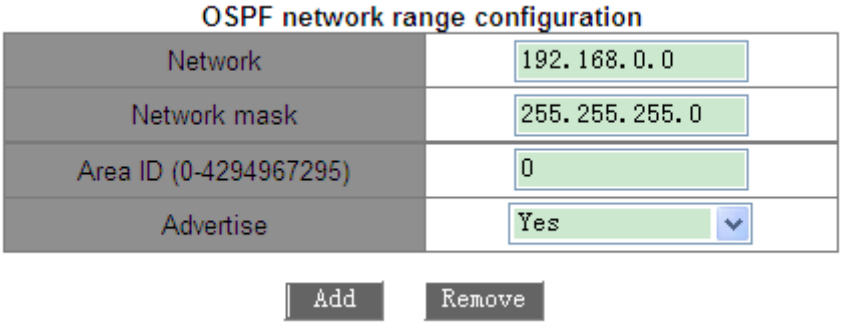


Рисунок 240 Настройка сетевого диапазона OSPF

Network

Формат: A.B.C.D

Функция: Задание IP-адреса сети.

Network mask

Функция: Задание маски подсети сети.

Описание: Маска сети и IP-адрес определяют диапазон сети.

Area ID

Диапазон: 0~4294967295

Функция: Настройка зоны для диапазона сети.

Описание: Если в зону добавляется сетевой диапазон, все внутренние маршруты сетевого диапазона не объявляются другим зонам.

Advertise

Варианты: Yes/No

По умолчанию: Yes

Функция: Объявлять/не объявлять дайджест-информацию о маршрутах в сетевом диапазоне.

1. Настройте зону для интерфейса VLAN.

Щелкните [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF process configuration] → [OSPF area configuration for port (must)], чтобы перейти на страницу настройки зоны для интерфейса VLAN, как показано на рисунке 241.

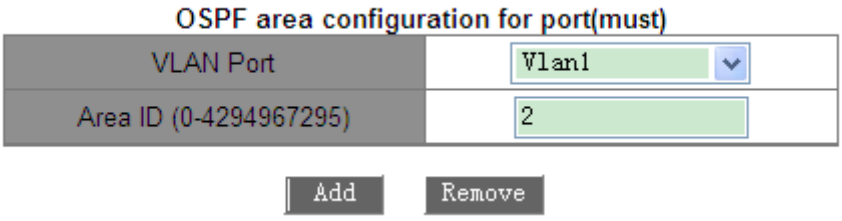


Рисунок 241 Настройка зоны для интерфейса VLAN.

Area ID

Диапазон: 0~4294967295

Функция: Настройте зону для интерфейса VLAN.

Описание: Если интерфейс VLAN добавляется в зону OSPF, OSPF включается на интерфейсе VLAN.

2. Настройте параметры аутентификации OSPF

Щелкните [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF TX-parameter configuration] → [OSPF authentication parameter configuration], чтобы перейти на страницу настройки аутентификации OSPF, как показано на рисунке 242.

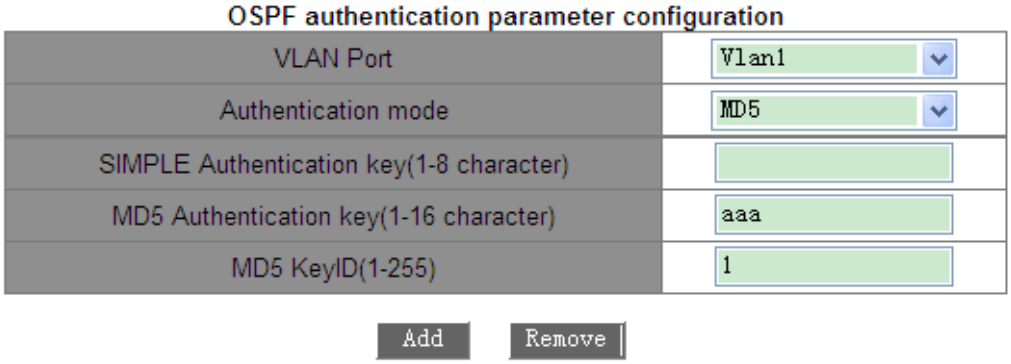


Рисунок 242 Настройка параметров аутентификации OSPF

Authentication mode

Варианты: SIMPLE/MD5

Функция: Настройте режим аутентификации для получения пакетов OSPF на указанном интерфейсе.

Описание: SIMPLE означает аутентификацию простым текстом. MD5 означает аутентификацию с шифрованием.

SIMPLE Authentication key

Диапазон: 1~8 символов

Функция: Настройка ключа для аутентификации SIMPLE.

Описание: Настройка этого параметра вступает в силу только в том случае, если в качестве режима аутентификации выбран SIMPLE.

MD5 Authentication key

Диапазон: 1~16 символов

Функция: Настройка ключа для аутентификации MD5.

Описание: Настройка этого параметра вступает в силу только в том случае, если в

качестве режима аутентификации выбран MD5.

MD5 Key ID

Диапазон: 1~255

Функция: Настройка ID ключа аутентификации MD5.

Предупреждение:

Для правильной отправки и получения OSPF идентичные параметры аутентификации должны быть настроены на обоих концах.

3. Настройте режим OSPF Rx/Tx для интерфейса VLAN.

Щелкните [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF TX-parameter configuration] → [Passive interface configuration], чтобы перейти на страницу настройки режим OSPF Rx/Tx, как показано на рисунке 243.

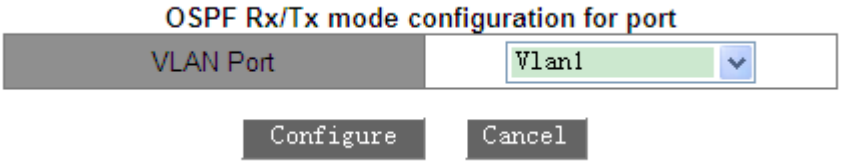


Рисунок 243 Настройка режима OSPF Rx/Tx для интерфейса VLAN

VLAN Port

Варианты: Интерфейсы VLAN, на которых должен быть включен OSPF.

Функция: Настройка указанного интерфейса VLAN только для получения (но не для отправки) пакетов OSPF.

Описание: По умолчанию все интерфейсы с поддержкой OSPF могут отправлять и получать пакеты OSPF.

4. Установите параметры таймера отправки пакетов OSPF.

Щелкните [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF TX-parameter configuration] → [OSPF packet sending timer configuration], чтобы перейти на страницу настройки параметров таймера отправки пакетов, как показано на рисунке 244.

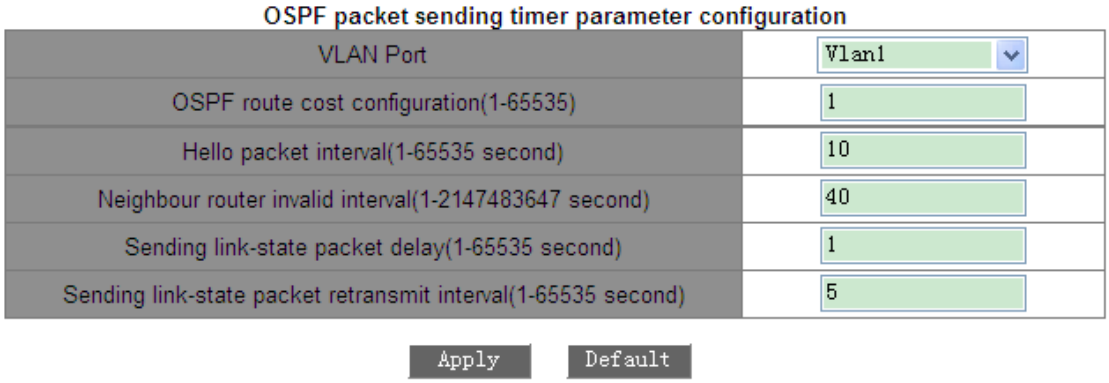


Рисунок 244 Настройка параметров таймера отправки пакетов OSPF.

OSPF route cost configuration

Диапазон: 1~65535 с

По умолчанию: 1 с

Функция: Настройка стоимости маршрута OSPF для указанного интерфейса.

Hello packet interval

Диапазон: 1~65535 с

По умолчанию: 10 с

Функция: Настройка интервала времени для отправки пакетов hello для указанного интерфейса. Описание: Коммутатор периодически отправляет пакеты hello соседним устройствам для обнаружения и поддержания отношений смежности и выбора DR и BDR.

Neighbour router invalid interval

Диапазон: 1~2147483647 с

По умолчанию: 40 с

Функция: Настройка временного интервала истечения срока действия маршрута к

смежным коммутаторам. Значение должно быть больше или равно четырехкратному интервалу пакета hello.

Описание: Если коммутатор не получает пакеты hello от смежного устройства в течение интервала, смежное устройство считается недоступным и недействительным.

Sending link-state packet delay

Диапазон: 1~65535 с

По умолчанию: 1 с

Функция: Настройка задержки отправки LSA на указанном интерфейсе.

Sending link-state packet retransmit interval

Диапазон: 1~65535 с

По умолчанию: 5 с

Функция: Задание интервала для повторной передачи LSA смежным коммутаторам на указанном интерфейсе.

Описание: После отправки LSA смежному устройству коммутатор сохраняет LSA до тех пор, пока не получит подтверждение от смежного устройства. Если коммутатор не получает подтверждение в течение интервала, он повторно передает LSA.

Предупреждение:

Для обеспечения нормальной работы OSPF параметры таймера должны быть одинаковыми между соседями OSPF.

5. Настройте параметры для импорта маршрутов OSPF.

Щелкните [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] →[Imported route parameter configuration] → [Imported route parameter configuration], чтобы перейти на страницу настройки импорта маршрутов OSPF, как показано на рисунке 245.

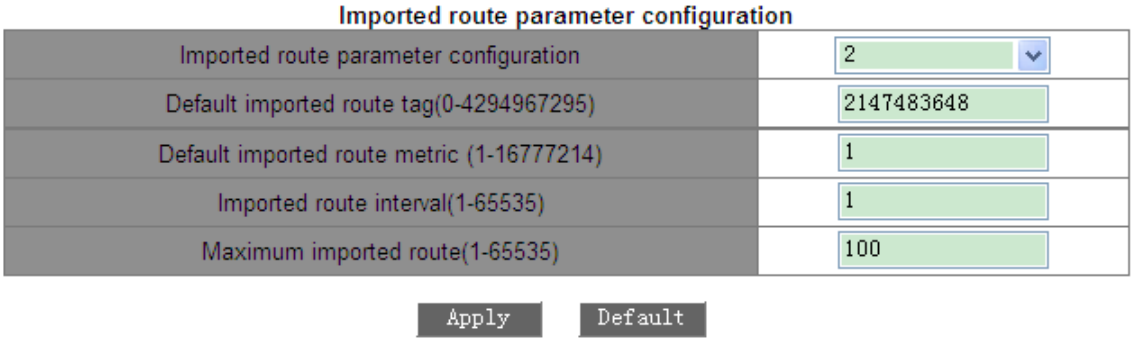


Рисунок 245 Настройка параметров импорта маршрутов OSPF.

Imported route parameter configuration

Варианты: 1/2

По умолчанию: 2

Функция: Настройка типа импортируемых маршрутов по умолчанию.

Описание: 1 указывает на внешние маршруты типа 1, а 2 указывает на внешние маршруты типа 2. Стоимость от маршрутизатора до пункта назначения внешнего маршрута типа 1 — это стоимость от маршрутизатора до соответствующего ASBR плюс стоимость от ASBR до пункта назначения внешнего маршрута. Стоимость от внутреннего маршрутизатора до пункта назначения внешнего маршрута типа 2 — это стоимость от ASBR до пункта назначения внешнего маршрута типа 2.

Default imported route tag

Диапазон: 0~4294967295

По умолчанию: 2147483648

Функция: Настройка метки импортируемых маршрутов по умолчанию.

Default imported route cost

Диапазон: 1~16777214

По умолчанию: 1

Функция: Настройка стоимости импортируемых маршрутов по умолчанию.

Imported route interval

Диапазон: 1~65535 с

По умолчанию: 1 с

Функция: Задание интервала импорта внешних маршрутов. OSPF периодически импортирует информацию о внешних маршрутах и распространяет эту информацию по всей AS.

Maximum imported route

Диапазон: 1~65535

По умолчанию: 100

Функция: Указание максимального количества маршрутов, которые могут быть импортированы OSPF за один раз.

6. Настройте импорт маршрутов других протоколов.

Щелкните [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [Imported route parameter configuration] → [Import external routing information], чтобы перейти на страницу настройки импорта внешних маршрутов, как показано на рисунке 246.

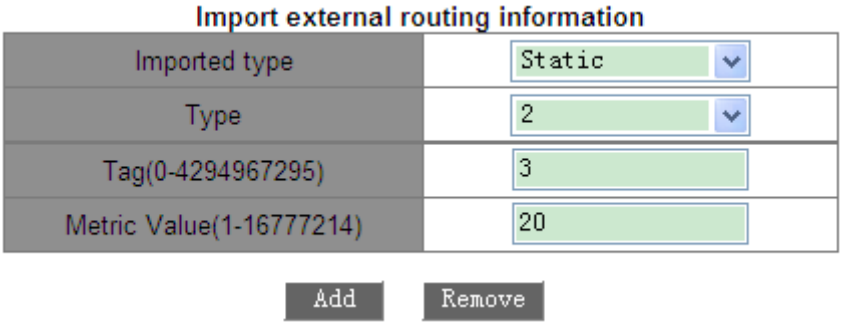


Рисунок 246 Настройка импорта маршрутов других протоколов.

Imported type

Варианты: Static/RIP/Connected/BGP

Функция: Настройка протокола маршрутизации.

Описание: Static указывает на импорт статических маршрутов; RIP указывает на импорт маршрутов RIP; Connected указывает на импорт маршрутов с прямым подключением; BGP указывает на импорт маршрутов BGP.

Type

Варианты: 1/2

Функция: Настройка типа импортируемых маршрутов.

Описание: 1 указывает на внешние маршруты типа 1, а 2 указывает на внешние маршруты типа 2.

Tag

Диапазон: 0~4294967295

Функция: Настройка метки импортируемых маршрутов.

Metric Value

Диапазон: 1~16777214

Функция: Настройте значение метрики импортированных маршрутов.

7. Установка приоритетов для протоколов маршрутизации

Щелкните[Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [Other parameter configuration] → [OSPF priority configuration], чтобы перейти на страницу настройки приоритетов для протоколов маршрутизации, как показано на рисунке 247.

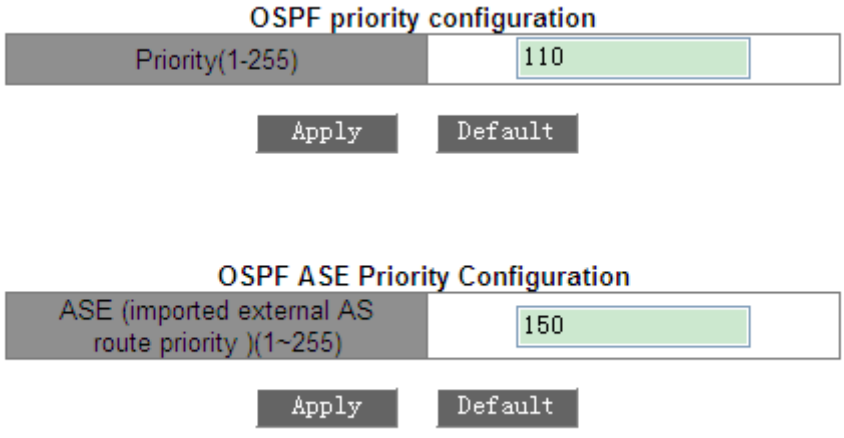


Рисунок 247 Установка приоритетов для протоколов маршрутизации

Priority

Диапазон: 1~255

По умолчанию: 110

Функция: Настройка приоритета OSPF.

ASE (imported external AS route priority)

Диапазон: 1~255

По умолчанию: 150

Функция: Настройка приоритета импортированных маршрутов.

Описание: Поскольку на коммутаторах уровня Layer-3 может быть включено несколько протоколов маршрутизации, важное значение приобретают совместное использование и выбор маршрута. Поэтому для каждого протокола маршрутизации устанавливается приоритет.

Если один и тот же маршрут обнаружен несколькими протоколами маршрутизации, допустимым является протокол с наивысшим приоритетом (наименьшее число).

8. Настройка тупиковой зоны.

Щелкните [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [Other parameter configuration] → [OSPF STUB area and default route cost], чтобы перейти на страницу настройки тупиковой зоны, как показано на рисунке 248.

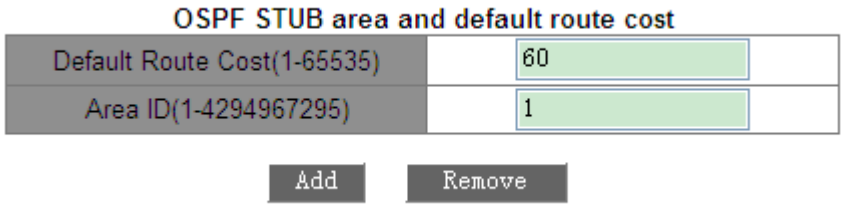


Рисунок 248 Настройка тупиковой зоны

Default Route Cost

Диапазон: 1~65535

Функция: Задание стоимости пути по умолчанию для тупиковой зоны.

Area ID

Диапазон: 1~4294967295

Функция: Настройка указанной зоны в качестве тупиковой зоны.

Предупреждение:

Магистральная зона, то есть зона 0, не может быть настроена как тупиковая зона.

9. . Настройте виртуальный канал OSPF.

Щелкните [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [Other parameter configuration] → [OSPF virtual link configuration], чтобы перейти на страницу настройки виртуального канала OSPF, как показано на рисунке 249.

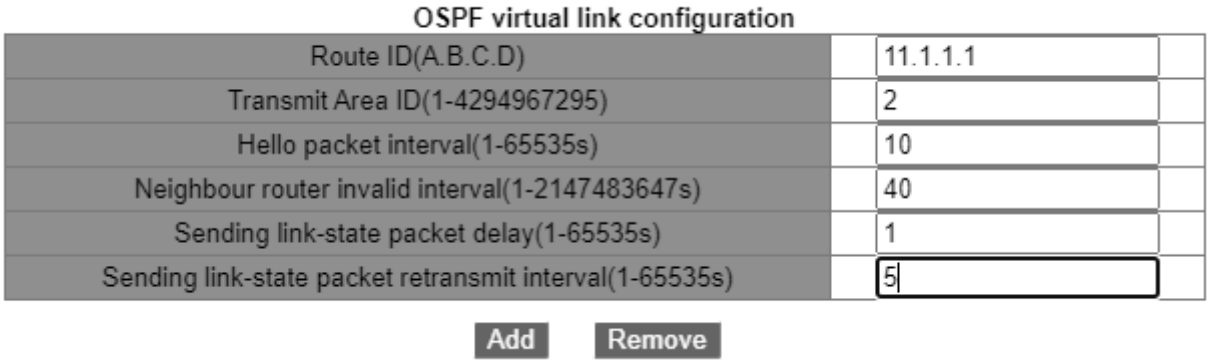


Рисунок 249 Настройка виртуальных каналов OSPF

Route ID

Формат: A.B.C.D

Функция: Задание RID для однорангового конца виртуального канала.

Transit Area ID

Диапазон: 1~4294967295

Функция: Указание транзитной зоны для виртуального канала.

Hello packet interval

Диапазон: 1~65535 с

По умолчанию: 10 с

Функция: Настройка интервала времени для отправки пакетов hello для указанного интерфейса. Описание: Коммутатор периодически отправляет пакеты hello соседним устройствам для обнаружения и поддержания отношений соседства и выбора DR и BDR.

Neighbour router invalid interval

Диапазон: 1~2147483647 с

По умолчанию: 40 с

Функция: Настройка временного интервала истечения срока действия маршрута к смежным коммутаторам. Значение должно быть больше или равно четырехкратному интервалу пакета hello.

Описание: Если коммутатор не получает пакеты hello от смежного устройства в течение интервала, смежное устройство считается недоступным и недействительным.

Sending link-state packet delay

Диапазон: 1~65535 с

По умолчанию: 1 с

Функция: Настройка задержки отправки LSA на указанном интерфейсе.

Sending link-state packet retransmit interval

Диапазон: 1~65535 с

По умолчанию: 5 с

Функция: Задание интервала для повторной передачи LSA смежным коммутаторам на указанном интерфейсе.

Описание: После отправки LSA смежному устройству коммутатор сохраняет LSA до тех пор, пока не получит подтверждение от смежного устройства. Если коммутатор не получает подтверждение в течение интервала, он повторно передает LSA.

Предупреждение:

Настройки параметров должны быть согласованы между обоими концами виртуального канала.

10. Задайте приоритет интерфейса VLAN

Щелкните [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [Other parameter configuration] → [Port DR priority configuration], чтобы перейти на страницу настройки приоритета интерфейса VLAN, как показано на рисунке 250.

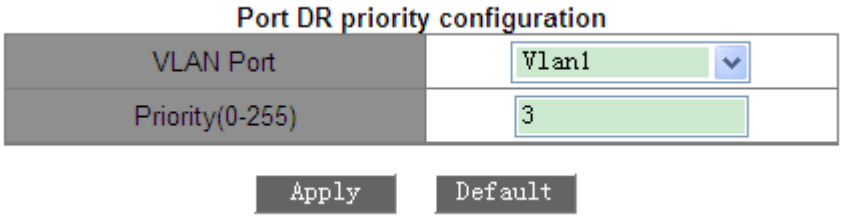


Рисунок 250 Настройка приоритета интерфейса VLAN.

Priority

Диапазон: 0~255

По умолчанию: 1

Функция: Задание приоритета интерфейса VLAN с поддержкой OSPF.

Описание: При выборе DR и BDR в качестве DR выбирается коммутатор с наибольшим значением этого параметра.

11. Просмотр информации OSPF.

Щелкните [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF process configuration] → [OSPF Enable/Disable], чтобы перейти на страницу информации OSPF, как показано на рисунке 251.

OSPF information

my router ID	192.168.0.22
preference	110
ase preference	150
export metric	1
export tag	2147483648

Рисунок 251 Информация OSPF

12. Просмотрите информацию внешних маршрутов OSPF.

Щелкните [Device Advanced Configuration] → [Route configuration] → [OSPF

configuration] → [OSPF debug] → [show ip ospf ase], чтобы перейти на страницу информации внешних маршрутов OSPF, как показано на рисунке 252.

OSPF Imported External AS Route Information

Destination	AdvRouter	NextHop	Age	SeqNumber	Type	Cost
7.7.7.0	2.2.2.2	2.2.2.3	1145	-2147483506	DTYPE_ASBR	1

Рисунок 252 Информация внешних маршрутов

13. Просмотрите статистику OSPF.

Щелкните [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF debug] → [show ip ospf cumulative], чтобы перейти на страницу статистики OSPF, как показано на рисунке 253.

OSPF Cumulative information

Type	In	Out
HELLO	23674	23823
DD	19	22
LS Req	8	6
LS Update	1394	548
LS Ack	406	970
ASE count	1	checksum 7938

Рисунок 253 Статистика OSPF

14. Просмотрите информацию базы данных OSPF

Щелкните [[Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF debug] → [show ip ospf database], чтобы перейти на страницу информации базы данных OSPF, как показано на рисунке 254.

OSPF database information

AREA 0

Router LSAs						
LS ID(Router ID)	ADV rtr	Age	Sequence	Cost	Checksum	
2.2.2.2	2.2.2.2	331	0x800001ea	1	49246	Type : Transit net / Cost : 1 / DR : 2.2.2.2 / Address: 2.2.2.2 Type : Virtual link / Cost : 1 / RouterID : 3.3.3.3 / Address: 3.3.3.1
1.1.1.1	1.1.1.1	340	0x80000228	0	59435	Type : Transit net / Cost : 1 / DR : 2.2.2.2 / Address: 2.2.2.1
3.3.3.3	3.3.3.3	330	0x80000231	2	36454	Type : Virtual link / Cost : 1 / RouterID : 2.2.2.2 / Address: 3.3.3.2

Network LSAs					
LS ID(DR's IP)	ADV rtr	Age	Sequence	Cost	Checksum
2.2.2.2	2.2.2.2	336	0x800000c0	1	64898

Summary Network LSAs					
LS ID(Net's IP)	ADV rtr	Age	Sequence	Cost	Checksum
20.1.1.0	1.1.1.1	521	0x80000178	65535	26468
5.5.5.0	3.3.3.3	333	0x80000006	4	33976
4.4.4.255	3.3.3.3	416	0x8000021e	3	26814
3.3.3.0	3.3.3.3	333	0x80000119	3	39318
3.3.3.0	2.2.2.2	336	0x800001ef	2	2643

ASBR Summary LSAs					
LS ID(Net's IP)	ADV rtr	Age	Sequence	Cost	Checksum

AREA 4

Router LSAs						
LS ID(Router ID)	ADV rtr	Age	Sequence	Cost	Checksum	
1.1.1.1	1.1.1.1	746	0x8000010e	0	13044	Type : Stub net / Cost : 1 / Network : 20.1.1.0 / NetMask: 255.255.255.0

Network LSAs					
LS ID(Router ID)	ADV rtr	Age	Sequence	Cost	Checksum

Summary Network LSAs					
LS ID(Net's IP)	ADV rtr	Age	Sequence	Cost	Checksum
5.5.5.0	1.1.1.1	319	0x80000001	65535	56937
2.2.2.255	1.1.1.1	319	0x80000007	65535	8493
4.4.4.255	1.1.1.1	319	0x80000001	65535	63571
3.3.3.0	1.1.1.1	319	0x80000003	65535	3903

ASBR Summary LSAs					
LS ID(ASBR's Rtr ID)	ADV rtr	Age	Sequence	Cost	Checksum
2.2.2.2	1.1.1.1	335	0x80000001	65535	2886

AS External LSAs									
LS ID(ASBR's Rtr ID)	ADV rtr	Age	Sequence	Cost	Checksum	ls_type	metric	ase_type	forward	tag

Рисунок 254 Информация базы данных OSPF

15. Просмотрите информацию о соседях OSPF.

Щелкните [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF debug] → [show ip ospf neighbor], чтобы перейти на страницу информации о соседях OSPF, как показано на рисунке 255.

OSPF Neighbor

interface p :20.1.1.1						
neighbor: area	router id	router IP	state	priority	DR	BDR
interface ip :2.2.2.1						
neighbor: area	router id	router IP	state	priority	DR	BDR
0	2.2.2.2	2.2.2.2	NFULL	1	2.2.2.2	2.2.2.1

Рисунок 255 Информация о соседях OSPF

16. Просмотрите информацию о маршрутизации OSPF.

Щелкните [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF debug] → [show ip ospf routing], чтобы перейти на страницу информации о маршрутизации OSPF, как показано на рисунке 256.

OSPF routes information

AS internal routes

Destination	Area	Cost	Dest Type	Next Hop	ADV rtr
20.1.1.0	4	1	DTYPE_NET	20.1.1.1	1.1.1.1
2.2.2.0	0	1	DTYPE_NET	2.2.2.1	2.2.2.2
3.3.3.0	0	2	DTYPE_NET	2.2.2.2	2.2.2.2
5.5.5.0	0	4	DTYPE_NET	2.2.2.2	3.3.3.3
4.4.4.0	0	3	DTYPE_NET	2.2.2.2	3.3.3.3

AS external routes

Destination	AdvRouter	NextHop	Age	SeqNumber	Dest Type	Cost
7.7.7.0	2.2.2.2	2.2.2.3	1245	0x8000008e	DTYPE_ASBR	1

Рисунок 256 Информация о маршрутизации OSPF

17. Просмотрите записи маршрутов.

Щелкните [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [show ip route], чтобы перейти на страницу информации о маршрутизации, как показано на рисунке 257.

Information Display

```
Total route items is 6, the matched route items is 6
Codes: C - connected, S - static, R - RIP derived, O - OSPF derived
       A - OSPF ASE, B - BGP derived, D - DVMRP derived

   Destination      Mask            Nexthop         Interface       Preference
C    2.2.2.0          255.255.255.0     0.0.0.0         Vlan2           0
O    3.3.3.0          255.255.255.0     2.2.2.2         Vlan2           110
O    4.4.4.0          255.255.255.0     2.2.2.2         Vlan2           110
O    5.5.5.0          255.255.255.0     2.2.2.2         Vlan2           110
A    7.7.7.0          255.255.255.0     2.2.2.3         Vlan2           200
C    20.1.1.0         255.255.255.0     0.0.0.0         Vlan1           0
```

Рисунок 257 Таблица маршрутизации

6.13.3.6 Типовой пример конфигурации

Требуется включить OSPF на всех коммутаторах и разделить всю AS на три зоны. Зона 2 не связана напрямую с Зоной 0. Требуется виртуальный канал между R2 и R3. В качестве транзитной зоны Зона 1 соединяет Зону 2 с Зоной 0. R2 и R3 служат ABR для пересылки информации о маршрутах между зонами.

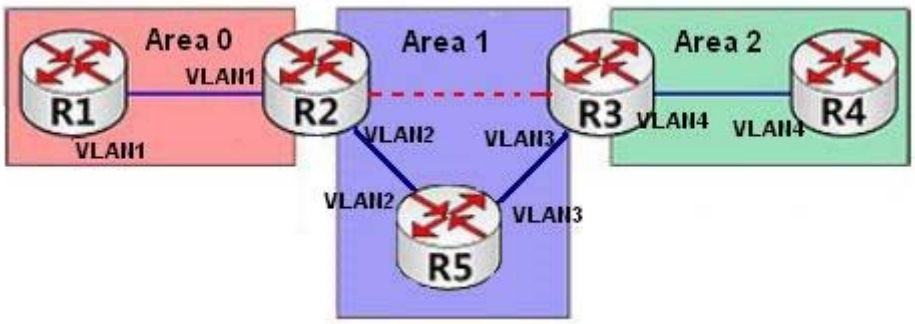


Рисунок 258 Пример типовой конфигурации OSPF

Настройка R1:

1. Установите IP-адрес интерфейса VLAN1 192.168.1.1 и маску подсети 255.255.255.0.

2. Задайте RID 192.168.1.1, как показано на рисунке 239.

3. Включите OSPF, как показано на рисунке 238.

4. Настройте диапазон сети. Установите IP-адрес сети 192.168.1.0, маску сети 255.255.255.0, Area ID 0 и значение параметра Advertise – Yes, как показано на

рисунке 240.

5. Добавьте интерфейс VLAN1 в зону 0, как показано на рисунке 241.

Настройка R2:

1. Установите IP-адрес интерфейса VLAN1 192.168.1.2 и маску подсети 255.255.255.0, а IP-адрес интерфейса VLAN2 192.168.2.1 и маску подсети 255.255.255.0.

2. Задайте RID 192.168.1.2, как показано на рисунке 239.

3. Включите OSPF, как показано на рисунке 238.

4. Настройте диапазон сети. Установите IP-адрес сети 192.168.1.0, маску сети 255.255.255.0, Area ID 0 и значение параметра Advertise – Yes. Установите IP-адрес сети 192.168.2.0, маску сети 255.255.255.0, Area ID 1 и значение параметра Advertise – Yes, как показано на рисунке 240.

5. Добавьте интерфейс VLAN2 в зону 0 и VLAN1 в зону 1, как показано на рисунке 241.

6. Настройте виртуальный канал. Установите идентификатор коммутатора уровня Layer-3 192.168.3.2, идентификатор транзитной зоны Transit Area ID 1, а также установите настройки по умолчанию для других параметров, как показано на рисунке 249.

Настройка R3:

1. Установите IP-адрес интерфейса VLAN3 192.168.3.2 и маску подсети 255.255.255.0, а IP-адрес интерфейса VLAN4 192.168.4.1 и маску подсети 255.255.255.0.

2. Задайте RID 192.168.3.2, как показано на рисунке 239.

3. Включите OSPF, как показано на рисунке 238.

4. Настройте диапазон сети. Установите IP-адрес сети 192.168.3.0, маску сети 255.255.255.0, Area ID 1 и значение параметра Advertise – Yes. Установите IP-адрес сети 192.168.4.0, маску сети 255.255.255.0, Area ID 2 и значение параметра Advertise – Yes, как показано на рисунке 240.

4. Добавьте интерфейс VLAN4 в зону 1 и VLAN3 в зону 2, как показано на рисунке 241.

5. Настройте виртуальный канал. Установите идентификатор коммутатора уровня Layer-3 192.168.1.2, идентификатор транзитной зоны Transit Area ID 1, а также установите настройки по умолчанию для других параметров, как показано на рисунке 249.

Настройка R4:

1. Установите IP-адрес интерфейса VLAN4 192.168.4.2 и маску подсети 255.255.255.0.
2. Задайте RID 192.168.4.2, как показано на рисунке 239.
3. Включите OSPF, как показано на рисунке 238.
4. Настройте диапазон сети. Установите IP-адрес сети 192.168.4.0, маску сети 255.255.255.0, Area ID 2 и значение параметра Advertise – Yes, как показано на рисунке 240.
5. Добавьте интерфейс VLAN4 в зону 2, как показано на рисунке 241.

Настройка R5:

1. Установите IP-адрес интерфейса VLAN2 192.168.2.2 и маску подсети 255.255.255.0, а IP-адрес интерфейса VLAN3 192.168.3.1 и маску подсети 255.255.255.0.
2. Задайте RID 192.168.2.2, как показано на рисунке 239.
3. Включите OSPF, как показано на рисунке 238.
4. Настройте диапазон сети. Установите IP-адрес сети 192.168.2.0, маску сети 255.255.255.0, Area ID 1 и значение параметра Advertise – Yes. Установите IP-адрес сети 192.168.3.0, маску сети 255.255.255.0, Area ID 1 и значение параметра Advertise – Yes, как показано на рисунке 240.
5. Добавьте интерфейс VLAN2 в зону 1 и VLAN3 в зону 1, как показано на рисунке 241.

6.14 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 259.

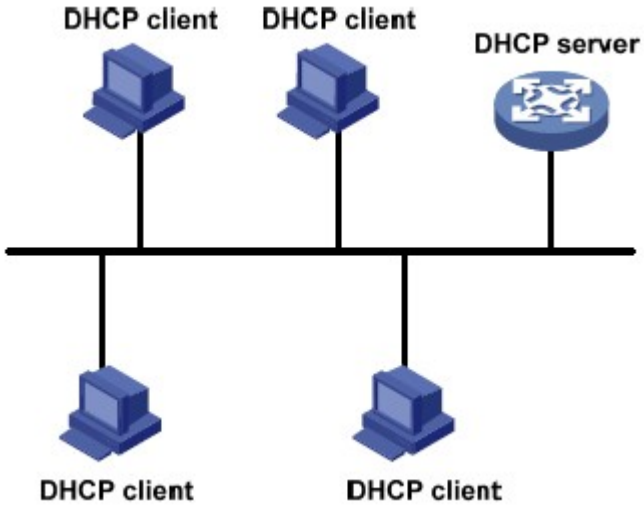


Рисунок 259 Типичное использование DHCP

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. 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.

6.14.1 Настройка сервера DHCP

6.14.1.1 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.

6.14.1.2 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.

6.14.1.3 Настройка через веб-интерфейс

1. Запустите сервер DHCP.

Щелкните [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Enable DHCP], чтобы запустить сервер DHCP, как показано на рисунке 260.

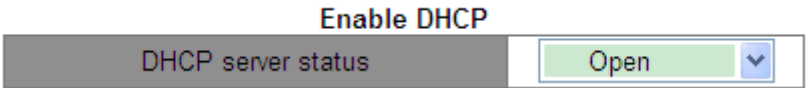


Рисунок 260 Запуск сервера DHCP

DHCP server status

Варианты: Open/Close

По умолчанию: Close

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

2. Статически выделите IP-адрес

Щелкните [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Address pool configuration], чтобы создать пул адресов DHCP, как показано на рисунке 261.

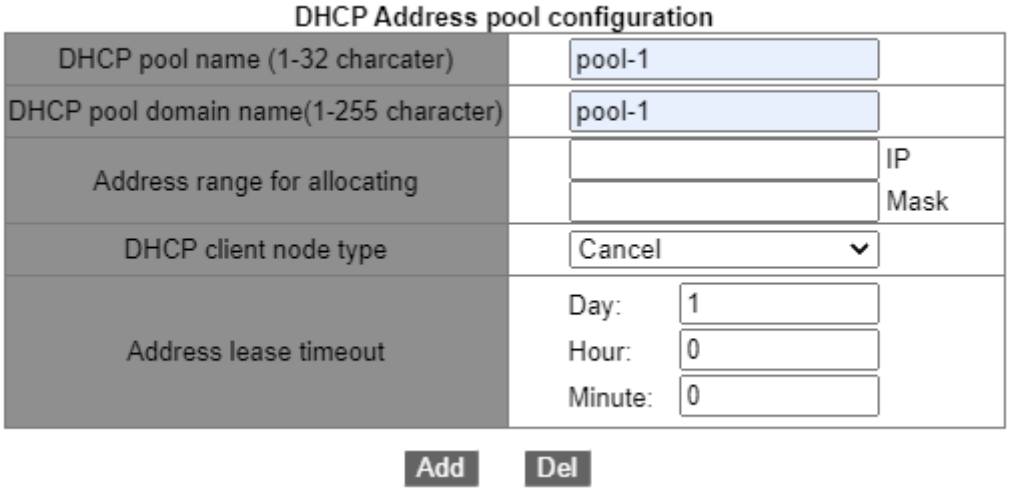


Рисунок 261 Создание пула адресов

DHCP pool name

Диапазон: 1~32 символа

Функция: задание имени пула IP-адресов.

DHCP pool domain name

Диапазон: 1~255 символов

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

Address lease timeout

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

Описание: Срок аренды статического адреса бесконечен. Настройка этого параметра недопустима для статического распределения.

Примечание:

- Статическое выделение IP-адреса можно рассматривать как получение IP-адреса из специального пула адресов, который содержит только один конкретный IP-адрес. Следовательно, пул адресов DHCP должен быть создан до статического выделения IP-адреса.
- Для каждого пула адресов DHCP можно настроить только один тип механизма распределения IP-адресов.

Щелкните [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Manual address pool configuration], чтобы перейти на страницу настройки статического распределения, как показано на рисунке 262.

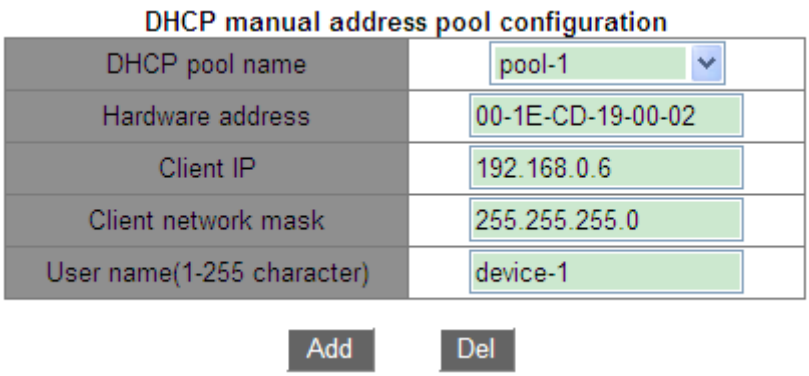


Рисунок 262 Выделение статического IP-адреса

DHCP pool name

Функция: Выбор созданного имени пула.

Hardware Address

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

Функция: настройка MAC-адреса клиента со статической

привязкой. **Client IP**

Формат: A.B.C.D

Функция: настройка IP-адреса клиента со статической привязкой.

Описание: 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.

Client network mask

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.

User Name

Диапазон: 1~255 символов

Функция: Настройка имени пользователя клиента.

3. Динамические IP-адреса

Щелкните [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Address pool configuration], чтобы перейти на страницу настройки динамического распределения, как показано на рисунке 263.

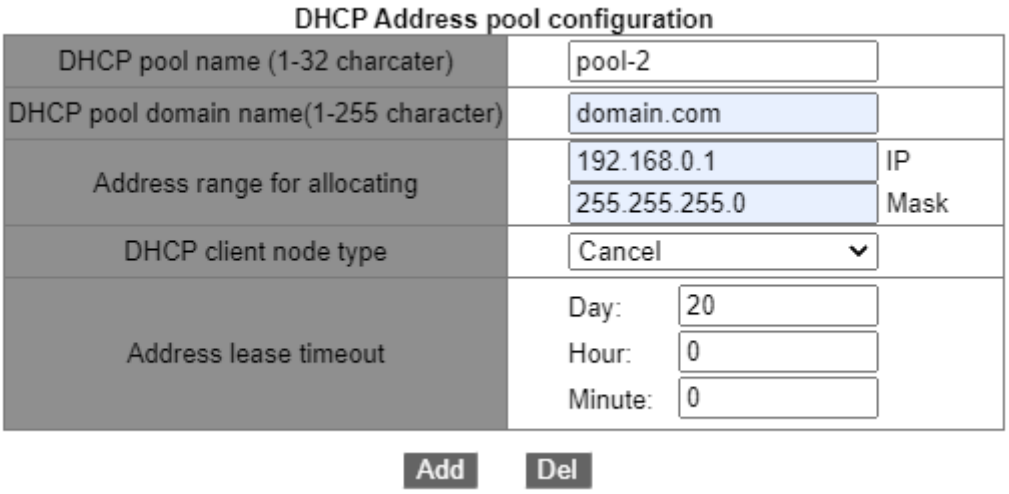


Рисунок 263 Динамические IP-адреса

DHCP pool name

Диапазон: 1~32 символа

Функция: задание имени пула IP-адресов.

DHCP pool domain name

Диапазон: 1~255 символов

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

Address range of allocating {IP · MASK}

Функция: Настройка диапазона 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.

Примечание:

В каждом пуле адресов можно настроить только один сегмент адресов.

DHCP client node type

Варианты: Cancel/Broadcast node/Peer-to-peer node/Mixed node/Hybrid node

По умолчанию: Cancel

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: Широковещательный узел получает сопоставление в широковещательном режиме. Одноранговый узел получает сопоставление путем отправки одноадресного пакета для связи с WINS-сервером. Смешанный узел получает сопоставление, отправив широковещательный пакет в первый раз. Если смешанный узел не может получить сопоставление в первый раз, он получает сопоставление, отправив одноадресный пакет для связи с WINS-сервером во второй раз. Гибридный узел получает сопоставление, отправляя одноадресный пакет для связи с WINS-сервером в первый раз. Если гибридный узел не может получить сопоставление в первый раз, он получает сопоставление, отправив широковещательный пакет во второй раз.

Address lease timeout

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

4. Настройте шлюз клиента DHCP

Щелкните [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Default Gateway Configuration], чтобы перейти на страницу настройки шлюза клиента DHCP, как показано на рисунке 264.

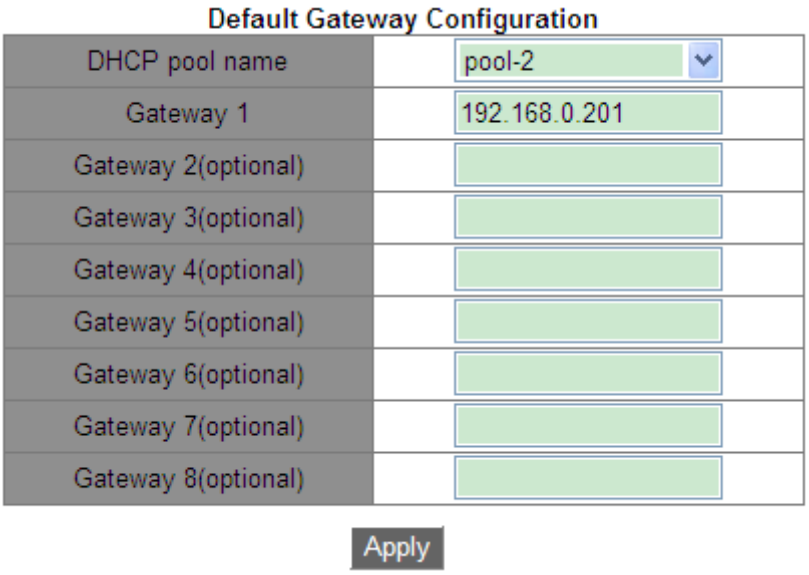


Рисунок 264 Настройка шлюза клиента DHCP

DHCP pool name

Функция: Выбор созданного имени пула.

Gateway 1~Gateway 8

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 8 шлюзов. Шлюз 1 имеет высший приоритет, а шлюз 8 — низший.

5. Настройте сервер DNS клиента DHCP

Щелкните [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Client DNS server configuration], чтобы перейти на страницу настройки сервера DNS клиента DHCP, как показано на рисунке 265.

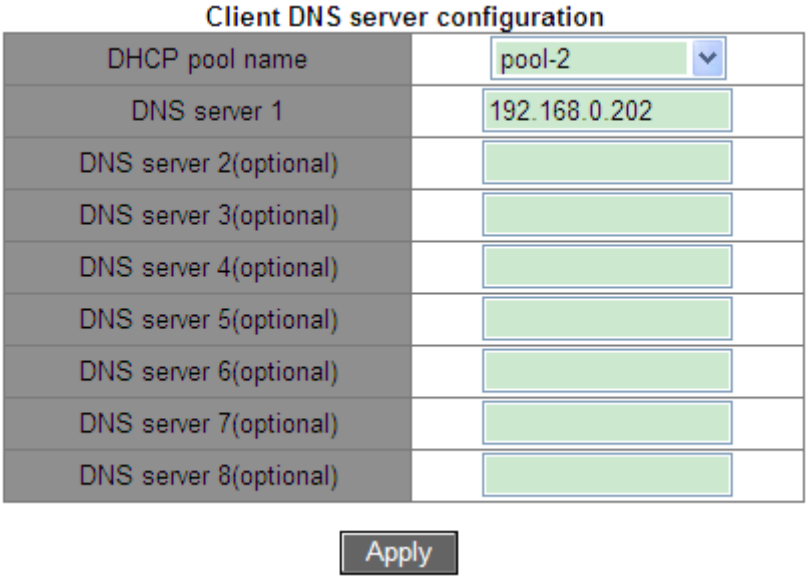


Рисунок 265 Настройка сервера DNS клиента DHCP

DHCP pool name

Функция: Выбор созданного имени пула.

DNS server 1~DNS server 8

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 8 серверов DNS. Сервер DNS 1 имеет высший приоритет, а сервер DNS 8 — низший.

6. Настройте сервер WINS клиента DHCP

Щелкните [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Client WINS server configuration], чтобы перейти на страницу настройки сервера WINS клиента DHCP, как показано на рисунке 266.

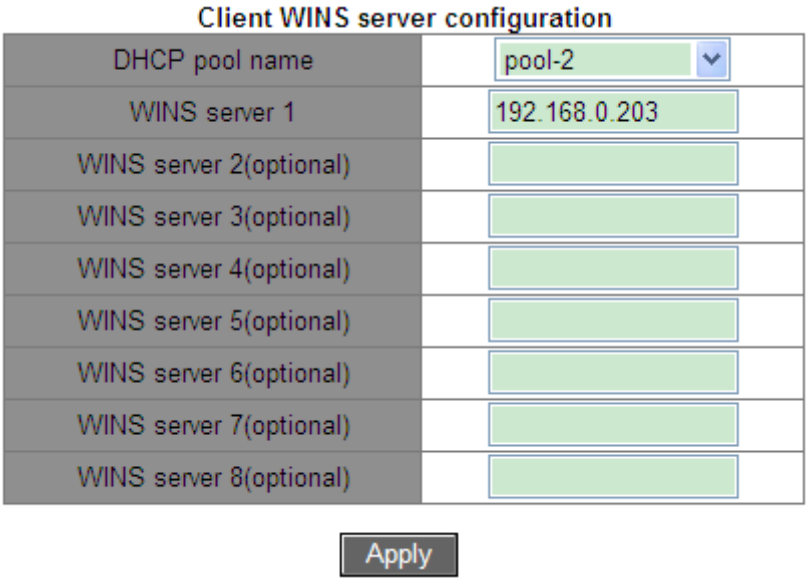


Рисунок 266Настройка сервера WINS клиента DHCP

DHCP pool name

Функция: Выбор имени созданного пула.

WINS сервер 1~WINS сервер 8

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 8 серверов WINS. Сервер WINS 1 имеет высший приоритет, а сервер WINS 8 — низший.

7. Настройте адрес TFTP-сервера клиента DHCP и имя загрузочного файла.

Щелкните [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [DHCP file server address configuration], чтобы перейти на страницу настройки адреса TFTP-сервера клиента DHCP и имени загрузочного файла, как показано на рисунке 267.

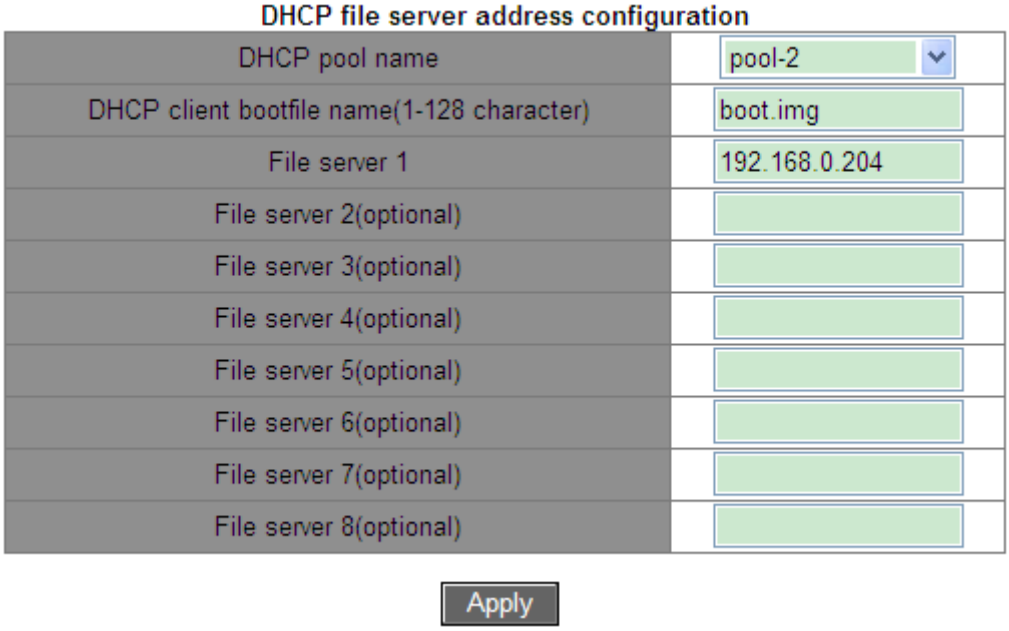


Рисунок 267 Настройка адреса TFTP-сервера клиента DHCP и имени загрузочного файла

DHCP pool name

Функция: Выбор имени созданного пула.

DHCP client bootfile name

Диапазон: 1~128 символов

Функция: Настройка имени файла запуска клиента, выделенного DHCP-сервером. При запуске бездискового устройства загрузочный файл необходимо загрузить с сервера, а затем импортировать.

File сервер 1~File сервер 8

Функция: Настройка адреса сервера TFTP клиента, выделенного DHCP-сервером. Для пула адресов DHCP можно настроить не более 8 файл-серверов. Файл-сервер 1 имеет высший приоритет, а файл-сервер WINS 8 — низший.

8. Настройте сетевой параметр DHCP

Щелкните [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [DHCP network parameter configuration], чтобы перейти на страницу настройки сетевого параметра DHCP, как показано на рисунке 268.

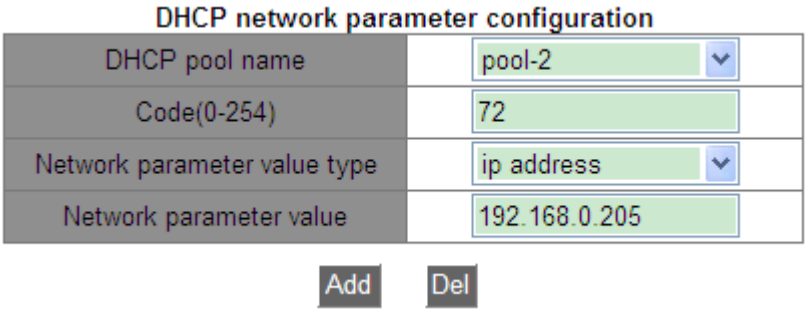


Рисунок 268 Настройка сетевого параметра DHCP

DHCP pool name

Функция: Выбор имени созданного пула.

Code

Диапазон: 0~254

Функция: Настройка параметра DHCP. DHCP сохраняет формат сообщения BootP для совместимости с BootP. Недавно добавленная функция BootP реализуется через поле **Option**. DHCP передает управляющую информацию и параметры конфигурации сети через поле **Option**, реализуя распределение IP-адресов и предоставляя клиенту более подробную информацию о конфигурации. Например, Option72 — это параметр WWW-сервера, который используется для указания адреса WWW-сервера, выделяемого клиенту.

Примечание:

- Дополнительные сведения об опциях DHCP см. в документе RFC2132.
- Веб-страница обеспечивает настройку общих параметров (например, адрес шлюза, адрес DNS-сервера и адрес WINS-сервера). Коды сетевых параметров не могут быть сконфигурированы как эти общие параметры.

Network parameter value type

Варианты: ascii/hex/ip address

Функция: Настройка типа значения сетевого параметра. ascii — это строка символов ascii, и ее диапазон настройки составляет от 1 до 255 символов. Hex — это шестнадцатеричное число, и длина его настройки должна быть четным числом в диапазоне от 1 до 510.

Network parameter value

Функция: Настройка соответствующего значения сетевого параметра на основе типа значения сетевого параметра.

9. Запрос конфигурации пула адресов DHCP

Щелкните [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Query DHCP address pool information], чтобы запросить конфигурацию пула адресов DHCP, как показано на рисунке 269.

DHCP Adress Pool Information

DHCP pool name	pool-2
DHCP pool domain name	domain.com
Address range for allocating	IP: 192.168.0.0 Mask: 255.255.255.0
DHCP client node type	
Address lease timeout	day: 20 hour: 0 minute:0 (0 day 0 hour 0 minute :valid forever)

Рисунок 269 Запрос конфигурации пула адресов DHCP

DHCP pool name

Функция: Выбор имени созданного пула.

10. . Настройка диапазона IP-адресов, которые не выделяются динамически в пуле адресов DHCP.

Щелкните [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Excluded address configuration], чтобы перейти на страницу настройки исключенных адресов, как показано на рисунке 270.

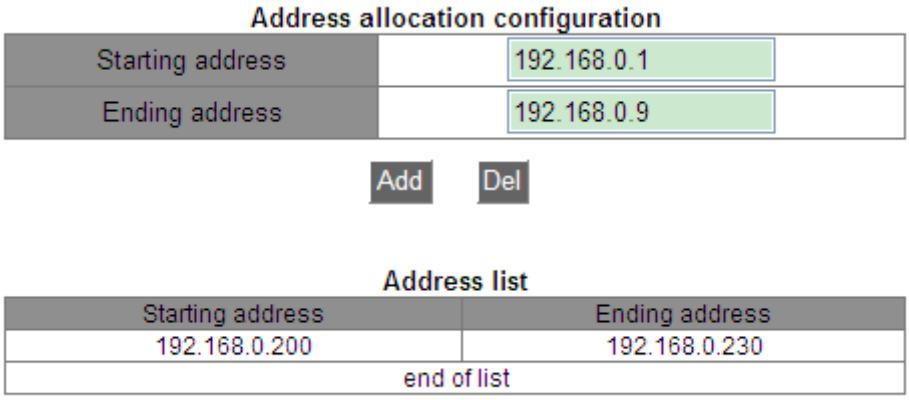


Рисунок 270 Настройка диапазона IP-адресов, которые не выделяются динамически в пуле адресов DHCP.

Start IP Address/End IP Address

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.

11. Просмотр статистики пакетов DHCP

Щелкните [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [DHCP packet statistics], чтобы просмотреть статистику пакетов DHCP, как показано на рисунке 271.

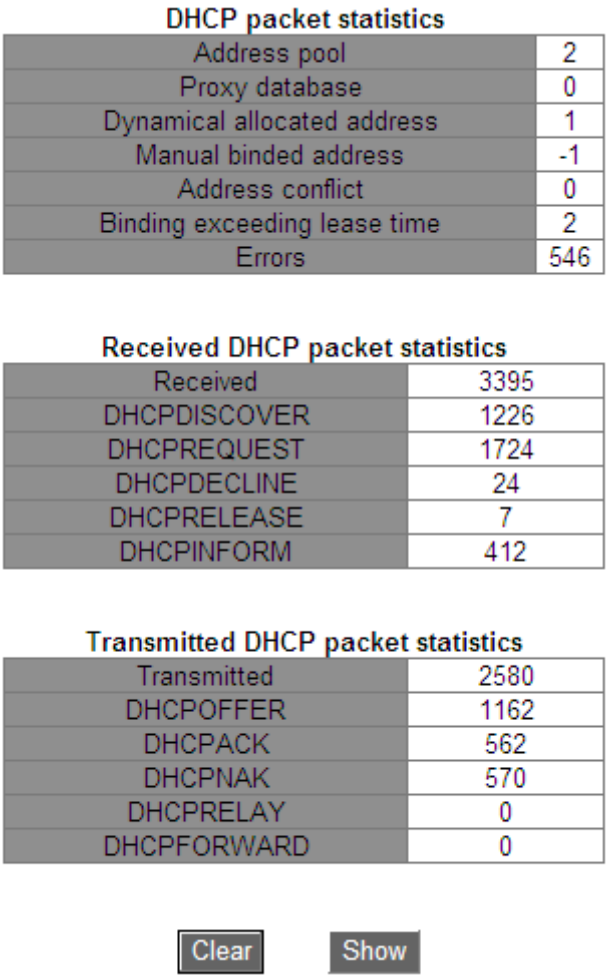


Рисунок 271 Просмотр статистики пакетов DHCP

Можно щелкнуть кнопку <Show>, чтобы обновить статистику пакетов данных DHCP в режиме реального времени, и кнопку <Clear>, чтобы очистить статистику полученных/отправленных пакетов данных DHCP.

12. Показ информации связывания IP-MAC

Щелкните [Device Advanced Configuration] → [DHCP configuration] → [DHCP debugging] → [Show IP-MAC binding], чтобы показать информацию связывания IP-MAC, как показано на рисунке 272.

Information Display

```
IP address          Hardware adress          Lease expiration
Type
192.168.0.23        44-37-E6-88-6E-90        Infinite
Manual
192.168.0.6         00-1E-CD-19-00-02        Infinite
Manual
Total dhcp binding items: 2, the matched: 2
```

Рисунок 272 Показ информации связывания IP-MAC

6.14.1.4 Типовой пример конфигурации

Как показано на рисунке 273, 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 192.168.0.1~192.168.0.9.

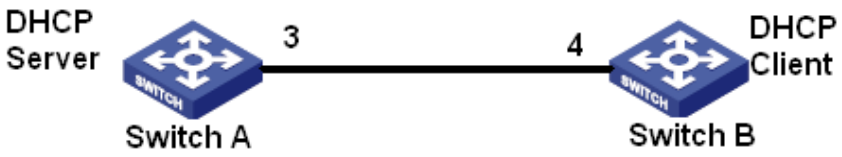


Рисунок 273 Пример типовой конфигурации DHCP

Статические IP-адреса

➢ Конфигурация коммутатора A:

1. Установите статус сервера DHCP в состояние Enable, как показано на рисунке 260.

2. Создайте IP-пул DHCP: pool-1, как показано на рисунке 261.

3. Привяжите MAC-адрес коммутатора B: 00-1e-cd-19-00-02 к IP-адресу: 192.168.0.6, задайте маску 255.255.255.0, как показано на рисунке 135.

➢ Конфигурация коммутатора B:

1. Выберите режим получения IP-адреса bootp-client или dhcp-client, как показано на рисунке 136.

2. Коммутатор B получает IP-адрес 192.168.0.6 и маску подсети 255.255.255.0 от DHCP-сервера, как показано на рисунке 274.

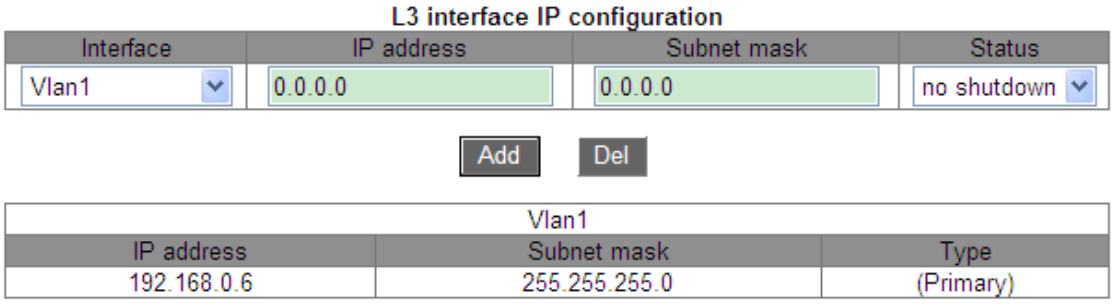


Рисунок 274 Клиент DHCP получает IP-адрес-1

Динамические IP-адреса

➢ Конфигурация коммутатора A:

1. Установите статус сервера DHCP в состояние Enable, как показано на рисунке 260.

2. Создайте пул IP-адресов DHCP: pool-2, установите доменное имя domain.com, диапазон адресов для выделения 192.168.0.3 (IP) и 255.255.255.0 (MASK) и время аренды до 20 дней., как показано на рисунке 263.

3. Настройте диапазон исключенных IP-адресов 192.168.0.1~192.168.0.9., как показано на рисунке 270.

➢ Конфигурация коммутатора B:

1. Выберите режим получения IP-адреса bootp-client или dhcp-client, как показано на рисунке 136.

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 275.

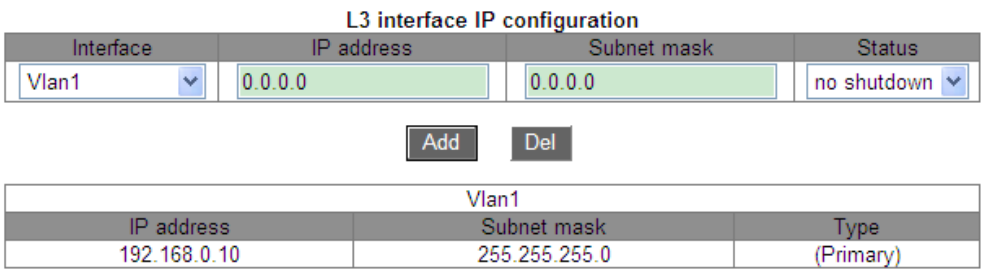


Рисунок 275 Клиент DHCP получает IP-адрес-2

6.15 Настройка ACL

6.15.1 Введение

Список управления доступом (ACL) позволяет пользователям настраивать правила сопоставления и режим обработки для пакетов во входящем направлении порта коммутатора для фильтрации пакетов. Он нацелен на эффективное предотвращение доступа неавторизованных пользователей к сети, контроль трафика и экономию сетевых ресурсов.

6.15.2 Записи и правила ACL

Запись ACL может содержать несколько правил, и в каждом правиле можно указать параметры сопоставления пакетов и обработки пакетов. Запись ACL необходимо создать до настройки правила. В нескольких правилах в одной записи ACL правило с меньшим идентификатором правила предшествует правилу с большим идентификатором правила. Входящий пакет сравнивается с записями ACL в порядке возрастания идентификаторов содержащихся в записи правил. Как только совпадение найдено, дальнейшее сравнение не проводится.

Записи ACL могут применяться к портам, VLAN и глобально. Когда несколько записей конфликтуют друг с другом, ACL, примененный к порту, имеет наивысший приоритет, тогда как ACL, примененный глобально, имеет самый низкий приоритет. Например, ACL1 (пакеты с IP-адресом назначения 192.168.0.3 будут отбрасываться) настроен на глобальное применение, ACL2 (пакеты с IP-адресом назначения 192.168.0.3 будут получены) настроен на применение к VLAN1, и ACL3 (пакеты с IP-адресом назначения 192.168.0.3 будут зеркалироваться) настроен для применения к порту 2/1. Порт 2/1 принадлежит VLAN1. ACL, применяемый к порту, предшествует ACL, применяемому к VLAN. Поэтому порт 2/1 зеркалирует пакеты с IP-адресом назначения 192.168.0.3. ACL, применяемый к VLAN, предшествует ACL, применяемому глобально . Таким образом, VLAN1 получает пакеты с IP-адресом назначения 192.168.0.3. В остальных случаях пакеты с IP-адресом назначения 192.168.0.3 отбрасываются.

Запись ACL – это набор из одного или нескольких правил. Следовательно, после применения записи ACL к порту/VLAN/глобально все правила, содержащиеся в этой записи ACL, будут применяться к порту/VLAN/глобально.

По умолчанию ACL, применяемый к порту/VLAN/глобально, вступает в силу раньше, чем ACL, который должен применяться к тому же порту/VLAN/глобально, но выпущен позже. Пользователи могут настроить приоритет записей ACL по мере необходимости.

6.15.3 Настройка через веб-интерфейс

1. Настройка записи ACL.

Щелкните[Device Advanced Configuration] → [ACL configuration] → [ACL Base Configuration] чтобы настроить запись ACL, как показано на рисунке 276.

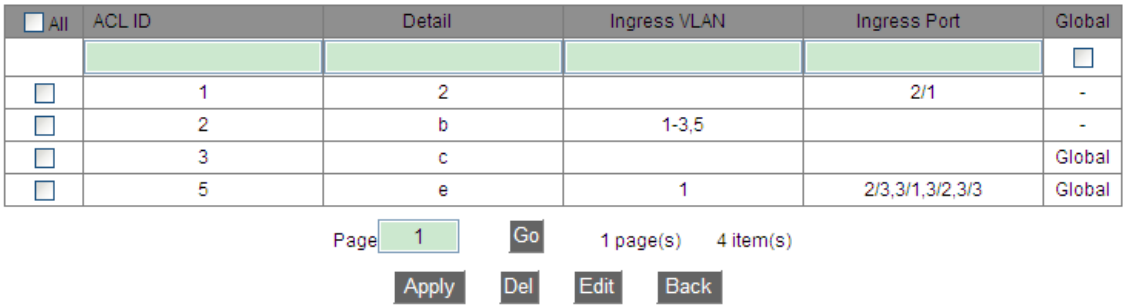


Рисунок 276 Настройка записи ACL

ACL ID

Диапазон: 1~1024

Функция: Настройка ACL ID. Изделие поддерживает не более 512 записей ACL. Если запись ACL применяется к нескольким портам, она применяется к каждому из портов. Аналогично, если запись ACL применяется к нескольким VLAN, она применяется к каждой из VLAN.

Описание: Если запись ACL применяется к непрерывному диапазону портов или VLAN, порты или сети VLAN могут быть разделены дефисом (-). Если запись ACL применяется к нескольким портам или сетям VLAN, не входящим в непрерывный диапазон, порты или сети VLAN могут быть разделены запятой (,).

Предупреждение:

Существуют некоторые системные записи ACL, и пользователи могут на самом деле настроить менее 512 записей ACL.

Detail

Диапазон: 1~127 символов

Функция: Настройка информации описания для записи ACL.

Ingress VLAN / Ingress Port/ Global

Функция: Настройка области применения записи ACL.

2. Отредактируйте запись ACL, как показано на рисунке 277.

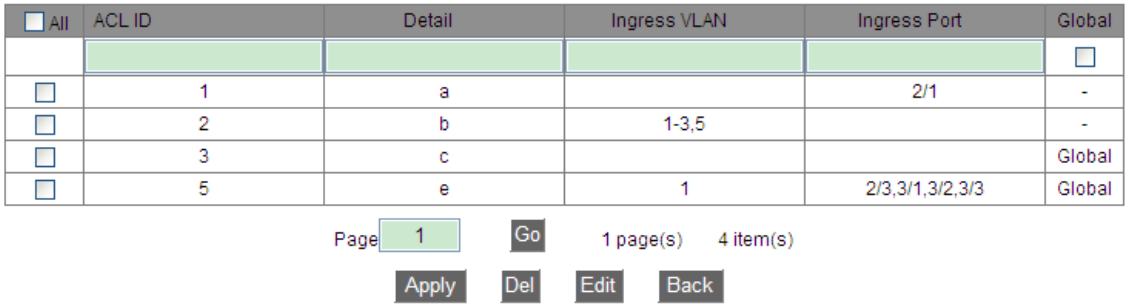


Рисунок 277 Редактирование записи ACL

Выберите запись ACL, щелкните <Del>, чтобы удалить запись ACL; щелкните <Edit>, чтобы изменить конфигурацию записи ACL.

3. Добавьте правило для записи ACL.

Щелкните созданную запись ACL на рисунке 276, чтобы перейти на рисунок 278, нажмите <Add Ruleo>, чтобы настроить правило для записи ACL.

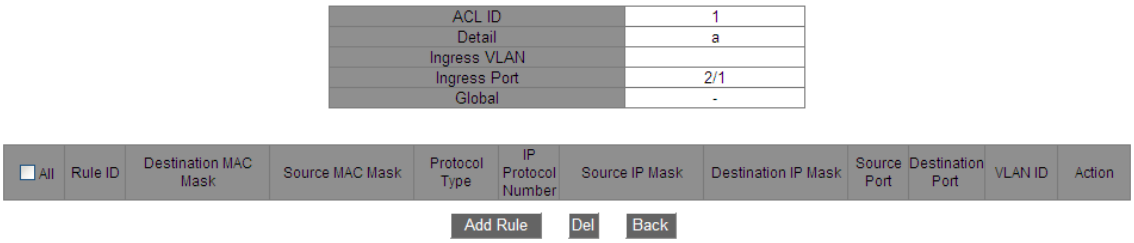


Рисунок 278 Отображение информации записи ACL

4. Настройте правило для записи ACL, как показано на рисунке 279.

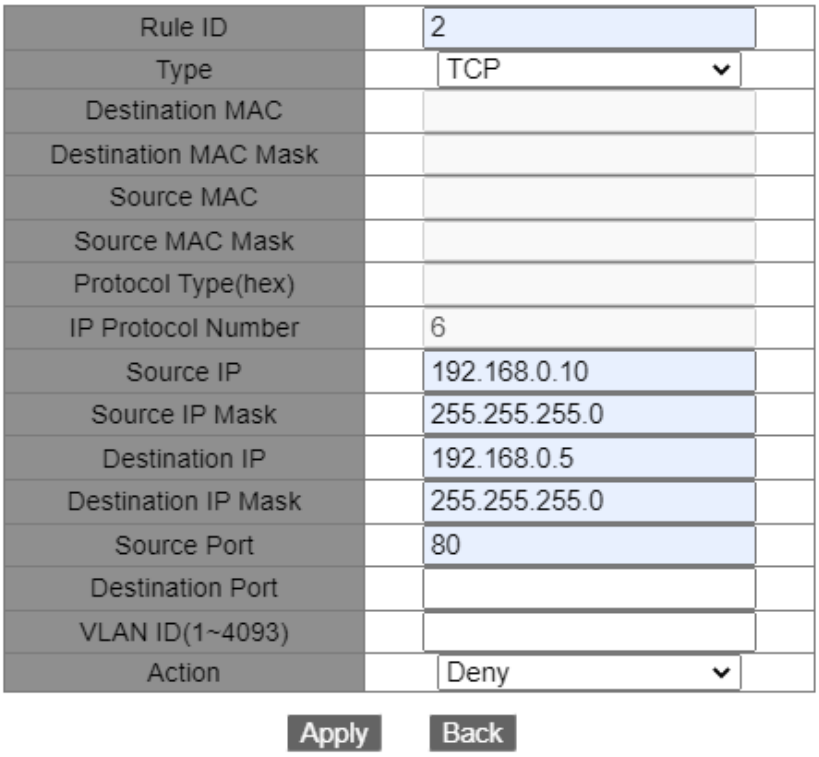


Рисунок 279 Настройка правила для записи ACL

Rule ID

Диапазон: 1~1024

Функция: Рисунок 279 Настройка идентификатора правила для записи ACL

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

Type

Варианты: Customized/IGMP/ICMP/TCP/UDP/MAC

По умолчанию: Customized

Функция: Настройка типа пакета для записи ACL

Destination MAC/ Destination MAC Mask

Функция: Настройка MAC-адреса получателя. В маске MAC-адреса получателя 1 указывает на сохраняемый бит MAC-адреса получателя, а 0 указывает на игнорируемый бит MAC-адреса получателя. **Source MAC/ Source MAC Mask**

Функция: Настройка MAC-адреса источника. В маске MAC-адреса источника1

указывает на сохраняемый бит MAC-адреса источника, а 0 указывает на игнорируемый бит MAC-адреса источника.

Protocol Type

Диапазон: 5DD-FFFF

Функция: Настройка типа протокола.

IP Protocol Number

Диапазон: 0~255

Функция: Настройка номер IP-протокола.

Source IP/ Source IP Mask

Функция: Настройка IP-адреса источника. В маске IP-адреса источника1 указывает на сохраняемый бит IP-адреса источника, а 0 указывает на игнорируемый бит IP-адреса источника.

Destination IP/ Destination IP Mask

Функция: Настройка IP-адреса назначения. В маске IP-адреса назначения 1 указывает на сохраняемый бит IP-адреса назначения, а 0 указывает на игнорируемый бит IP-адреса назначения.

Source Port

Диапазон: 0~65535

Функция: Настройка номера исходного порта.

Destination Port

Диапазон: 0~65535

Функция: Настройка номера порта назначения.

VLAN ID

Диапазон: 1~4093

Функция: Настройка VLAN ID.

Action

Варианты: Permit/Deny/Mirror to CPU/ Mirror to Port/Redirect to CPU/ Redirect to Port

По умолчанию: Permit

Функция: Настройка режима обработки пакетов для успешно сопоставленных пакетов.

Описание: **Permit** указывает на получение успешно сопоставленных пакетов; **Deny** указывает на отбрасывание успешно сопоставленных пакетов; **Mirror to CPU** указывает на получение успешно сопоставленных пакетов и их зеркалирование на ЦП; **Mirror to Port** указывает на получение успешно согласованных пакетов и их зеркалирование на указанный порт; **Redirect to CPU** указывает на перенаправление успешно сопоставленных пакетов на ЦП; **Redirect to Port** указывает на перенаправление успешно сопоставленных пакетов на указанный порт.

5. Запрос записи ACL.

Щелкните [Device Advanced Configuration] → [ACL configuration] → [ACL Search] чтобы запросить запись ACL, как показано на рисунке 280.

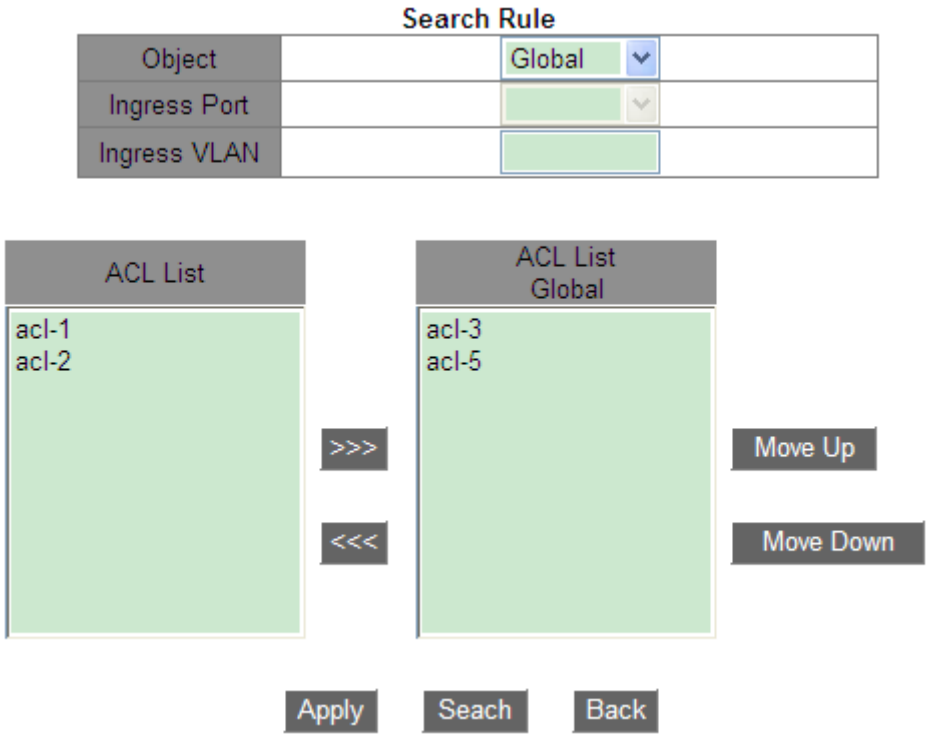


Рисунок 280 Запрос ACL

Object

Варианты: Global/ Port/ VLAN

Функция: Выбор области применения для запрашиваемых записей ACL.

Ingress Port

Функция: Выбор порта применения для записей ACL, которые будут запрашиваться, когда для параметра **Object** установлено значение **Port**. **Ingress VLAN**

Функция: Выбор VLAN применения для записей ACL, которые будут запрашиваться, когда для параметра **Object** установлено значение

VLAN.

Список ACL в нижней правой части показывает найденные записи ACL.

6. Примените записи ACL к объекту и настройте приоритет для записей ACL, как показано на рисунке 281.

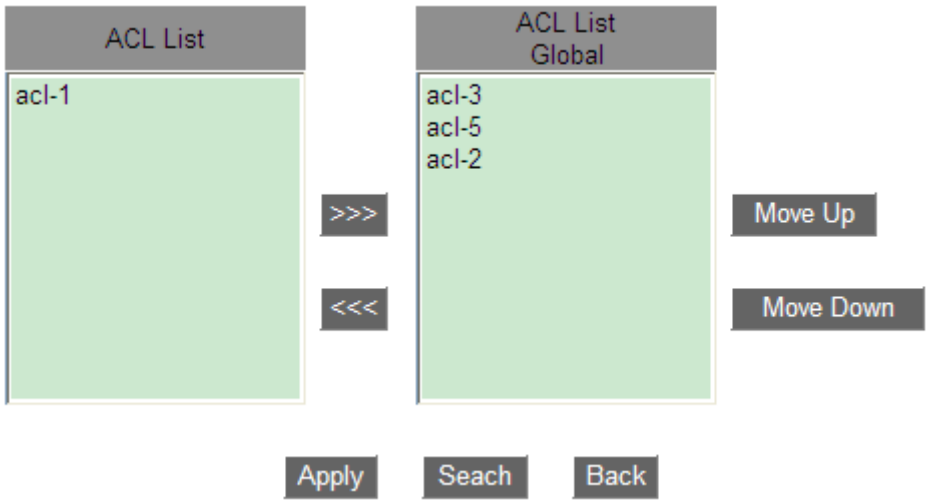


Рисунок 281 Настройка приоритета записи ACL

Переместите запись ACL, которую нужно применить к объекту, в список ACL справа. Выберите запись и щелкните < Move Up > или < Move Down >, чтобы изменить приоритет записей ACL, применяемых к объекту. Записи ACL сверху вниз в списке расположены в порядке убывания приоритета.

6.15.4 Типовой пример конфигурации

Порт 2/1 отбрасывает TCP-пакеты с исходного порта 80 с хоста в сегменте сети 192.168.1.0 на хост в сегменте сети 192.168.0.0.

Настройка:

1. Настройте запись ACL 1, применяемую к порту 2/1, как показано на рисунке 276.

2. Настройте правило ACL, задайте Type – TCP, Source IP – 192.168.1.5, Source IP Mask – 255.255.255.0, Destination IP – 192.168.0.5, Destination IP Mask – 255.255.255.0, Source Port – 80, Action – deny, как показано на рисунке 279.

6.16 Конфигурация QoS

6.16.1 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.
QoS в основном включает в себя идентификацию служб, управление перегрузками и предотвращение перегрузок.
Идентификация служб: Объекты идентифицируются на основе определенных правил соответствия. Например, объекты могут быть тегами приоритета, переносимыми пакетами, приоритетом, отображаемым портами и VLAN, или другой информацией о приоритете. Идентификация служб предварительным условием для QoS. 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.

6.16.2 CAR

Гарантированная скорость доступа QoS (CAR) — это тип политики ограничения скорости. Эта политика цитирует правило ACL для идентификации потока, ограничивает скорость порта для соответствующего пакета и отбрасывает поток, выходящий за пределы диапазона (параметры width и burst), предусмотренного политикой QoS в пакете.

6.16.3 Примечание

QoS Remark цитирует правило ACL для идентификации потока и снова указывает приоритет (значение DSCP или COS) для соответствующего пакета.

6.16.4 Принцип работы

Каждый порт коммутаторов этой серии поддерживает 8 очередей кэширования, от 0 до 7 в порядке возрастания приоритета.

Можно настроить сопоставление между приоритетом и очередями. Когда кадр достигает порта, коммутатор определяет очередь для кадра в соответствии с информацией в заголовке кадра. Коммутатор поддерживает два режима сопоставления очереди для определения приоритета: CoS и DSCP.

- Значение CoS зависит от приоритета тега 802.1Q в пакете. Сопоставление между значением CoS и очередью можно настроить.
- Значение DSCP зависит от части пакета TOD/DSCP. Сопоставление между значением DSCP и очередью можно настроить.

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: WRR (Weighted Round Robin) и приоритетные очереди.

- WRR 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.
- Режим планирования очереди с приоритетом может строго гарантировать наивысший приоритет пересылки для пакета с наивысшим приоритетом, который в основном используется при передаче важного сигнала. Как только кадр попадает в очередь с высоким приоритетом, система останавливает планирование данных очереди с низким приоритетом и обрабатывает данные в очереди с высоким приоритетом. Только когда очередь с высоким приоритетом пуста, система может начать обработку данных в очереди с более низким приоритетом.

6.16.5 Настройка через веб-интерфейс

1. Включите функцию QoS.

Щелкните [Device Advanced Configuration] → [QoS configuration] → [Enable QoS] → [Enable/Disable QoS], чтобы включить QoS, как показано на рисунке 282.

Рисунок 282 Включение QoS

QoS Status

Варианты: Open/Close

По умолчанию: Close

Функция: Включение/выключение глобальной функции QoS.

2. Добавление/удаление карты классов

[Device Advanced Configuration] → [QoS configuration] → [Class-map configuration] → [Add/Remove class-map], чтобы добавить/удалить карту классов, как показано на рисунке 283.

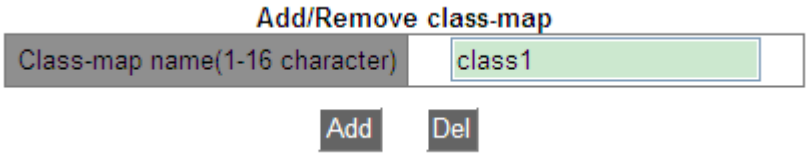


Рисунок 283 Добавление/удаление карты классов

Class-map name

Диапазон: 1~16 символов

Функция: Настройка имени карты классов. Щелкните <Add> / <Del>, чтобы создать/удалить карту классов.

3. Настройте сопоставления карты классов

Щелкните [Device Advanced Configuration] → [QoS configuration] → [Class-map configuration]

→ [Class-map configuration], чтобы перейти на страницу настройки карты классов, как показано на рисунке 284.

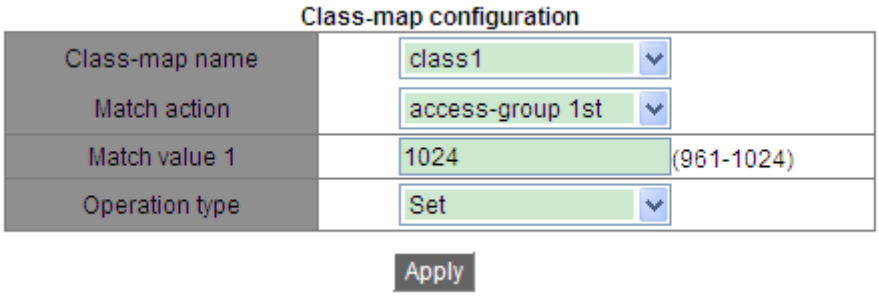


Рисунок 284 Настройка сопоставления карты классов

Class-map name

Варианты: Все созданные карты классов

Match action

По умолчанию: access-group 1st

Функция: Настройте действие сопоставления карты классов

Match value 1

Диапазон: 961~1024

Функция: Сопоставление указанной записи ACL. Для совпадения в таблице ACL должно быть задано действие permit.

Operation type

Варианты: Set/Del

Функция: Задать/удалить действие сопоставления карты классов.

4. Добавление/удаление карты политик

Щелкните [Device Advanced Configuration] → [QoS configuration] → [Policy-map configuration]

→ [Add/Remove policy-map], чтобы добавить/удалить карту политик, как показано на рисунке 285.

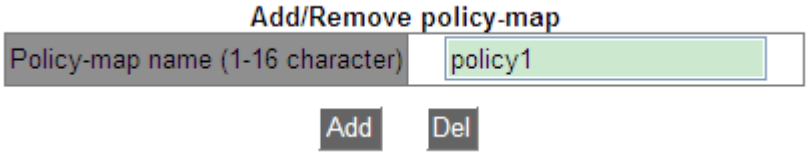


Рисунок 285 Добавление/удаление карты политик

Policy-map name

Диапазон: 1~16 символов

Функция: Настройка имени карты политик. Щелкните <Add>/<Del>, чтобы создать/удалить таблицу политик.

5. Настройка полосы пропускания карты политик

Щелкните [Device Advanced Configuration] → [QoS configuration] → [Policy-map configuration]

→ [Policy-map bandwidth configuration], чтобы перейти на страницу настройки полосы пропускания карты политик, как показано на рисунке 286.

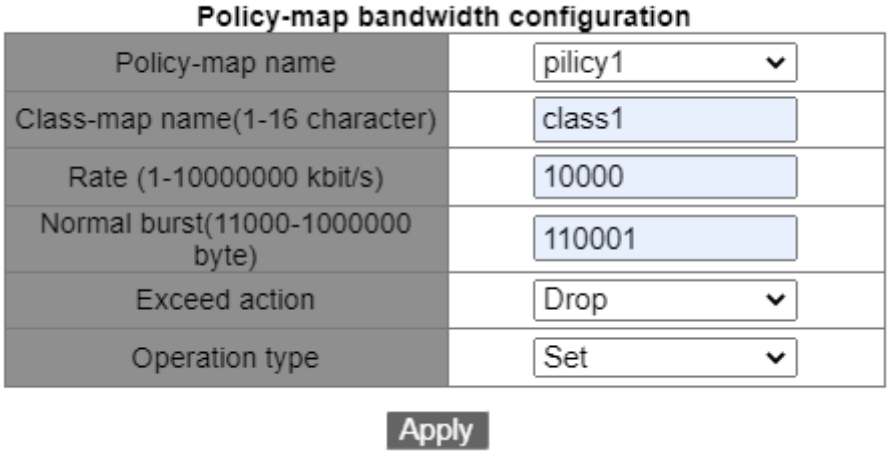


Рисунок 286 Настройка полосы пропускания карты политик

Policy-map name

Варианты: Все созданные карты политик

Class-map name

Варианты: Все созданные карты классов

Rate

Диапазон: 1-10000000 кбит/с

Функция: Настройка значения скорости.

Normal burst

Диапазон: 11000-1000000 байт

Функция: Настройка значения параметра normal burst.

Exceed action

Варианты: Drop

Функция: Применить политику отбрасывания для пакета, соответствующего карте классов, но превышающего предельное значение скорости.

Operation type

Варианты: Set/Del

Функция: Задать/удалить настройку полосы пропускания карты политик

6. Настройка приоритетной перемаркировки карты политик

Щелкните [Device Advanced Configuration] → [QoS configuration] → [Policy-map configuration] → [Policy-map priority configuration], чтобы перейти на страницу настройки приоритетов карты политик, как показано на рисунке 287.

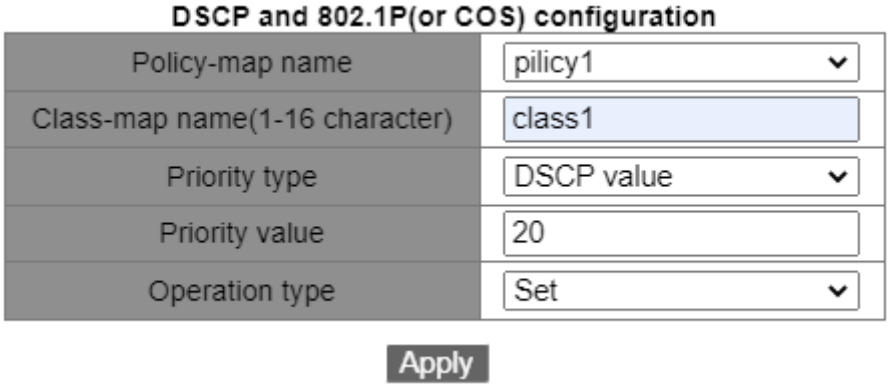


Рисунок 287 Настройка перемаркировки приоритетов

Policy-map name

Варианты: Все созданные карты политик

Class-map name

Варианты: Все созданные карты классов

Priority type

Варианты: Значение DSCP /значение COS

Функция: Выбор типа приоритета для перемаркировки.

Priority value

Варианты: 0~63（значение DSCP）/0~7（значение COS）

Функция: Настройка значения перемаркировки приоритета.

Описание: Применение политики перемаркировки для значения приоритета пакета, соответствующего карте классов.

Operation type

Варианты: Set/Del

Функция: Настройка/удаление перемаркировки приоритетов карты политик.

7. Примените карту политик к порту

Щелкните [Device Advanced Configuration] → [QoS configuration] → [Apply QoS to the port] → [Apply policy-map to port], чтобы применить карту политик к порту, как показано на рисунке 288.

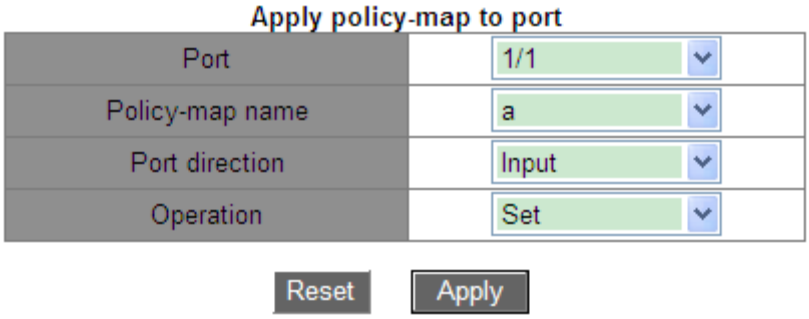


Рисунок 288 Применение карты политик к порту

Policy-map name

Варианты: Все созданные карты политик

Port direction

Варианты: Input

Функция: Эта таблица политик применяется во входном направлении порта, чтобы реализовать ограничение скорости или перемаркировку приоритета для пакета, полученного через порт.

Operation type

Варианты: Set/Del

Функция: Настроить/удалить функцию применения карты политик к порту.

Предупреждение:

- Применяйте к порту только одну карту политик.
- Конфигурация режима доверия порта и применение карты политик к порту являются взаимоисключающими.

8. Настройте режим доверия порта.

Щелкните [Device Advanced Configuration] → [QoS Configuration] → [Apply QoS to port] → [Port trust mode configuration], чтобы перейти на страницу настройки режима доверия порта, как показано на рисунке 289.

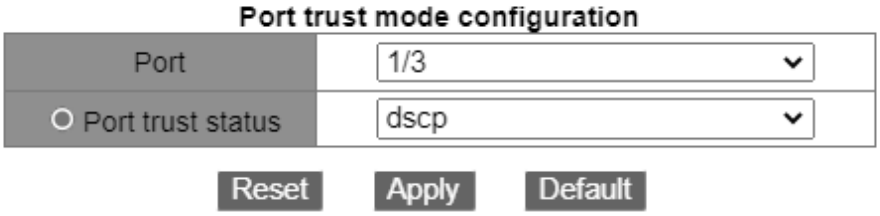


Рисунок 289 Настройка режим доверия порта

Port

Варианты: все порты коммутатора.

Port trust status

Варианты: cos/cos and pass through dscp/dscp/dscp and pass through cos/port

По умолчанию: Если полученный портом пакет является IP-пакетом, по умолчанию используется dscp; если это не IP-пакет, а тегированный пакет, по умолчанию используется значение cos. Если это не IP-пакет, и нетегированный пакет, порт не имеет режима доверия по умолчанию и сохранит пакет в очереди 0.

Функция: Настройка статуса доверия портов коммутатора.

Описание: **cos** и **cos and pass through dscp** означает, что порт доверяет значению CoS. Очередь для сохранения полученного портом пакета определяется значением CoS и сопоставлением очереди. Если пакет не имеет значения CoS, он ставится в очередь в соответствии со значением CoS, равным 0. Различия между **cos** и **coss and pass through dscp** заключается в том, что **cos** изменяет значение DSCP пакета на значение в сопоставлении между CoS и DSCP во время пересылки пакета, но **cos and**

pass through dscp не изменяет значение DSCP пакета во время пересылки пакета.

dscp и **dscp and pass through cos** означают, что порт доверяет значению DSCP. Очередь для сохранения полученного портом пакета определяется значением DSCP и сопоставлением очереди. Если пакет не имеет значения DSCP, он ставится в очередь в соответствии со значением DSCP, равным 0. Различия между **dscp** и **dscp and pass through cos** заключается в том, что **dscp** изменяет значение CoS на значение в сопоставлении между DSCP и CoS во время пересылки пакета, но **dscp and pass through cos** не изменяет значение CoS пакета во время пересылки пакета.

Port priority

Варианты: 0~7

По умолчанию: 0

Функция: Назначение приоритета физического порта. Пакеты, полученные от порта, ставятся в очередь в соответствии с назначенным приоритетом, а не в соответствии с приоритетом, переносимым пакетами. Пакеты, полученные от порта с приоритетом 0, помещаются в очередь 0, а пакеты, полученные от порта с приоритетом 1, помещаются в очередь 1. Остальное можно выполнить таким же образом.

9. Настройка значения CoS по умолчанию.

Щелкните [Device Advanced Configuration] → [QoS Configuration] → [Apply QoS to port] → [Port default CoS configuration], чтобы перейти на страницу настройки значения CoS по умолчанию, как показано на рисунке 290.

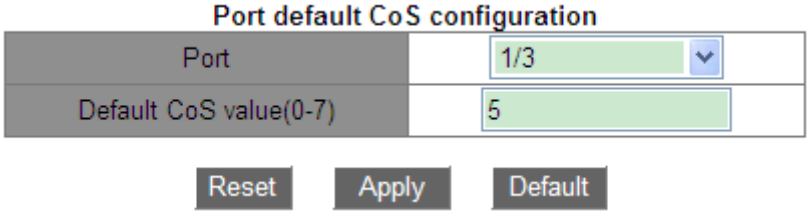


Рисунок 290 Настройка значения CoS по умолчанию.

Port

Варианты: все порты коммутатора.

Default CoS value

Варианты: 0~7

По умолчанию: 0

Функция: Настройка значения CoS по умолчанию для порта.

Пояснение: Когда пакет не помечен, приоритет в теге, добавленном к пакету, равен значению CoS по умолчанию для порта.

10. . Настройка режима планирования очереди портов на приоритетную очередь.

Щелкните [Device Advanced Configuration] → [QoS Configuration] → [Egress-queue configuration] → [Port Egress-queue work mode configuration], чтобы перейти на страницу настройки режима приоритетной очереди, как показано на рисунке 291.

Рисунок 291 Настройка режима выходной очереди

Egress-queue Work Mode

Варианты: PQ/WRR

По умолчанию: PQ

Функция: Настройка режима исходящей очереди для выбранного порта. 11. Настройка весовых WRR для порта.

Щелкните [Device Advanced Configuration] → [QoS Configuration] → [Egress-queue configuration] → [Port Egress-queue wrr weight configuration], чтобы перейти на страницу настройки весовых WRR, как показано на рисунке 292.

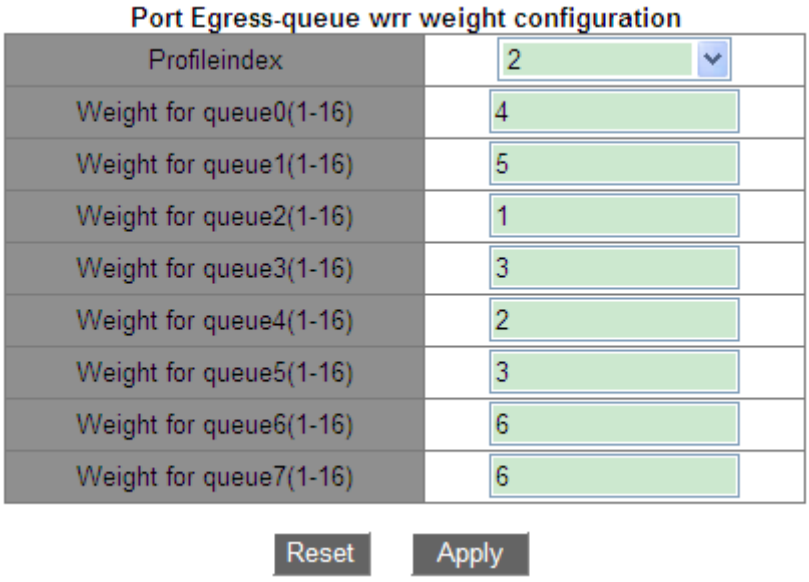


Рисунок 292 Настройка весовых коэффициентов

Profileindex

Варианты: 1~6

По умолчанию: 1

Функция: Настройка групп значений весов.

Пояснение: Коммутатор поддерживает не более 6 групп значений весов.

{Weight for queue0, Weight for queue1, Weight for queue2, Weight for queue3, Weight for queue4, Weight for queue5, Weight for queue6, Weight for queue7}

Варианты: {0~15, 0~15, 0~15, 0~15, 0~15, 0~15, 0~15}

По умолчанию: {1, 2, 3, 4, 5, 6, 7, 8}

Функция: Настройка значений весовых коэффициентов. Абсолютное значение веса не имеет смысла. WRR распределяет полосу пропускания в соответствии с 8 соотношениями весовых значений.

Описание: Если значение веса одной очереди равно 0, эта очередь имеет наивысший приоритет, и ее пакеты будут пересылаться с наивысшим приоритетом. Если значение веса нескольких очередей равно 0, наивысший приоритет пересылки отдается данным

из очереди с высоким приоритетом, имеющим значение 0. Затем пересылаются данные со значением веса 0 из очереди с низким приоритетом. Когда отправлены все данные со значением веса 0, коммутатор начинает пересылать данные других очередей в соответствии с коэффициентом веса.

12. Настройте режим планирования WRR для порта и привяжите к порту весовой коэффициент, как показано на рисунке 293.

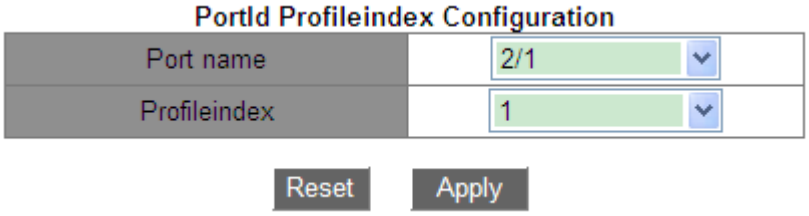


Рисунок 293 Настройка режима планирования WRR

Port name

Варианты: все порты коммутатора.

Функция: Выбор порта для задания режима планирования WRR.

Profileindex

Варианты: 1~6

Функция: Выбор весового соотношения WRR для порта.

13. . Настройте сопоставление между значением CoS и очередью.

Щелкните [Device Advanced Configuration] → [QoS Configuration] → [Egress-queue configuration] → [Mapping CoS values to egress queue], чтобы перейти на страницу настройки сопоставления между значением CoS и очередью, как показано на рисунке 294.

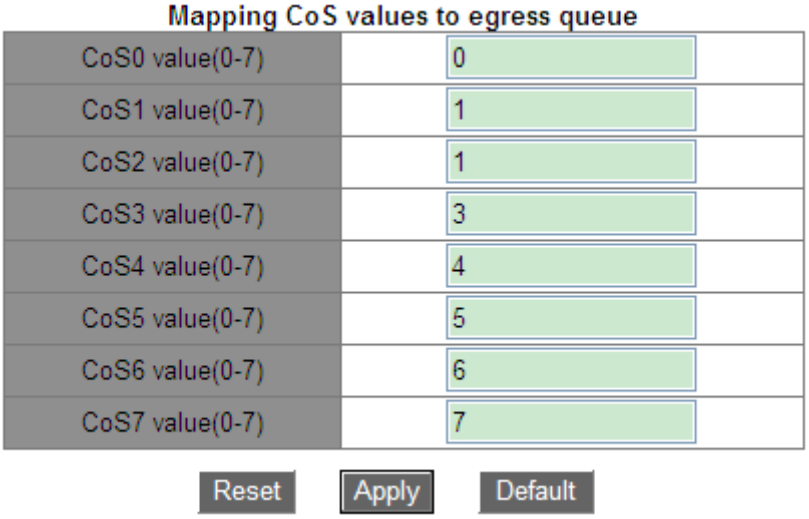


Рисунок 294 Настройка сопоставления между значением CoS и очередью.

{COS value, Queue-ID}

Варианты: {0~7, 0~7}

По умолчанию: Значение CoS 0 сопоставляется с очередью 0; Значение CoS 1 сопоставляется с очередью 1; Значение CoS 2 сопоставляется с очередью 2; Значение CoS 3 сопоставляется с очередью 3; Значение CoS 4 сопоставляется с очередью 4; Значение CoS 5 сопоставляется с очередью 5; Значение CoS 6 сопоставляется с очередью 6; Значение CoS 7 сопоставляется с очередью 7;

Функция: Настройка сопоставления между значением CoS и очередью.

Пояснение: Каждое значение CoS может быть сопоставлено только с одной очередью. Несколько значений CoS могут быть сопоставлены с одной очередью.

14. . Настройте сопоставление между значением DSCP и очередью.

Щелкните [Device Advanced Configuration] → [QoS Configuration] → [Egress-queue configuration] → [Mapping DSCP values to egress queue], чтобы перейти на страницу настройки сопоставления между значением DSCP и очередью, как показано на рисунке 295.

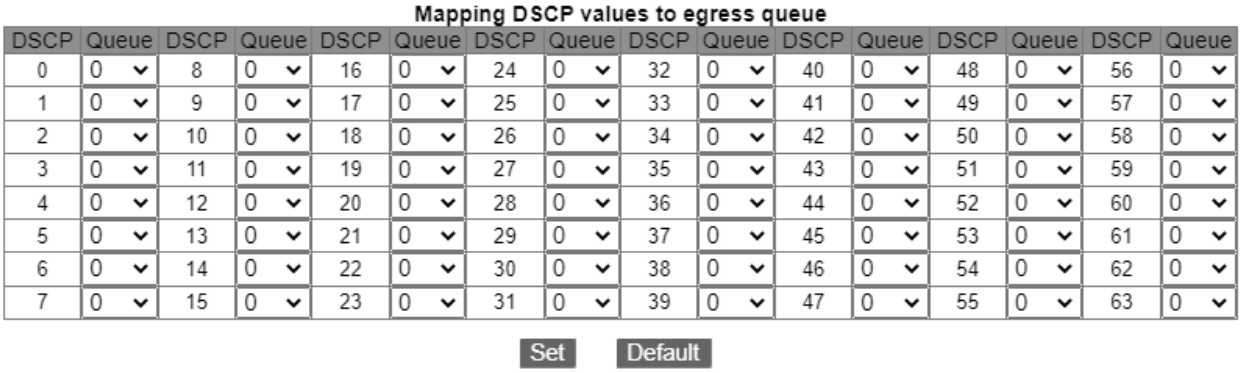


Рисунок 295 Настройка сопоставления между значением DSCP и очередью.

{DSCP, Queue value} Варианты: {0~63, 0~7}
По умолчанию: Значение DSCP 0~7 сопоставляется с очередью 0; значение DSCP 8~15 сопоставляется с очередью 1; значение DSCP 16~23 сопоставляется с очередью 2; значение DSCP 24~31 сопоставляется с очередью 3; значение DSCP 32~39 сопоставляется с очередью 4; значение DSCP 40~47сопоставляется с очередью 5; значение DSCP 48~55 сопоставляется с очередью 6; значение DSCP 56~63 сопоставляется с очередью 7. Функция: Настройте сопоставление между значением DSCP и очередью.

Пояснение: Каждое значение DSCP может быть сопоставлено только с одной очередью. Несколько значений DSCP могут быть сопоставлены с одной очередью. Щелкните <Set>, чтобы установить новое сопоставление между значением DSCP и очередью, <Del>, чтобы восстановить сопоставление по умолчанию между значением DSCP и очередью.

15. Настройте сопоставления между значением CoS и значением DSCP.

Щелкните [Device Advanced Configuration] → [QoS Configuration] → [QoS mapping configuration] → [CoS-to-DSCP mapping], чтобы перейти на страницу настройки сопоставления CoS и DSCP, как показано на рисунке 296.

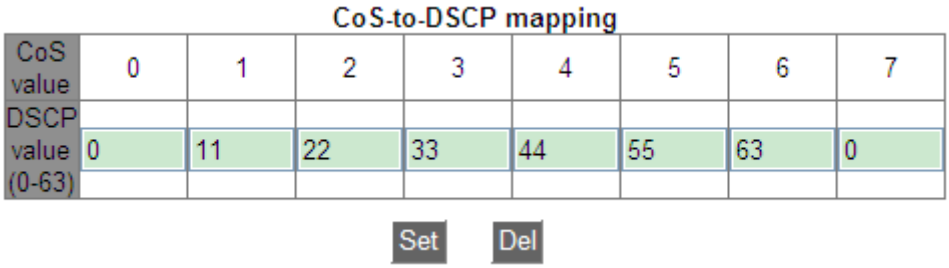


Рисунок 296 Настройка сопоставления между CoS и DSCP.

DSCP value

Options: 0~63

По умолчанию: Значение CoS 0 сопоставляется со значением DSCP 0; значение CoS 1 сопоставляется со значением DSCP 8; значение CoS 2 сопоставляется со значением DSCP 16; значение CoS 3 сопоставляется со значением DSCP 24; значение CoS 4 сопоставляется со значением DSCP 32; значение CoS 5 сопоставляется со значением DSCP 40; значение CoS 6 сопоставляется со значением DSCP 48; значение CoS 7 сопоставляется со значением DSCP 56.

Функция: Настройка сопоставления между CoS и DSCP. Когда режим доверия порта — CoS, значение DSCP пакета может быть изменено в соответствии с этим сопоставлением.

Пояснение: Несколько значений CoS могут быть сопоставлены с одним значением DSCP.

Щелкните <Set>, чтобы установить новое сопоставление между CoS и DSCP, <Del>, чтобы восстановить сопоставление по умолчанию между CoS и DSCP.

16. . Настройте сопоставления между значением DSCP и значением CoS.

Щелкните [Device Advanced Configuration] → [QoS Configuration] → [QoS mapping configuration] → [DSCP-to-CoS mapping], чтобы перейти на страницу настройки сопоставления DSCP и CoS, как показано на рисунке 297.

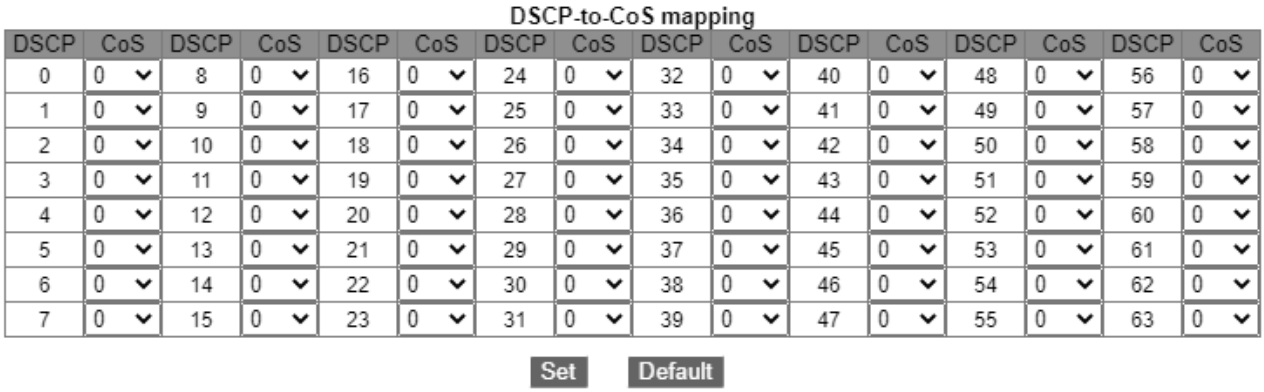


Рисунок 297 Настройка сопоставления между DSCP и CoS.

{DSCP value, COS value}

Варианты: {0~63, 0~7}

По умолчанию: Значение DSCP 0~7 сопоставляется со значением CoS 0; значение DSCP 8~15 сопоставляется со значением CoS 1;

значение DSCP 16~23 сопоставляется со значением CoS 2; значение DSCP 24~31 сопоставляется со значением CoS 3; значение DSCP 32~39 сопоставляется со значением CoS 4; значение DSCP 40~47 сопоставляется со значением CoS 5; значение DSCP 48~55 сопоставляется со значением CoS 6; значение DSCP 56~63 сопоставляется со значением CoS 7.

Функция: Настройка сопоставления между DSCP и CoS. Когда режим доверия порта DSCP, значение CoS пакета может быть изменено в соответствии с этим сопоставлением.

Пояснение: Не более 8 значений могут DSCP быть сопоставлены с одним значением CoS.

Щелкните <Set>, чтобы установить новое сопоставление между значением DSCP и CoS, <Del>, чтобы восстановить сопоставление по умолчанию между значением DSCP и CoS.

17. . Настройте сопоставления между значением DSCP и значением DSCP.

Щелкните [Device Advanced Configuration] → [QoS Configuration] → [QoS mapping configuration] → [DSCP-to-DSCP mutation mapping], чтобы перейти на страницу настройки сопоставления DSCP и DSCP, как показано на рисунке 298.

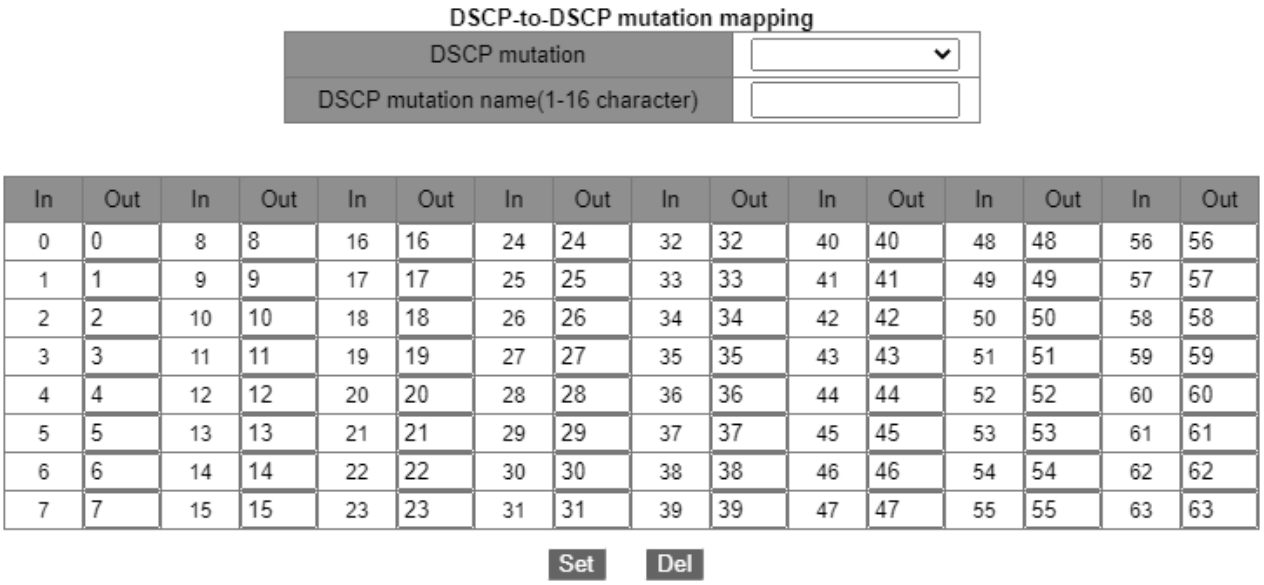


Рисунок 298 Настройка сопоставления между DSCP и DSCP.

DSCP mutation name

Диапазон: 1~16 символов

Функция: Задание имени изменения DSCP.

{ In , Out }

Варианты: {0~63, 0~63}

Функция: Настройка сопоставления между DSCP и DSCP. Чтобы изменить значение DSCP пакета, используйте это сопоставление, когда выходной порт пересылает пакет.

Пояснение: Не более 8 значений могут DSCP быть сопоставлены с одним значением DSCP.

Щелкните <Set>, чтобы установить новое сопоставление между значением DSCP и DSCP, <Del>, чтобы восстановить сопоставление по умолчанию между значением DSCP и DSCP. Коммутаторы серии поддерживают не более 28 сопоставлений для изменения DSCP.

Предупреждение:

Очередь для сохранения пакетов определяется исходным сопоставлением между значением DSCP и очередью.

18. Примените сопоставление мутаций DSCP на порту.

Щелкните [Device Advanced Configuration] → [QoS Configuration] → [Apply QoS to port] → [Apply DSCP mutation mapping], чтобы перейти на страницу настройки, как показано на рисунке 299.

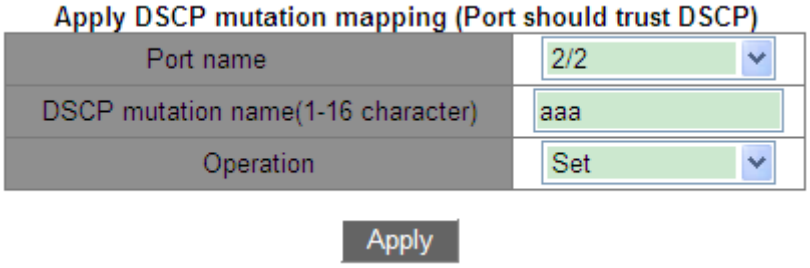


Рисунок 299 Применение сопоставления мутаций DSCP на порту.

Port name

Варианты: все порты коммутатора.

Функция: Выбор порта для использования мутаций DSCP.

DSCP mutation name

Варианты: Имя сопоставления DSCP – DSCP:

Функция: Настройка сопоставления мутаций DSCP с использованием порта.

Operation

Варианты: Set/Del

Функция: Добавить/удалить сопоставление мутаций DSCP с использованием порта.

6.16.6 Типовой пример конфигурации

Как показано на рисунке 300, порты 1, 2, 3 и 4 пересылают пакеты на порт 5. Значение DSCP принятого пакета порта 1 равно 6, режим доверия — DSCP pass CoS, а пакеты, поступающие на порт 1, соответствуют очереди 3. Значение CoS принятого пакета порта 2 равно 2, режим доверия — CoS pass DSCP, а пакеты, поступающие на порт 2,

соответствуют очереди 1. Значение CoS принятого пакета порта 3 равно 2, значение DSCP для него равно 32, режим доверия — DSCP, а пакеты, поступающие на порт 3, соответствуют очереди 2. Значение DSCP принятого пакета порта 4 равно 26, значение CoS для него равно 3, режим доверия — CoS, а пакеты, поступающие на порт 4, соответствуют очереди 3. Порт 5 использует режим планирования WRR.

Процесс настройки:

1. Включите QoS, как показано на рисунке 282.

2. Установите режим доверия порта 1 – DSCP pass CoS, порта 2 – CoS pass DSCP, порта 3 – DSCP и порта 4 – CoS, как показано на рисунке 289.

3. Режимы CoS-to-DSCP и DSCP-to-CoS используют сопоставление по умолчанию; это означает, что значение CoS для пересылаемых пакетов порта 3 изменяется на 4, а значение DSCP для пересылаемых пакетов порта 4 изменяется на 24.

4. Привяжите значение CoS 2 к очереди 1, а значение CoS 3 – к очереди 3, как показано на рисунке 294.

5. Привяжите значение DSCP 6 к очереди 3, а значение DSCP 32 – к очереди 2, как показано на рисунке 295.

6. Настройте режим планирования очереди порта 5 WRR, (см. рисунок 291; используйте весовой коэффициент очереди по умолчанию, как показано на рисунке 293.

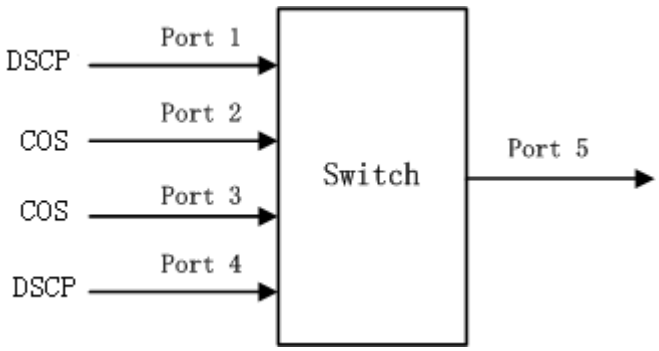


Рисунок 300 Пример настройки QoS

Пакеты порта 1 и порта 4 попадают в очередь 3, пакеты порта 2 попадают в очередь 1, пакеты порта 3 попадают в очередь 2. Согласно сопоставлению между очередью и весом, вес очереди 1 равен 2, вес очереди 2 равен 3, а вес очереди 3 равен 4, поэтому доля полосы пропускания, выделенная пакетам во входящей очереди 1, равна 2/(2+3+4), доля полосы пропускания, выделенная пакетам во входящей очереди 2, равна 3/(2+3+4), а для пакетов во входящей очереди 3 выделяется 4/(2+3+4). Среди них пакеты порта 1 и порта 4 попадают в очередь 3, поэтому они пересылаются в соответствии с правилом First In, First out (FIFO), но общая пропорция пропускной способности порта 1 и порта 4 должна быть 4/(2+3+4).

6.17 Настройка IEC61850

6.17.1 Введение

В настоящее время коммутаторы прозрачны для других функциональных объектов в сетях подстанций. Для мониторинга коммутаторов необходимы инструменты, отличные от IEC61850, такие как EMS, Web, интерфейс командной строки и OPC, что приводит к несогласованности и неудобству настройки сети и управления ею.

Чтобы решить эти проблемы, мы создаем модели для коммутаторов в соответствии со стандартом IEC61850 и вводим коммутаторы в системы автоматизации подстанций в качестве интеллектуальных электронных устройств (IED), обеспечивая единое представление мониторинга автоматизации подстанции, облегчая планирование решений интеграции и управления, а также экономя затраты на строительство и техническое обслуживание.

Предупреждение:

Файл моделирования по умолчанию switch.cid, предоставленный производителем, уже в коммутатор. Если заказчику необходимо импортировать другие файлы моделирования, обратитесь к разделу Служба передачи файлов.

6.17.2 Настройка через веб-интерфейс

1. Включите IEC61850

Щелкните [Device Advanced Configuration] → [IEC61850 Configuration] → [IEC61850 Configuration], чтобы перейти на страницу настройки IEC61850, как показано на рисунке 301.

Рисунок 301 Настройка IEC61850

IEC61850 Function

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение или выключение функции IEC61850.

2. Настройка IEC 61850

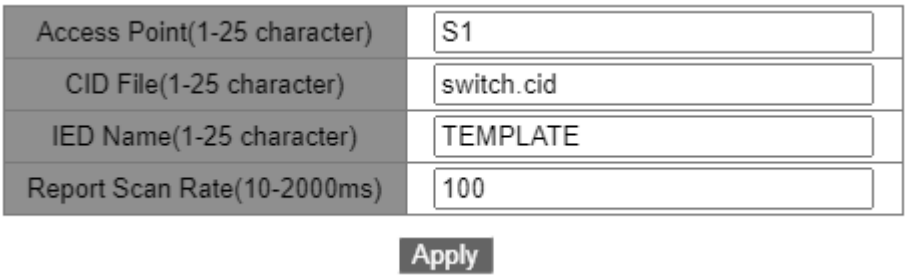


Рисунок 302 Настройка IEC61850

Access Point

Диапазон: 0~25 символов

По умолчанию: S1

Функция: Настройка имени точки доступа, соответствующей IED в файле CID.

CID File

Диапазон: 1~25 символов

По умолчанию: switch.cid

Функция: Настройка имени актуального файла моделирования CID при запуске функции IEC61850.

IED Name

Диапазон: 1~25 символов

По умолчанию: TEMPLATE

Функция: Настройка имени логического устройства, соответствующего IED в файле CID.

Report Scan Rate

Диапазон: 10~2000 мс

По умолчанию: 100 мс

Функция: Настройка интервала сканирования информации об узле устройства.

Предупреждение:

Настройки имени точки доступа и IED должны соответствовать имени точки доступа и IED в указанном файле моделирования. В противном случае функцию IEC61850 включить нельзя.

6.18 Настройка GOOSE Trigger

GOOSE-Trigger определяет, следует ли подписываться на пакет GOOSE в соответствии с MAC-адресом получателя и идентификатором APP ID пакета GOOSE. Если устройство подписано на пакет GOOSE, GOOSE-Trigger получает текущее время и информацию о состоянии коммутатора, содержащуюся в пакете (IEC61850 периодически запрашивает значение состояния коммутатора в режиме опроса. Если статус коммутатора меняется, он отправляет MMS REPORT).

Щелкните [Device Advanced Configuration] → [Goose configuration] → [Goose configuration], чтобы перейти на страницу настройки Goose, как показано на рисунке 303.

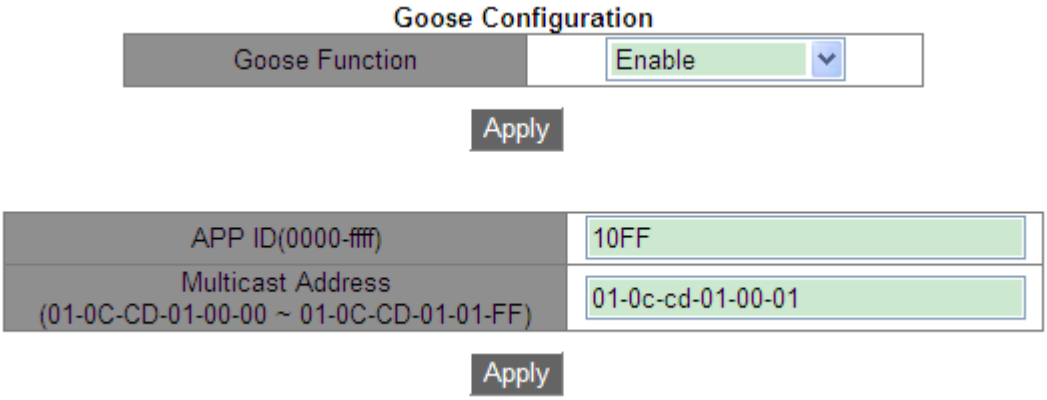


Рисунок 303 Настройка GOOSE Trigger

Goose Function

Варианты: Enable/Disable

По умолчанию: Disable
Функция: Включение/выключение функции GOOSE Trigger. Устройство может подписываться на пакеты GOOSE после включения функции Goose.

APP ID

Варианты: 0x0000~0xffff

По умолчанию: 0x10ff

Функция: Настройка APP ID пакетов GOOSE для подписки. После включения GOOSE Trigger устройство подпишется на пакеты GOOSE с идентификатором APP ID, соответствующим конфигурации.

Multicast Address

Варианты: 01-0C-CD-01-00-00~01-0C-CD-01-01-FF

По умолчанию: 01-0C-CD-01-00-01

Функция: Настройка MAC-адреса пакетов GOOSE для подписки. После включения GOOSE Trigger устройство подпишется на пакеты GOOSE с MAC-адресом, соответствующим конфигурации.

6.19 IGMP Snooping

6.19.1 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.

6.19.2 Основная концепция

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 генератора 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.

6.19.3 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).

6.19.4 Настройка через веб-интерфейс

1. Включите IGMP Snooping.

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [IGMP Snooping configuration] → [Enable IGMP Snooping], чтобы перейти на страницу глобальной настройки IGMP Snooping, как показано на рисунке 304.

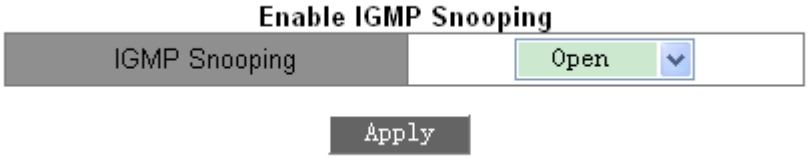


Рисунок 304 Включение IGMP Snooping

IGMP Snooping

Варианты: Open/Close

По умолчанию: Close

Функция: Включение или выключение глобального протокола IGMP Snooping. IGMP Snooping и GMRP нельзя включить одновременно.

2. Настройте параметры IGMP Snooping.

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [IGMP Snooping configuration] → [IGMP Snooping configuration], чтобы перейти на страницу настройки IGMP Snooping, как показано на рисунке 305.

Рисунок 305 Настройка IGMP Snooping

VLAN ID

Варианты: все созданные VLAN ID

Snooping state

Варианты: Open/Close

По умолчанию: Close

Функция: Включение или выключение функции VLAN IGMP Snooping.

Предварительным условием для этой функции является включение глобальной функции IGMP Snooping.

Static IP

Формат: A.B.C.D

По умолчанию: 192.168.0.2

Функция: Настройка исходящего IP-адреса для отправки пакетов.

3. Настройте параметры запроса IGMP, как показано на рисунке 306.

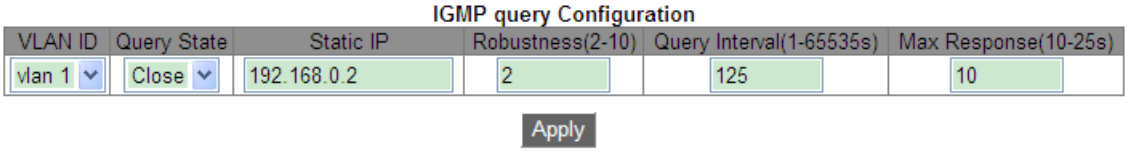


Рисунок 306 Настройка запроса IGMP

VLAN ID

Варианты: Все созданные VLAN ID

Функция: Выбор VLAN ID для включения функции запроса IGMP.

Query State

Варианты: Open/ Close

По умолчанию: Close

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

Предупреждение:

Функции Query и Snooping являются взаимоисключающими в VLAN. Это означает, что если функция Query включена, то функция Snooping должна быть отключена в одной VLAN; если Snooping включена, то Query должна быть отключена.

Static IP

Формат: A.B.C.D

По умолчанию: 192.168.0.2

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

Robustness

Диапазон: 2~10

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.

Query Interval

Диапазон: 1~65535 с

По умолчанию: 125 с

Функция: Настройка интервала отправки пакета запроса.

Max Response

Диапазон: 10~25 с

По умолчанию: 10 с

Функция: Настройка максимального времени ответа на пакет запроса.

После завершения настройки IGMP Configuration показывает информацию о конфигурации IGMP, как показано на рисунке 307.

IGMP Configuration

VLAN ID	Snooping State	Query State	Static IP	Robustness	Query Interval(s)	Max Response(s)
1	Close	Open	192.168.0.2	2	125	10
2	Open	Close	192.168.0.2	0	0	0

Рисунок 307 Конфигурация IGMP

4. Настройте статические параметры многоадресной рассылки IGMP Snooping.

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [IGMP Snooping configuration] → [IGMP Snooping static multicast configuration], чтобы перейти на страницу настройки статических параметров IGMP Snooping, как показано на рисунке 308.

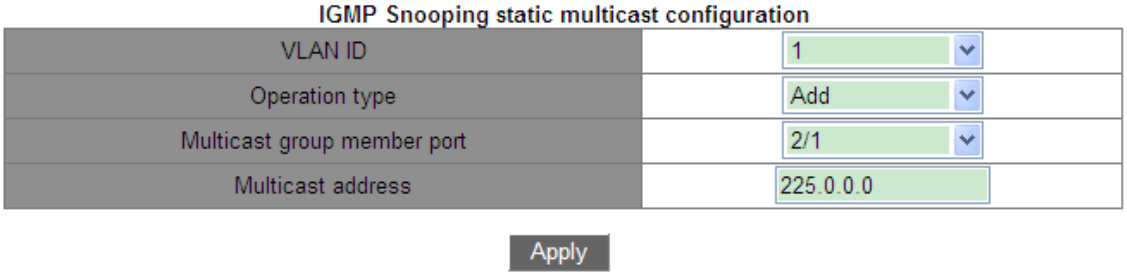


Рисунок 308 Настройка группы многоадресной рассылки IGMP Snooping

VLAN ID

Варианты: все созданные VLAN ID

Operation Type

Варианты: Add/Del

По умолчанию: Add

Функция: Добавить/удалить порт-участник группы многоадресной рассылки.

Multicast group member port

Варианты: все порты коммутатора.

Функция: Выбор порта для добавления в группу или удаления из группы многоадресной рассылки. Если порт подключен к хосту и хост получает данные определенной группы многоадресной рассылки, этот порт можно настроить для присоединения к статической группе многоадресной рассылки, и он станет статическим портом-участником.

Multicast address

Диапазон: 224.0.1.0~239.255.255.255

Функция: Ввод адреса группы многоадресной рассылки.

Описание: Когда вновь добавленный статический адрес многоадресной рассылки изучается динамически, этот

статический адрес многоадресной рассылки будет охватывать динамический адрес многоадресной рассылки.

5. Просмотр записей многоадресной рассылки.

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [IGMP Snooping configuration] → [Show IGMP Snooping information], чтобы отобразить записи многоадресной рассылки, как показано на рисунке 309.

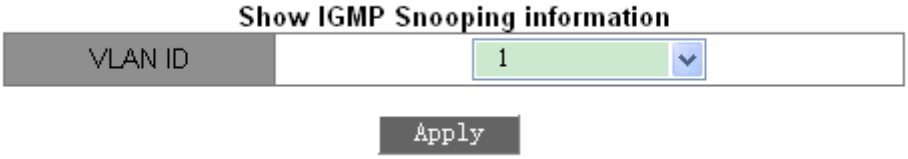


Рисунок 309 Список участников многоадресной рассылки

Просмотр записей многоадресной рассылки в выбранной VLAN.

6.19.5 Пример типового использования

Как показано на рисунке 310, 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.

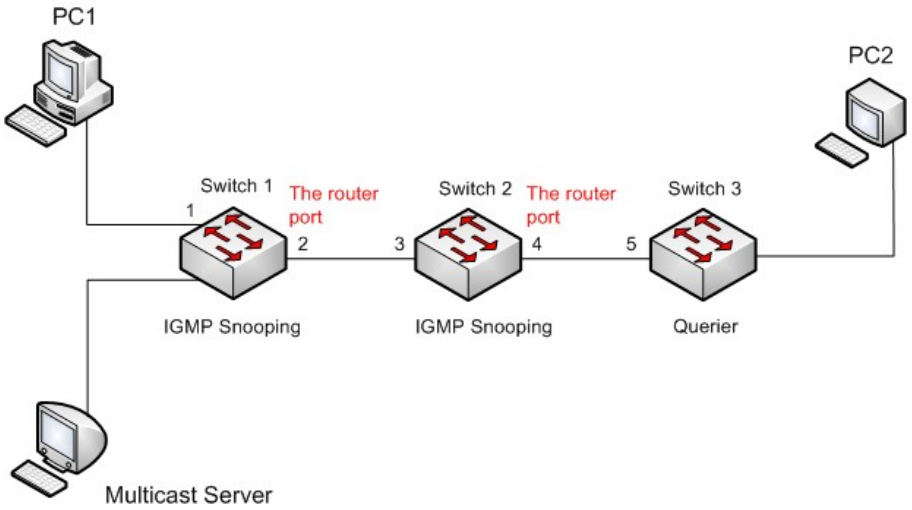


Рисунок 310 Пример использования IGMP Snooping

- 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.

6.20 GMRP

6.20.1 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. 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.

6.20.2 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.

6.20.3 Реализация

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.

6.20.4 Настройка через веб-интерфейс

1. Включите глобальный протокол GMRP.

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [GMRP configuration] → [GMRP configuration], чтобы перейти на страницу настройки GMRP, как показано на рисунке 311.

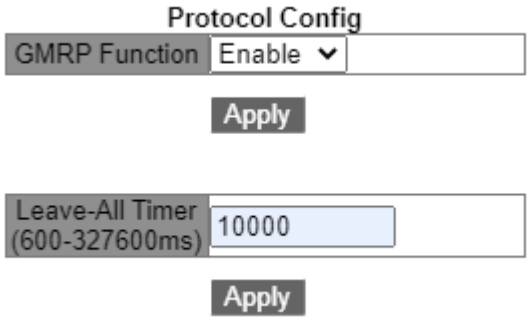


Рисунок 311 Глобальная настройка GMRP

GMRP function

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение глобальной функции GMRP. Функцию нельзя использовать вместе с функцией IGMP Snooping.

Leave-All timer

Диапазон: 600 ~ 327600 мс

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 на порту, как показано на рисунке 312.

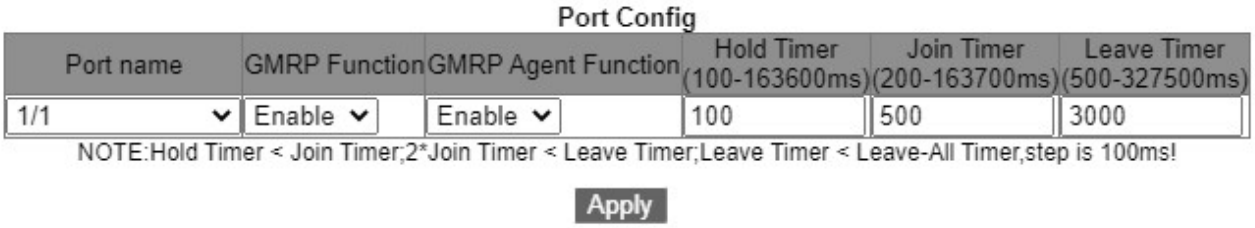


Рисунок 312 Настройка функции GMPR на порту

Port name

Варианты: все порты коммутатора.

GMRP Function

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение функции GMRP на порту.

GMRP Agent Function

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение функции агента GMRP на порту.

Предупреждение:

- Порт агента не может распространять запись агента.
- Предпосылкой включения функции агента GMRP на порте является включение функции GMRP на порту.

Hold Timer

Диапазон: 100-163600 мс

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: 200-163700 мс

По умолчанию: 500 мс

Значение должно быть кратно 100. Лучше установить одинаковое время таймеров Join на всех портах с поддержкой GMRP.

Leave Timer

Диапазон: 500 ~ 327500 мс

По умолчанию: 3000 мс

Значение должно быть кратно 100. Лучше установить одинаковое время таймеров Leave на всех портах с поддержкой GMRP.

3. Добавьте запись агента GMRP.

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [GMRP configuration] → [GMRP agent configuration], чтобы перейти на страницу настройки агента GMRP, как показано на рисунке 313.

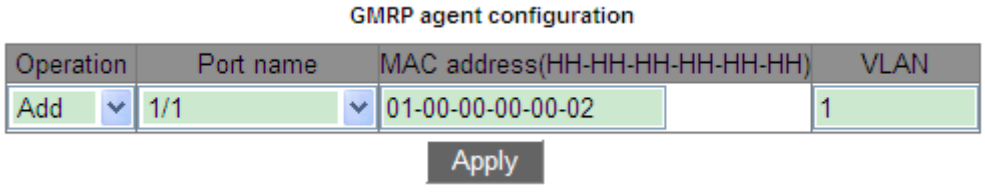


Рисунок 313 Настройка записи агента GMRP

Operation

Варианты: Add/Del

По умолчанию: Add

Функция: Добавление или удаление записи.

Port name

Варианты: все настроенные порты агента

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

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.

4. Просмотрите настройки GMRP.

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [GMRP configuration] → [Show GMRP configuration], чтобы показать настройки GMRP, как показано на рисунке 314.

Information Display

```
---------------- Gmrp Information -----------------
Gmrp status : enable
Gmrp Timers(milliseconds)
LeaveAll    :  10000  [default : 10000]


Interface Ethernet2/1 status    : Gmrp Enable
                                : Gmrp Agent Disable
     Gmrp Timers(milliseconds)
        Hold  :   100  [default :   100]
        Join  :   500  [default :   500]
        Leave :  3000  [default :  3000]

     Gmrp last PDU Origin:
        00-1e-cd-12-4b-63

Interface Ethernet1/1 status    : Gmrp Enable
                                : Gmrp Agent Enable
     Gmrp Timers(milliseconds)
        Hold  :   100  [default :   100]
        Join  :   500  [default :   500]
        Leave :  3000  [default :  3000]

     Gmrp last PDU Origin:
        00-00-00-00-00-00
```

Рисунок 314 Информация о конфигурации GMRP

5. Просмотрите запись агента GMRP.

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [GMRP configuration] → [Show GMRP agent configuration], чтобы показать записи агента GMRP, как показано на рисунке 315.

Information Display

Index	MAC-Address	VLAN	Port(s)
1	01-00-00-00-00-02	1	Ethernet1/1

Рисунок 315 Запись агента GMRP

6. Отображаются участники многоадресной рассылки этой записи агента на подключенном соседнем устройстве, как показано на рисунке 316.

Должны выполняться следующие условия:

- Функция GMRP включена на взаимосвязанных устройствах.
- Два порта, которые соединяют устройства, должны быть портами распространения, а порт распространения на локальном устройстве должен быть в идентификаторе VLAN ID записи агента.

GMRP Dynamic Multicast List

Index	Multicast MAC	VLAN ID	Member Port
1	01-00-00-00-00-02	1	2

Рисунок 316 Динамическая таблица многоадресной рассылки GMRP

GMRP dynamic multicast

Состав: {Index, Multicast MAC, VLAN ID, Member Port}

Функция: Просмотр динамических записей многоадресной рассылки GMRP.

6.20.5 Типовой пример конфигурации

Как показано на рисунке 317, 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.

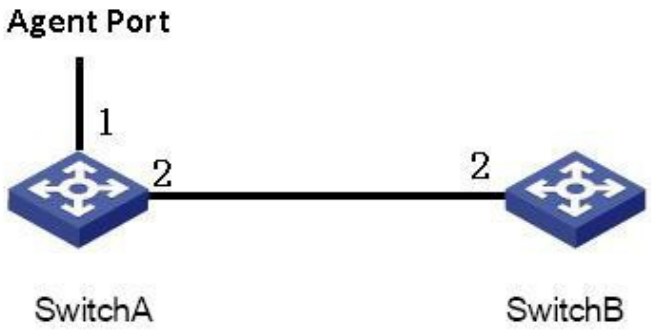


Рисунок 317 Сеть GMRP

Конфигурация коммутатора A:

1. Включите глобальную функцию GMRP на коммутаторе A; установите для таймера LeaveAll значение по умолчанию, как показано на рисунке 311.

2. Включите функцию GMRP и функцию агента на порту 1; включите только функцию GMRP на порту 2; установите таймеры на значения по умолчанию, как показано на рисунке 312.

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 313.

Конфигурация коммутатора B:

4. Включите глобальную функцию GMRP на коммутаторе B; установите для таймера LeaveAll значение по умолчанию, как показано на рисунке 311.

5. Включите функцию GMRP на порту 2; установите таймеры на значения по умолчанию, как показано на рисунке 312. В таблице 12 перечислены динамически полученные записи многоадресной рассылки GMRP на коммутаторе B.

Таблица 12 Динамические записи многоадресной рассылки

Атрибуты порта 2 коммутатора A	**Атрибуты порта 2 коммутатора A**	**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=2	Access VID=2	MAC: 01-00-00-00-00-01 VLAN ID: 2 Порт-участник 2

6.21 Настройка IGMP

6.21.1 Введение

Протокол Internet Group Management Protocol (IGMP) — это протокол для управления членством в группах многоадресной рассылки. Он работает в конце сети, устанавливает и поддерживает членство в группе многоадресной рассылки между хостом IP и соседними маршрутизаторами многоадресной рассылки.

Есть три версии протокола IGMP: IGMPv1, IGMPv2 и IGMPv3. Это устройство не поддерживает IGMPv3.

Основные различия между IGMPv1 и IGMPv2 состоят в следующем:

(1) IGMPv2 использует формальный механизм выбора запрашивающего, который выбирает маршрутизатор с более низким IP-адресом в качестве запрашивающего. IGMPv1 не имеет механизма выбора запрашивающего. Различные протоколы маршрутизации используют разные механизмы выбора.

(2) IGMPv2 добавляет сообщение Leave Group. Когда хост покидает группу, хост активно отправляет пакет Leave Group. IGMPv1 не отправляет активно пакет Leave Group.

(3) Max Resp Time: новое поле, добавленное в пакеты Query. Параметр указывает допустимое максимальное время ответа, установленное источником запроса. Значение по умолчанию – 10 секунд.

(4) Сообщение Group-Specific Query: Запрашивающему разрешено выполнять операцию запроса для указанной группы, а не для всех групп, отправив сообщение Group-Specific Query.

Примечание:

В этой главе под маршрутизаторами понимаются коммутаторы уровня Layer-3.

6.21.2 Принцип работы

Далее используется IGMPv2 в качестве примера для описания механизма реализации IGMP.

(1) Механизм выбора источника запроса: Все маршрутизаторы IGMPv2 изначально считают себя источниками запроса и отправляют пакет Query. Когда маршрутизатор получает пакет запроса от маршрутизатора, чей IP-адрес меньше, чем его IP-адрес, он отказывается от роли запрашивающего и становится не запрашивающим. Маршрутизатор с наименьшим IP-адресом в конечном итоге выбирается в качестве запрашивающего.

Пакет General Query: Запрашивающий периодически отправляет пакет General Query, чтобы проверить, есть ли порты-участники в группе многоадресной рассылки. IP-адрес назначения пакета всегда 224.0.0.1.

Пакет Membership Report: Когда хост в группе получает пакет Query, он возвращает пакет ответа участника. Когда хост хочет присоединиться к группе, он активно отправляет пакет IGMP Report запрашивающему, чтобы присоединиться к группе многоадресной рассылки, в которой заинтересован хост.

Механизм подавления участника: Когда хост получает пакет Query, он запускает таймер задержки ответа со значением в диапазоне от 0 до D (максимальное значение). Когда таймер хоста истекает раньше других таймеров хостов в том же сегменте сети, хост

отправляет пакет Membership Report. При получении пакета Membership Report другие хосты останавливают свои таймеры и не генерируют пакет Membership Report. Этот процесс называется механизмом подавления участника.

(3) Механизм выхода: Когда хост намеревается покинуть группу многоадресной рассылки, он отправляет пакет Leave Group с IP-адресом назначения 224.0.0.2.

Пакет Group-Specific Query: Хост отправляет пакет Leave Group при выходе из группы многоадресной рассылки. После получения от хоста пакета Leave Group запрашивающий отправляет пакет Group-Specific Query, чтобы проверить, является ли хост последним участником группы многоадресной рассылки. Если запрашивающий получает пакеты Report от других членов группы, он продолжает поддерживать группу многоадресной рассылки. В противном случае запрашивающий прекращает пересылку данных в группу многоадресной рассылки.

Запращивающий

Query interval: 125 с, интервал времени для отправки пакета General Query.

Last Listener Query Interval: Значение Max Resp Time в пакете Group-Specific Query, то есть интервал передачи. Значение по умолчанию 1 с.

Query Response Interval: Значение Max Resp Time в пакете General Query. Значение по умолчанию 10 с. Хост, получивший пакет General Query, должен дать ответ в течение этого интервала. Значение должно быть меньше интервала запроса.

6.21.3 Настройка через веб-интерфейс

1. Включите протокол IGMP

IGMP запускается вместе с запуском Protocol Independent Multicast (PIM). Его нельзя запустить отдельно.

По умолчанию: Disable

2. Настройте параметры группы IGMP

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [IGMP configuration] → [IGMP group parameter configuration], как показано на рисунке 318.

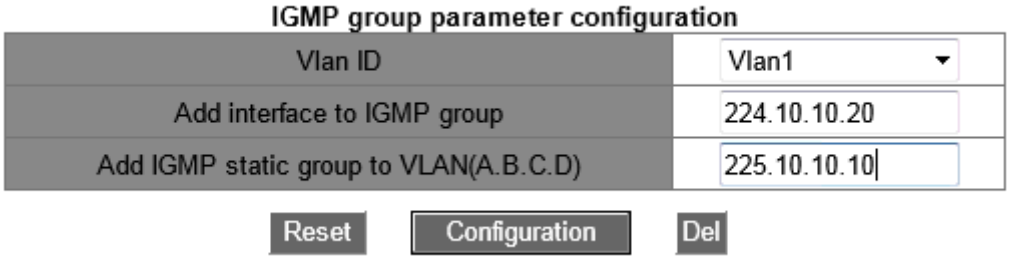


Рисунок 318 Настройка параметров группы IGMP

Vlan ID

Варианты: Созданный интерфейса VLAN Layer-3

По умолчанию: Vlan 1

Функция: Выбор интерфейса VLAN Layer-3 для добавления в группу многоадресной рассылки.

Add interface to IGMP group

Формат: A.B.C.D

Функция: Указать IP-адрес группы многоадресной рассылки, в которую необходимо добавить коммутатор, и добавить интерфейс 3-го уровня коммутатора в группу многоадресной рассылки с указанным адресом многоадресной рассылки. По умолчанию для группы многоадресной рассылки не определен ни один участник многоадресной рассылки.

Add IGMP static group to VLAN(A.B.C.D)

Формат: A.B.C.D

Функция: Указать IP-адрес группы многоадресной рассылки, в которую необходимо статически добавить интерфейс Layer-3 коммутатора.

3. Настройте параметры запроса IGMP

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [IGMP configuration] → [IGMP query parameter configuration], как показано на рисунке 319.

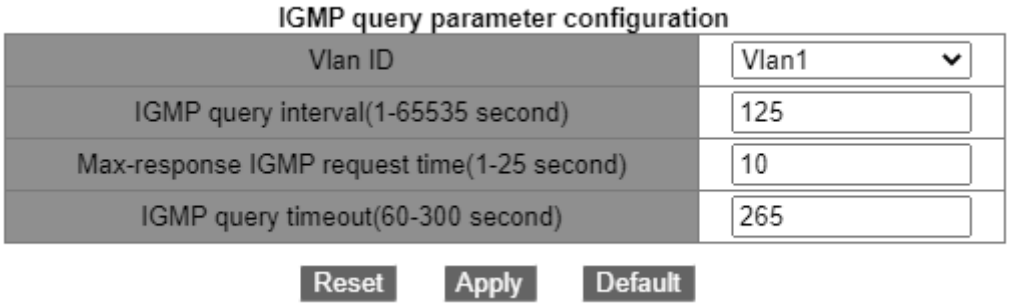


Рисунок 319 Настройка параметров запроса IGMP

Vlan ID

Варианты: Созданный интерфейс Layer-3 VLAN

По умолчанию: Vlan 1

Функция: Выбор интерфейса VLAN Layer-3 для настройки.

Настройте интервал запросов для источника запросов IGMP для периодической отправки сообщений Query (1-65535 с)

Диапазон：1~65535 с

По умолчанию: 125 с

Функция: Настройка интервала запросов для источника запросов IGMP для периодической отправки сообщений Query.

Настройте максимальное время ответа интерфейса на пакеты запросов IGMP (1-25 с)

Диапазон: 1-25 с

По умолчанию: 10 с

Функция: Настройте максимальное время ответа интерфейса на пакеты запросов IGMP.

Описание：Когда хосты желают присоединиться к группе многоадресной рассылки, хост, который первым отвечает на пакет запроса от запрашивающего и желает

присоединиться к группе многоадресной рассылки, должен отправить запрашивающему пакет отчета об участии в течение максимального времени ответа. Это максимальное время ответа является максимальным временем запроса. Если хост не может отправить пакет Membership Report в течение максимального времени запроса, запрашивающий считает, что ветвь, в которой находится хост, пуста, и эта ветвь будет удалена.

Настройте время ожидания пакетов запросов IGMP для интерфейса (60-300 с)

Диапазон: 60 ~300 с

По умолчанию: 265 с

Функция: Настройка времени ожидания пакетов запросов IGMP для интерфейса.

Описание: Если не запрашивающему не удается получить пакет Query от запрашивающего в течение определенного интервала, интерфейс на не запрашивающем устройстве автоматически становится запрашивающим. Этот интервал называется таймаутом. Как правило, таймаут равен удвоенному интервалу запроса плюс максимальное время ответа.

4. Настройка версии IGMP

Щелкните[Device Advanced Configuration] → [Multicast protocol configuration] → [IGMP configuration] → [IGMP version configuration], как показано на рисунке 304.

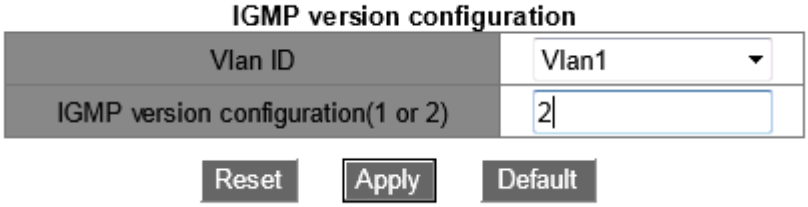


Рисунок 320 Настройка версии IGMP

Vlan ID

Варианты: Созданный интерфейса VLAN Layer-3

По умолчанию: Vlan 1

Функция: Выбор интерфейса VLAN Layer-3 для настройки.

IGMP version configuration (1 or 2)

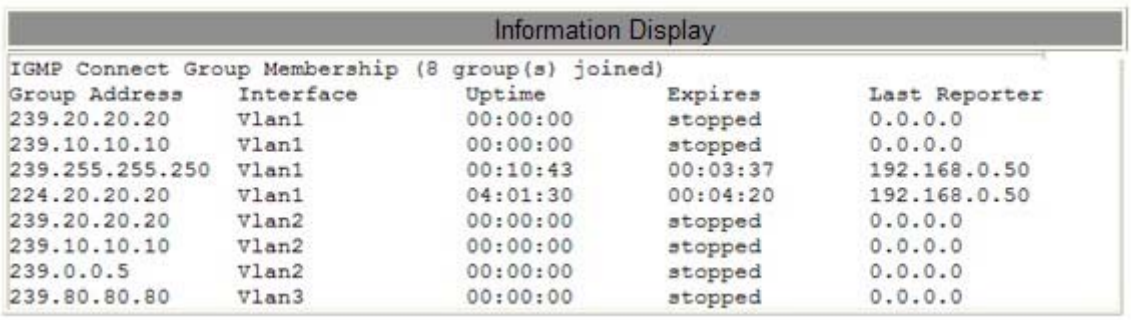
Варианты: 1~2

По умолчанию: версия 2

Функция: Настройка интерфейса Layer-3 для запуска версии 1 или версии 2.

5. Показ групп IP IGMP

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [IGMP configuration] → [show ip igmp groups], как показано на рисунке 321.



Information Display

IGMP Connect Group Membership (8 group(s) joined)

Group Address	Interface	Uptime	Expires	Last Reporter
239.20.20.20	Vlan1	00:00:00	stopped	0.0.0.0
239.10.10.10	Vlan1	00:00:00	stopped	0.0.0.0
239.255.255.250	Vlan1	00:10:43	00:03:37	192.168.0.50
224.20.20.20	Vlan1	04:01:30	00:04:20	192.168.0.50
239.20.20.20	Vlan2	00:00:00	stopped	0.0.0.0
239.10.10.10	Vlan2	00:00:00	stopped	0.0.0.0
239.0.0.5	Vlan2	00:00:00	stopped	0.0.0.0
239.80.80.80	Vlan3	00:00:00	stopped	0.0.0.0

Рисунок 321 Информация групп IP IGMP

Как показано на рисунке 321, в таблице 23 представлены поля выходных сообщений.

Таблица 23 Сообщения IGMP

Group Address	IP-адрес группы многоадресной рассылки
Interface	Интерфейс VLAN Layer-3 на коммутаторе, через который проходит пакет, предназначенный для группы многоадресной рассылки.
Uptime	Прошедшее время поддержания активности группы многоадресной рассылки, представленное в формате чч:мм:сс.
Expires	Оставшееся время поддержания активности группы многоадресной рассылки, представленное в формате чч:мм:сс. Stopped означает, что время ожидания группы многоадресной рассылки никогда не истекает.
Last Reporter	IP-адрес хоста, который последним присоединяется к группе многоадресной рассылки.

6. Показ интерфейса IP IGMP

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [IGMP configuration] → [show ip igmp interface], как показано на рисунке 322.

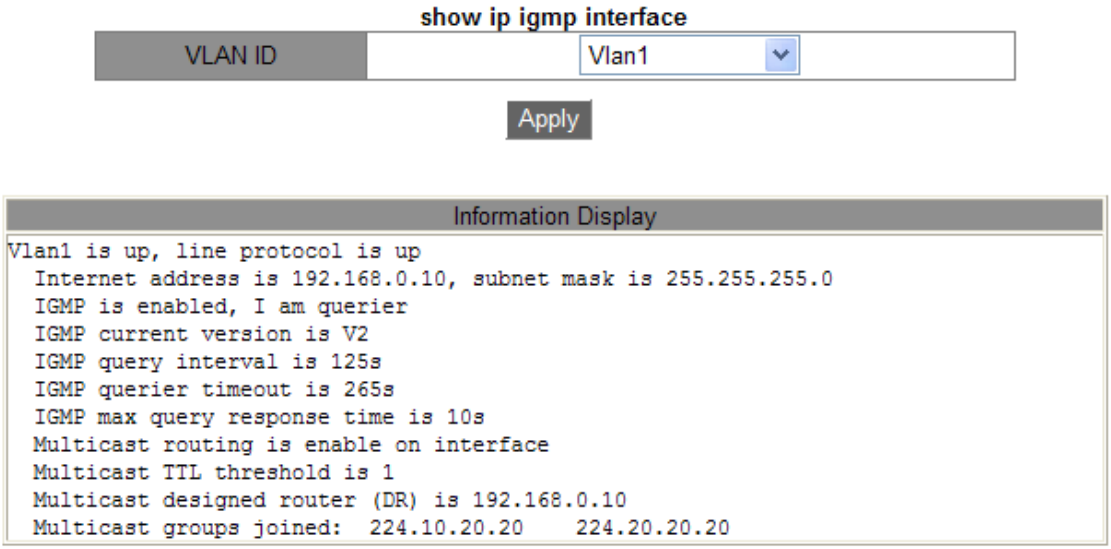


Рисунок 322 Информация интерфейса IP IGMP

Vlan ID

Варианты: Созданный интерфейса VLAN Layer-3

По умолчанию: Vlan 1

Функция: Выбор интерфейса VLAN Layer-3 для просмотра.

Information Display

Информацию интерфейса IP IGMP можно отобразить, щелкнув <Apply>.

6.22 Настройка PIM

Protocol Independent Multicast (PIM), выполняет проверку Reverse Path Forwarding (RPF) для многоадресных пакетов с использованием существующей таблицы маршрутизации одноадресной рассылки, чтобы создать записи маршрутизации многоадресной рассылки и сформировать дерево переадресации многоадресной рассылки. PIM поддерживает два режима: PIM – Dense Mode (PIM-DM) и PIM – Sparse Mode (PIM-SM).

Примечание:

В этой главе под маршрутизаторами понимаются коммутаторы уровня Layer-3.

6.22.1 Настройка PIM-DM

6.22.1.1 PIM-DM. Введение

PIM-DM (PIM Dense Mode) использует режим Push для передачи многоадресных данных и обычно применяется к небольшим сетям с относительно высокой плотностью участников групп многоадресной рассылки.

Основные принципы PIM-DM следующие:

PIM-DM предполагает, что в каждой подсети сети существует по крайней мере один участник группы многоадресной рассылки, поэтому данные многоадресной рассылки будут рассылаться на все узлы в сети. Затем PIM-DM удаляет ветвь без пересылки многоадресных данных, оставляя только ветвь, содержащую получателя. Это явление Flooding-pruning (наполнение-отсечение) происходит периодически, и обрезанные ветви также могут периодически восстанавливаться до состояния пересылки.

Когда участник группы многоадресной рассылки появляется на узле, подлежащем сокращению, PIM-DM использует механизм Graft для активного возобновления пересылки многоадресных данных, чтобы сократить время, необходимое узлу для возврата в состояние пересылки.

Как правило, путь пересылки пакета данных в плотном режиме представляет собой дерево источника (Source Tree) –дерево пересылки, в котором источник многоадресной рассылки является «корнем», а участник группы многоадресной рассылки — «листом». Поскольку Source Tree использует кратчайший путь от источника многоадресной рассылки к получателю, оно также называется деревом кратчайшего пути Shortest Path Tree (SPT).

6.22.2 Настройка через веб-интерфейс

1. Включите GVRP

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [PIM-DM configuration] → [Enable PIM-DM], чтобы перейти на страницу настройки PIM-DM, как показано на рисунке 323.

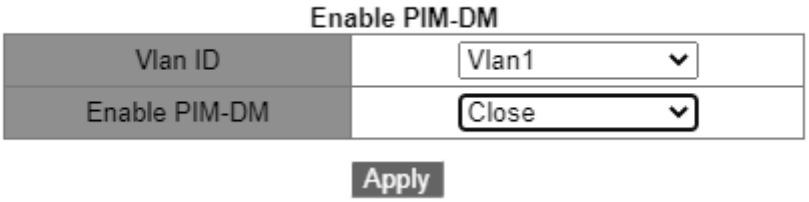


Рисунок 323 Включение PIM-DM

Vlan ID

Варианты: Созданный интерфейс Layer-3 VLAN

По умолчанию: Vlan 1

Enable PIM-DM

Варианты: enable/Close

По умолчанию：Close

Функция: включение функции PIM-DM для интерфейса Layer-3

6.22.3 PIM-SM. Введение

PIM-SM использует режим "pull" для формирования дерева многоадресной пересылки между приемниками данных и передатчиком в соответствии с требованиями получателей данных.

Дерево пересылки PIM-SM формируется в два этапа: Шаг 1: Создайте дерево переадресации, состоящее из дерева Rendezvous Point Tree (RPT) и дерева Shortest Point Tree (SPT) с центром в точке Rendezvous Point (RP). Шаг 2: Переключитесь на SPT, сформированное между приемниками данных и передатчиком.

Дерево пересылки PIM-SM формируется с центром в RP. Источник многоадресной

рассылки передает данные на RP по SPT, а RP пересылает данные многоадресной рассылки получателям по RPT.

6.22.4 Основная концепция

RP — очень важный маршрутизатор в дереве пересылки PIM-SM. Он объединяет сообщения Prune/Join получателей, а также многоадресные данные источника многоадресной рассылки.

RPT: формирует дерево пересылки между получателями и RP, которое также называется деревом пересылки RPT.

Маршрутизатор Bootstrap Router (BSR) в основном распространяет позицию RP и соответствующую информацию на маршрутизаторы в сети. Кандидаты BSR (C-BSR) и RP (C-PR) настраиваются сетевыми администраторами, и можно настроить один или несколько C-BSR и C-PR. C-BSR с более высоким приоритетом в конечном счете выбирается в качестве подлинного BSR.

6.22.5 Принцип работы PIM-SM

Механизм регистрации:

BSR отправляет информацию о местоположении RP по всей сети PIM-SM в многоадресном режиме. Следовательно, источник многоадресной рассылки знает положение RP. Когда источник многоадресной рассылки имеет многоадресные данные для пересылки, он инкапсулирует данные в регистрационный пакет и отправляет его соответствующему RP в одноадресном режиме. RP декапсулирует многоадресные данные из регистрационного пакета и направляет их получателям.

Механизм остановки регистрации:

При получении регистрационного пакета от источника многоадресной рассылки RP знает IP-адрес источника многоадресной рассылки. Поэтому RP отправляет пакет Join (S,G) источнику многоадресной рассылки S.

Когда пакет перенаправляется на назначенный маршрутизатор (DR) источника многоадресной рассылки шаг за шагом, запись (S,G) устанавливается на всех маршрутизаторах, через которые проходит пакет, и дерево пересылки SPT от RP к

источнику многоадресной рассылки S сформировано. Источник многоадресной рассылки использует дерево пересылки SPT для отправки данных многоадресной рассылки на RP.

При получении данных многоадресной рассылки от источника многоадресной рассылки RP отправляет пакет остановки регистрации источнику многоадресной рассылки, чтобы уведомить источник многоадресной рассылки не инкапсулировать данные многоадресной рассылки в пакеты регистрации, а передавать данные многоадресной рассылки напрямую. Этот процесс называется механизмом остановки регистрации.

Коммутация SPT:

Когда источник многоадресной рассылки находится далеко от RP, но близко к получателям, если источник многоадресной рассылки все еще использует RP для пересылки данных, задержка получателя будет увеличена. Решением этой проблемы является механизм коммутации SPT.

Когда DR приемника получает данные многоадресной рассылки, он считает, что данные пересылаются по пути от источника многоадресной рассылки к DR, а затем к получателю. Следовательно, DR отправляет пакет Join (S,G) источнику многоадресной рассылки S, и запись (S,G) устанавливается на всех маршрутизаторах, через которые проходит пакет. Когда пакет соединения (S,G) достигает источника многоадресной рассылки S шаг за шагом, между приемниками и DR источника многоадресной рассылки формируется дерево пересылки SPT.

Когда получатель получает многоадресные данные, пересылаемые по дереву переадресации SPT, он отправляет пакет Prune на RP, чтобы уведомить RP о том, что многоадресные данные были перенаправлены от источника многоадресной рассылки к получателю по дереву переадресации SPT и дерево пересылки RPT не требуется. Маршрутизаторы, через которые проходит пакет Prune, удаляют исходящий интерфейс, соответствующий записи (S,G), и обновляют запись (*,G).

Коммутация SPT не является обязательной. Маршрутизатор многоадресной рассылки может выбрать, использовать ли SPT или RPT для пересылки данных.

6.22.6 Настройка через веб-интерфейс

1. Включите GVRP

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [PIM-SM configuration] → [Enable PIM-SM], чтобы перейти на страницу настройки PIM-SM, как показано на рисунке 324.

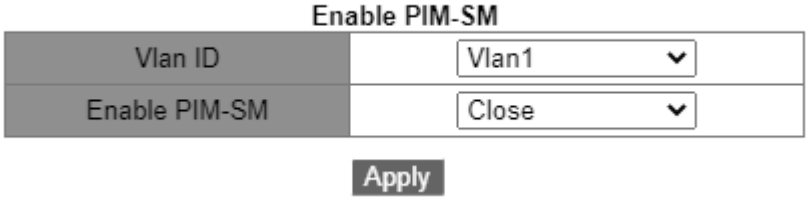


Рисунок 324 Включение PIM-SM

Vlan ID

Варианты: Созданный интерфейс Layer-3 VLAN

По умолчанию: Vlan 1

Start PIM-SM

Варианты: enable/Close

По умолчанию: /Close

Функция: включение функции PIM-SM для интерфейса Layer-3

2. Настройте интерфейс в качестве граничного PIM-SM BSR

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [PIM-SM configuration] →[Set interface as PIM-SM BSR border], чтобы перейти на страницу настройки граничного PIM-SM BSR, как показано на рисунке 325.

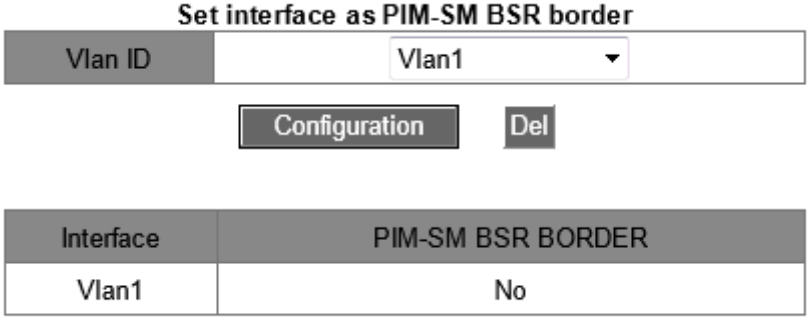


Рисунок 325 Настройка граничного PIM-SM BSR

Vlan ID

Варианты: Созданный интерфейс Layer-3 VLAN

По умолчанию: Vlan 1

Функция：настройка интерфейса Layer-3, который присоединился к сети PIM-SM, в качестве граничного PIM-SM BSR.

Примечание:

После настройки интерфейса VLAN уровня 3 в качестве граничного BSR этот интерфейс будет блокировать распространение сообщений BSR.

3. Настройте маршрутизатор в качестве кандидата BSR

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [PIM-SM configuration] → [Set router as BSR candidate], чтобы перейти на страницу настройки кандидата BSR, как показано на рисунке 326.

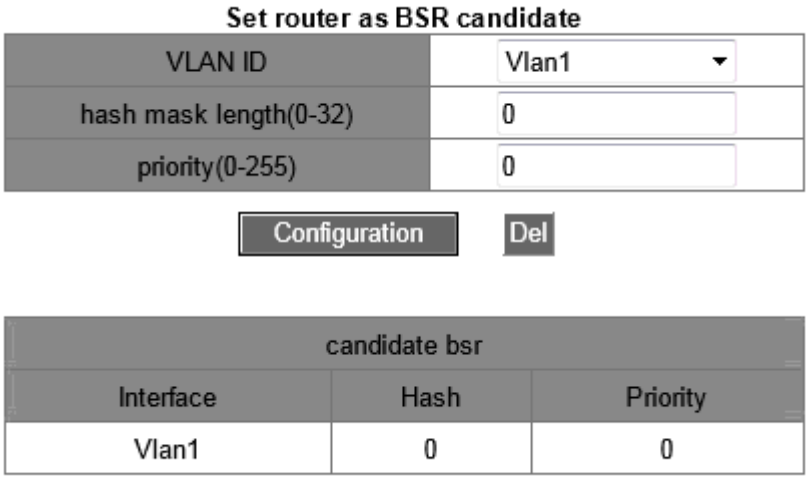


Рисунок 326 Настройка кандидата BSR

Vlan ID

Варианты: Созданный интерфейс Layer-3 VLAN

По умолчанию: Vlan 1

Функция：Настроить IP-адрес интерфейса VLAN 3 уровня как IP-адрес C-BSR, чтобы отправлять

сообщения BSR всем соседям PIM интерфейса.

hash mask length (0-32)

Диапазон: 0~32

По умолчанию: 0

Функция: настройка длины хэш-маски. Длина хэш-маски — это число бывших битов в хэш-маске, которые будут использоваться в операции И с адресом многоадресной рассылки.

priority (0-255):

Диапазон :0~255

По умолчанию: 0

Функция: настройка приоритета кандидата BSR

Примечание :

- Все многоадресные группы с одинаковой длиной хэш-маски взаимодействуют с одним итем же RP. Например, если длина хэш-маски установлена равной 20, группы многоадресной рассылки с одинаковыми прежними 20 битами в своих многоадресных адресах используют один и тот же RP.
- Большее значение приоритета указывает на более низкий приоритет. C-BSR с более высоким приоритетом является подлинным BSR. Если C-BSR имеют одинаковый приоритет, C-BSR с наивысшим IP-адресом является подлинным BSR.

4.Настройте маршрутизатор в качестве кандидата RP

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [PIM-SM configuration] →[Set router as RP candidate], чтобы перейти на страницу настройки кандидата RP, как показано на рисунке 327.

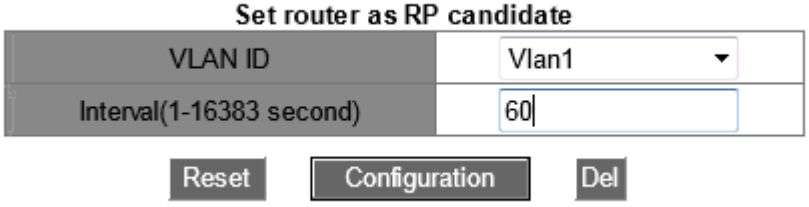


Рисунок 327 Настройка кандидата RP

Vlan ID

Варианты: Созданный интерфейс Layer-3 VLAN

По умолчанию: Vlan 1

Функция：Настроить IP-адрес интерфейса VLAN 3 уровня как IP-адрес C-RP. Этот IP-адрес будет использоваться для получения пакетов регистрации и пакетов Join/Prune, а также для создания деревьев пересылки.

Interval(1-16383 second)

Диапазон: 1~16383 с

По умолчанию: 60 с

Функция: Интервал отправки C-BSR пакетов уведомлений в BSR.

6.22.7 Типовой пример конфигурации

Как показано на рисунке 328, маршрутизаторы Router1, Router2, Router3, Router4 могут поддерживать протокол PIM-SM, S означает источник, а R означает приемники.

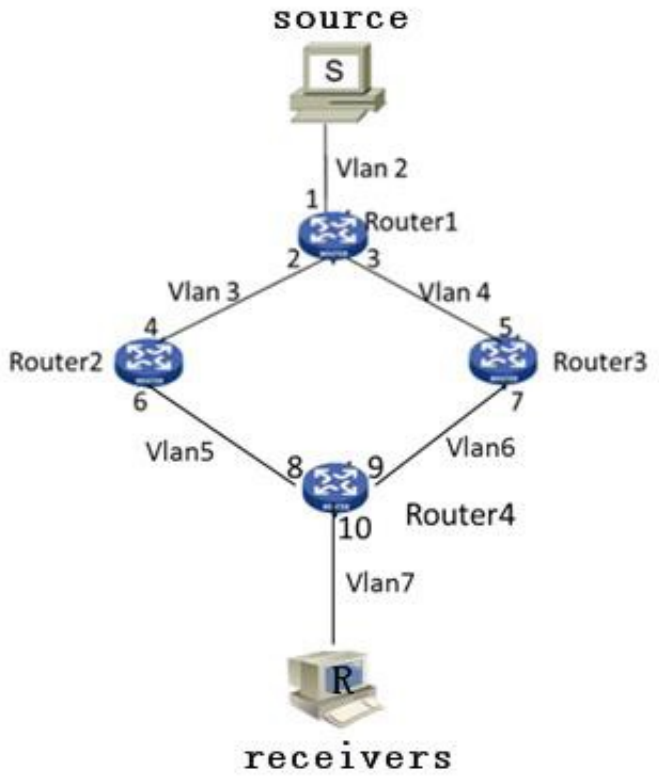


Рисунок 328 Пример PIM SM

1. Настройте идентификаторы маршрутизатора и включите протокол Open Shortest Path First (OSPF). Подробную информацию о процессе настройки см. в разделе 6.12.3 «Настройка OSPF».

2. Настройка маршрутизатора Router1:

- Создайте VLAN 2, VLAN 3 и VLAN 4 и добавьте порт 1 к VLAN 2, порт 2 к VLAN 3 и порт 3 к VLAN 4. Подробную информацию о процессе настройки см. в разделе 5.4 «Настройка VLAN».

- Настройте интерфейсы уровня 3. Установите IP-адрес интерфейса Layer-3 порта 1 20.0.0.2, IP-адрес интерфейса Layer-3 порта 2 – 30.0.0.2 и IP-адрес интерфейса Layer-3 порта 3 – 40.0.0.4. Подробную информацию о процессе настройки см. в разделе 6.2 «Настройка интерфейса L3».

- Включите PIM-SM, как показано на рисунке 324. Включите PIM-SM на каждом созданном интерфейсе VLAN Layer-3 и настройте интервал запроса пакетов, как показано на рисунке 330.

3. Настройка маршрутизатора Router2:

- Создайте VLAN 3, VLAN 5 и добавьте порт 4 к VLAN 3, порт 6 к VLAN 5.

- Настройте интерфейсы Layer-3. Установите IP-адрес интерфейса Layer-3 порта 4 30.0.0.4, IP-адрес интерфейса Layer-3 порта 6 – 50.0.0.4.

- Включите PIM-SM, как показано на рисунке 324, включите PIM-SM на каждом созданном интерфейсе VLAN Layer-3 и настройте интервал запроса пакетов, как показано на рисунке 330.

4. Настройка маршрутизатора Router3:

- Создайте VLAN 4, VLAN 6 и добавьте порт 5 к VLAN 4, порт 7 к VLAN 6.

- Настройте интерфейсы Layer-3. Установите IP-адрес интерфейса Layer-3 порта 5 30.0.0.4, IP-адрес интерфейса Layer-3 порта 7 – 60.0.0.4.

- Включите PIM-SM, как показано на рисунке 324, включите PIM-SM на каждом созданном интерфейсе VLAN Layer-3 и настройте интервал запроса пакетов, как показано на рисунке 330.

5. Настройка маршрутизатора Router4:

- Создайте VLAN 5, VLAN 6 и VLAN 7 и добавьте порт 8 к VLAN 5, порт 9 к VLAN 6 и порт 10 к VLAN 7.

- Настройте интерфейсы уровня 10. Установите IP-адрес интерфейса Layer-3 порта 8 50.0.0.8, IP-адрес интерфейса Layer-3 порта 9 – 60.0.0.9 и IP-адрес интерфейса Layer-3 порта 10 – 70.0.0.10.

- Включите PIM-SM, как показано на рисунке 324, включите PIM-SM на каждом созданном интерфейсе VLAN Layer-3 и настройте интервал запроса пакетов, как показано на рисунке 330.

6. Настройте граничный BSR (не обязательно), как показано на рисунке 325. Настройте интерфейс Layer-3 как граничный PIM-SM BSR.

7. Настройте C-BSR, как показано на рисунке 326, установите порт 2 Router1 как C-BSR, значение приоритета по умолчанию равным 0 и значение длины хэш-маски по умолчанию равным 0.

8. Настройте C-RP, как показано на рисунке 327, установите порт 4 Router1 и порт 5 Router3 как C-RP, значение интервала запросов 60 секунд.

Примечание:

- Router 1, Router 2 и Router 3 могут быть настроены как C-BSR, подлинный BSR может быть определен путем выбора, или конкретный маршрутизатор может быть указан как BSR.
- После настройки интерфейса в качестве граничного BSR этот интерфейс будет блокировать получение или передачу сообщений BSR. Нужно настроить границу BSR только на интерфейсе, который должен блокировать сообщения BSR. Границу BSR не нужно настраивать для всех маршрутизаторов.

6.23 Общая настройка многоадресной рассылки

6.23.1 DR. Введение

Маршрутизатор Designated Router (DR) является единственным ретранслятором многоадресных данных в общей сети. DR должен быть выбран независимо от того, подключен ли он к источнику многоадресной рассылки или к получателям. В режиме PIM-SM пакеты Hello маршрутизаторов PIM сравниваются для выбора маршрутизатора PIM с наивысшим приоритетом в качестве DR.

DR на стороне источника многоадресной рассылки в основном отправляет пакеты регистрации и данные многоадресной рассылки, а DR на принимающей стороне отправляет пакеты IGMP Join к RP.

6.23.2 Настройка через веб-интерфейс

1. Задайте приоритет DR

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [Multicast common configuration] → [Set DR priority], чтобы перейти на страницу настройки приоритета DR, как показано на рисунке 329.

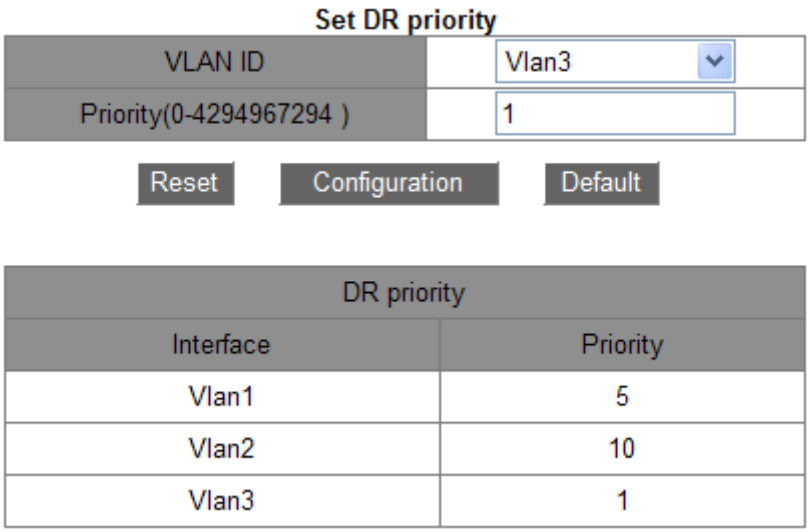


Рисунок 329 Настройка приоритета DR

Vlan ID

Варианты: Созданный интерфейса VLAN Layer-3

По умолчанию: Vlan 1

Функция: Выбор интерфейса VLAN Layer-3 для настройки.

Priority (0-4294967294)

Варианты: 0-4294967294

По умолчанию: 1

Функция: Настройка приоритета выбранного интерфейса VLAN Layer-3.

Default

Щелкните **Default,** чтобы восстановить значение настройки приоритета по умолчанию.

DR priority

Отображение приоритета интерфейса VLAN Layer-3.

2. Настройка интервала запроса PIM Hello

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [Multicast common configuration] → [PIM Hello Query-Interval configuration], чтобы перейти на страницу настройки интервала запроса PIM Hello, как показано на рисунке 330.

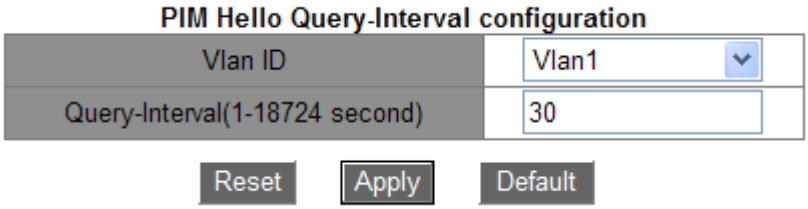


Рисунок 330 Настройка интервала запроса PIM Hello

Vlan ID

Варианты: Созданный интерфейса VLAN Layer-3

По умолчанию: Vlan 1

Query-Interval(1-18724 秒)

Варианты: 1~18724 с

По умолчанию: 30 с

Функция: Настройка интервала для интерфейса Layer-3 для передачи пакетов

Hello, чтобы обнаружить смежные маршрутизаторы PIM.

3. Отображение IP Mroute

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [Multicast common configuration] → [show ip mroute], чтобы просмотреть IP Mroute, как показано на рисунке 331.

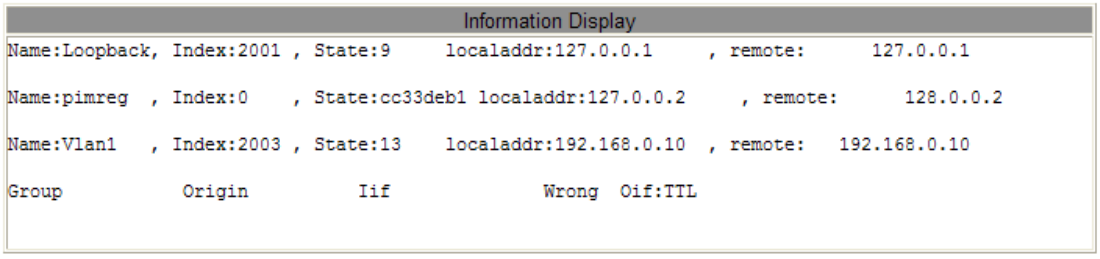


Рисунок 331 Отображение IP Mroute

6.24 Проверка и отладка

Команды проверки и отладки в основном используются для отображения конфигурации PIM коммутатора.

1. Просмотр информации об IP-интерфейсе PIM

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [Inspect and debug] → [show ip pim interface], чтобы просмотреть IP-интерфейс PIM, как показано на рисунке 332.

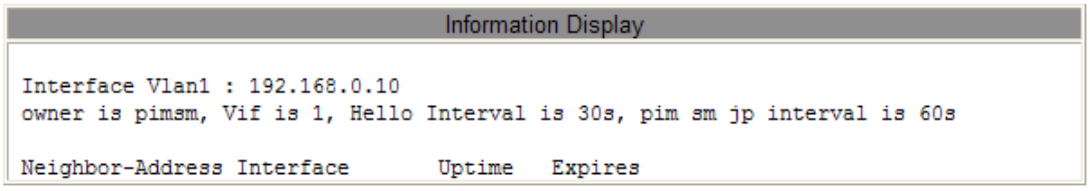


Рисунок 332 Информация интерфейса IP PIM

2. Просмотр информации о соседе IP PIM

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [Inspect and debug] → [show ip pim neighbor], чтобы просмотреть соседнее устройство IP PIM, как показано на рисунке 333.

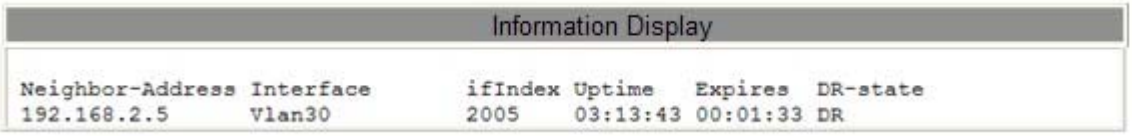


Рисунок 333 Информация о соседе IP PIM

3. Просмотр информации о маршрутизаторе BSR IP PIM

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [Inspect and debug] → [show ip pim bsr-router], чтобы просмотреть информацию о маршрутизаторе BSR IP PIM, как показано на рисунке 334.

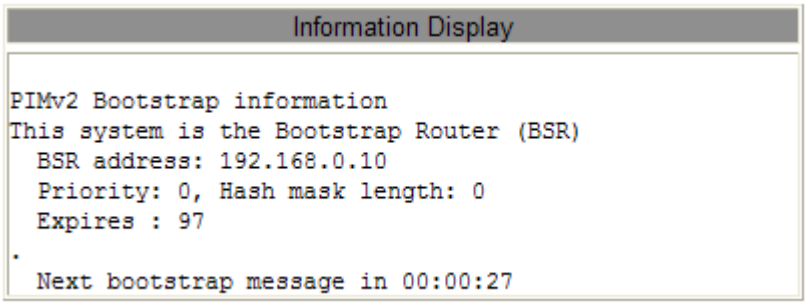


Рисунок 334 Информация о маршрутизаторе BSR IP PIM

4. Просмотр информации об IP PIM Mroute SM

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [Inspect and debug] → [Show ip pim mroute sm], чтобы просмотреть информацию об IP PIM Mroute SM, как показано на рисунке 335.

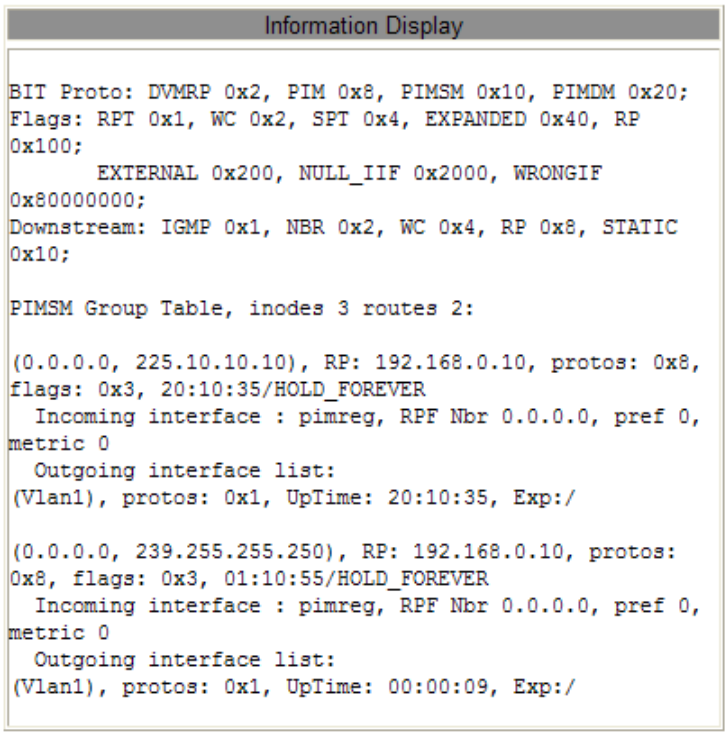


Рисунок 335 Информация об IP PIM Mroute SM

Примечание:

Записи маршрутизации PIM-SM генерируются из-за запуска многоадресных потоков данных.

5. Просмотр IP-адреса RP для группы многоадресной рассылки

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [Inspect and debug] → [Show ip pim rp], чтобы просмотреть IP-адрес RP, как показано на рисунке 336.

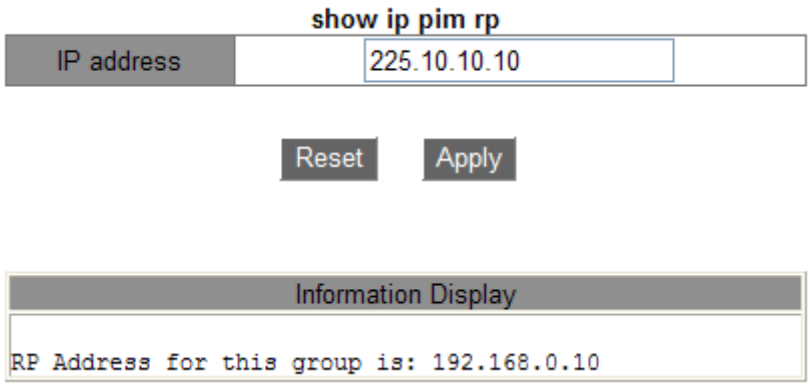


Рисунок 336 Информация RP

IP Address

Вариант: IP-адрес группы многоадресной рассылки

Функция: Введите IP-адрес группы многоадресной рассылки и щелкните <Apply>, отобразится IP-адрес RP для этой многоадресной группы. Если группа многоадресной рассылки не существует, отображается информация о том, что эта группа недоступна.

6. Просмотр информации о сопоставлении IP PIM RP

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [Inspect and debug] → [Show ip pim rp mapping], чтобы просмотреть информацию о сопоставлении IP PIM RP, как показано на рисунке 337.

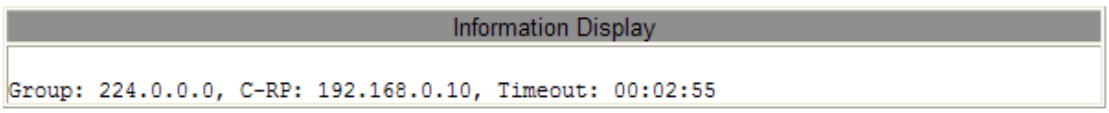


Рисунок 337 Информация о сопоставлении IP PIM RP

6.25 Настройка обработки незарегистрированных потоков многоадресной рассылки

6.25.1 Введение

Незарегистрированные многоадресные пакеты относятся к многоадресным пакетам без соответствующих записей о пересылке на коммутаторе. При получении незарегистрированного многоадресного пакета коммутатор транслирует пакет в пределах VLAN (все порты, кроме входного). Это требует значительной полосы пропускания сети, что влияет на скорость передачи. В этом случае может быть включена функция отбрасывания незарегистрированных пакетов многоадресной рассылки. Если функция включена, при получении незарегистрированного многоадресного пакета коммутатор отбрасывает его, а не пересылает.

6.25.2 Настройка через веб-интерфейс

1. Настройка действия при получении незарегистрированного многоадресного пакета.

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [Unregistered multicast action configuration], чтобы перейти на страницу настройки действия при получении незарегистрированного многоадресного пакета, как показано на рисунке 338.

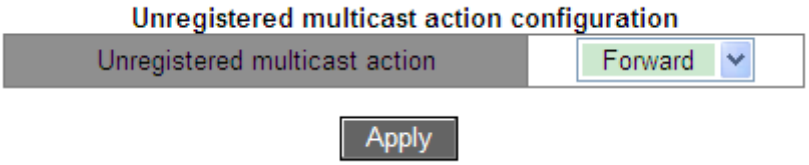


Рисунок 338 Настройка действия при получении незарегистрированного многоадресного пакета

Unregistered multicast action

Варианты: Forward/Discard

По умолчанию: Forward

Функция: Настройка действия при получении незарегистрированного многоадресного пакета.

2. Настройте порта мониторинга многоадресного потока, как показано на рисунке 339.

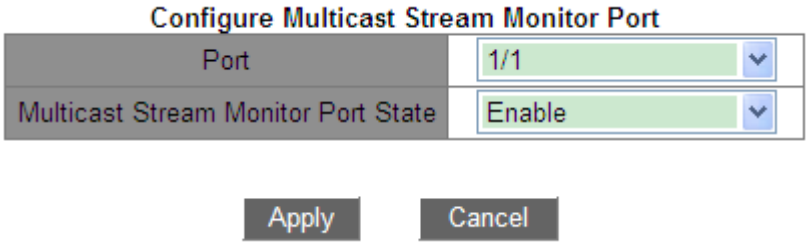


Рисунок 339 Настройка порта мониторинга многоадресного потока

Multicast Stream Monitor Port

Варианты: Disable/Enable

По умолчанию: Disable

Функция: Настройка порта мониторинга многоадресного потока. Этот порт мониторинга перенаправляет потоки службы многоадресной рассылки (включая зарегистрированный поток службы многоадресной рассылки и незарегистрированный поток службы многоадресной рассылки), полученные другими портами в той же сети VLAN. Эта функция в основном используется для мониторинга многоадресной рассылки.

Примечание:

- Когда при получении незарегистрированного многоадресного пакета настроено как отбрасывание, порт мониторинга многоадресного потока настроить нельзя.
- Если порт мониторинга многоадресной рассылки доступен, незарегистрированный поток многоадресной рассылки перенаправляется только на порт мониторинга многоадресной рассылки. Если нет доступного порта мониторинга многоадресной рассылки, незарегистрированный поток многоадресной рассылки перенаправляется на все порты VLAN.
- Порт мониторинга многоадресной рассылки не поддерживает протокол многоадресной рассылки; поэтому его нельзя настроить как порт-участник многоадресной рассылки.

6.26 Статическая настройка многоадресной рассылки

6.26.1 Введение

Таблица адресов многоадресной рассылки можно настроить статически. В таблицу адресов многоадресной рассылки добавляется запись в виде {VLAN ID, Multicast MAC address, Multicast member port}, и сообщение многоадресной рассылки будет перенаправлено на соответствующий порт-участник в соответствии с записью.

6.26.2 Настройка через веб-интерфейс

1. Добавьте статическую запись многоадресной рассылки

Щелкните [Device Advanced Configuration] → [Multicast protocol configuration] → [Static Multicast Configuration], чтобы перейти на страницу настройки статической записи многоадресной рассылки, как показано на рисунке 340.

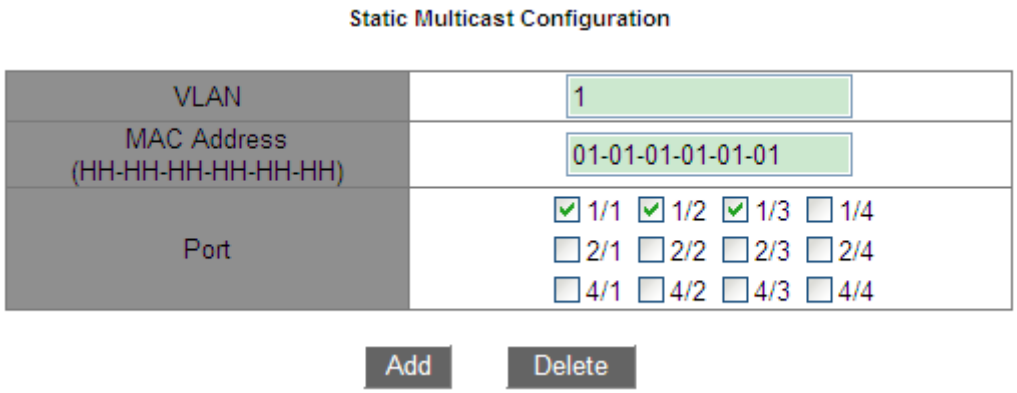


Рисунок 340 Добавление статической записи многоадресной рассылки

VLAN

Варианты: Все существующие идентификаторы VLAN

Функция: задание VLAN ID статической записи многоадресной рассылки. Только порты VLAN могут пересылать это сообщение многоадресной рассылки.

MAC Address

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

Функция: Настройка адреса группы многоадресной рассылки. Младший бит в старшем байте равен 1.

Port

Функция: выбор портов адреса многоадресной рассылки. Если хост, подключенный к порту, хочет получать определенные данные группы многоадресной рассылки, статически добавьте этот порт в группу многоадресной рассылки и сделайте его статическим портом-участником.

Щелкните кнопку <Add>, чтобы добавить статическую запись многоадресной рассылки; щелкните кнопку <Delete>, чтобы удалить статическую запись многоадресной рассылки.

2.Просмотрите статические записи многоадресной рассылки, как показано на рисунке 341.

VLAN	MAC Address	Port
2	03-01-01-01-01-01	1/1 1/4
1	01-01-01-01-01-01	1/1 1/2 1/3
1	01-00-00-00-00-01	1/1 1/2

Рисунок 341 Просмотр статических записей многоадресной рассылки

6.27 LLDP

6.27.1 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.

6.27.2 Настройка через веб-интерфейс

1. Включите LLDP.

Щелкните [Device Advanced Configuration] → [LLDP configuration] → [LLDP configuration], чтобы перейти на страницу настройки LLDP, как показано на рисунке 342.

Рисунок 342 Включение LLDP

LLDP configuration

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение LLDP.

2. Включите функцию адреса управления TLV, как показано на рисунке 343.

Рисунок 343 Включение функцию адреса управления TLV

TLV Management Address

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Отправка IP-адреса интерфейса (то есть основного IP-адреса первого интерфейса VLAN, в котором находится этот порт) на подключенное устройство, когда эта функция отключена. Если IP-адрес не настроен для интерфейса VLAN, где находится этот порт, IP-адрес интерфейса — 127.0.0.1. Отправка IP-адреса интерфейса и всех IP-адресов, настроенных для текущего устройства, на подключенное устройство, когда эта функция включена. Можно отправить не более 64 адресов управления TLV.

Предупреждение:

Когда на локальном устройстве включена функция управления адресом TLV и подключающееся

соседнее устройство может анализировать функцию TLV, оно может правильно

отображать все настроенные IP-адреса локального коммутатора.

3. Просмотр информации LLDP.

Щелкните [Device Advanced Configuration] → [LLDP configuration] → [Show lldp], чтобы отобразить информацию LLDP, как показано на рисунке 344 ~ рисунке 347.

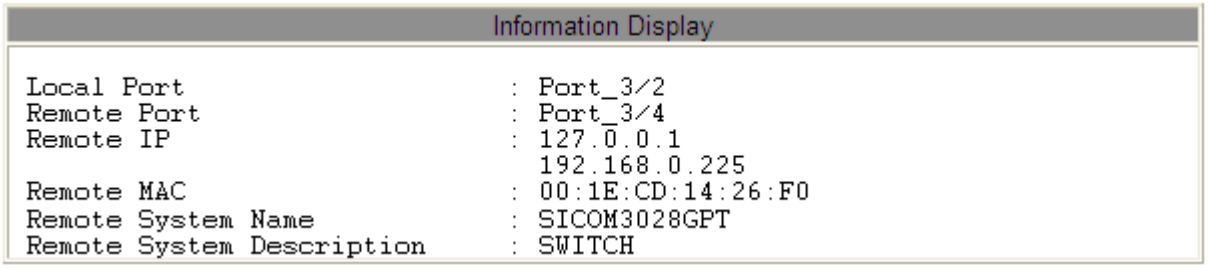


Рисунок 344 Информация LLDP-1 Функция TLV Management Address включена

На предыдущем рисунке показано условие, при котором IP-адрес не настроен для первого интерфейса VLAN, где находится порт 3/4.

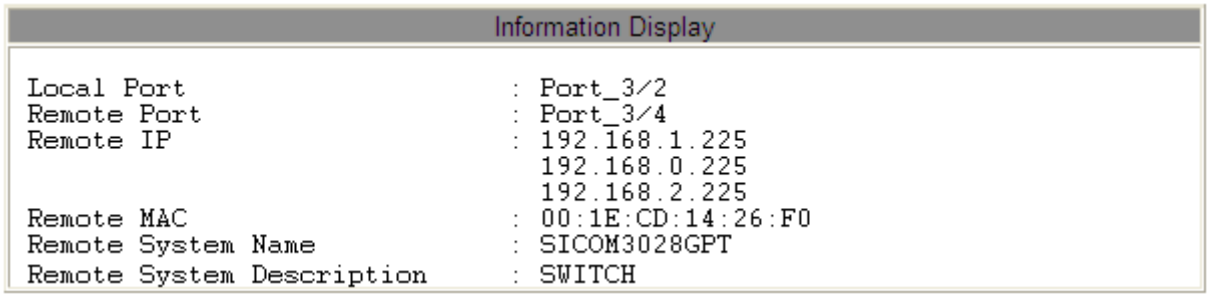


Рисунок 345 Информация LLDP-2 Функция TLV Management Address включена

На предыдущем рисунке показано условие, при котором первичный IP-адрес первого интерфейса VLAN, где находится порт 3/4, равен 192.168.1.225.

Когда функция TLV Management Address включена, отображаемая информация LLDP включает в себя подключенный локальный порт коммутатора и удаленный порт соседнего устройства, IP-адрес интерфейса, все настроенные IP-адреса, MAC-адрес и системную информацию соседнего устройства.

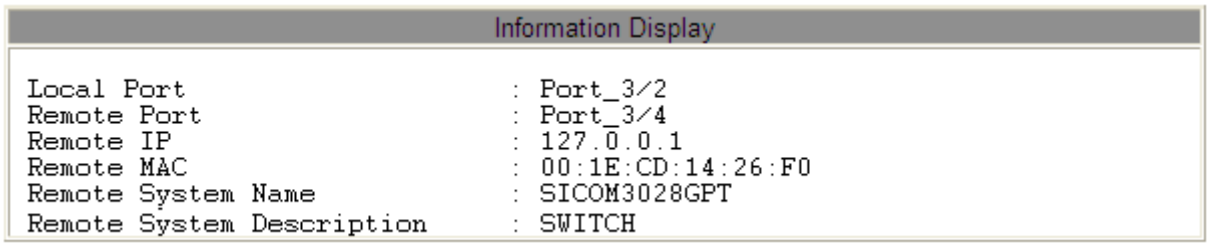


Рисунок 346 Информация LLDP-1 Функция TLV Management Address выключена

На предыдущем рисунке показано условие, при котором IP-адрес не настроен для первого интерфейса VLAN, где находится порт 3/4.

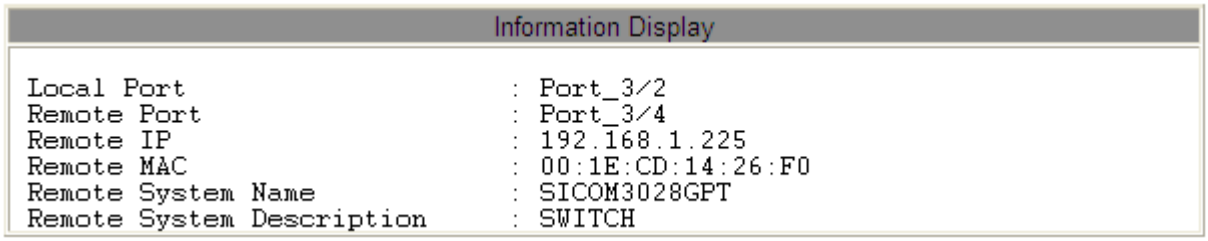


Рисунок 347 Информация LLDP-2 Функция TLV Management Address выключена

На предыдущем рисунке показано условие, при котором первичный IP-адрес первого интерфейса VLAN, где находится порт 3/4, равен 192.168.1.225.

Когда функция TLV Management Address выключена, отображаемая информация LLDP включает в себя подключенный локальный порт коммутатора и удаленный порт соседнего устройства, IP-адрес интерфейса, MAC-адрес и системную информацию соседнего устройства.

Предупреждение:

Для отображения информации LLDP устройства с поддержкой этой функции должны быть подключены друг к другу.

6.28 RMON

6.28.1 Обзор

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.

6.28.2 Группы RMON

RMON (RFC2819) определяет несколько групп RMON. Устройства серии поддерживают группу статистики, группу истории, группу событий и группу сигналов тревоги в общедоступной MIB. Каждая группа поддерживает до 32 записей.

- 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.

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.

Предупреждение:

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, попеременно генерируются сигналы повышения и падения значения.

6.28.3 Настройка через веб-интерфейс

1. Щелкните [Device Advanced Configuration] → [RMON configuration] → [RMON Statistics], чтобы перейти на страницу статистики RMON, как показано на рисунке 348.

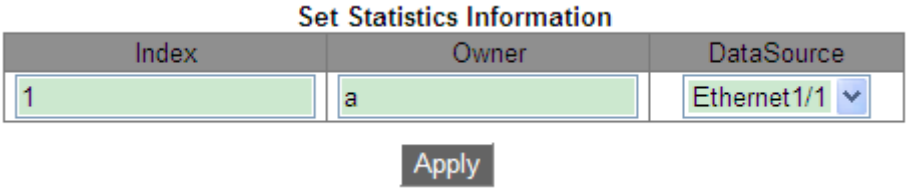


Рисунок 348 Статистика RMON

Index

Диапазон: 1~65535

Функция: Настройка номера записи статистики.

Owner

Диапазон: 1~32 символа

Функция: Настройка имени записи статистики.

DataSource

Функция: Выбор порта для сбора статистики.

2. Щелкните[Device Advanced Configuration] → [RMON configuration] → [RMON History], чтобы перейти на страницу истории RMON, как показано на рисунке 349.

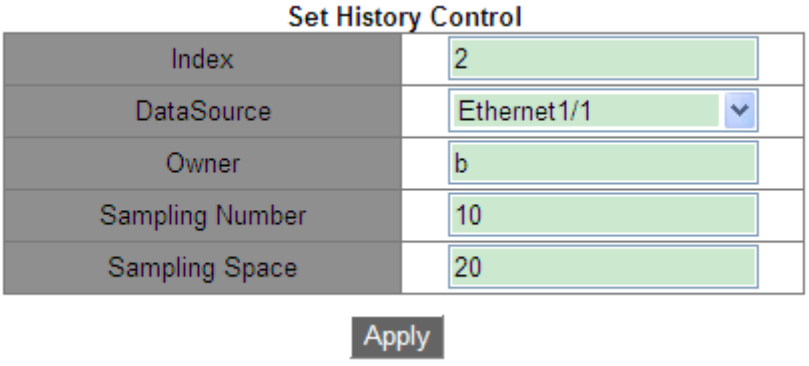


Рисунок 349 Таблица истории RMON

Index

Диапазон: 1~65535

Функция: Настройка номера записи истории.

DataSource

Функция: Выбор порта для сбора информации.

Owner

Диапазон: 1~32 символа

Функция: Настройка имени записи истории.

Sampling Number

Диапазон: 1~65535

Функция: Настройка количества выборок для порта.

Sampling Space

Диапазон: 1~3600 с

Функция: Настройка периода выборки для порта.

3. Щелкните [Device Advanced Configuration] → [RMON configuration] → [RMON Event], чтобы перейти на страницу RMON Event, как показано на рисунке 350.

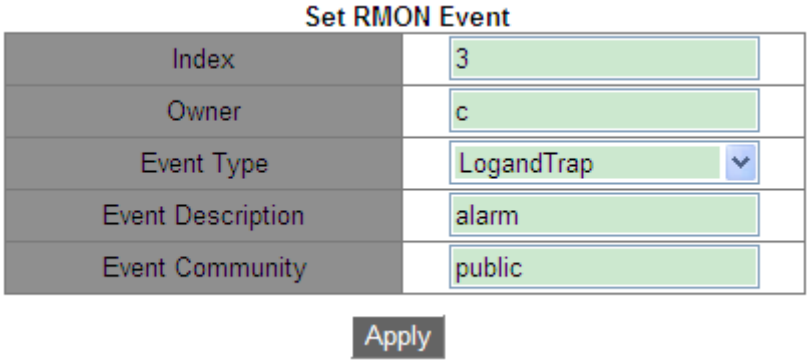


Рисунок 350 Таблица RMON Event

Index

Диапазон: 1~65535

Функция: Настройка порядкового номера записи событий.

Owner

Диапазон: 1~30 символов

Функция: Настройка имени записи события.

Event Type

Варианты: NONE/LOG/Snmp-Trap/Log and Trap

По умолчанию: NONE

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

Event Description

Диапазон: 1~126 символов

Функция: Описание события.

Event Community

Диапазон: 1~126 символов

Функция: Задание имени сообщества для отправки события trap. Значение должно совпадать со значением в SNMP.

4. Щелкните [Device Advanced Configuration] → [RMON configuration] → [RMON Alarm], чтобы перейти на страницу RMON Alarm, как показано на рисунке 351.

Set RMON Alarm

Index	4
Counter Type	1213 Counter
1213 Counter	IfInOctets
RMON Counter	InDropEvents
Owner	d
1213 DataSource	Ethernet1/1
RMON DataSource	
Sampling Type	Absolute
Alarm Type	RisingAlarm
Sampling Space	20
Rising Threshold	100
Falling Threshold	20
Rising EventIndex	3
Falling EventIndex	3

Apply

Рисунок 351 Таблица RMON Alarm

Index

Диапазон: 1~65535

Функция: Настройка номера записи сигнала тревоги.

Counter Type

Варианты: 1213 Counter/ RMON Counter

Функция: Выбор типа узла MIB.

1213 Counter/RMON Counter

Функция: Задание типа аварийной сигнализации RMON.

Owner

Диапазон: 1~31 символ

Функция: Настройка имени записи сигнала тревоги.

1213 DataSource

Функция: Выбор порта для отслеживания информации.

RMON DataSource

Варианты: идентификатор номера записи статистики в таблице статистики RMON

Функция: Отслеживание информации о порте в таблице статистики RMON.

Sampling Type

Варианты: Absolute/Delta

По умолчанию: Absolute

Функция: Absolute указывает на выборку на основе абсолютного значения. Значение переменной извлекается напрямую, когда приближается конец периода выборки. Delta указывает выборку на основе изменения значения. Значение изменения переменной за период выборки извлекается, когда приближается конец периода.

Alarm Type

Варианты: RisingAlarm/FallingAlarm/RisOrFallAlarm

По умолчанию: RisingAlarm

Функция: Выбор типа сигнала тревоги, включая сигнал по переднему фронту, сигнал по заднему фронту, а также сигнал по переднему и заднему фронту.

Sampling Space

Диапазон: 1~65535

Функция: Настройка периода выборки.

Rising Threshold

Диапазон: 0~65535

Функция: Настройка порогового значения по нарастанию. Когда значение выборки превышает порог повышения и типом тревоги является RisingAlarm или RisOrFallAlarm, срабатывает тревога и активируется индекс событий повышения.

Falling Threshold

Диапазон: 0~65535

Функция: Настройка порогового значения по понижению. Когда значение выборки ниже порога понижения и типом тревоги является FallingAlarm или RisOrFallAlarm, срабатывает тревога и активируется индекс событий понижения.

Rising EventIndex

Диапазон: 0~65535

Функция: Настройте индекс события нарастания, то есть режим обработки сигналов тревоги по нарастанию.

Falling EventIndex

Диапазон: 0~65535

Функция: Настройте индекс события убывания, то есть режим обработки сигналов тревоги по убыванию.

6.29 VRRP

Примечание:

В этой главе под маршрутизаторами понимаются коммутаторы уровня Layer-3.

6.29.1 Введение

Протокол Virtual Router Redundancy Protocol (VRRP) добавляет несколько маршрутизаторов, которые могут действовать как сетевые шлюзы, в группу VRRP, которая образует виртуальный маршрутизатор. Маршрутизаторы в группе VRRP

выбирают главный маршрутизатор с помощью механизма выбора VRRP, а другие маршрутизаторы в группе становятся резервными. Когда главный маршрутизатор выходит из строя, резервные маршрутизаторы выбирают новый главный маршрутизатор, который берет на себя ответственность вышедшего из строя главного маршрутизатора. Это обеспечивает бесперебойную передачу данных без изменения конфигурации.

Примечание: В коммутаторах этой серии VRRP поддерживают только SICOM3028GPT-L3GT, SICOM3028GPT-L3FT, SICOM3028GPT-L3G и SICOM3028GPT-L3F уровня Layer-3.

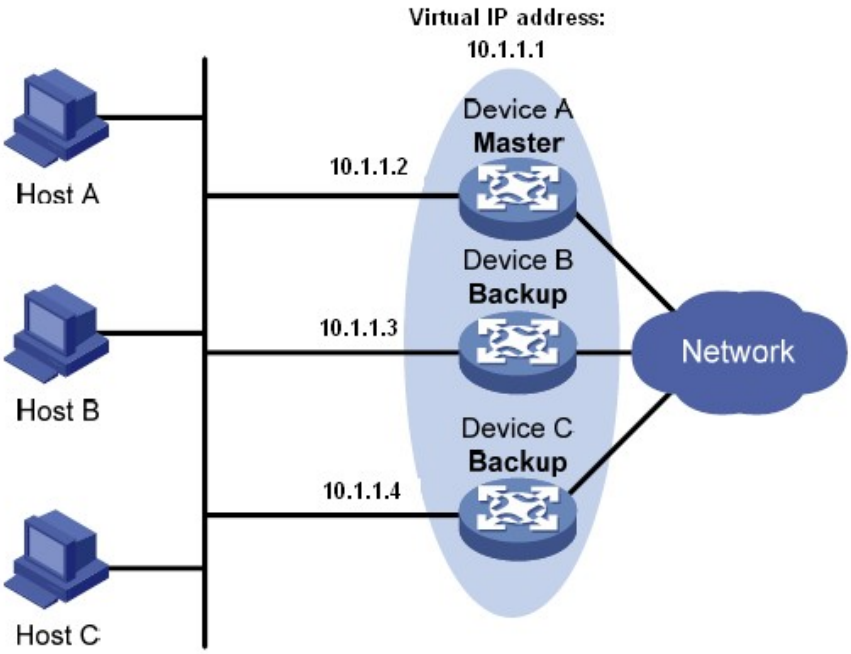


Рисунок 352 VRRP

Как показано на рисунке 352, устройства Device A, Device B и Device C образуют виртуальный маршрутизатор с IP-адресом. Хосты могут взаимодействовать с внешними сетями через виртуальный маршрутизатор только в том случае, если IP-адрес виртуального маршрутизатора настроен как следующий переход маршрута по умолчанию на хостах. Виртуальный маршрутизатор состоит из одного главного и нескольких резервных коммутаторов. Главный маршрутизатор работает как шлюз. Когда он выходит из строя, один из резервных маршрутизаторов берет на себя ответственность вышедшего из строя главного маршрутизатора действовать как шлюз.

Предупреждение:

- IP-адрес виртуального маршрутизатора может быть либо неиспользуемым IP-адресом в сегменте, в котором находится группа VRRP, либо IP-адресом интерфейса маршрутизатора в группе VRRP.
- Маршрутизатор, IP-адрес интерфейса которого совпадает с адресом виртуального маршрутизатора, является владельцем IP-адреса.
- В каждой группе VRRP есть только один владелец IP-адреса.

6.29.2 Выбор главного маршрутизатора

VRRP выбирает главный маршрутизатор.

1. Маршрутизатор с высшим приоритетом в группе VRRP выбирается главным. Главный маршрутизатор периодически отправляет объявления VRRP, чтобы информировать другие маршрутизаторы в группе VRRP о том, что он работает должным образом.

Примечание:

Приоритет VRRP находится в диапазоне от 0 до 255. Чем больше значение, тем выше приоритет.
Приоритеты от 1 до 254 настраиваются. Приоритет 0 зарезервирован для специального использования, а приоритет 255 — для владельца IP-адреса.

2. Резервные маршрутизаторы получают приоритеты других маршрутизаторов в группе путем обмена пакетами VRRP.

- Если приоритет главного маршрутизатора в объявлении выше его собственного приоритета, маршрутизатор остается резервным.
- Если приоритет главного маршрутизатора в объявлении ниже, чем собственный приоритет маршрутизатора, маршрутизатор берет на себя роль главного маршрутизатора в вытесняющем режиме и остается резервным в невытесняющем режиме.

- Если в течение определенного периода времени объявления VRRP не поступают, маршрутизатор считает, что главный маршрутизатор выходит из строя, и отправляет объявления VRRP, чтобы начать новый выбор главного маршрутизатора.

Примечание:

- Невытесняющий режим: Когда маршрутизатор в группе VRRP становится главным, он остается главным до тех пор, пока работает нормально, даже если резервному маршрутизатору позднее будет присвоен более высокий приоритет.
- Вытесняющий режим: Когда резервный маршрутизатор обнаруживает, что ее приоритет выше, чем у главного маршрутизатора, резервный маршрутизатор отправляет объявления VRRP, чтобы начать новые выборы главного маршрутизатора в группе VRRP.

6.29.3 Мониторинг указанного интерфейса

Если интерфейс uplink маршрутизатора в группе VRRP выходит из строя, обычно группа VRRP не может знать об отказе интерфейса uplink. Если маршрутизатор является главным, узлы в локальной сети не могут получить доступ к внешним сетям. Эту проблему можно решить, осуществляя мониторинг указанного интерфейса uplink. В случае сбоя интерфейса uplink приоритет главного устройства автоматически снижается на указанное значение, и маршрутизатор с более высоким приоритетом в группе VRRP становится главным.

6.29.4 Настройка через веб-интерфейс

1. Создание/удаление группы VRRP.

Щелкните [Device Advanced Configuration] → [VRRP Configuration] → [Create/Remove VRRP], чтобы перейти на страницу настройки группы VRRP, как показано на рисунке 353.

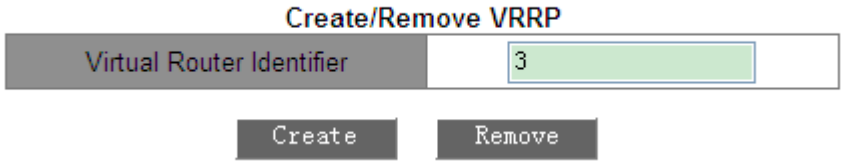


Рисунок 353 Создание группы VRRP

Virtual Router Identifier

Диапазон: 1~255

Функция: Задание ID группы VRRP.

Примечание: Коммутаторы серии поддерживают не более 10 групп VRRP.

2. Задание IP-адреса виртуального маршрутизатора.

Щелкните [Device Advanced Configuration] → [VRRP Configuration] → [VRRP Initialization], чтобы перейти на страницу инициализации VRRP, как показано на рисунке 354.

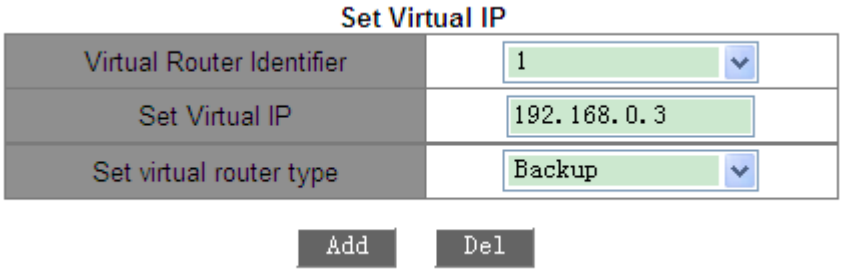


Рисунок 354 Задание IP-адреса виртуального маршрутизатора.

Set Virtual IP

Формат: A.B.C.D

Функция: Задание IP-адреса виртуального маршрутизатора.

Примечание: IP-адрес виртуального маршрутизатора должен находиться в том же сегменте сети, что и IP-адрес интерфейса.

Set virtual router type

Варианты: Master/Backup

Описание: Master указывает, что текущее устройство является владельцем IP-адреса виртуального маршрутизатора. Backup указывает, что текущее устройство не является владельцем IP-адреса виртуального маршрутизатора.

3. Настройте интерфейс Layer-3 для VRRP, как показано на рисунке 355.

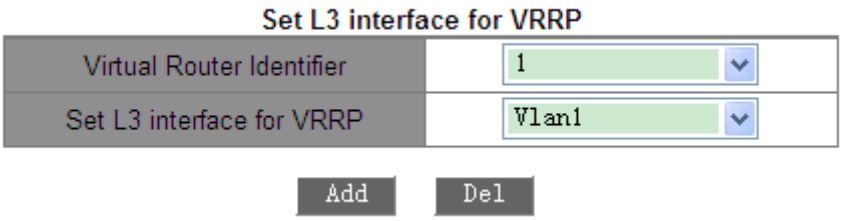


Рисунок 355 Настройка интерфейса Layer-3 для VRRP

Функция: Настройка интерфейса Layer-3 для указанной группы VRRP.

4. Настройка рабочего режима группы VRRP.

Щелкните [Device Advanced Configuration] → [VRRP Configuration] → [Set preempt mode], чтобы перейти на страницу настройки рабочего режима VRRP, как показано на рисунке 356.

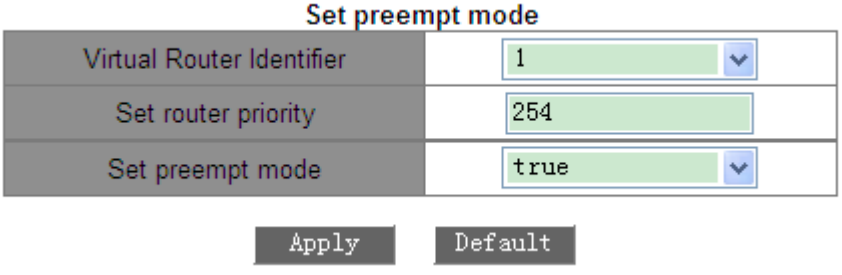


Рисунок 356 Настройка рабочего режима группы VRRP

Set router priority

Диапазон: 1~254

По умолчанию: 100 (для не являющего владельцем IP-адреса)

Функция: Задание приоритета маршрутизатора в группе VRRP.

Set preempt mode

Варианты: true/false

По умолчанию: true

Функция: Настройка рабочего режима виртуального маршрутизатора.

Описание: True указывает на вытесняющий режим, a false указывает на невытесняющий режим.

5. Задание интервала передачи объявлений.

Щелкните [Device Advanced Configuration] → [VRRP Configuration] → [Set advertisement interval , monitor interface and connectivity check], чтобы перейти на страницу настройки, как показано на рисунке 357.

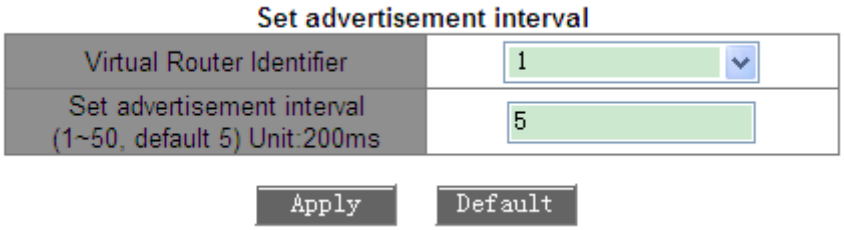


Рисунок 357 Настройка интервала передачи объявлений

Set advertisement interval

Диапазон: 1~50 (Ед. изм: 200 мс)

По умолчанию: 5×200 мс

Функция: Установите интервал, через который главный маршрутизатор будет отправлять объявления VRRP.

6. Настройте отслеживаемый интерфейс, как показано на рисунке 358.

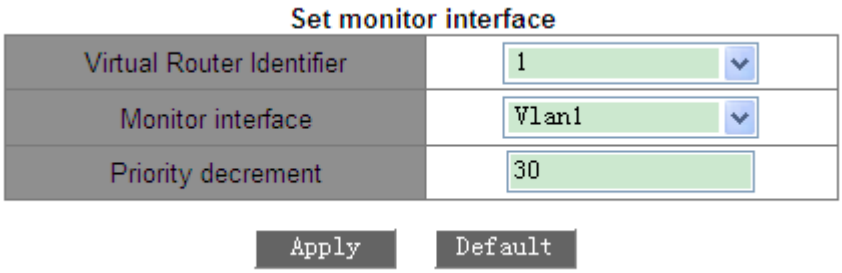


Рисунок 358 Настройка отслеживаемого интерфейса

Monitor Interface

Функция: Выбор интерфейса VLAN для мониторинга.

Priority decrement

Диапазон: 1~253

Функция: Настройка значения декремента приоритета.

7. Настройте проверку подключения, как показано на рисунке 359.

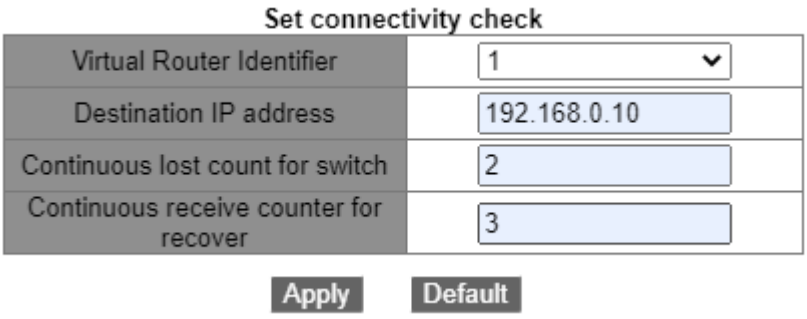


Рисунок 359**Настройка проверки подключения**

Destination IP Address

Формат: A.B.C.D

Функция: Можно осуществлять мониторинг канала uplink, задав IP-адрес назначения. Когда происходит сбой канала uplink, и хост в локальной сети не может получить доступ к внешней сети через маршрутизатор, нужно уведомить VRRP о снижении приоритета маршрутизатора до указанного значения. Следовательно, приоритет других маршрутизаторов в резервной группе выше, чем приоритет этого маршрутизатора, и один из них становится главным маршрутизатором, гарантируя, что связь между хостом и внешней сетью в LAN не прерывается. После восстановления канала uplink нужно уведомить VRRP о восстановлении приоритета маршрутизатора.

Continuous lost count for switch

Диапазон: 2-100 с

Функция: настройка времени непрерывного отсутствия соединения на порту до его переключения. Continuous receive counter for recover

Диапазон: 2-100 с

Функция: Диапазон времени восстановления канала uplink.

Предупреждение:

- Владелец IP-адреса виртуального маршрутизатора не может быть настроен в качестве отслеживаемого интерфейса.
- Приоритет главного маршрутизатора после уменьшения должен быть меньше, чем у резервного маршрутизатора.

8. Настройка параметров аутентификации VRRP.

Щелкните [Device Advanced Configuration] → [VRRP Configuration] → [VRRP Authentication], чтобы перейти на страницу настройки параметров аутентификации VRRP, как показано на рисунке 360.

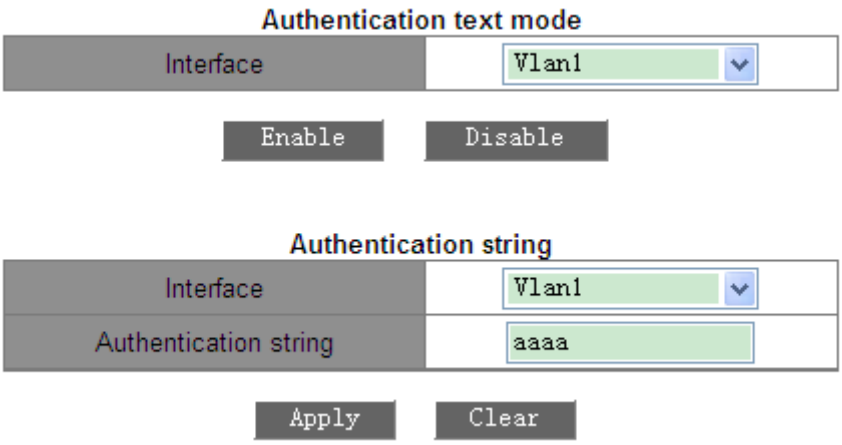


Рисунок 360 Настройка параметров аутентификации VRRP

Authentication text mode

Функция: Включение интерфейса, требующего простой аутентификации. Маршрутизатор, отправляющий пакет VRRP, добавляет в пакет ключ аутентификации. Маршрутизатор, получивший пакет, сравнивает ключ аутентификации в пакете с

локальным ключом аутентификации. Если два ключа аутентификации идентичны, пакет считается законным и истинным. В противном случае пакет является нелегитимным.

Authentication string

Диапазон: 1~8 символов

Функция: Настройка строки аутентификации.

9. Включите группу VRRP.

Щелкните [Device Advanced Configuration] → [VRRP Configuration] → [VRRP Initialization] , чтобы перейти на страницу инициализации VRRP, как показано на рисунке 361.

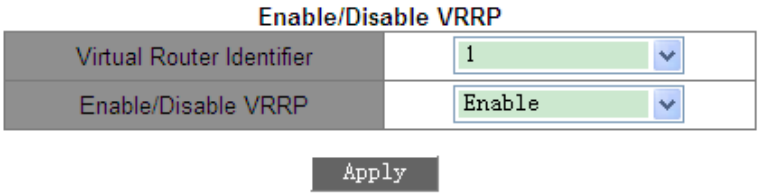


Рисунок 361 Включение VRRP

Функция: Включение функции группы VRRP.

10. Информация VRRP

Щелкните [Device Advanced Configuration] → [VRRP Configuration] → [VRRP information] , чтобы перейти на страницу информации VRRP, как показано на рисунке 362.

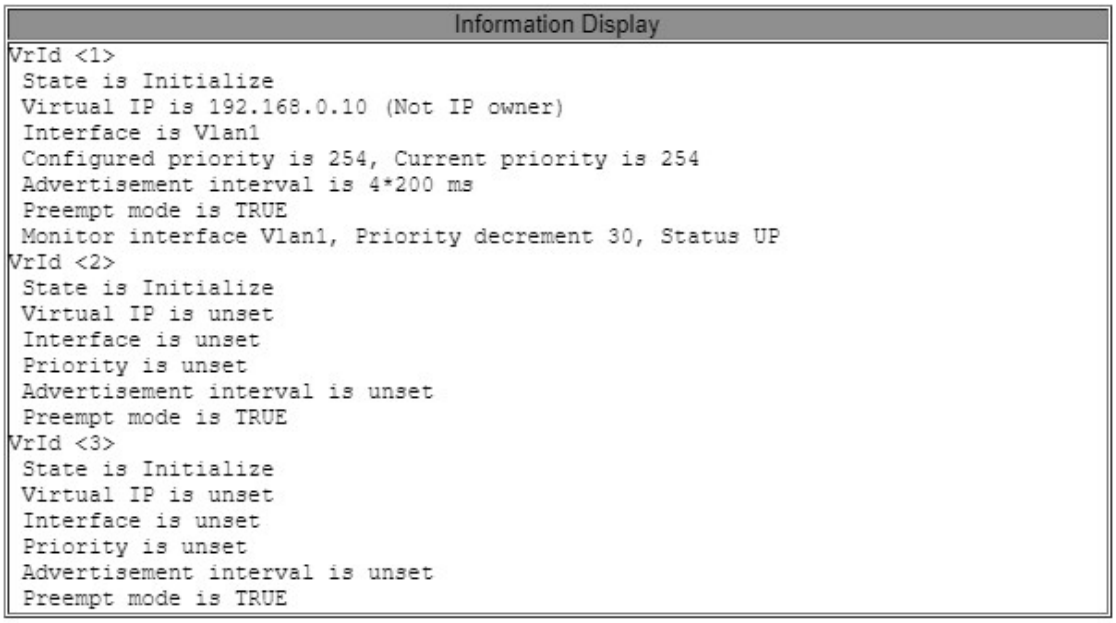


Рисунок 362 Информация VRRP

6.29.5 Типовой пример конфигурации

Как показано на рисунке 363, коммутатор A и коммутатор B образуют виртуальный маршрутизатор с IP-адресом 192.168.2.4. Хост A может связываться с хостом B через виртуальный маршрутизатор. Когда коммутатор A работает должным образом, он является главным в группе VRRP. При отказе коммутатора A или VLAN 3 коммутатор B становится главным.

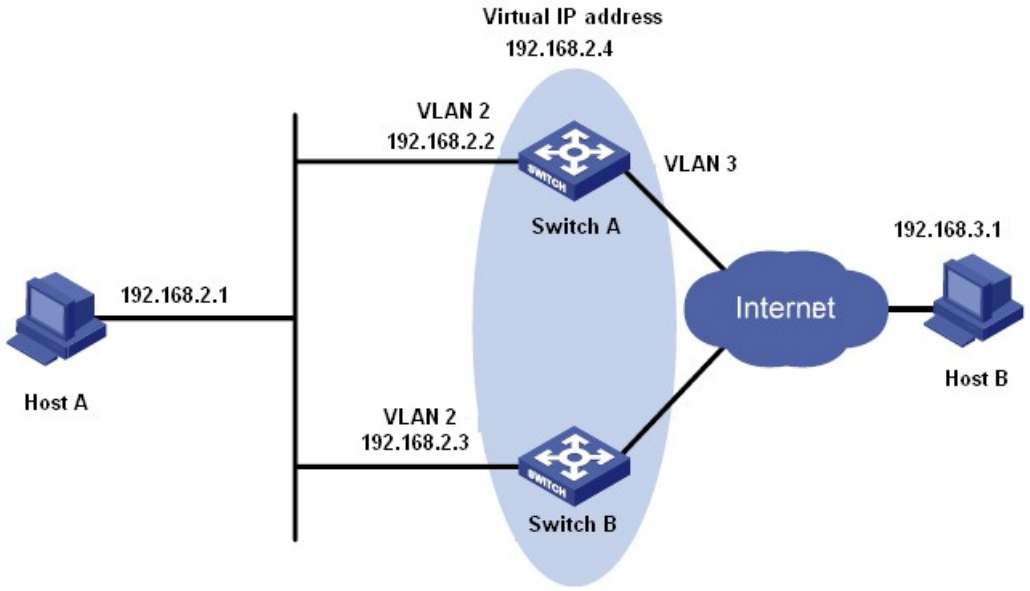


Рисунок 363 Пример типовой конфигурации VRRP

Конфигурация коммутатора A:

1. Установите IP-адрес интерфейса VLAN 2 192.168.2.2 и маску подсети 255.255.255.0.
2. Создайте группу VRRP 1, как показано на рисунке 353.
3. Задайте виртуальный IP-адрес группы VRRP 192.168.2.4 и тип маршрутизатора Backup, как показано на рисунке 354.
4. Настройте VLAN 2 как интерфейс Layer-3 для группы VRRP 1, как показано на рисунке 355.
5. Установите приоритет коммутатора A в группе VRRP равным 110, а значение preemptive mode – false, как показано на рисунке 356.
6. Настройте VLAN 3 в качестве контролируемого интерфейса и установите декремент приоритета 30, как показано на рисунке 358.
7. Включите группу VRRP 1, как показано на рисунке 361.

Конфигурация коммутатора B:

1. Установите IP-адрес интерфейса VLAN 2 192.168.2.3 и маску подсети 255.255.255.0.
2. Создайте группу VRRP 1, как показано на рисунке 353.
3. Задайте виртуальный IP-адрес группы VRRP 192.168.2.4 и тип маршрутизатора Backup, как показано на рисунке 354.
4. Настройте VLAN 2 как интерфейс Layer-3 для группы VRRP 1, как показано на рисунке 355
5. Установите приоритет коммутатора B в группе VRRP равным 100, а значение preemptive mode – false, как показано на рисунке 356.
6. Включите группу VRRP 1, как показано на рисунке 361.

6.30 Настройка SNTP

6.30.1 Введение

Простой протокол сетевого времени (SNTP) синхронизирует время между сервером и клиентом с помощью запросов и ответов. Как клиент коммутатор синхронизирует время с сервером по пакетам сервера. Для одного коммутатора можно настроить несколько серверов SNTP, но активным может быть только один.

Клиент SNTP отправляет запрос на каждый сервер один за другим через одноадресную рассылку. Сервер, который первым дает ответ, находится в активном состоянии. Остальные серверы находятся в неактивном состоянии.

Предупреждение:

- Для синхронизации времени по SNTP необходим активный SNTP-сервер.
- Вся информация о времени, передаваемая в протоколе SNTP, является стандартной информацией о времени часового пояса 0.

6.30.2 Настройка через веб-интерфейс

1. Включите протокол SNTP.

Щелкните [Device Advanced Configuration] → [SNTP configuration] → [SNTPserver configuration], чтобы перейти на страницу настройки SNTP, как показано на рисунке 364.

Рисунок 364 Включение SNTP

SNTP State

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение SNTP

Предупреждение:

Протоколы SNTP и NTP являются взаимоисключающими. Поскольку NTP и SNTP используют один и тот же

номер порта UDP, их нельзя использовать одновременно.

2. Просмотр информации о конфигурации SNTP.

Щелкните [Device Advanced Configuration] → [SNTP configuration] → [SNTP information], чтобы просмотреть настройки SNTP, как показано на рисунке 365.

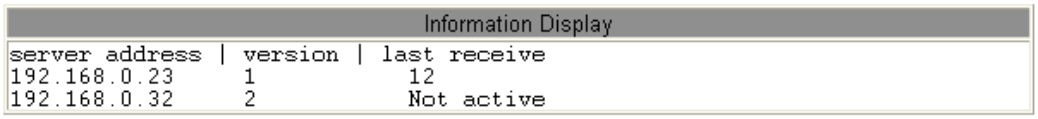


Рисунок 365 Страница настроек SNTP

Значение Last receive отображает время, прошедшее с момента последней синхронизации.

6.31 Настройка NTP

6.31.1 Введение

Протокол сетевого времени (NTP) синхронизирует время между распределенными серверами и клиентами. NTP синхронизирует часы всех сетевых устройств, обеспечивая согласованность времени между всеми устройствами. Это позволяет устройствам предоставлять несколько приложений в одно и то же время. Локальная система с поддержкой NTP может не только синхронизировать свои часы с другими источниками часов, но и служить источником часов для других устройств.

Как показано на рисунке 366, двусторонняя задержка (T4-T1) - (T3-T2) и смещение часов ((T2-T1) + (T3-T4)) / 2 могут быть рассчитаны на основе обмена NTP-пакетами, благодаря чему достигается высокоточная синхронизация часов между устройствами.

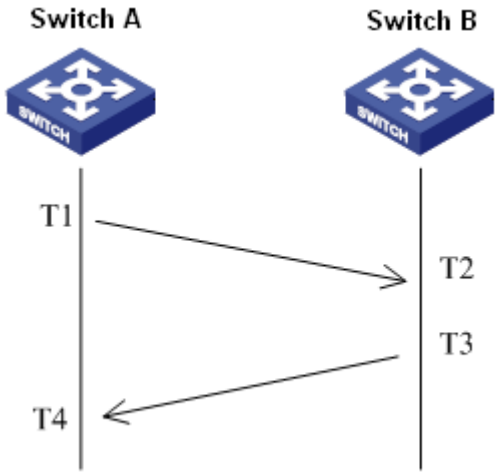


Рисунок 366 NTP

6.31.2 Режимы работы NTP

NTP может использовать следующие режимы для синхронизации времени. При необходимости можно выбрать соответствующий режим работы.

Режим клиент/сервер: В этом режиме клиент отправляет пакеты синхронизации часов (режим клиента) на сервер. После получения пакетов сервер автоматически работает в режиме сервера и отправляет ответные пакеты (режим сервера). После получения ответных пакетов клиент синхронизируется с оптимальными часами сервера.

Одноранговый режим: В этом режиме активный одноранговый узел отправляет пакеты

синхронизации часов (режим активного одноранговой узла) пассивному одноранговому узлу. После получения пакетов пассивный одноранговый узел автоматически работает в пассивном одноранговом режиме и отправляет ответные пакеты (пассивный одноранговый режим). На основе обмена пакетами устройства устанавливают одноранговый режим. Активный одноранговый узел и пассивный одноранговый узел могут синхронизировать время друг с другом. Если оба одноранговых узла синхронизировали время с других устройств, одноранговый узел с большим уровнем часов синхронизирует время с одноранговым узлом с меньшим уровнем часов.

Режим вещания: В этом режиме сервер вещания периодически рассылает пакеты синхронизации часов (режим вещания). После получения пакетов клиент широковещательной рассылки отправляет на сервер пакеты синхронизации часов (режим клиента). После получения пакетов запроса сервер отправляет пакеты ответа (режим сервера). Сервер и клиент выполняют синхронизацию часов, обмениваясь восемью пакетами запросов и ответов. Режим многоадресной рассылки Клиент многоадресной рассылки периодически отправляет пакеты запроса синхронизации многоадресной рассылки (режим клиента) на сервер многоадресной рассылки. После получения пакетов сервер отправляет одноадресные ответные пакеты (режим сервера). Затем сервер и клиент выполняют синхронизацию часов, обмениваясь одноадресными запросами синхронизации часов и ответными пакетами.

6.31.3 Настройка через веб-интерфейс

1. Включение NRP.

Щелкните [Device Advanced Configuration] → [NTP configuration] → [NTP Global Configuration], чтобы перейти на страницу глобальной настройки NTP, как показано на рисунке 367.

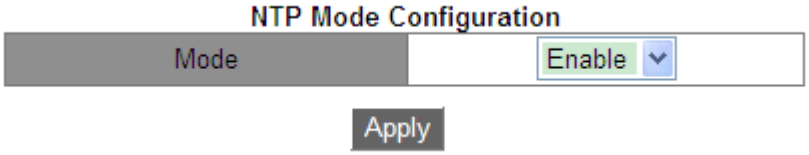


Рисунок 367 Включение NTP

Mode

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение или выключение функции глобальной службы NTP.

Предупреждение:

- Поскольку NTP и SNTP используют один и тот же номер порта UDP, их нельзя использовать одновременно.
- Можно также настроить службу NTP и сохранить конфигурацию, когда служба NTP отключена. Включение службы NTP не влияет на конфигурацию службы NTP.

2. Настройте одноадресную передачу NTP, как показано на рисунке 368.

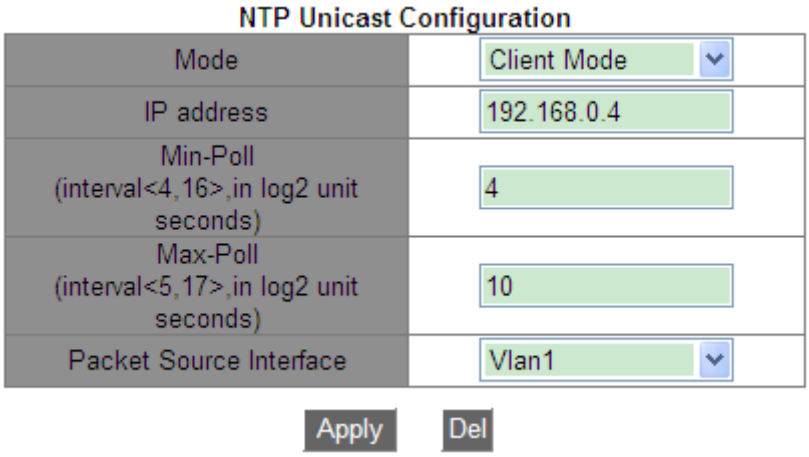


Рисунок 368 Настройка NTP Unicast

NTP State

Варианты: Client Mode/Peer Mode

Функция: Выбор рабочего режима NTP.

Описание: Client Mode указывает, что рабочий режим NTP является режимом клиент/сервер; Peer Mode указывает, что рабочий режим NTP является одноранговым.

IP Address

Формат: A.B.C.D

Описание: Когда используется режим клиент/сервер, IP-адрес – это адрес NTP-сервера. Когда принимается одноранговый режим, IP-адрес является адресом пассивного однорангового узла.

Min-Poll

Диапазон: от 4 до 16. Интервал=2^n с (n - значение этого параметра)

По умолчанию: 4. В этом случае интервал составляет 16 с (2^4).

Функция: Настройка минимального интервала запроса для обмена пакетами NTP между локальным устройством и сервером.

Max-Poll

Диапазон: от 5 до 17. Интервал=2^n с (n - значение этого параметра)

По умолчанию: 10. В этом случае интервал составляет 1024 с (2_{10}).

Функция: Настройка максимального интервала запроса для обмена пакетами NTP между локальным устройством и сервером.

Packet source interface

Функция: Указание порта для отправки пакетов NTP.

Описание: Когда используется режим клиент/сервер, локальное устройство отправляет пакеты NTP на сервер. IP-адрес источника в пакетах – это основной IP-адрес порта.

Когда используется режим клиент/сервер, локальное устройство отправляет пакеты NTP одноранговому узлу. IP-адрес источника в пакетах – это основной IP-адрес порта.

Предупреждение:

- Если используется режим клиент/сервер, нужно только выполнить предыдущую настройку на клиенте.
- Настроенные часы сервера NTP должны быть синхронизированы, прежде чем обеспечивать синхронизацию времени для других устройств.
- Если используется одноранговый режим, нужно только выполнить предыдущую настройку на активном одноранговом устройстве.
- Min-Poll ≤ Max-Poll.
- Значения Min-Poll одноранговых узлов NTP должны быть одинаковыми.

3. Настройте сервер многоадресной рассылки NTP.

Щелкните [Device Advanced Configuration] → [NTP configuration] → [Multicast Server Configuration], чтобы перейти на страницу настройки сервера многоадресной рассылки, как показано на рисунке 369.

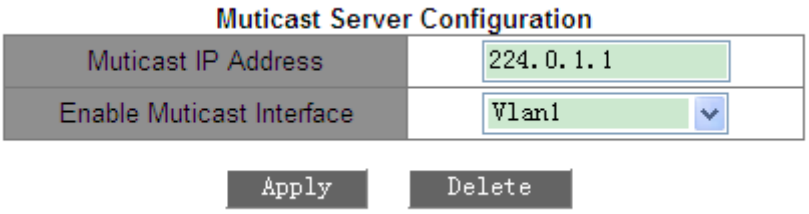


Рисунок 369 Настройка сервера многоадресной рассылки

Multicast IP Address

Формат: A.B.C.D

Функция: Настройка IP-адреса многоадресной рассылки. Если IP-адрес многоадресной рассылки не указан, адрес 224.0.1.1 принимается по умолчанию.

Enable Multicast Interface

Функция: Указание порта многоадресной рассылки.

4. Настройте клиента сервер многоадресной рассылки NTP.

Щелкните [Device Advanced Configuration] → [NTP configuration] → [Multicast Client Configuration], чтобы перейти на страницу настройки клиента многоадресной рассылки, как показано на рисунке 370.

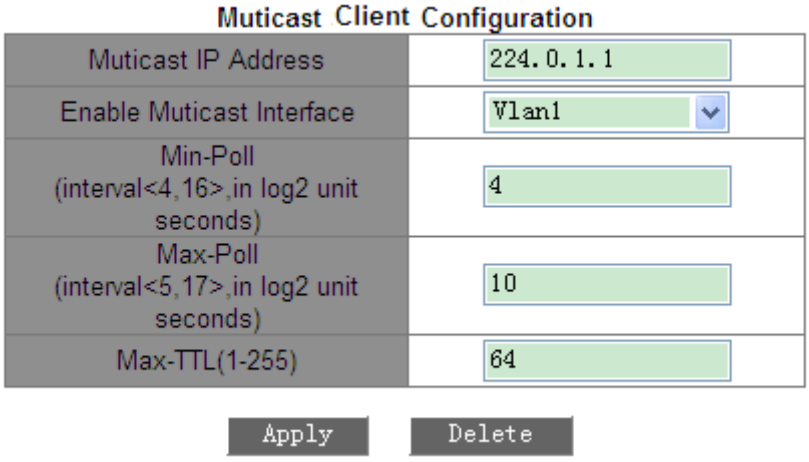


Рисунок 370 Настройка клиента многоадресной рассылки

Multicast IP Address

Формат: A.B.C.D

Функция: Настройка IP-адреса, используемого в режиме многоадресной рассылки. Если IP-адрес многоадресной рассылки не указан, 224.0.1.1 используется по умолчанию.

Enable Multicast Interface

Функция: Указание порта многоадресной рассылки.

Min-Poll

Диапазон: от 4 до 16. Интервал=2^n с (n - значение этого параметра)

По умолчанию: 4. В этом случае интервал составляет 16 с (2^4).

Функция: Настройка минимального интервала запроса для обмена пакетами NTP между локальным устройством и сервером.

Max-Poll

Диапазон: от 5 до 17. Интервал=2^n с (n - значение этого параметра)

По умолчанию: 10. В этом случае интервал составляет 1024 с (2^{10}).

Функция: Настройка максимального интервала запроса для обмена пакетами NTP между локальным устройством и сервером.

Max-TTL

Диапазон: 1~255

По умолчанию: 64

Функция: Настройка максимального TTL для запросов многоадресной рассылки, отправляемых клиентом многоадресной рассылки.

5. Настройте широковещательный сервер NTP.

Щелкните [Device Advanced Configuration] → [NTP configuration] → [Broadcast Server Configuration] , чтобы перейти на страницу настройки широковещательного сервера, как показано на рисунке 371.

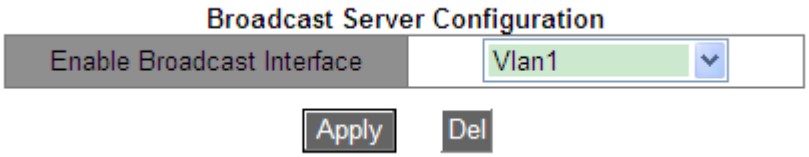


Рисунок 371 Настройка широковещательного сервера

Enable Broadcast Interface

Функция: Указание широковещательного порта.

6. Настройте широковещательного клиента NTP.

Щелкните [Device Advanced Configuration] → [NTP configuration] → [Broadcast Client Configuration], чтобы перейти на страницу настройки широковещательного клиента, как показано на рисунке 372.

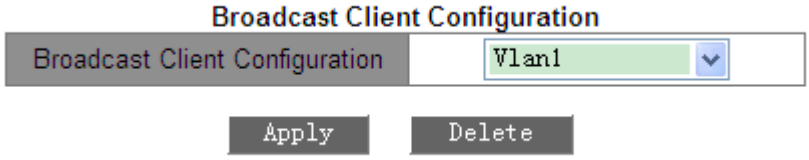


Рисунок 372 Настройка широковещательного клиента

Broadcast Client Configuration

Функция: Указание широковещательного порта.

7. Настройте эталонные часы.

Щелкните [Device Advanced Configuration] → [NTP configuration] → [Reference Clock Configuration], чтобы перейти на страницу настройки эталонных часов, как показано на рисунке 373.

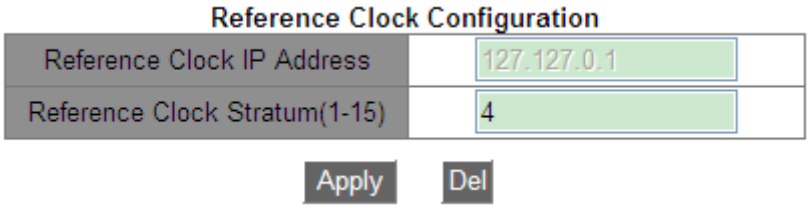


Рисунок 373 Настройка эталонных часов

Reference Clock IP Address

Формат: 127.127.t.u

По умолчанию: 127.127.0.1

Описание: t в 127.127.0.1 указывает тип опорных часов, а u указывает идентификатор экземпляра. В настоящее время поддерживается только 127.127.0.1. То есть системные часы служат эталонными часами.

Reference Clock Stratum

Диапазон: 1~15

По умолчанию: 4

Функция: Настройка уровня эталонных часов.

Описание: Уровень часов указывает на точность часов. Чем больше значение, тем ниже точность. Если уровень равен 16, часы не синхронизированы и, следовательно, не могут служить эталонными часами

Предупреждение:

В настоящее время только сам коммутатор может служить эталонными часами. Перед настройкой этого элемента
необходимо подтвердить требования системы к синхронизации времени.

6.31.4 Пример типовой конфигурации

- Настройка одноранговой режима:

Как показано на рисунке 374, необходимо настроить локальные часы на коммутаторе D в качестве эталонных часов и установить их уровень равным 2. Коммутатор A работает в режиме клиента, а коммутатор D служит NTP-сервером. Коммутатор B работает в одноранговом режиме, а коммутатор A является его одноранговым узлом. Коммутатор B является активным одноранговым узлом, а коммутатор A — пассивным одноранговым узлом.

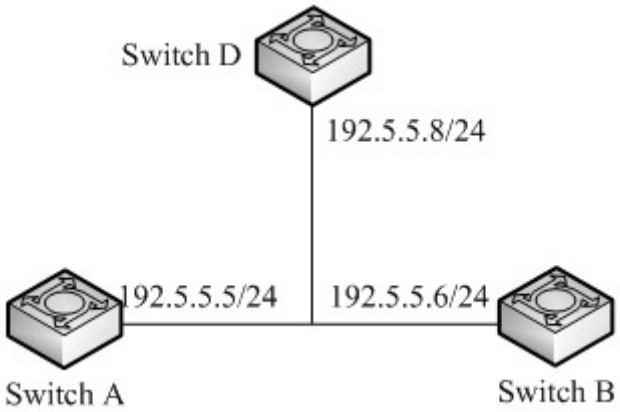


Рисунок 374 Сеть в одноранговом режиме

Конфигурация коммутатора B:

1. Включите NTP, как показано на рисунке 367.

2. Установите IP-адрес эталонных часов 127.127.0.1 и уровень часов 2, как показано на рисунке 373.

Конфигурация коммутатора A:

3. Включите NTP, как показано на рисунке 367.

4. Установите IP-адрес сервера NTP 192.5.5.8, значение Min-Poll – 4, Max-Poll – 10, NTP Source – VLAN 1, как показано на рисунке 368.

Конфигурация коммутатора B:

5. Включите NTP, как показано на рисунке 367.

6. Установите IP-адрес одноранговой узла NTP 192.5.5.5, значение Min-Poll – 4, Max-Poll – 10, NTP Source – VLAN 1, как показано на рисунке 368.

➢ Настройка режима многоадресной рассылки:

Как показано на рисунке 375, необходимо настроить локальные часы на коммутаторе D в качестве эталонных часов и установить их уровень равным 2. Коммутатор D работает в режиме сервера многоадресной рассылки. Режим сервера многоадресной рассылки настроен на порт VLAN 2. Коммутатор A и коммутатор B работают в режиме клиента многоадресной рассылки. Режим клиента многоадресной рассылки настроен на порт VLAN 2.

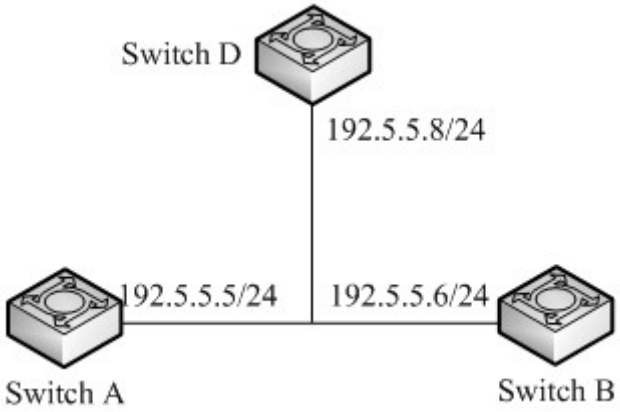


Рисунок 375 Сеть в режиме многоадресной рассылки

Конфигурация коммутатора D:

1. Включите NTP, как показано на рисунке 367.

2. Установите IP-адрес эталонных часов 127.127.0.1 и уровень часов 2, как показано на рисунке 373.

3. Настройте сервер многоадресной рассылки: Задайте IP-адрес многоадресной рассылки 224.0.1.1 и порт VLAN 2, как показано на рисунке 369.

Конфигурация коммутатора A и коммутатора B:

4. Включите NTP, как показано на рисунке 367.

5. Настройте клиента многоадресной рассылки: Установите IP-адрес многоадресной рассылки 224.0.1.1, port – VLAN 2, Min-Poll – 4, Max-Poll – 10, Max-TTL – 64, как показано на рисунке 370.

- Настройка широковещательного режима:

Как показано на рисунке 376, необходимо настроить локальные часы на коммутаторе D в качестве эталонных часов и установить их уровень равным 2. Коммутатор D работает в режиме широковещательного сервера. Режим широковещательного сервера настроен на порт VLAN 2. Коммутатор A и коммутатор B работают в режиме широковещательного клиента. Режим широковещательного клиента настроен на VLAN 2.

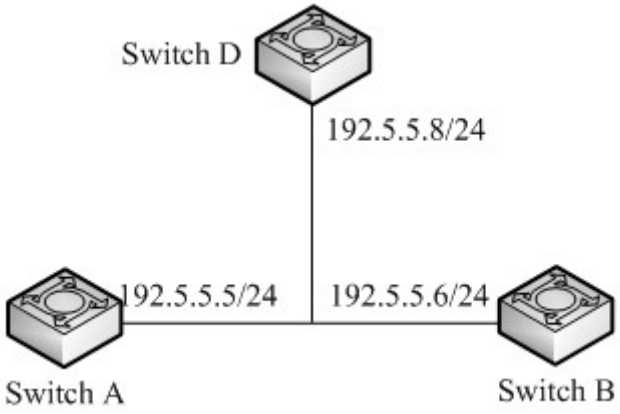


Рисунок 376 Сеть в широковещательном режиме

Конфигурация коммутатора D:

1. Включите NTP, как показано на рисунке 367.
2. Установите IP-адрес эталонных часов 127.127.0.1 и уровень часов 2, как показано на рисунке 373.
3. Настройте широковещательный сервер: Настройте широковещательный порт на VLAN 2, как показано на рисунке 371.

Конфигурация коммутатора A и коммутатора B:

4. Включите NTP, как показано на рисунке 367.
5. Настройте широковещательного клиента: Настройте широковещательный порт на VLAN 2, как показано на рисунке 372.

6.32 Настройка PTP

6.32.1 Введение

Протокол точного времени (PTP) с высокой точностью синхронизирует независимые часы на распределенных узлах системы измерения и управления. Протокол

синхронизирует фазу и частоту с точностью до ±100 нс. Примечание: В серии устройств PTP поддерживают только модели SICOM3028GPT-L2GT, SICOM3028GPT-L2FT, SICOM3028GPT-L3GT и SICOM3028GPT-L3FT.

6.32.2 Основные концепции

1. Домен PTP

Сеть, в которой применяется PTP, является доменом PTP. Домен PTP имеет только одни главные часы. Все остальные устройства синхронизируют время по ним.

2. Порт PTP

Порт с поддержкой PTP называется портом PTP.

3. Узел часов

Узлы в домене PTP являются узлами часов. PTP определяет следующие узлы часов:

- обычный тактовый генератор (OC)

  В домене PTP узел OC имеет только один порт, участвующий в синхронизации часов. Порт синхронизирует время с тактовым узлом восходящей линии связи или с тактовым узлом нисходящей линии связи.

- Граничный тактовый генератор (BC)

  В домене PTP узел BC имеет один или несколько портов PTP, участвующих в синхронизации часов. Если только один порт PTP участвует в синхронизации часов, порт синхронизирует время от узла часов восходящей линии или к узлу часов нисходящей линии. Если в синхронизации часов участвуют несколько портов PTP, один из этих портов синхронизирует время от узла синхронизации восходящей линии связи, а другие порты синхронизируют время с узлами синхронизации нисходящей линии связи. Когда BC служат источником синхронизации, они могут доставлять время на узлы синхронизации нисходящей линии связи через несколько портов PTP.

- Прозрачные часы (TC)

  Узлу TC не нужно синхронизировать время с другими узлами часов. Он имеет несколько портов PTP. Эти порты только пересылают пакеты PTP и проверяют задержку пересылки, но не выполняют синхронизацию часов. Часы прозрачной передачи делятся на следующие типы:

Прозрачные часы End-to-End Transparent Clock (E2ETC): напрямую пересылают не-PTP-пакеты и участвуют в расчете задержки для всего канала.

Прозрачные часы Peer-to-Peer Transparent Clock (P2PTC): напрямую пересылают пакеты Sync, Follow_Up и Announce, завершают другие пакеты PTP и участвуют в расчете задержки каждого сегмента канала.

4. Связь между парой узлов синхронных часов:

Узел, отправляющий информацию о синхронизации часов, находится в ведущем режиме (master), а узлы, получающие информацию, являются подчиненными (slave) узлами.

Часы узла master являются ведущими часами, а часы узла slave — подчиненными.

Порт, отправляющий информацию о синхронизации часов, находится в ведущем режиме (master), а порты, получающие информацию, являются подчиненными (slave) узлами.

6.32.3 Принципы синхронизации

1. Выбор гроссмейстерских часов

Все узлы часов выбирают гроссмейстерские часы в домене PTP, обмениваясь пакетами Announce с информацией об уровне часов и идентификаторе часов. Затем определяются отношения ведущий/подчиненный между узлами и портами ведущий/подчиненный на узлах. С помощью этого процесса по всему домену PTP устанавливается связующее дерево с гроссмейстерскими часами в качестве корня. Затем главные часы периодически посылают пакеты Announce подчиненным часам. Если подчиненные часы не получают пакеты Announce от главных часов в течение определенного периода, главные часы считаются недействительными и начинается новый выбор.

Пакеты Announce содержат следующую информацию для выбора гроссмейстерских часов: гроссмейстерский приоритет 1, тактовый слой, точность часов, гроссмейстерский приоритет 2 и идентификатор часов. Информация сравнивается в следующей процедуре: часы с наименьшим гроссмейстерским приоритетом 1 выбираются в качестве гроссмейстерских часов; если часы имеют одинаковое значение

гроссмейстерского приоритета 1, часы с наименьшим часовым слоем выбираются гроссмейстерскими часами; аналогичным образом, если часы имеют одинаковые значения для гроссмейстерского приоритета 1, слоя часов, точности часов, гроссмейстерского приоритета 2, часы с наименьшим идентификатором часов выбираются в качестве гроссмейстерских часов.

2. Принципы синхронизации

Главные и подчиненные часы обмениваются пакетами синхронизации, записывают время отправки и получения пакетов и вычисляют общую задержку между главными и подчиненными часами на основе разницы во времени. Если сетевой путь симметричен, однонаправленная задержка составляет половину общей задержки. Подчиненные часы настраивают местное время в соответствии с разницей во времени между главными и подчиненными часами и однонаправленной задержкой, реализуя синхронизацию времени от главных часов.

PTP поддерживает два механизма измерения задержки:

Механизм запроса-ответа: используется для измерения сквозной задержки всего канала. Одноранговый механизм: используется для измерения задержки между двумя точками. По сравнению с механизмом запроса-ответа, одноранговый механизм измеряет задержку каждого сегмента канала связи.

6.32.4 Настройка через веб-интерфейс

1. Включите PTP на порту.

Щелкните [Device Advanced Configuration] → [PTP configuration] → [PTP configuration], чтобы перейти на страницу настройки PTP, как показано на рисунке 377.

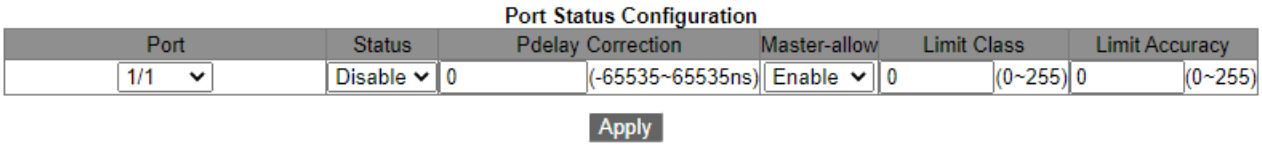


Рисунок 377 Включение PTP на порту

Состояние

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение функции PTP порта.

Pdelay Correction

Диапазон: -65535~65535 нс

По умолчанию: 0 нс

Функция: Настройте компенсацию задержки канала PTP.

Описание: При фиксированном смещении между ведущими и ведомыми часами необходимо настроить параметр ведомых часов для синхронизации фазы.

Master-allow

Варианты: Enable/Disable

По умолчанию: Enable

Функция: Этот параметр определяет, разрешено ли использовать текущий порт в качестве главного порта для запуска часов синхронизации. Если выбрано значение **Enable**, узел часов может синхронизировать другие сетевые часы через этот порт. Если выбрано значение **Disable** , узел часов не может синхронизировать другие сетевые часы через этот порт. Это предотвращает влияние узла часов на другие сетевые часы.

Limit Class

Диапазон: 0~255

По умолчанию: 0

Функция: Чтобы предотвратить влияние внешних источников синхронизации на текущую информацию о системных часах, настройте предельное значение уровня часов, чтобы ограничить уровень часов в пакете Announce, полученном этим портом. Если уровень синхронизации в пакете Announce, полученном этим портом, превышает предельное значение (то есть значение уровня часов меньше предельного значения),

измените уровень часов в пакете, чтобы он соответствовал предельному значению. В противном случае уровень часов в пакете не обрабатывается. Когда предельное значение равно 0, уровень часов в пакете Announce не ограничен.

Limit Accuracy

Диапазон: 0~255

По умолчанию: 0

Функция: Чтобы предотвратить влияние внешних источников синхронизации на текущую информацию о системных часах, настройте предельное значение точности часов, чтобы ограничить точность часов в пакете Announce, полученном этим портом. Если точность часов в пакете Announce, полученном этим портом, превышает предельное значение (то есть значение точности часов меньше предельного значения), измените точность часов в пакете, чтобы она соответствовала предельному значению. В противном случае точность часов в пакете не обрабатывается. Когда предельное значение равно 0, точность часов в пакете Announce не ограничена.

2. Настройте параметры PTP, как показано на рисунке 378.

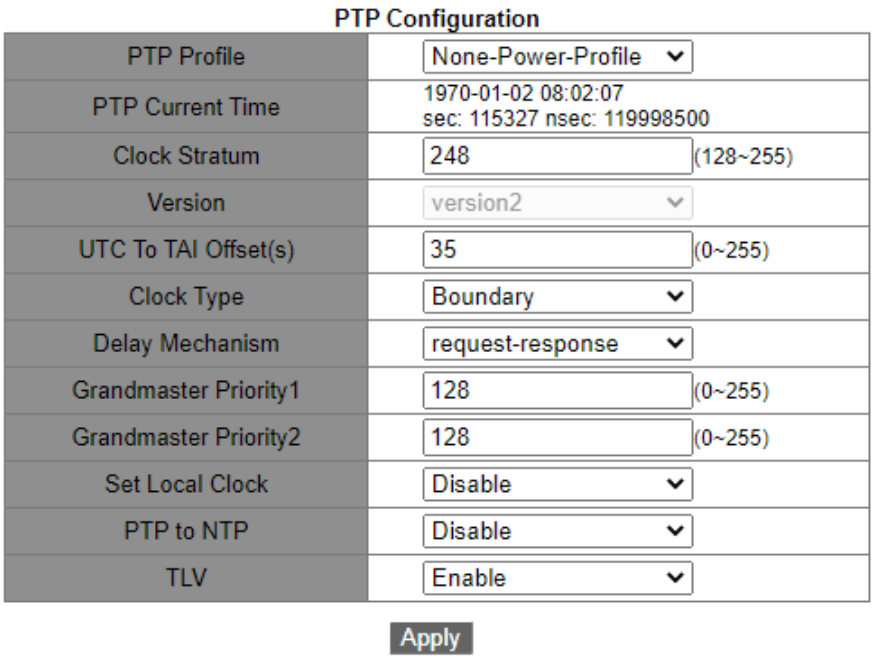


Рисунок 378 Настройка PTP

PTP Profile

Варианты: Power-Profile/None-Power-Profile

По умолчанию: None-Power-Profile

Функция: Настройка профиля PTP Профиль PTP указывает набор функций приложения PTP. Описание: Power-Profile — это набор функций PTP, которые позволяют использовать коммутатор в электроэнергетике. Например, «механизм задержки» принудительно настраивается как одноранговый, а TLV принудительно включается.

PTP Current Time

Функция: Просмотр информации о часах PTP коммутатора. Время PTP отображается в формате TAI.

Clock Stratum

Диапазон: 128~255

По умолчанию: 248

Функция: Выбор уровня часов.

Описание: Если часы имеют одинаковое значение гроссмейстерского приоритета 1, часы с наименьшим уровнем часов выбираются гроссмейстерскими часами. Если часы получают время от часов GPS, слой часов может быть автоматически сконфигурирован как 6, 7, 52 или 187, чтобы улучшить возможность быть избранными в качестве гроссмейстерских часов.

Пояснение: Уровень часов может быть настроен как 255, когда тип часов «только Slave». В ином случае уровень часов нельзя настроить как 255.

Примечание:

Когда GPS находится в фиксированном состоянии, уровень часов равен 6 (точность часов равна 0x21); когда GPS находится в состоянии блокировки, уровень часов равен 6 (точность часов равна 0x20); когда происходят сбои GPS, уровень часов равен 7 (точность часов составляет 0x23); когда время удержания истекает после сбоя GPS, уровень часов составляет 52 или 187 (точность часов составляет 0x30).

Version

Варианты: version2

По умолчанию: version2

Функция: Выбор версии PTP.

UTC To TAI Offset

Диапазон: 0~255 с

По умолчанию: 35 с

Функция: Настройка смещения UTC-To-TAI. Значение может быть перезаписано значением UTCOffSet, полученным из пакетов GPS или Announce главных часов. Соотношение между UTC, TAI и Offset следующее: UTC=TAI-Offset.

Clock Type

Варианты: Boundary/E2E/P2P/Slave-only

По умолчанию: Boundary

Функция: Выбор типа часов PTP.

Описание: Slave-only указывает, что часы ОС могут быть только подчиненными часами.

Delay Mechanism

Варианты: request-response/peer-to-peer

По умолчанию: request-response

Функция: Настройка механизма измерения задержки PTP.

Предупреждение:

- Узел часов, имеющий несколько доменов, должен быть настроен на граничный тип часов.
- Механизм задержки часов BC/OC может быть установлен на режим запрос-ответ или одноранговый.
- Если тип часов TC — E2ETC, механизм измерения задержки должен быть установлен в режим запрос-ответ.
- Если тип часов TC — P2PTC, механизм измерения задержки должен быть установлен в одноранговый режим.
- Механизм измерения задержки для всех устройств в одном и том же домене PTP должен быть одинаковым, поэтому типы всех часов TC в домене PTP должны быть одинаковыми.

Grandmaster priority1/Grandmaster priority2

Диапазон: 0~255

По умолчанию: 128

Функция: Настройка Grandmaster priority1 и Grandmaster priority2.

Описание: Grandmaster priority1 и Grandmaster priority2 используются для выбора гроссмейстерских часов. Часы с наименьшим гроссмейстерским приоритетом выбираются гроссмейстерскими часами.

Set Local Clock

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение или отключение функции синхронизации локального системного времени RTC с часами PTP. Локальное системное время RTC отображается в формате UTC.

PTP to NTP

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Обновлять/не обновлять время NTP временем PTP.

TLV

Варианты: Enable/Disable

По умолчанию: Enable

Функция: Включение TLV означает, что пакеты Announce содержат поле TLV.

Выключение TLV означает, что пакеты Announce не содержат поле TLV.

3. Настройте параметры TLV, как показано на рисунке 379.

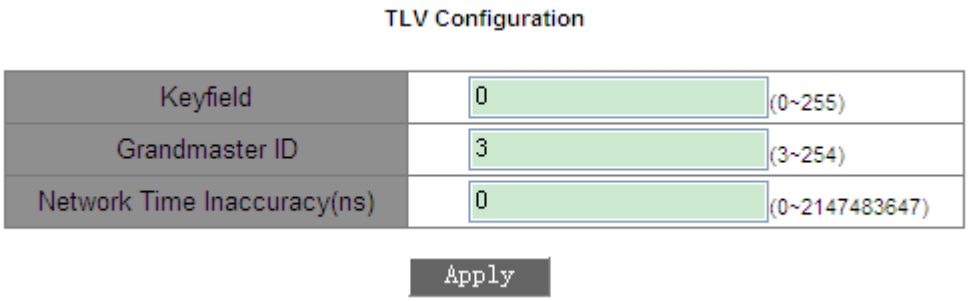


Рисунок 379 Настройка параметров TLV

Keyfield

Диапазон: 0~255

По умолчанию: 0

Функция: Настройка параметра Keyfield гроссмейстерских часов. Если тип поля TLV, переносимого пакетами Announce, — ALTERNATE_TIME_OFFSET_INDICATOR, этот параметр необходимо настроить.

Grandmaster ID

Диапазон: 3~254

По умолчанию: 3

Функция: Настройка идентификатора гроссмейстерских часов. Если тип поля TLV, переносимого пакетами Announce, — ORGANIZATION_EXTENSION, этот параметр необходимо настроить.

Network Time Inaccuracy

Диапазон: 0~2147483647 нс

По умолчанию: 0 нс

Функция: Настройка погрешности сетевого времени PTP. Если тип поля TLV, переносимого пакетами Announce, — ORGANIZATION_EXTENSION, этот параметр необходимо настроить как накопленную погрешности времени в наихудшем сетевом пути.

4. Настройка домена PTP

Щелкните [Device Advanced Configuration] → [PTP configuration] → [PTP Domain Configuration], чтобы перейти на страницу настройки домена PTP, как показано на рисунке 380.

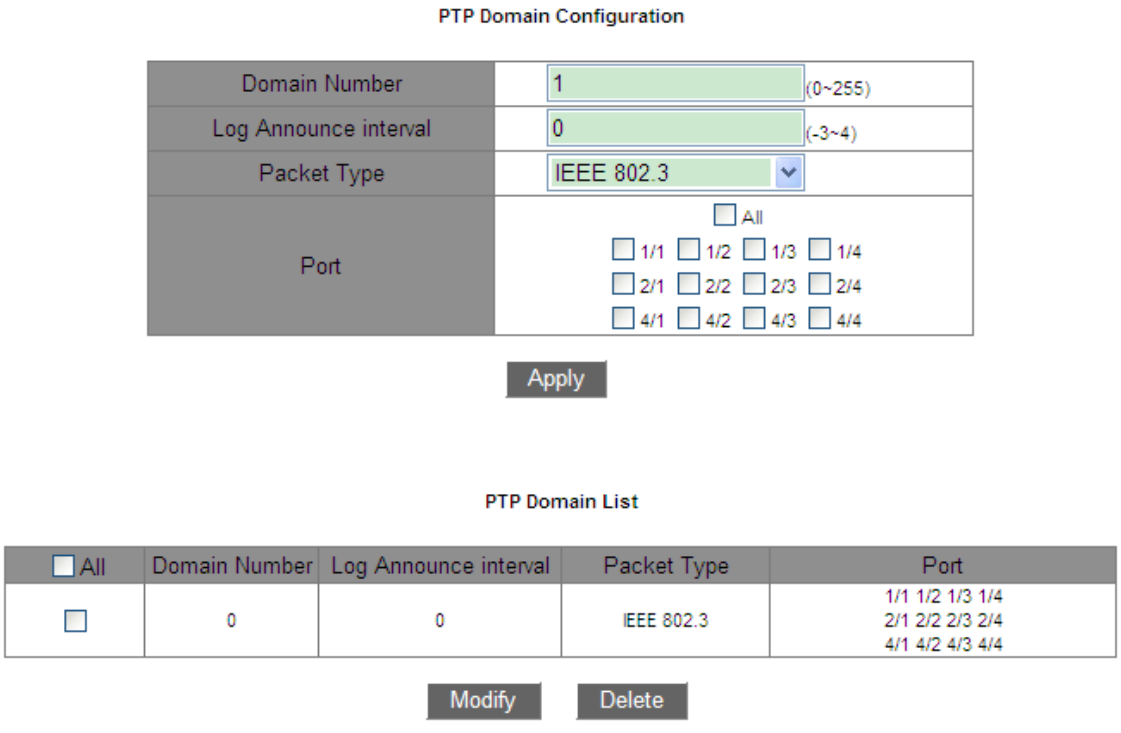


Рисунок 380 Настройка домена PTP

Domain Number

Диапазон: 0~255

По умолчанию: 0

Функция: Настройка идентификатора домена PTP.

Log Announce interval

Диапазон: -3~4

По умолчанию: 0

Функция: Настройка показателя интервала Announce.

Описание: Каждый узел отправляет пакеты Announce с интервалом 2^n с (n – показатель степени).

Packey Type

Варианты: IEEE802.3/IPv4 UDP

По умолчанию: IEEE802.3

Функция: Выбор типа пакетов, несущих информацию PTP.

Port

Функция: Выбор порта устройства в текущем домене PTP.

Примечание:

- Домен 0 — это PTP-домен системы по умолчанию, который нельзя удалить.
- Конфигурации типов пакетов всех устройств в одном домене PTP должны быть согласованными.
- Порт можно добавить только в один домен.

6.33 SyncE Configuration

6.33.1 Введение

Synchronous Ethernet (SyncE) синхронизирует функции PHY коммутаторов. Это позволяет обеспечить согласованную частоту между коммутаторами разных уровней. Если функция SyncE включена, PTP может обеспечить точность синхронизации ±50 нс. Как показано на рисунке 381, коммутатор B использует SyncE для синхронизации частоты передачи данных от коммутатора A; Коммутатор C также использует SyncE для синхронизации частоты передачи данных с коммутатора B, что в конечном итоге

обеспечивает постоянную частоту для всех коммутаторов во всей сети. Примечание: В серии устройств функцию SyncE поддерживают только модели SICOM3028GPT-L2GT, SICOM3028GPT-L2FT, SICOM3028GPT-L3GT и SICOM3028GPT-L3FT.

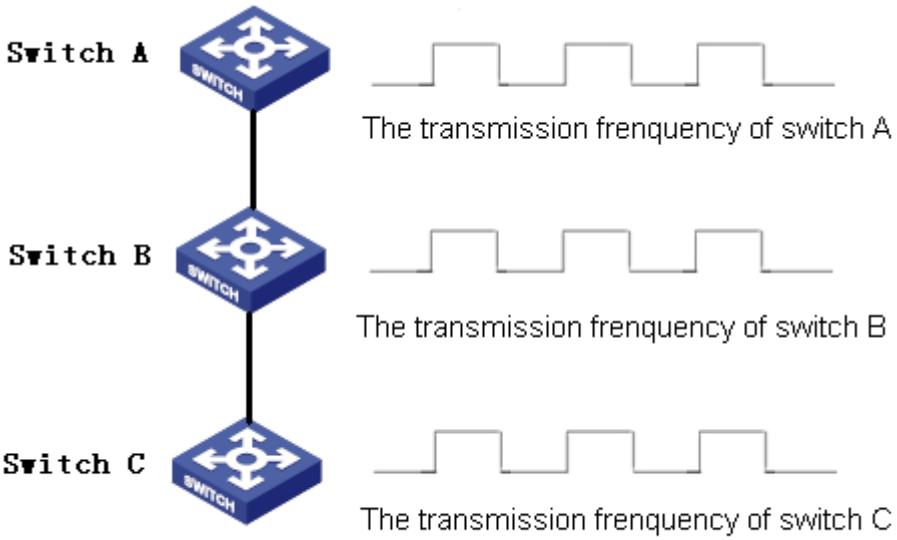


Рисунок 381 SyncE

Предупреждение:

- Коммутатор с поддержкой SyncE должен быть подключен к синхронизированному коммутатору линии связи uplink или главным часам.
- Поскольку функция SyncE синхронизирует только частоту, ее необходимо использовать вместе с PTP.
- Когда PTP используется вместе с SyncE, рекомендуется сначала включить SyncE, а затем включить и настроить PTP.

6.33.2 Настройка через веб-интерфейс

Включите режим SyncE. Щелкните [Device Advanced Configuration] → [Sync Ethernet Configuration] → [Sync Ethernet Mode], чтобы перейти на страницу настройки SyncE, как показано на рисунке 382.

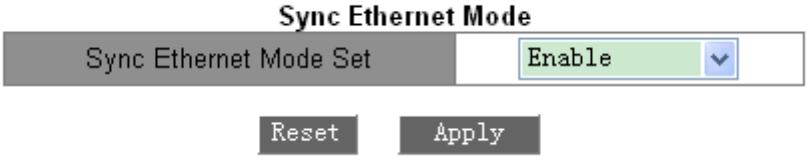


Рисунок 382 Настройка режима SyncE

Sync Ethernet Mode Set

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение фунции Sync Ethernet.

Описание: После включения функции коммутатор будет синхронизировать частоту с подключенным коммутатором линии связи uplink.

6.33.3 Типовой пример конфигурации

Как показано на рисунке 383, порт 1 коммутатора A подключен к порту 2 коммутатора B, а порт 3 коммутатора B подключен к порту 4 коммутатора C. Коммутатор A является ведущим (тип часов BC). Коммутатор B использует тип часов P2PTC. Коммутатор C является ведомыми часами (тип часов BC) и синхронизирует время с коммутатором A с помощью протоколов SyncE и PTP. Механизм измерения задержки одноранговый.

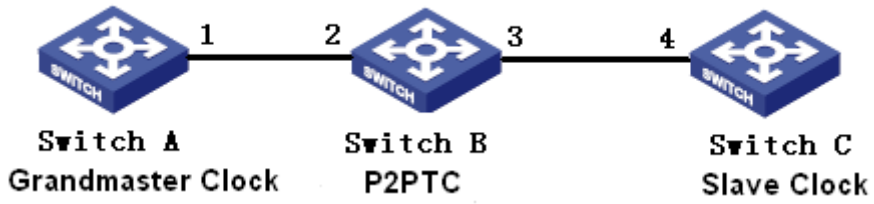


Рисунок 383 Пример настройки PTP+SyncE

Конфигурация коммутатора A:

1. Включите PTP на порту 1 коммутатора A, как показано на рисунке 377.

2. Установите тип часов Boundary. Поскольку коммутатор A является ведущими часами, он должен иметь высший гроссмейстерский приоритет 1. В этом примере установите гроссмейстерский приоритет priority1 128, а механизм измерения задержки peer-to-peer, как показано на рисунке 378.

Конфигурация коммутатора B:

3. Включите SyncE на коммутаторе B, как показано на рисунке 382.

4. Включите PTP на порту 2 и порту 3 коммутатора B, как показано на рисунке 377.

5. Установите тип часов P2PTC, гроссмейстерский приоритет 1 – 210 и механизм измерения задержки – одноранговый, как показано на рисунке 378.

Конфигурация коммутатора C:

6. Включите SyncE на коммутаторе C, как показано на рисунке 382.

7. Включите PTP на порту 4 коммутатора C, как показано на рисунке 377.

8. Установите тип часов Boundary, гроссмейстерский приоритет 1 – 220 и механизм измерения задержки – одноранговый, как показано на рисунке 378.

6.34 Настройка GPS

6.34.1 Введение

Глобальная система позиционирования (GPS) — это продвинутая сложная система спутникового позиционирования с глобальным и непрерывным высокоточным трехмерным позиционированием в режиме реального времени и возможностью точной синхронизации.

Модуль синхронизации часов GPS коммутаторов этой серии представляет собой элементарный прикладной модуль синхронизации, разработанный на основе GPS. Модуль получает информацию со спутника, выводит второй импульсный сигнал, точно синхронизированный с международным стандартным временем, и синхронизирует информацию о точном времени со всей системой, чтобы обеспечить службу синхронизации времени.

Примечание: В серии устройств расширенную синхронизацию часов GPS поддерживают только модели SICOM3028GPT-L2GT, SICOM3028GPT-L2FT, SICOM3028GPT-L3GT и SICOM3028GPT-L3FT.

6.34.2 Настройка через веб-интерфейс

Настройте GPS: Щелкните [Device Advanced Configuration] → [GPS configuration] → [GPS configuration], чтобы перейти на страницу настройки GPS, как показано на рисунке 384.

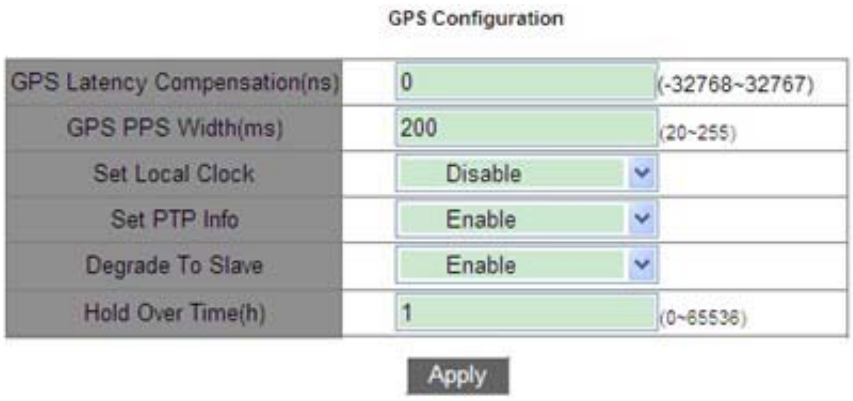


Рисунок 384 Настройка GPS

GPS Latency Compensation

Диапазон: -32768~32767 нс

По умолчанию: 0 нс

Функция: Настройка компенсации задержки GPS.

GPS PPS Width

Диапазон: 20~255 мс

По умолчанию: 200 мс

Функция: Настройка ширины PPS GPS.

Set Local Clock

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение или отключение функции синхронизации локального системного времени RTC с часами GPS. Локальное системное время RTC отображается в формате UTC.

Set PTP Info

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение или отключение функции синхронизации времени PTP с часами GPS. Время PTP отображается в формате TAI. TAI_Time-GPS_time=19 с.

Degrade To Slave

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Разрешить/не разрешить текущим часам снижаться до часов Slave при возникновении сбоев GPS.

Hold Over Время

Диапазон: 0~65535 ч

По умолчанию: 1 ч

Функция: Когда происходят сбои GPS, GPS по-прежнему будет использоваться в качестве источника часов для синхронизации времени PTP текущего устройства, если GPS находится в удержании в течение определенного времени. Когда время удержания истекает, значение уровня часов устройства будет автоматически настроено на 187, и, если включена функция понижения до Slave, запустится повторная процедура выбора главных часов. Если функция понижения до Slave отключена, уровень часов устройства будет автоматически настроен на 52 и также произойдет выбор новых главных часов.

6.34.3 Типовой пример конфигурации

Как показано на рисунке 385, коммутатор A получает информацию точного времени через модуль GPS и синхронизирует информацию со всей сетью через PTP. Коммутатор A является главными часами (BC), на коммутаторе B (BC) есть домен 1 и домен 2, а коммутатор C является подчиненными часами, синхронизирует время с

коммутатора A с помощью протоколов PTP.

Коммутатор B подключен к другому источнику синхронизации внешней сети. Эта внешняя сеть не зависит от текущих системных часов. Когда GPS неисправен, коммутатор B может получать информацию о времени из источников внешней сети через протокол PTP и синхронизировать информацию о времени со всей сетью.

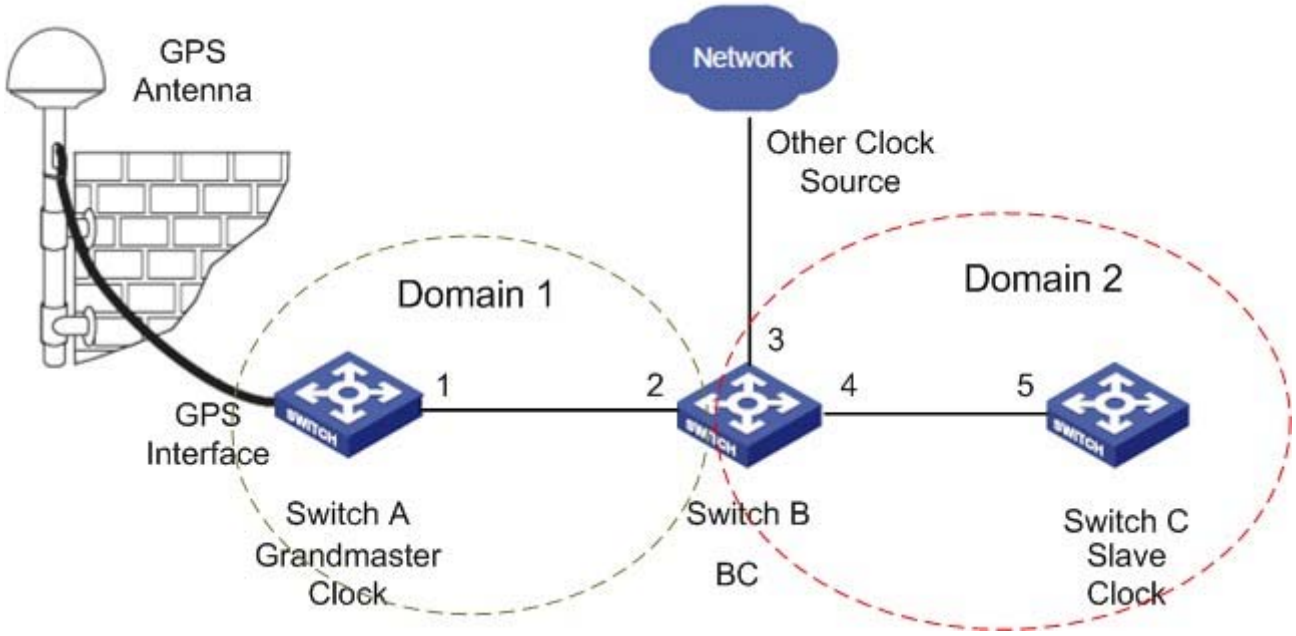


Рисунок 385 Пример настроек GPS+PTP

Конфигурация коммутатора A:

1. Настройте информацию GPS. Включите PTP и разрешите понижение GPS до ведомого, как показано на рисунке 384.

2. Включите PTP на порту 1 коммутатора A, как показано на рисунке 377.

3. Установите тип часов Boundary. Механизм задержки – одноранговый, как показано на рисунке 378.

4. Настройте домен 1, добавьте порт 1 в домен 1, как показано на рисунке 380.

Конфигурация коммутатора B:

1. Включите PTP на порту 2 и порту 4 коммутатора B, как показано на рисунке 377.

2. Включите PTP на порту 3 коммутатора B, запретите режим master для порта 3, установите значение класса равным 53, ограничьте точность до 33, как показано на рисунке 377.

3. Установите тип часов Boundary, механизм задержки – одноранговый, как показано на рисунке 378.

4. Настройте домен 1 и домен 2, добавьте порт 2 в домен 1, порт 3 и порт 4 в домен 2, как показано на рисунке 380.

Конфигурация коммутатора C:

1. Включите PTP на порту 5 коммутатора C, как показано на рисунке 377.

2. Установите тип часов Boundary, механизм задержки – одноранговый, как показано на рисунке 378.

3. Настройте домен 2, добавьте порт 5 в домен 2, как показано на рисунке 380.

6.35 Настройка IRIG-B

6.35.1 Введение

Код Inter Range Instrumentation Group (IRIG) - это стандарт времени, установленный American Range Commanders Council (RRC). Код IRIG широко применяется в различных областях, включая военный, коммерческий и промышленный секторы. Коды IRIG делятся на шесть последовательных двоичных форматов временного кода: IRIG-A, IRIG-B, IRIG-D, IRIG-E, IRIG-G и IRIG-H. Среди этих форматов наиболее широко используется IRIG-B. Временной кадр для стандарта IRIG-B составляет 1 секунду, что означает, что один кадр данных с информацией о времени передается каждую секунду. Этот кадр данных содержит информацию о дне года (1~366), часах, минутах и секундах. Примечание: Среди коммутаторов этой серии только SICOM3028GPT-L3GT, SICOM3028GPT-L3FT, SICOM3028GPT-L2GT и SICOM3028GPT-L2FT поддерживают расширенную синхронизацию часов GPS.

6.35.2 Настройка через веб-интерфейс

Настройте IRIG-B: Щелкните [Device Advanced Configuration] → [IRIG B configuration] → [IRIG B configuration], чтобы перейти на страницу настройки IRIG-B, как показано на рисунке 386.

Рисунок 386 Настройка параметров IRIG-B

IRIG-B Slot ID

Функция: Выберите настраиваемый модуль IRIG-B.

PPS Width

Диапазон: 20~255 мс

По умолчанию: 200 мс

Функция: Настройка ширины PPS.

IRIG-B format

Варианты: Irig-b000~Irig-b007

По умолчанию: Irig-b004

Функция: Выбор выходного формата IRIG-B.

VPP

Варианты: 3/4/4.5/5/6/7/8/9/10Vp-p

По умолчанию: 4.5Vp-p

Функция: Настройка выхода IRIG-B VP-P для модуляции AM.

Modulate Ratio

Варианты: 3:1/4:1/5:1/6:1

По умолчанию: 3:1

Функция: Настройка коэффициента модуляции AM для IRIG-B.

Parity Mode

Варианты: Even/Odd

По умолчанию: Even

Функция: Выбор режима четности для IRIG-B.

6.36 Настройка TACACS+

6.36.1 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 387 показана структура.

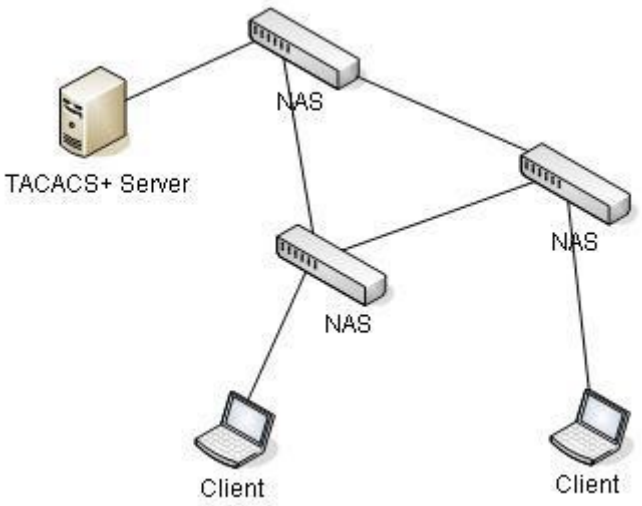


Рисунок 387 Структура TACACS+

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.

6.36.2 Настройка через веб-интерфейс

1. Включите TACACS+.

Щелкните [Device Advanced Configuration] → [TACACS-PLUS Configuration] → [TACACS-PLUS configuration] , чтобы перейти на страницу настройки TACACS+, как показано на рисунке 388.

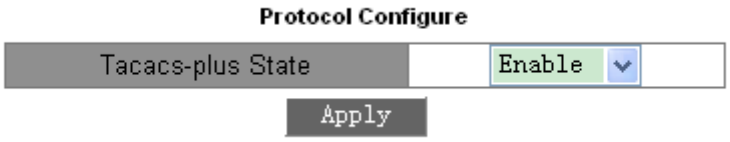


Рисунок 388 Включение TACACS+

TACACS-PLUS State

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение TACACS+.

2. Настройте сервер TACACS+, как показано на рисунке 389.

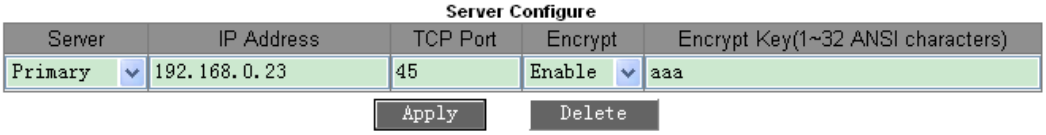


Рисунок 389 Конфигурация сервера TACACS+

Server

Варианты: Primary/Secondary

По умолчанию: Primary

Функция: Выбор типа сервера.

IP Address

Формат: A.B.C.D

Функция: Введите IP-адрес сервера.

TCP port

Диапазон: 1~65535

По умолчанию: 49

Функция: Задание количества портов, которые получают запросы аутентификации NAS.

Encrypt

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение шифрования пакетов. Если функция включена, требуется ключ.

Encrypt Key

Диапазон: 1~32 символа

Описание: 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+.

После завершения настройки Sever Configured показывает информацию о конфигурации сервера, как показано на рисунке 390.

Server Configured			
Primary Server	192.168.0.23	49	Encrypt
Secondary Server	192.168.0.32	45	Unencrypt

Рисунок 390 Список настроек сервера

6.36.3 Типовой пример конфигурации

Как показано на рисунке 391, 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.

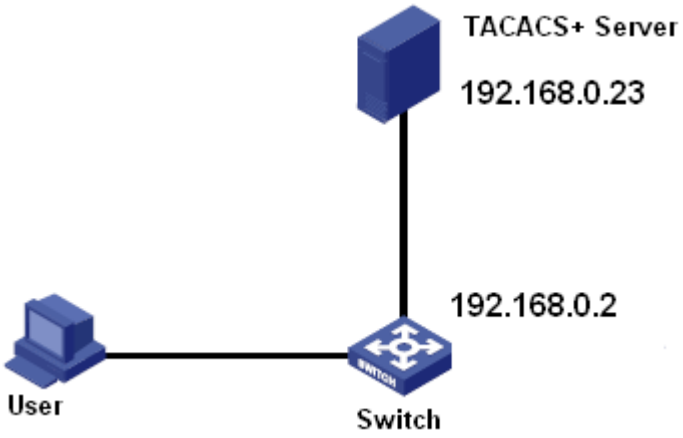


Рисунок 391 Пример аутентификации TACACS+

1. Включите TACACS+, как показано на рисунке 388.
2. Настройка сервера TACACS+. Задайте IP-адрес сервера 192.168.0.23 и значение ключа Encrypt aaa, включите функцию Encrypt, как показано на рисунке 389.
3. При входе в коммутатор через веб-интерфейс выберите Local, при входе в коммутатор через telnet выберите TACACS+, как показано на рисунке 403.
4. Настройте имя пользователя и пароль bbb, зашифруйте ключ aaa на сервере TACACS+.
5. При входе в коммутатор через веб-интерфейс введите имя пользователя admin и пароль 123, чтобы пройти локальную аутентификацию.
6. При входе в коммутатор через Telnet введите имя пользователя и пароль bbb, чтобы пройти аутентификацию TACACS+.

6.37 Настройка RADIUS

6.37.1 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 392 показана структура.

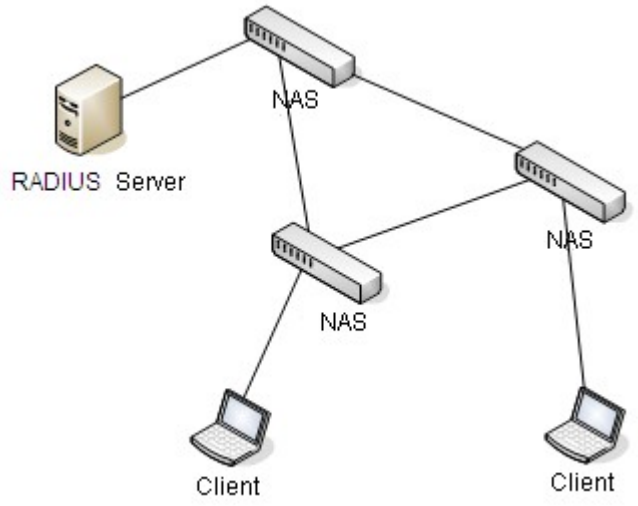


Рисунок 392 Структура RADIUS

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.

6.37.2 Настройка через веб-интерфейс

1. Настройте параметры RADIUS

Щелкните [Device Advanced Configuration] → [RADIUS configuration] → [RADIUS configuration], чтобы перейти на страницу настройки RADIUS, как показано на рисунке 393.

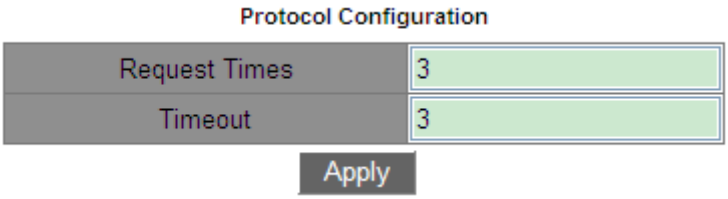


Рисунок 393 Настройка параметров RADIUS

Request Times

Диапазон: 1~3

По умолчанию: 3

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.

Timeout

Диапазон: 1~3

По умолчанию: 3

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.

2. Настройте сервер RADIUS, как показано на рисунке 394.

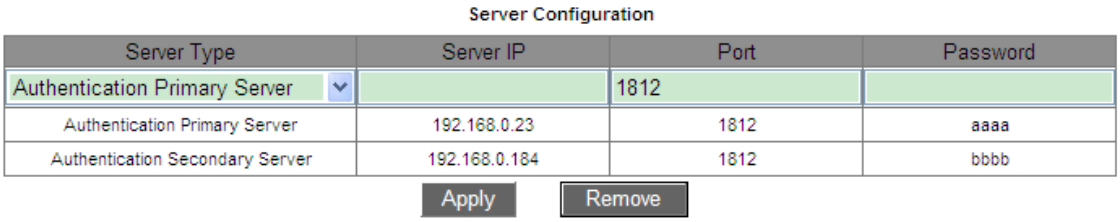


Рисунок 394 Настройка сервера RADIUS

Server Type

Варианты: Authentication Primary Server/Authentication Secondary Server

Функция: Настройка первичного или вторичного сервер RADIUS. Если первичный сервер недоступен, для аутентификации будет использоваться вторичный сервер.

Server IP

Формат: A.B.C.D

Функция: Настройка IP-адреса сервера RADIUS.

Port

Диапазон: 1~65535

По умолчанию: 1812

Функция: Задание порта UDP сервера RADIUS.

Password

Диапазон: 1~32 символа

Функция: Настройка пароля сервера RADIUS.

6.37.3 Типовой пример конфигурации

Как показано на рисунке 395, 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 — аааа.

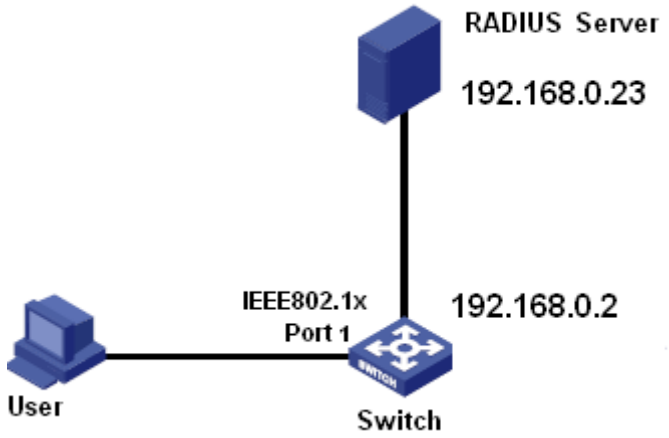


Рисунок 395 Пример аутентификации RADIUS

1. Задайте IP-адрес сервера аутентификации 192.168.0.23 и пароль аааа, как показано на рисунке 394.
2. Настройки IEEE802.1x: включить IEEE802.1X глобально. Включите IEEE802.1x для порта 1. Оставьте настройки по умолчанию для других параметров. Подробности см. в разделе 6.38 Настройка IEEE802.1X.
3. Установите dot1x для аутентификации RADIUS, как показано на рисунке 403.
4. Установите для имени пользователя и пароля на сервере RADIUS значение ссс, для ключа шифрования — аааа.
5. Установите и запустите клиентское ПО 802.1x на ПК. Введите ссс в качестве имени пользователя и пароля. Затем пользователь может пройти аутентификацию и получить доступ к коммутатору через порт 1.

6.38 Настройка IEEE802.1X

6.38.1 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 на рисунке 146. Аутентификация и авторизация пользователя при управлении доступом на основе порта требуют следующих элементов:

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.

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.

6.38.2 Настройка через веб-интерфейс

1. Включите глобальный протокол IEEE802.1x.

Щелкните [Device Advanced Configuration] → [IEEE802.1x configuration] → [IEEE802.1x configuration], чтобы перейти на страницу настройки IEEE802.1x, как показано на рисунке 396.

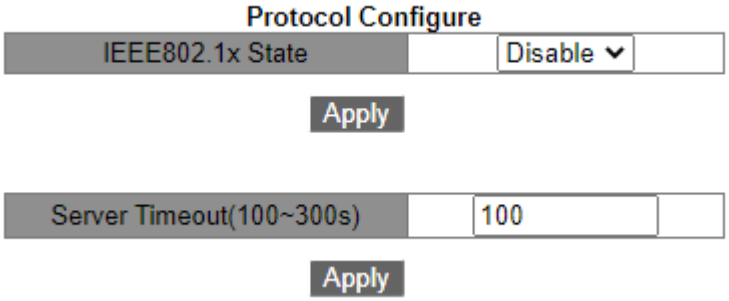


Рисунок 396 Включение глобального IEEE802.1x

IEEE802.1x State

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение глобальных функций безопасности IEEE802.1x.

Server Timeout

Диапазон: 100~300 с

По умолчанию: 100 с

Функция: После того, как устройство отправляет сообщение RADIUS Access-Request на сервер аутентификации, устройство запускает этот таймер. Если устройство не получит ответ от сервера аутентификации до истечения времени ожидания, устройство повторно отправит сообщение запроса аутентификации.

2. Настройте порт, на котором включен IEEE802.1x, как показано на рисунке 397.

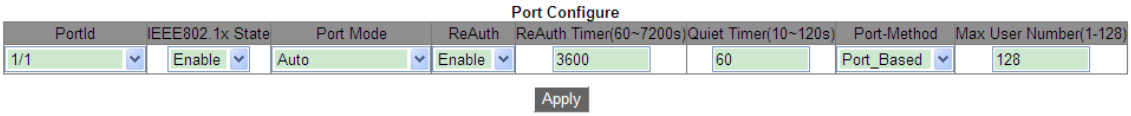


Рисунок 397 Настройка порта IEEE802.1x

PortId

Варианты: все порты коммутатора.

IEEE802.1x State

Options: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение IEEE802.1x для порта.

Описание: Когда эта функция включена, обмен данными пользователей через порт зависит от режима порта IEEE802.1x.

Режим порта

Варианты: Unauthorized-force/Auto/Authorized-force

По умолчанию: Auto

Функция: Выбор режима аутентификации для порта.

Описание: **Unauthorized-force** 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. Авто означает, что в начальном состоянии порт неавторизован, и порт не позволяет пользователям получать доступ к сетевым ресурсам. Если пользователь проходит аутентификацию, порт переходит в авторизованное состояние и позволяет пользователям получать доступ к сетевым ресурсам. Если пользователю не удастся пройти аутентификацию, порт перейдет в неавторизованное состояние и не позволит пользователям получить доступ к сетевым ресурсам. **Authorized-force** означает, что порт всегда находится в авторизованном состоянии и позволяет пользователям получать доступ к сетевым ресурсам без аутентификации.

ReAuth

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Требуется ли регулярная повторная аутентификация при успешной аутентификации.

ReAuth Timer

Диапазон: 60~7200 с

По умолчанию: 3600 с

Функция: Установка временного интервала для повторной аутентификации после успешной аутентификации.

Quiet Timer

Диапазон: 10~120 с

По умолчанию: 60 с

Функция: В случае сбоя аутентификации начинается период молчания (QuietPeriod). В период молчания сервер не отвечает на запросы аутентификации от клиента. После окончания периода молчания сервер снова начинает принимать запросы аутентификации.

Port-Method

Варианты: Port_ Based/ MAC_ Based

По умолчанию: Port_ Based

Функция: Настройка режима управления доступом для портов с поддержкой IEEE802.1x.

Описание: 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.

Max User Number

Диапазон: 1~128

По умолчанию: 128

Функция: Настройка максимального количество пользователей с доступом через порт с поддержкой IEEE802.1x.

Описание: Конфигурация действительна только для портов с управлением доступом на основе MAC-адресов.

3. Просмотр конфигурации IEEE802.1X

Щелкните [Device Advanced Configuration] → [IEEE802.1x configuration] → [IEEE802.1x information], чтобы просмотреть настройки IEEE802.1x, как показано на рисунке 398.

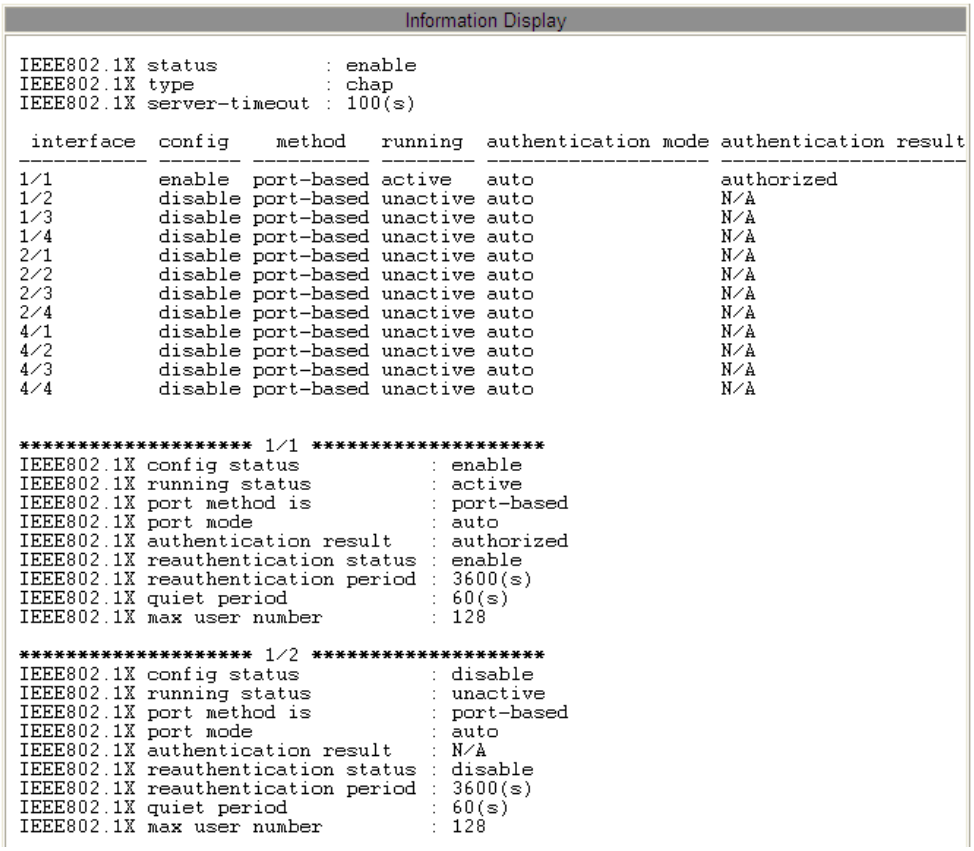


Рисунок 398 Просмотр настроек IEEE802.1X

4. Настройте группу IEEE802.1X

Щелкните [Device Advanced Configuration] → [IEEE802.1x configuration] → [IEEE802.1x Group configuration], чтобы перейти на страницу настройки группы IEEE802.1x, как показано на рисунке 399.

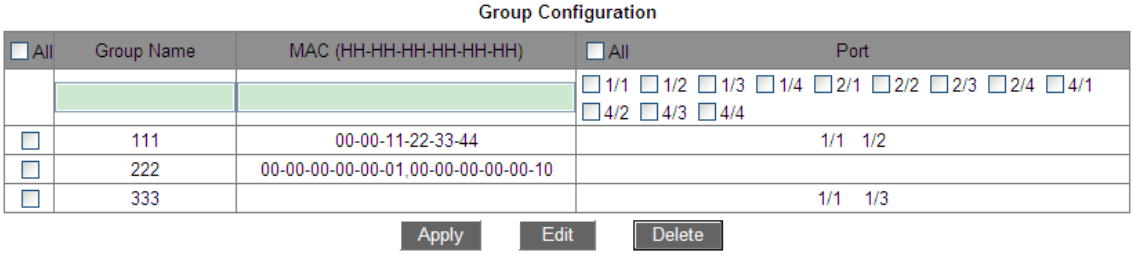


Рисунок 399 Настройка группы IEEE802.1x

Group Name

Диапазон: 1~16 символов

Функция: Настройка имени группы.

MAC

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

Функция: Настройка MAC-адреса группы. В одну группу можно добавить несколько MAC-адресов, при этом MAC-адреса разделяются однобайтовыми запятыми.

Port

Функция: Добавление портов в группу.

Примечание:

Группа аутентификации пользователя позволяет настраивать только MAC-адрес или номер порта.

5. Настройка информации пользователя IEEE802.1x

Щелкните Click [Device Advanced Configuration] → [IEEE802.1x configuration] → [IEEE802.1x User configuration], чтобы перейти на страницу настройки пользователя IEEE802.1x, как показано на рисунке 400.

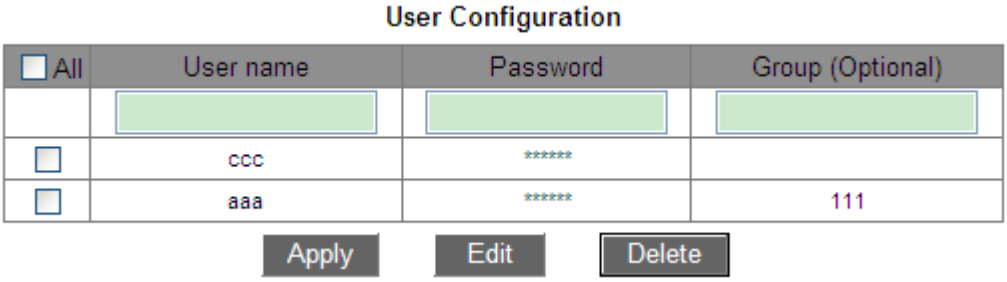


Рисунок 400 Настройка пользователя IEEE802.1x

User Name

Диапазон: 1~16 символов

Функция: Настройка имени пользователя IEEE802.1x.

Password

Диапазон: 1~16 символов

Функция: Настройка пароля IEEE802.1X.

Group

Функция: Привязка пользователя к группе.

Описание: Если текущий пользователь привязан к группе аутентификации пользователей, только пользователь, чей MAC-адрес и номер порта доступа совпадают с привязанной группой, может пройти аутентификацию и получить доступ к коммутатору. Также допускается, чтобы текущий пользователь не был привязан ни к какой группе аутентификации пользователей. В этом случае пользователи могут проводить аутентификацию, используя любой MAC-адрес и номер порта.

6. Просмотр информации о пользователе IEEE802.1x в режиме онлайн

Щелкните[Device Advanced Configuration] → [IEEE802.1x configuration] → [IEEE802.1x On-line user], чтобы просмотреть информации о пользователе IEEE802.1x в режиме онлайн, как показано на рисунке 401.

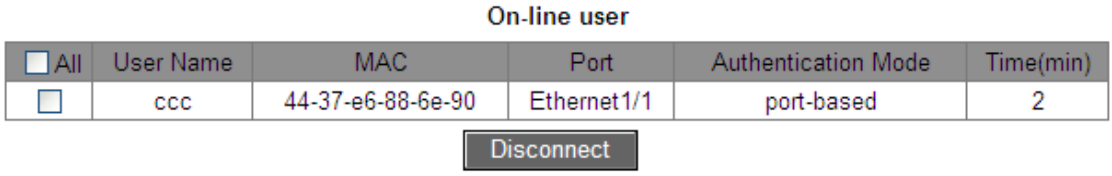


Рисунок 401 Просмотр информации о пользователе IEEE802.1x в режиме онлайн

Можно выбрать одного или нескольких пользователей и нажать <Disconnect>, чтобы отключить выбранных пользователей от коммутатора.

6.38.3 Типовой пример конфигурации

Как показано на рисунке 402, клиент подключен к порту 1 коммутатора. Включите IEEE802.1x для порта 1 и выберите режим аутентификации Auto. Имя пользователя и пароль для локальной аутентификации ccc, а имя пользователя и пароль для удаленной аутентификации ddd. Сохраните значения по умолчанию для остальных параметров.

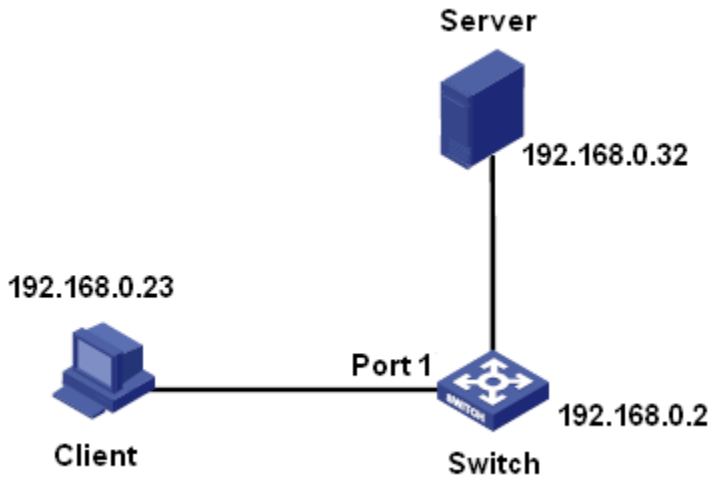


Рисунок 402 Пример настроек IEEE802.1X

➢ Настройка локальной аутентификации

1. Включите глобальный протокол IEEE802.1x, как показано на рисунке 396.

2. Установите dot1x для локальной аутентификации, как показано на рисунке 403.

3. Задайте имя пользователя и пароль ccc, как показано на рисунке 400.

4. Включите IEEE802.1x для порта 1 и выберите режим аутентификации Auto, как показано на рисунке 397.

5. Установите клиентское ПО аутентификации 802.1x и запустите его. Введите имя пользователя и пароль ccc, чтобы пройти аутентификацию. Теперь можно осуществить доступ к коммутатору.

➢ Настройка удаленной аутентификации

Можно ознакомиться с примером типовой конфигурации в 6.37 Настройка RADIUS.

6.39 Настройка аутентификации при входе

Настройте режим доступа к коммутатору, режим аутентификации и порядок аутентификации.

Щелкните [Device Advanced Configuration] → [Authentication login configuration] → [Authentication login configuration], чтобы перейти на страницу настройки аутентификации при входе, как показано на рисунке 403.

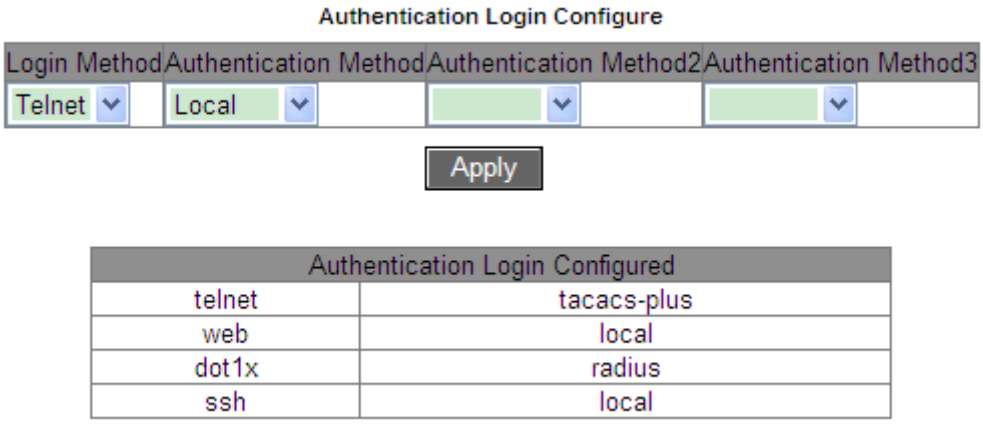


Рисунок 403 Настройка аутентификации при входе

Login Method

Варианты: Telnet/Web/dot1x/SSH

Функция: Выбор режима доступа к коммутатору.

Authentication Method/Authentication Method 2/Authentication Method 3

Варианты: Local/TACACS+/RADIUS/ RADIUS+ Local/ TACACS Plus+ Local

По умолчанию: Локальный

Функция: Выбор порядка аутентификации. Сначала выполняется метод аутентификации method 1. Если аутентификация не удалась, применяется метод аутентификации method 2. Если и метод аутентификации 1, и метод аутентификации 2 неудачны, выполняется метод аутентификации method 3.

Описание: **Local** означает использование для аутентификации имени пользователя и пароля, установленных локально. **TACACS+** означает использование для аутентификации имени пользователя и пароля, установленных на сервере TACACS+. **RADIUS** означает использование для аутентификации имени пользователя и пароля, установленных на сервере RADIUS.

Предупреждение:

При использовании dot1x для для доступа к коммутатору можно выбрать только один режим аутентификации.

6.40 Настройка диагностики

6.40.1 Проверка канала связи

6.40.1.1 Введение

Проверка канала использует периодическое взаимодействие пакетов протокола для оценки подключения канала и отображения состояния связи порта. В случае неисправности проблема может быть обнаружена и устранена вовремя.

Порт, для которого включена проверка состояния соединения, периодически (каждую 1 с) отправляет пакеты для проверки состояния соединения. Если порт не получает пакет проверки канала от одноранговой стороны в течение времени ожидания приема (5 с), это означает, что канал неисправен, и порт отображает состояние ошибки Rx. Если порт получает пакет проверки канала от одноранговой стороны, и пакет показывает, что пакет проверки канала получен от локального узла в течение периода

ожидания приема (5 с), порт отображает нормальное состояние. Если порт получает пакет проверки канала от одноранговой стороны, но пакет показывает, что пакет проверки канала не получен от локального узла в течение периода ожидания приема (5 с), порт отображает состояние ошибки Tx. Если связь с портом не работает, порт отображает состояние Link Down.

Порт, для которого отключена проверка состояния канала, работает в пассивном режиме. Это значит, что он не отправляет пакет проверки связи в активном режиме. Однако после получения пакета проверки канала от удаленного узла этот порт немедленно возвращает пакет проверки канала, чтобы проинформировать удаленный узел о том, что он получил пакет проверки канала.

Примечание:

Если кольцевой/резервный порт DRP, для которого включена проверка канала, неисправен (например, прием ненормальный, отправка ненормальная или он отключен), кольцевой протокол DRP заблокирует этот кольцевой/резервный порт.

6.40.1.2 Настройка через веб-интерфейс

1. Включите проверку канала связи для порта.

Щелкните [Device Advanced Configuration] → [Diagnosis Configuration] → [Link Check], чтобы перейти на страницу настройки проверки канала связи, как показано на рисунке 404.

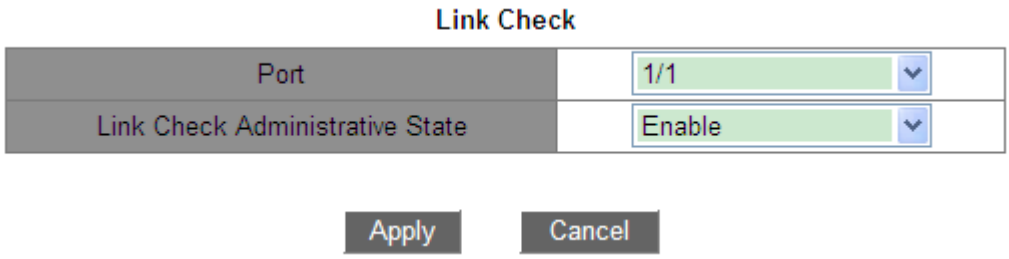


Рисунок 404 Включение проверки канала связи для порта

Link Check Administrative State

Варианты: Disable/Enable

По умолчанию: Disable

Функция: Включение/выключение проверки канала связи для порта.

Предупреждение:

Если одноранговое устройство не поддерживает эту функцию, функция должна быть на подключенном порту локального устройства.

2. Отобразите состояние проверки канала связи на порту, как показано на рисунке 405.

Port	Link Check State
1/1	Link Down
1/2	Disable
1/3	Disable
1/4	Disable
2/1	Normal
2/2	Link Down
2/3	Disable
2/4	Rx Fault
4/1	Disable
4/2	Disable
4/3	Disable
4/4	Disable

Рисунок 405 Отображение состояние проверки канала связи на порту

Link Check State

Варианты: Normal/Rx Fault/Disable/Tx Fault/Link Down

Описание: Если для порта включена функция Link Check и порт нормально отправляет и принимает данные, отображается Normal. Если одноранговое устройство не получает пакеты обнаружения от устройства, отображается Tx Fault. Если устройство не получает пакеты обнаружения от одноранговое устройства, отображается Rx Fault. Если порт отключен, отображается Link Down. Если функция Link Check не включена для порта, отображается Disable.

6.40.2 Виртуальный кабельный тестер

6.40.2.1 Введение

VCT (Virtual Cable Tester) использует технологию Time Domain Reflectometry (TDR) для определения состояния витой пары. Он передает импульсный сигнал кабелю и обнаруживает отражение импульсного сигнала для обнаружения неисправности кабеля. Если в кабеле происходит аварийное переключение, часть или вся энергия импульса будет отражаться обратно к источнику, когда передаваемый импульсный сигнал достигает конца кабеля или точки повреждения, и технология VCT может измерять время прибытия сигнала в точку повреждения и время возврата к отправителю, затем вычисляет расстояние в соответствии со временем.

Технология VCT может обнаруживать среду соединения, соединяющую медные порты Ethernet, и отправлять обратно результат обнаружения. VCT может обнаруживать следующие типы повреждений кабеля:
Short: означает короткое замыкание. Это замыкание двух и более проводов. Open: означает разомкнутую цепь. В кабеле могут быть оборванные провода. Normal: означает нормальное кабельное соединение.
Imped: означает несоответствие импеданса. Например, импеданс кабеля Cat.5 составляет 100 Ом, импеданс терминаторов на обоих концах кабеля должен быть 100 Ом, чтобы избежать отражения волны и ошибки данных.
Fail: означает, что тест VCT не пройден.

6.40.2.2 Настройка через веб-интерфейс

Определение кабеля

Щелкните [Device Advanced Configuration] → [Diagnosis Configuration] → [Virtual Cable Tester], чтобы перейти на страницу настройки виртуального кабельного тестера, как показано на рисунке 406.

Virtual Cable Tester

All/Port	Port Type	Cable Pairs	Cable Status	Cable Length(m)
2/1	GE	(1,2)	No history	No history
		(3,6)	No history	No history
		(4,5)	No history	No history
		(7,8)	No history	No history
2/2	GE	(1,2)	No history	No history
		(3,6)	No history	No history
		(4,5)	No history	No history
		(7,8)	No history	No history
2/3	GX	(1,2)	No history	No history
		(3,6)	No history	No history
		(4,5)	No history	No history
		(7,8)	No history	No history
2/4	GX	(1,2)	No history	No history
		(3,6)	No history	No history
		(4,5)	No history	No history
		(7,8)	No history	No history

Test Test LinkDown Test LinkUp

Рисунок 406 Обнаружение VCT

6.41 Настройка обнаружения петель

6.41.1 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.

6.41.2 Настройка через веб-интерфейс

Настройте функцию обнаружения петель для порта.

Щелкните [Device Advanced Configuration] → [Loop Detect configuration] → [Loop Detect configuration], чтобы перейти на страницу настройки обнаружения петель, как показано на рисунке 407.

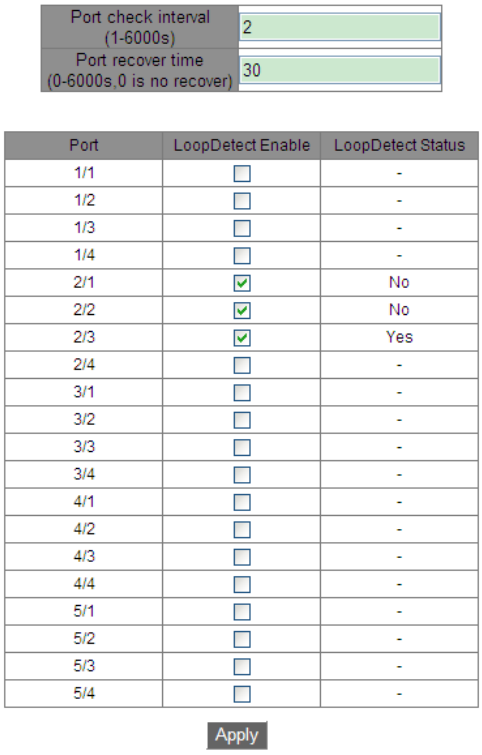


Рисунок 407 Включение функции обнаружения петель для порта

Port check interval

Диапазон: 1~6000 с

По умолчанию: 2 с

Функция: Настройка интервала времени для отправки пакетов обнаружения петель.

Port recovery time

Диапазон: 0~6000 с

По умолчанию: 30 с

Функция: Настройка времени восстановления порта, 0 указывает, что порт не может быть подключен автоматически.

Loop Detect Enable

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение или выключение функции обнаружения петель для порта.

Loop Detect Status

Варианты: Yes/No

Функция: Показать наличие петель в сети, когда функция обнаружения петель порта включена. Yes указывает на наличие петель, а No указывает на отсутствие петель.

6.41.3 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 408.

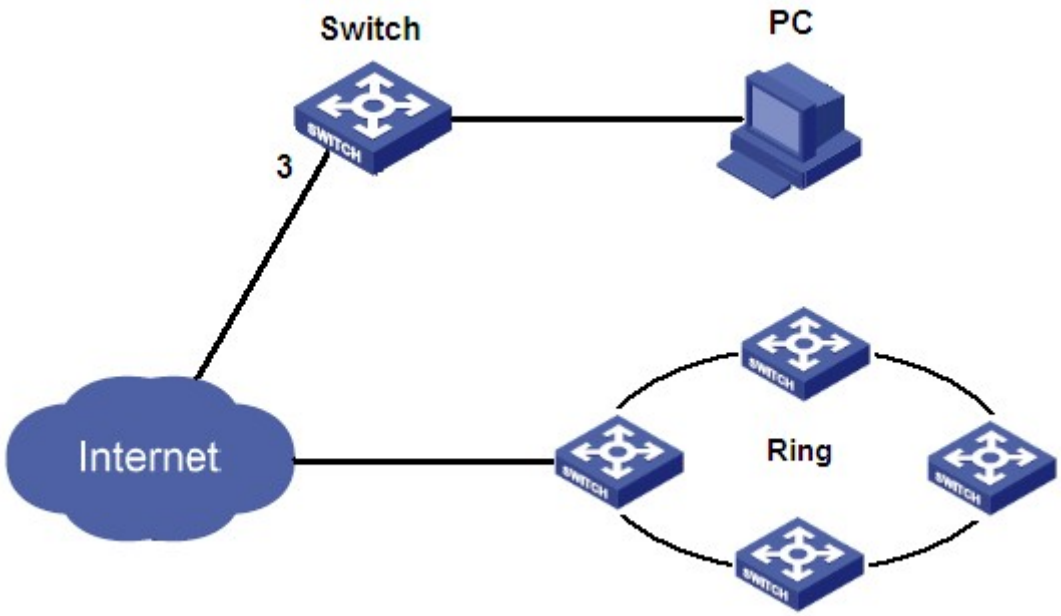


Рисунок 408 Пример обнаружения петли

Конкретная конфигурация:

Включите функцию обнаружения петель для порта 3, как показано на рисунке 407.

6.42 Защита CRC порта

6.42.1 Обзор

После того, как функция защиты портов CRC включена, может быть реализовано периодическое обнаружение пакетов с ошибками CRC. Если количество пакетов ошибок CRC превышает ожидаемый порог во время обнаружения, выключите порт. Подключите порт через некоторое время и продолжайте обнаружение. Интервал времени для отправки пакетов обнаружения ошибок CRC и время восстановления порта можно настроить в программном обеспечении.

6.42.2 Настройка через веб-интерфейс

Настройте функцию защита CRC порта.

Щелкните [Device Advanced Configuration] → [CRC Protect configuration] → [CRC Protect configuration], чтобы перейти на страницу настройки защиты CRC, как показано на рисунке 409.

Port check interval (1-6000s)	5
Port recover time (0-6000m,0 is no recover)	5

Port	Port CRC Protect Enable	Port CRC Protect Status	CRC Threshold(1-10000)packets
1/1	☐	-	10
1/2	☐	-	10
1/3	☐	-	10
1/4	☐	-	10
2/1	☐	-	10
2/2	☐	-	10
2/3	☐	-	10
2/4	☐	-	10
3/1	☐	-	10
3/2	☐	-	10
3/3	☐	-	10

Рисунок 409 Включение защиты CRC

Port check interval

Диапазон: 1~6000 с

По умолчанию: 5 с

Функция: Настройка времени обнаружения пакетов с ошибками CRC. Если количество пакетов ошибок CRC превышает ожидаемый порог, выключите порт.

Диапазон: 0~6000 мин

По умолчанию: 5 м

Функция: Настройка времени восстановления порта, 0 указывает, что порт не может быть подключен автоматически.

Port CRC Protect Enable

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение или выключение функции защиты CRC. Этот механизм обнаружения работает только для порта с включенной функцией защиты CRC.

Port CRC Protect Status

Варианты: -- / Yes / No

Описание: Yes: функция защиты портов CRC включена, а порт находится в состоянии linkdown из-за ошибки CRC. No: функция защиты портов CRC включена, а порт находится в состоянии linkup. -- функция защиты портов CRC не включена.

CRC Threshold

Диапазон: 1~10000 пакетов

По умолчанию: 10 пакетов

Функция: Настройка порогового значения CRC.

Приложение: Аббревиатуры

Аббревиатура	Полное написание
ABR	Area Border Router
ACL	Access Control List
AS	Autonomous System
ASBR	Autonomous System Boundary Router
ARP	Address Resolution Protocol
BC	Boundary Clock
BDR	Backup Designated Router
BootP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
CAR	Committed Access Rate
CIST	Common and Internal Spanning Tree
CLI	Command Line Interface
CoS	Class of Service
CST	Common Spanning Tree
DD	Database Description
DHCP	Dynamic Host Configuration Protocol
DHP	Dual Homing Protocol
DNS	Domain Name System
DR	Designated Router
DSCP	Differentiated Services CodePoint
DST	Daylight Saving Time
E2ETC	End-to-End Transparent Clock
FTP	File Transfer Protocol
GARP	Generic Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol

GPS	Global Positioning System
GVRP	GARP VLAN Registration Protocol
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IED	Intelligent Electronic Device
IGMP	Internet Group Management Protocol
IGMP Snooping	Internet Group Management Protocol Snooping
IRIG	Inter Range Instrumentation Group
IST	Internal Spanning Tree
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
LSA	Link State Advertisement
LSAck	Link State Acknowledgment
LSDB	Link State Database
LSR	Link State Request
LSU	Link State Update
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
OC	Ordinary Clock
OID	Object Identifier
OSPF	Open Shortest Path First
P2PTC	Peer-to-Peer Transparent Clock
PTP	Precision Time Protocol

PVLAN	Private VLAN
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RID	Router ID
RIP	Routing Information Protocol
RMON	Remote Network Monitoring
RSTP	Rapid Spanning Tree
SFTP	Protocol Secure File Transfer Protocol
RTC	Real Time Clock
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
TACACS+	Terminal Access Controller Access Control System
TC	Transparent Clock
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
USM	User-Based Security Model
VLAN	Virtual Local Area Network
VRRP	Virtual Router Redundancy Protocol
WINS	Windows Internet Naming Service
WRR	Weighted Round Robin

Контакты

Для получения технической поддержки пишите на наш адрес электронной почты: support@kyland.com.ru
Офис продаж: sales@kyland.com.ru

Для получения информации об оборудовании, документации, актуальной информации обращайтесь на сайт: https://kyland.com.ru/