Промышленный управляемый модульный

Коммутатор STEZ47xx

Руководство пользователя

Оглавление

1. Описание устройства

1.1. Введение

Коммутаторы серии STEZ47xx, основанные на полностью гигабитной коммутационной платформе, являются промышленными Ethernet-коммутаторами, использующими технологию управления IEC61850 MMS, что обеспечивает унифицированное моделирование и управление. Коммутаторы имеют модульную конструкцию для гибкой конфигурации, расширяемый IRIG-B модуль, GPS модуль, последовательным портом, модулем HSR / PRP и многие другие модули. Кроме того, коммутаторы соответствуют стандартам электроэнергетики IEC61850-3 и IEEE1613.

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

1.2. Модели серии

В портфолио серии STEZ47xx входят следующие коммутаторы второго и третьего уровня (см ниже). Перечень артикулов и наименований не исчерпывающий. Данное руководство применяется ко всем коммутаторам серии STEZ47xx.

- **STEZ4700G-CH-L2-PTP** (артикул 70010019) – шасси управляемого коммутатора L2, 7 слотов для установки модулей, поддержка до 28 гигабитных портов, PTPv2, без установленных источников питания, поддержка горячей замены источников питания;
- **STEZ4700G-CH-L2** (артикул 70010020) - шасси управляемого коммутатора L2, 7 слотов для установки модулей, поддержка до 28 гигабитных портов, без установленных источников питания, поддержка горячей замены источников питания;
- **STEZ4700-CH-L2-PTP** (артикул 70010021) – шасси управляемого коммутатора L2, без установленных источников питания, 7 слотов для установки модулей, поддержка до 4 гигабитных портов и до 24х 100 Мбит/с портов, PTPv2, без установленных источников питания, поддержка горячей замены источников питания;
- **STEZ4700-CH-L2** (артикул 70010022) – шасси управляемого коммутатора L2, 7 слотов для установки модулей, поддержка до 4 гигабитных портов и до 24х 100 Мбит/с портов, без установленных источников питания, поддержка горячей замены источников питания;
- **STEZ4700G-CH-L3-PTP** (артикул 70010023) – шасси управляемого коммутатора L3, 7 слотов для установки модулей, поддержка до 28 гигабитных портов, PTPv2, без установленных источников питания, поддержка горячей замены источников питания;
- **STEZ4700G-CH-L3** (артикул 70010024) – шасси управляемого коммутатора L3, 7 слотов для установки модулей, поддержка до 28 гигабитных портов, без установленных источников питания, поддержка горячей замены источников питания;

- **STEZ4700-CH-L3-PTP** (артикул 70010025) – шасси управляемого коммутатора L3, 7 слотов для установки модулей, поддержка до 4 гигабитных портов и до 24х 100 Мбит/с портов, PTPv2, без установленных источников питания, поддержка горячей замены источников питания;
- **STEZ4700-CH-L3** (артикул 70010026) – шасси управляемого коммутатора L3, 7 слотов для установки модулей, поддержка до 4 гигабитных портов и до 24х 100 Мбит/с портов, без установленных источников питания, поддержка горячей замены источников питания.

Источники питания для коммутаторов серии STEZ47xx:

- **STEZ4700-PW-HV** (артикул 70010027) – источник питания для шасси STEZ47xx-CH-xx, 100-240VAC/110-220VDC (85-264VAC/77-300VDC) резервированные источники питания, поддержка горячей замены источников питания).

Основные модули (полный список можно получить по запросу):

- **STEZ4700-MOD1-4GSFP** (артикул 70010028) – модуль для шасси STEZ47xx-CHxx для слота №1, 4 порта 100/1000 Base-X SFP;
- **STEZ4700-MOD1-4GSFP-DDM** (артикул 70010029) – модуль для шасси STEZ47xx-CHxx для слота №1, 4 порта 100/1000 Base-X SFP, поддержка DDM;
- **STEZ4700-MOD1-4G** (артикул 70010030) – модуль для шасси STEZ47xx-CHxx для слота №1, 4 порта 10/100/1000 Base-TX;
- **STEZ4700-MOD1-2G-2GSFP** (артикул 70010031) – модуль для шасси STEZ47xx-CHxx для слота №1, 2 порта 10/100/1000 Base-TX, 2 порта 100/1000 Base-X SFP;
- **STEZ4700-MOD-4G** (артикул 70010032) – модуль для шасси STEZ4700G-CHxx для слотов №2 - 7, 4 порта 10/100/1000 Base-TX;
- **STEZ4700-MOD-4GSFP** (артикул 70010033) – модуль для шасси STEZ4700G-CHxx для слотов №2 - 7, 4 порта 100/1000 Base-X SFP;
- **STEZ4700-MOD-4GSFP-DDM** (артикул 70010034) – модуль для шасси STEZ4700G-CHxx для слотов №2 - 7, 4 порта 100/1000 Base-X SFP, поддержа DDM;
- **STEZ4700-MOD-4SFP** (артикул 70010035) – модуль для шасси STEZ4700-CHxx для слотов №2 - 7, 4 порта 100 Base-X SFP;
- **STEZ4700-MOD-4SFP-DDM** (артикул 70010036) – модуль для шасси STEZ4700-CHxx для слотов №2 - 7, 4 порта 100 Base-X SFP, поддержка DDM;
- **STEZ4700-MOD-4** (артикул 70010037) – модуль для шасси STEZ47xx-CHxx для слотов №2 - 7, 4 порта 10/100 Base-TX;
- **STEZ4700-MOD-2G-2GSFP** (артикул 70010038) – модуль для шасси STEZ4700G-CHxx для слотов №2 - 7, 2 порта 10/100/1000 Base-TX, 2 порта 100/1000 Base-X SFP;
- **STEZ4700-MOD-HSR/PRP-G** (артикул 70010039) – модуль для шасси STEZ4700G-CHxx для слотов №2 - 7, HSR/PRP с 2 портами 10/100/1000 Base-Tx;
- **STEZ4700-MOD-HSR/PRP-GSFP** (артикул 70010040) – модуль для шасси STEZ4700G-CHxx для слотов №2 - 7, HSR/PRP с 2 портами 100/1000 Base-X SFP;
- **STEZ4700-MOD-4FX-MM** (артикул 70010049) – модуль для шасси STEZ47xx-CHxx для слотов №2 - 7, 4 порта 10/100 Base-FX MM, разъем SC, 1310 нм, 5 км.

1.3. Функции программного обеспечения

Коммутаторы серии STEZ47xx предоставляют множество программных функций, удовлетворяющих различные требования клиентов.

- Протоколы резервирования: RSTP/STP, MSTP, ST-Ring, DRP, VRRP
- Протоколы маршрутизации: OSPFv2, RIP, статическая маршрутизация
- Поддержка мультикаст протоколов: IGMP Snooping, GMRP и static multicast
- VLAN, PVLAN, QoS и ARP
- Управление шириной канала: port trunk, port rate limiting
- Протоколы синхронизации времени: GPS, IRIG-B, PTP(IEEE1588-2008), ITU-T.G.8261/G.8262, SNTP и NTP
- Безопасность: ACL, port isolate, IEEE802.1x, TACACS+, RADIUS, SSH, SSL
- Диагностика: port mirroring, LLDP, контроль линии, loop detect, CRC protect
- Обновление ПО через FTP, загрузка / выгрузка конфигурационного файла
- Port mirroring, LLDP, контроль линии
- Функции уведомления: port alarm, power alarm, ring alarm, конфликт IP/MAC адресов, temperature alarm и port traffic alarm
- Управление устройством: CLI, Telnet (SSH), Web.

2. Управление коммутатором

Управление коммутатором возможно посредством:

- Консольного порта
- Telnet/SSH
- Web браузера

2.1. Тип просмотра

После подключения в Command Line Interface (CLI) через консольный порт или Telnet (SSH), возможно получить различный доступ, переключение между ними можно получить с помощью следующих команд.

Отображение	Тип	Доступный функционал	Команды для смены уровня привилегий
SWITCH>	Основной режим	View recently used commands. View software version. View response information for ping operation.	Input "enable" to enter the Privileged mode.
SWITCH#	Привилегированный режим	Upload/Download configuration file. Restore default configuration. View	Input "configure terminal" to enter the Configuration mode from the Privileged mode.

		response information for ping operation. Restart the switch. Save current configuration. Display current configuration. Update software.	Input "exit" to return to the General mode.
SWITCH(config)#	Режим конфигурации	Configure switch functions	Input "exit" or "end" to return to the Privileged mode.

Когда коммутатор конфигурируется через интерфейс командной строки, то можно использовать для получения справки по команде "?". В справочной информации есть разные форматы описания параметров. Например, <1, 255> означает диапазон чисел; <H.H.H.H> означает IP-адрес; <H:H:H:H:H:H> означает MAC-адрес; слово<1,31> означает диапазон строк. Кроме того, с помощью ↑ и ↓ можно делать прокрутку недавно использовавшихся команд.

2.2. Управление коммутатором через консольный порт

Доступ к коммутатору можно получить через его консольный порт и гипертерминал ОС Windows или другого программного обеспечения, поддерживающего подключение через последовательный порт, например HTT3.3. В следующем примере показано, как использовать Hyper Terminal для доступа к коммутатору через консольный порт.

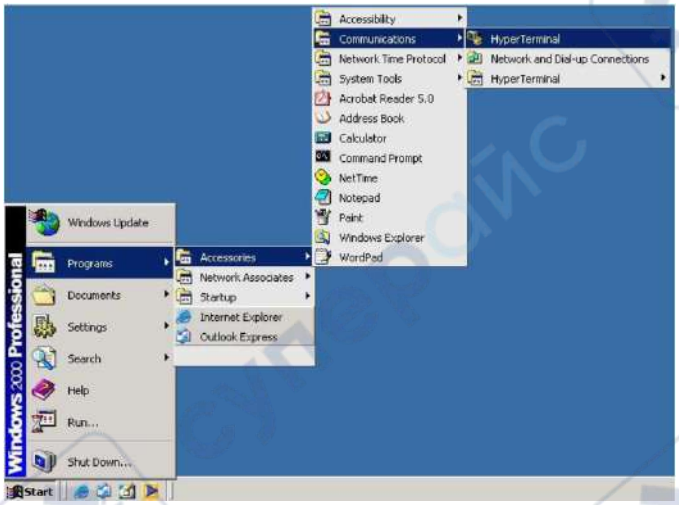
Консольные порты поддерживают разъемы RJ45 и Mini USB. При необходимости можно выбрать любой из двух разъемов. Если выбрать разъем Mini USB для одного порта и разъем RJ45 для другого, при подключении обоих портов будет работать только консольный порт с разъемом Mini USB.

RJ45 Connector

Подключите 9-пиновый консольный порт на PC в консольный кабель на коммутаторе с помощью консольного кабеля DB9-RJ45.

Mini-USB Connector

- Установите "Mini USB_driver.exe". Программу можно найти в папке [Software download] в поставляемом CD. Подключите USB порт на PC консольным кабелем к коммутатору с Mini USB кабелем.
- На рабочем столе Windows выберите Пуск > Программы > Стандартные > Связь > Hyper Terminal



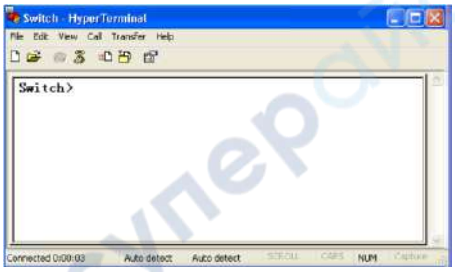
Можно использовать любой другой эмулятор терминала, такой как Putty.

- Введите имя для нового соединения

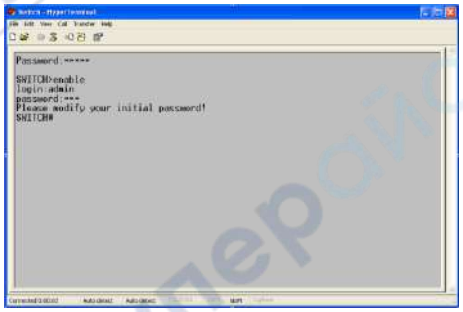
- Выберите номер COM порта для его использования

- Настройка свойств COM порта: 115200 для бит в секунду, 8 для бит данных, None для четности, 1 для стоповых битов и none для управления потоком.

- Появится окно входа в систему. Введите имя пользователя и пароль (пароль такой же, как и для Web браузера), затем нажмите enter.



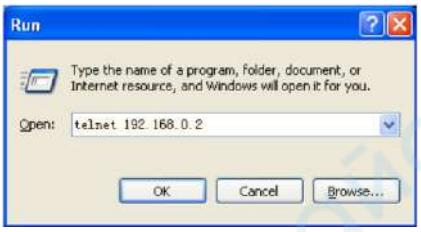
- Введите команду “enable”, пользователь по умолчанию “admin” и пароль “ISTOK” для доступа в привилегированный режим.



2.3. Управление коммутатором через Telnet

Пользователи могут использовать Telnet для настройки коммутаторов.

- Набрать telnet *IP адрес коммутатора* из командной строки windows (или любой аналог). По умолчанию адрес: 192.168.0.2.



- Появится окно входа в систему. Введите имя пользователя и пароль (“admin” / ”STEZ” по умолчанию), затем нажмите enter.

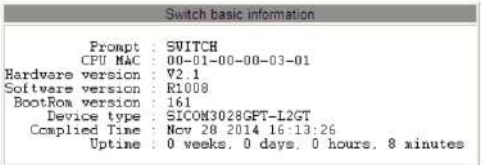
2.4. Управление коммутатором через Web

- Запустите web-браузер
- Наберите http:// и IP адрес коммутатора. Нажмите Enter
- Появится окно входа
- Введите имя пользователя и пароль. Имя пользователя и пароль по умолчанию – “admin” / “STEZ”
- Нажмите Enter или кнопку OK, затем появится главный интерфейс веб-управления

3. Статус коммутатора

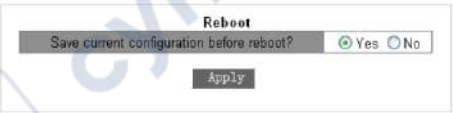
3.1. Базовая информация

Основная информация о коммутаторе включает MAC-адрес, версию аппаратного обеспечения, версию программного обеспечения, версию BootROM, тип устройства, дату компиляции и время работы. Нажмите [Информация об устройстве] → [Основная информация о коммутаторе] в дереве навигации, чтобы отобразить основную информацию о коммутаторе, как показано на рисунке ниже.



4. Обслуживание коммутатора

В дереве навигации вы можете нажать [Save current running-config], чтобы сохранить текущую конфигурацию, или [Reboot - перезагрузить с конфигурацией по умолчанию], чтобы перейти на страницу, показанную на рисунке ниже. Затем вы можете нажать <Yes>, чтобы восстановить конфигурацию по умолчанию.



4.1. Перезагрузка

Чтобы перезагрузить устройство, нажмите [Switch maintenance] → [Reboot] в дереве навигации, чтобы войти в интерфейс перезагрузки, как показано на рисунке ниже.

Перед перезагрузкой подтвердите сохранение текущей конфигурации. Если вы выберете «Yes», коммутатор запустит текущую конфигурацию после перезагрузки. Если вы выберете «No», коммутатор использует предыдущую сохраненную конфигурацию. Если конфигурация не была сохранена, коммутатор восстановит конфигурацию по умолчанию после перезагрузки.

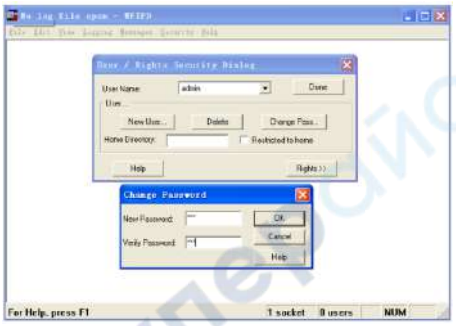
4.2. Обновление прошивки (firmware)

Регулярные обновления программного обеспечения могут помочь уменьшить количество ошибок при работе 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 помощь сервера FTP/TFTP/SFTP.

4.2.1. Обновление ПО через FTP

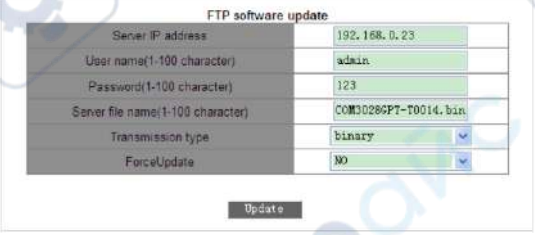
Установите FTP-сервер. Ниже в качестве примера используется программное обеспечение WFTPD для ознакомления с конфигурацией FTP-сервера и обновлением программного обеспечения.

Нажмите [Security] → [Users/Rights]. Откроется диалоговое окно "Users/Rights Security Dialog". Нажмите <New User> для создания нового FTP пользователя, как показано на рисунке ниже. Создайте имя пользователя и пароль, для примера, имя пользователя "admin" и пароль "123". Нажмите <OK>.



Введите путь хранения файла обновления в «Home Directory», как показано на рисунке ниже. Нажмите <Done>.

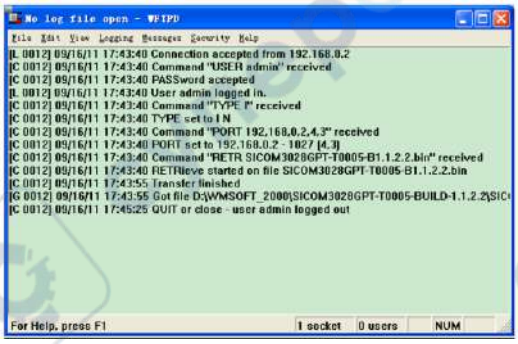
Нажмите [Switch maintenance] → [FTP software update] в навигационном дереве для показа окна обновления ПО через FTP, как показано на рисунке ниже. Введите IP адрес FTP сервера, имя FTP пользователя, пароль и имя файла на сервере. Нажмите <Update>.



- **Transmission type**
  Значения: binary/ascii
  По умолчанию: binary
  Функция: выбор стандарта передачи файлов.
  Описание: **ascii** означает использование стандарта ASCII для передачи файла; **binary** означает использование двоичного стандарта для передачи файла.
- **ForceUpdate**
  Значения: YES/NO
  По умолчанию: NO
  Функция: выберите метод обработки, если версия программного обеспечения не соответствует аппаратному обеспечению коммутатора.
  Описание: 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 системной аномалии или даже сбою загрузки.

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



Дождитесь окончания обновления.

Когда обновление будет завершено, перезагрузите устройство и откройте страницу основной информации о коммутаторе, чтобы проверить, успешно ли выполнено обновление и активна ли новая версия.

4.2.2. Обновление ПО через TFTP

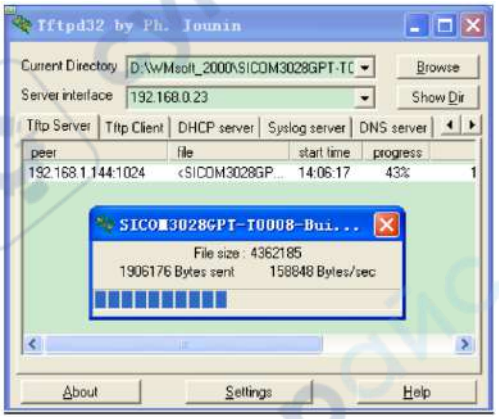
Установите TFTP-сервер. Ниже в качестве примера используется программное обеспечение TFTPD для ознакомления с конфигурацией сервера TFTP.

В "Current Directory" выберете путь до обновляемого файла на сервере. Введите IP адрес сервера в "Server interface".

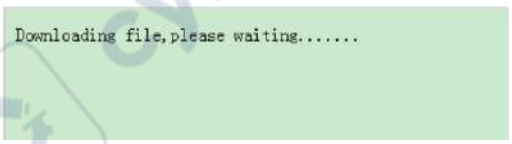
Нажмите [Switch maintenance] → [TFTP software update] в навигационном дереве, откроется окно обновления ПО через TFTP, как показано на рисунке ниже. Введите IP адрес TFTP сервера и имя файла на сервере. Нажмите <Update> и ожидайте окончания обновления.

- **Transmission type**
  Значения: binary/ascii
  По умолчанию: binary
  Функция: выбор стандарта передачи файлов.
  Описание: **ascii** означает использование стандарта ASCII для передачи файла; **binary** означает использование двоичного стандарта для передачи файла.
- **ForceUpdate**
  Значения: YES/NO
  По умолчанию: NO
  Функция: выберите метод обработки, если версия программного обеспечения не соответствует аппаратному обеспечению коммутатора.
  Описание: 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 системной аномалии или даже сбою загрузки.

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



Дождитесь окончания обновления.

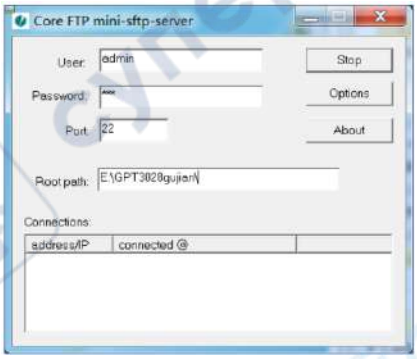


Когда обновление будет завершено, перезагрузите устройство и откройте страницу основной информации о коммутаторе, чтобы проверить, успешно ли выполнено обновление и активна ли новая версия.

4.2.3. Обновление ПО через SFTP

Протокол безопасной передачи файлов (SFTP) — это протокол передачи файлов на основе SSH. Он обеспечивает зашифрованную передачу файлов для обеспечения безопасности. В следующем примере MSFTP используется для описания конфигурации сервера SFTP и процесса обновления микропрограммы.

Добавьте SFTP пользователя, как показано на рисунке ниже. Введите пользователя и пароль, например, admin / 123. Назначьте порт 22. Введите путь для сохранения firmware файла в “Root path”.



Обновление firmware показано на рисунке ниже.

- **Server IP address**
  Формат: A.B.C.D
  Описание: Настройка IP-адреса SFTP-сервера.
- **{ User name, Password }**
  Диапазон: {1~99 символов, 1~99 символов}
  Описание: Введите имя пользователя и пароль, созданные на SFTP-сервере.
  Server file name
  Диапазон: 1~99 символов
  Описание: Настройка имени файла обновления микропрограммы, хранящегося на SFTP-сервере.
- **ForceUpdate**
  Варианты: YES/NO
  По умолчанию: NO
  Функция: выберите метод обработки, если версия программного обеспечения не соответствует аппаратному обеспечению коммутатора.
  Описание: 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 системной аномалии или даже сбою загрузки.

Когда обновление будет завершено, как показано на рисунке ниже, активируйте версию программного обеспечения и перезагрузите устройство, откройте страницу

«System Information», чтобы проверить, успешно ли выполнено обновление и активна ли новая версия.

5. Базовая конфигурация

5.1. Базовая конфигурация коммутатора

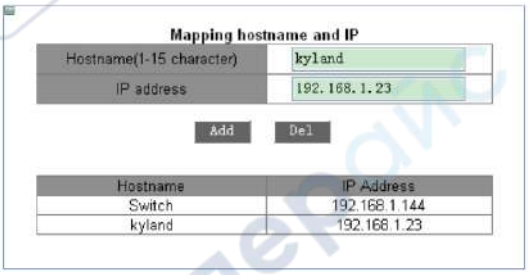
Базовая конфигурация коммутатора включает в себя hostname, mapping between host и IP address, и switch clock.

Настройка имени хоста (hostname).

Нажмите [Device Basic Configuration] → [Switch Basic Configuration] → [Basic Config] для входа на страницу базовой конфигурации, как показано на рисунке ниже.

- **Hostname**
  Диапазон: 1-30 символов
  По умолчанию: SWITCH
  Функция: Установите подсказку в интерфейсе командной строки коммутатора.
  Метод: Нажмите <Apply>, чтобы активировать новое имя хоста. Нажмите <Reset>, чтобы отменить текущую настройку и использовать предыдущее имя хоста.

  Настройка сопоставления между именем хоста и IP-адресом, как показано на рис. ниже.



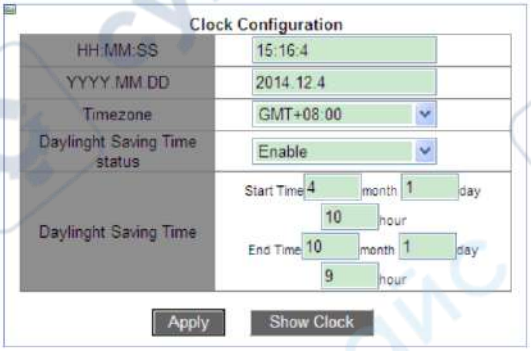
- **{Host name, IP address}**
  Формат: {1–15 символов, A.B.C.D}
  Функция: в соответствии с сопоставлением используйте имя хоста для доступа к соответствующему устройству.
  Метод: введите правильное имя хоста и IP-адрес. Затем нажмите <Add>, чтобы установить запись сопоставления имени хоста и IP-адреса, или <Del>, чтобы удалить запись сопоставления.
  Пример. После успешной настройки сопоставления между именем хоста «Switch» и IP-адресом «192.168.0.4» вы можете пропинговать коммутатор с помощью команды ping host Switch вместо ping 192.168.0.4.

  Настройка часов

Вы можете установить системную дату и время. Коммутаторы этой серии поддерживают часы реального времени (RTC). Даже если они выключены, они продолжают синхронизироваться.

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

Нажмите [Device Basic Configuration] → [Switch Basic Configuration] → [Clock configuration], чтобы открыть страницу конфигурации часов, как показано на рисунке ниже.



- **HH:MM:SS**
  Диапазон: значение HH находится в диапазоне от 0 до 23, а значение 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 ДД для марта — от 1 до 31, а для апреля — от 1 до 30. Вы можете настроить его в соответствии с реальной ситуацией.
- **Timezone**
  Функция: выберите местный часовой пояс.
- **Daylight Saving Time status**
  Опции: Enable/Disable
  По умолчанию: Disable
  Функция: включить или отключить летнее время. Летом после включения летнего времени часы будут переведены на один час вперед.
- **Daylight Saving Time**
  Настройте временной сегмент для перехода на летнее время.

5.2. Управление конфигурациями пользователей

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

Уровень пользователя	Описание
Guest (Гость)	самый низкий уровень, пользователи “Gues” могут только просматривать конфигурацию коммутатора, но не могут выполнять настройку или модификацию. Пользователи “Guest” не могут получить доступ к следующим функциям: обновление программного обеспечения, управление пользователями, передача файлов, перезагрузка, сохранение текущей конфигурации и загрузка по умолчанию.
System (Система)	Средний уровень, пользователи “System” имеют определенные права доступа и настройки. Пользователи “System” не могут получить доступ к следующим функциям: обновление программного обеспечения, управление пользователями, передача файлов, перезагрузка и загрузка по умолчанию. Примечание. Пользователь “System” может изменить пароль текущего пользователя.
Admin (Администратор)	Самый высокий уровень, пользователи с правами администратора имеют права на выполнение всех функций.

5.2.1. Веб конфигурирование

Конфигурирование пользователей.

Нажмите [Device Basic Configuration] → [User Configuration] → [User Configuration] to для перехода на страницу конфигурирования, как показано ниже.

- **Name**
  Диапазон: 1~16 символов
- **Service**
  Опции: console/telnet/ssh/web
  Функция: выбор режима доступа переключения для текущего пользователя. Можно выбрать один или несколько режимов доступа.
- **Level**
  Опция: Guest/System/Admin
  По умолчанию: Guest
  Опция: Выберите уровень пользователя, пользователи разных уровней имеют разные права на операции.
- **Authen-Type**
  Опция: Password/Key/Password или Key
  По умолчанию: Password

Функция: выбран тип аутентификации, который будет использоваться при доступе текущего пользователя к коммутатору. При выборе пароля необходимо настроить параметр «**Password**». При выборе ключа необходимо настроить **Key name**.

- **Password**
  Диапазон: 1~32 символа
  Функция: настройка пароля, который будет использоваться при доступе текущего пользователя к коммутатору.
- **Key name**
  Функция: выберите имя ключа, которое будет использоваться при доступе текущего пользователя к коммутатору в режиме ssh.

Модификация и удаление пользователей.

Щелкните на запись пользователя в списке конфигурации пользователя. Вы можете изменить и удалить конфигурацию пользователя, как показано на рисунке ниже.

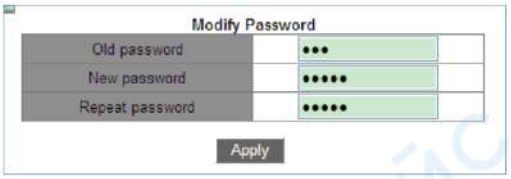
Конфигурирование SSH Key.

Щелкните [Device Basic Configuration] → [User Configuration] → [SSH Key Configuration] для входа в SSH key configuration страницу, как показано на рисунке ниже.

- **Key Name**
  Диапазон: 1~16 символов
- **Key Type**
  Обязательная конфигурация: RSA
  Коммутаторы этой серии поддерживают только алгоритм ключа RSA.
- **Key Value**
  Формат: {имя алгоритма, открытый ключ, информация о ключе}
  Имя алгоритма: ssh-rsa | ssh-dsa
  Открытый ключ: основан на 64 кодах и имеет длину менее 2048 байт.
  Информация о ключе: дополнительная информация о ключе
  Функция: настроить открытый ключ, соответствующий клиенту. Как правило, открытый ключ генерируется программным обеспечением Puttygen и копируется в значение ключа сервера, закрытый ключ сохраняется в клиенте.

Изменение пароля у конкретного пользователя.

Щелкните [Device Basic Configuration] → [User Configuration] → [Modify Password] для входа на страницу с изменением пароля, как показано на рисунке ниже.



- **New password/Repeat password**
  Диапазон: 1~32 символа

Настройка тайм-аутов для режимов доступа коммутатора

Щелкните [Device Basic Configuration] → [User Configuration] → [Timeouts Configuration] для входа на страницу изменений, как показано на рисунке ниже.

- **Time**
  Диапазон: 0~44640 мин.
  По умолчанию: 5 мин для console/ssh/telnet; 10 минут для веб.
  Функция: настроить время ожидания входа пользователя и время отключения. Отсчет времени начинается, когда пользователь завершит все настройки, и система автоматически выйдет из режима доступа, когда время закончится. Когда время установлено на 0, пользовательская функция тайм-аута и отключения отключена. В этом случае сервер не будет определять, истекло ли время входа пользователя в систему, и поэтому пользователь не выйдет из текущего режима входа.

5.3. Конфигурация портов

5.3.1. Конфигурация физического порта

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

Щелкните [Device Basic Configuration] → [Port configuration] → [Ethernet port configuration] → [Physical port configuration] для входа на страницу конфигурации, как показано на рисунке ниже.

- **Port**
  Опции: все порты коммутатора

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

- **Alias**
  Диапазон: 1~64 символа
  Функция: настроить псевдоним 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; cross означает, что порт поддерживает только перекрестный кабель; normal означает, что порт поддерживает только прямой кабель.c
- **Admin Status**
  Варианты: shutdown/no shutdown
  По умолчанию: no shutdown
  Функция: Разрешить передачу данных на порт или нет.
  Описание: no shutdown означает, что порт включен и разрешает передачу данных; shutdown указывает, 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/половина, 10M/полный, 100M/половина, 100M/полный, 1000M/половина, 1000M/полный
  По умолчанию: auto
  Функция: настройка скорости порта и режима дуплекса.
  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 канала. Если вы установили для порта принудительную скорость или дуплекс, убедитесь, что настройки скорости или режима дуплекса на обоих концах соединения одинаковы.
- **Linkup delay**
  Диапазон: 0~600 (единица измерения: 1/60 с)
  По умолчанию: 0 с
  Функция: Настройка времени задержки соединения порта. Оба конца соединения должны иметь одинаковую конфигурацию задержки соединения.

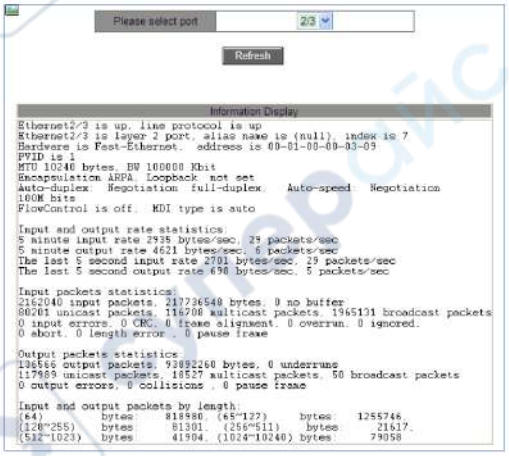
Вы можете просмотреть информацию о порте на основе конфигурации порта Ethernet и условий связи, как показано на рисунке ниже.

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

5.3.2. Информация по порту

Щелкните [Device Basic Configuration] → [Port configuration] → [Port debug and maintenance] → [Show port information] для перехода на страницу информации. Она содержит информацию о состоянии подключения порта, тип порта, статистику входящих/исходящих пакетов и другую информацию, как показано на рисунке ниже.



5.4. Конфигурация VLAN

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 оптимизирует 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.

5.4.1. Port-based VLAN

Раздел VLAN может быть либо на основе порта, либо на основе MAC-адреса. Коммутаторы этой серии поддерживают разделение VLAN на основе портов. Члены VLAN могут быть определены на основе портов коммутатора. После добавления порта в указанную VLAN порт может пересылать пакеты с тегом для VLAN.

Port Type

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

- Untag port: пакеты, пересылаемые портом без тегов, не имеют тегов VLAN. Порты Untag обычно используются для подключения к терминалам, которые не поддерживают 802.1Q. По умолчанию все порты коммутатора являются портами без тегов и принадлежат VLAN1.
- Tag port: все пакеты, пересылаемые портом тега, содержат тег VLAN. Порты тегов обычно используются для подключения сетевых передающих устройств.

Port Mode

- Access: в режиме доступа порт должен быть удален и добавлен в одну VLAN; порт нельзя пометить и добавить в какую-либо VLAN.
- Trunk: в режиме магистрали порт должен быть удален и добавлен в сеть PVID VLAN; порт может быть помечен/снят с тега и добавлен в любую другую VLAN.

PVID

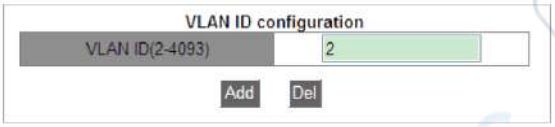
Каждый порт имеет PVID. При получении нетегированного пакета порт добавляет к пакету тег в соответствии с PVID. PVID по умолчанию для всех портов равен 1. PVID порта доступа — это идентификатор VLAN, к которой принадлежит порт, и его нельзя настроить. PVID магистрального порта может быть настроен как один из идентификаторов VLAN, разрешенных через порт. В таблице ниже показано, как коммутатор обрабатывает полученные и пересылаемые пакеты в зависимости от режима порта, типа порта и PVID.

Обработка полученных пакетов		**Обработка пакетов для пересылки**	
Untagged packets	**Tagged packets**	**Port Type**	**Packet Processing**
Добавить PVID tag к пакетам	➢ Если идентификатор VLAN в пакете есть в списке разрешенных VLAN, примите пакет. ➢ Если идентификатор VLAN в пакете находится в списке разрешенных VLAN, пакет отбрасывается.	Untag	Пересылать пакеты после удаления tag
		Tag	Сохранять tag и пересылать пакет

5.4.2. Веб конфигурирование

Создание и удаление VLAN

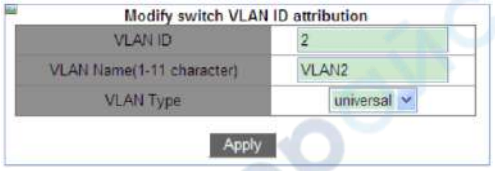
Щелкнуть [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Create/Remove VLAN] → [VLAN ID allocation] для входа на страницу конфигурирования VLAN, как показано на рисунке ниже.



- **VLAN ID**
  Диапазон: 2~4093.
  Функция: Используйте разные идентификаторы VLAN для различения VLANов.
  Описание: Коммутаторы этой серии поддерживают до 4093 VLAN.
  Метод: Нажмите <Add>, чтобы создать VLAN; нажмите <Remove>, чтобы удалить указанный VLAN.

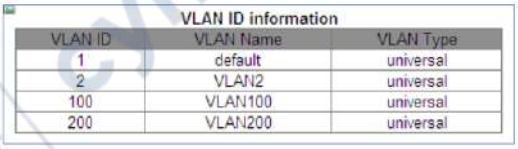
Конфигурирование имени VLAN

Щелкнуть [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Create/Remove VLAN] → [VLAN ID attribution configuration] для входа на страницу конфигурирования имени VLAN, как показано на странице ниже.



- **VLAN ID**
  Диапазон: все созданные VLAN.
  Функция: введите идентификатор VLAN, имя которой необходимо изменить.
- **VLAN Name**
  Диапазон: 1~11 символов
  Функция: введите имя VLAN с указанным идентификатором.
- **VLAN Type**
  Опции: universal
  По умолчанию: universal

После завершения настройки на странице «Информация об идентификаторе VLAN» отображается информация об атрибутах всех созданных сетей VLAN, как показано на рисунке ниже:

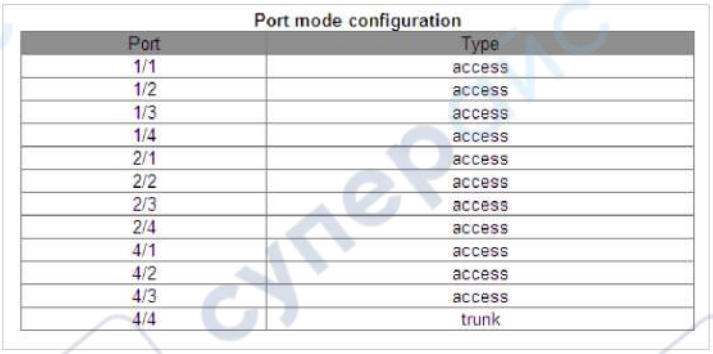


Конфигурирование режима порта

Щелкнуть [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Port type configuration] → [Set port mode (Trunk/Access)] для входа на страницу конфигурирования типа порта, как показано на странице ниже.

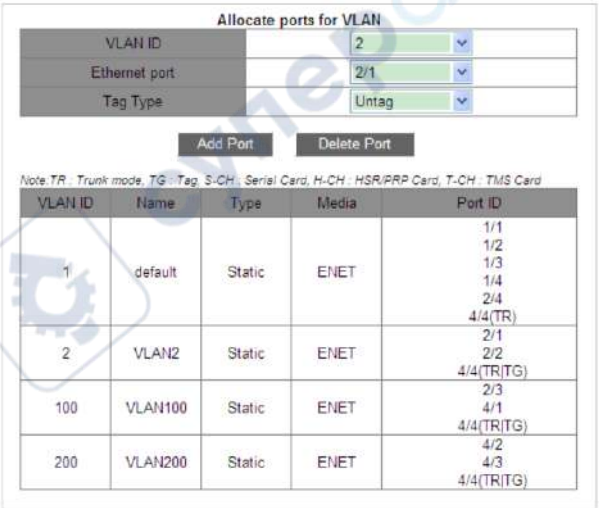
- **Port**
  Опция: все порты коммутатора.
- **Type**
  Опция: access / trunk
  По умолчанию: access
  Функция: Выберите режим для указанного порта. Каждый порт поддерживает только один режим.

После завершения настройки на странице «Конфигурация режима порта» будут перечислены все типы портов, как показано на рисунке ниже.



Назначение портов для созданных VLANов

Щелкнуть [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Allocate ports for VLAN] → [Allocate ports for VLAN] для входа на страницу конфигурирования портов для VLANов, как показано на странице ниже.



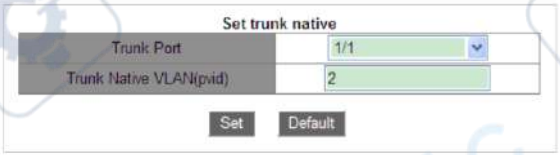
- **Tag Type**
  Опция: Tag / Untag

Функция: Выберите тип порта, который необходимо добавить в VLAN.

- В режиме доступа (access) с порта должен быть снят тег и добавлен в один из VLAN.
- У порта в режиме trunk должен быть удален tag и добавлен в PVID VLAN; порт может быть помечен/снят с тега и добавлен в любой другой VLAN.

Конфигурирование PVID для trunk портов.

Щелкнуть [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Trunk port configuration] → [VLAN setting for trunk port] для входа на страницу конфигурирования trunk портов для VLANов, как показано на странице ниже.



- **Trunk port**
  Опция: все trunk порты
- **Trunk Native VLAN (pvid)**
  Опция: все созданные VLANы
  По умолчанию: 1
  Функция: Конфигурирование PVID для trunk порта.
  Описание: Независимо от того, существует ли порт в VLAN или существует в VLAN в виде Untag/tag, после указания PVID этот порт будет добавлен в VLAN в виде Untag.
  Метод: Нажмите <Default>, чтобы восстановить PVID выбранного trunk порта на 1.

Конфигурирование VLAN для trunk портов показана на рисунке ниже.

- **Trunk port**
  Опция: все trunk порты
- **Tag Type**
  Опция: Tag / Untag
  Функция: Выбор типа trunk порта для добавления VLAN
- **Trunk Allow VLAN List**
  Опция: все созданные VLANы
  По умолчанию: все созданные VLANы
  Функция: Конфигурирование VLANов для выбора trunk порта.
  После завершения настройки отображается информация о VLAN всех портов Trunk портов, как показано на рисунке ниже.

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

Конфигурирование ingress правило VLAN для порта.

Щелкнуть [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Enable/Disable VLAN ingress rule] → [Enable/Disable VLAN ingress rule] для входа на страницу конфигурации правила входа VLAN, как показано на рисунке ниже.

Опции: Enable / Disable
По умолчанию: Enable
Функция: Включить или отключить правило входа VLAN для порта.
Описание: если эта функция включена, порт сверяет идентификатор VLAN пакета с его разрешенным списком 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 вся информация о правилах входа VLAN, как показано на рисунке ниже.

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

Конфигурирование VLAN-aware.

Щелкнуть [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [VLAN-aware] → [VLAN-aware] для входа на страницу конфигурации VLAN ingress, как показано на рисунке ниже.

Опции: Aware / Unaware
По умолчанию: Aware
Функция: Когда выбрано 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 неизвестного одноадресного пакета и пересылает пакет на любой порт (широковещательно); устройство не оценивает идентификатор VLAN для

известного одноадресного пакета и пересылает пакет на соответствующий порт в соответствии с таблицей MAC-адресов.

Просмотр информации о всех созданных VLAN.

Щелкнуть [Device Basic Configuration] → [VLAN configuration] → [VLAN debug and maintenance] → [Show VLAN] для входа на информационную страницу о VLANax, как показано на рисунке ниже.

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)

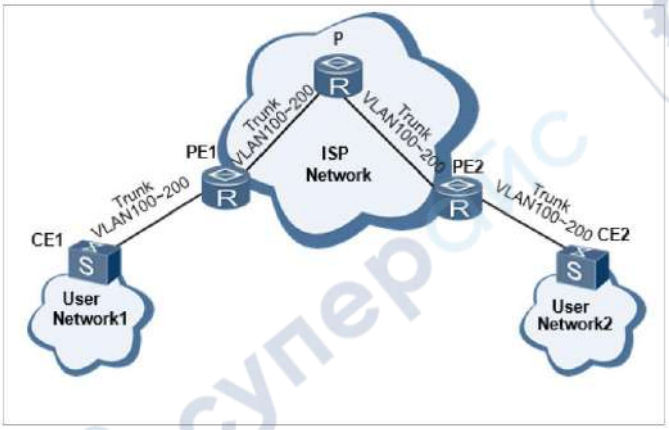
5.5. QinQ конфигурация

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 прозрачную передачу 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 пользователя доступа, как показано на рисунке ниже. Сеть пользователя 1 и 2, предполагается, что они расположены в двух разных местах и имеют доступ к магистрали через PE1 и PE2 ISP соответственно.

Если пользователю необходимо соединить VLAN100~VLAN200 сети 1 с VLAN100~VLAN200 сети 2, оба подключенных интерфейса CE1, PE1, P и PE2, CE2 должны быть настроены как свойство магистрали и разрешить VLAN100~VLAN200 пройти через.

Этот метод конфигурации делает VLAN пользователя видимой в магистральной сети, а не прозрачной передачей. Это не только потребляет ресурсы идентификатора VLAN поставщика услуг (обычно только 4094 идентификатора VLAN), но также требует, чтобы поставщик услуг управлял номером VLAN пользователя. В этом случае структура сети слишком плотная, и изменения планирования сети интернет-провайдера или клиента повлияют на всю сеть, что приведет к плохой гибкости сети.



Технология QinQ добавляет еще один уровень тегов 802.1Q. к сообщению тега 802.1Q. Таким образом, сообщение, доставляемое в магистральной сети, имеет два уровня тегов 802.1Q (один тег общедоступной сети, один тег частной сети), сеть интернет-провайдера должна предоставить только идентификатор VLAN для другого идентификатора VLAN из той же пользовательской сети, что экономит ISP VLAN ID решает проблему нехватки ресурсов ISP network VLAN ID. И это может сделать прозрачную передачу частной сети VLAN по общедоступной сети, а также предоставить простое решение VPN уровня 2 для небольших MAN (городская сеть) или LAN (локальная сеть).

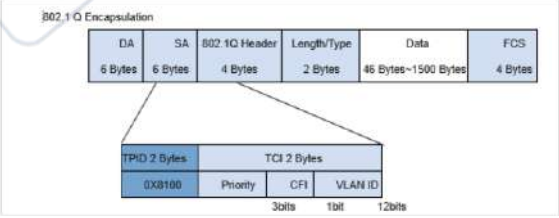
5.5.1. Функции QinQ, поддерживаемые устройством

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

Базовый QinQ: Базовый QinQ, также называемый туннелем уровня 2 QinQ, реализуется на основе режима интерфейса. После того, как базовая функция QinQ интерфейса включена, когда интерфейс получает сообщение, устройство записывает VLAN Tag для VLANa 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.

5.5.2. Настройка значение TPID внешнего тега VLAN QinQ

Как показано на рисунке ниже, 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.



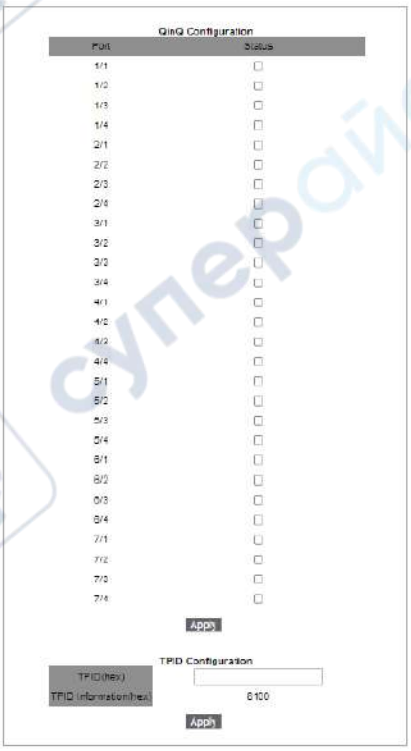
Устройства разных производителей могут устанавливать в поле TPID тега внешней VLAN QinQ разные значения. Для обеспечения совместимости с устройствами других производителей устройство предоставляет функцию изменения значения TPID тега внешней VLAN QinQ. Настроив значение TPID, сообщение QinQ, отправляемое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

Расположение файла TPID кадра Ethernet и типа протокола кадра без тега VLAN совпадают. Чтобы избежать проблем с пересылкой и обработкой пакетов в сети, значение TPID не может быть установлено ни в какое значение из следующей таблицы:

Protocol type	Value
ARP	0x0806
RARP	0x8035
IP	0x0800
IPv6	0x86DD
PPPoE	0x8863/0x8864
MPLS	0x8847/0x8848
IPX/SPX	0x8137
LACP	0x8809
802.1x	0x888E
HGMP	0x88A7
Device reserved	0xFFFD/0xFFFE/0xFFFF

5.5.3. Настройка через веб интерфейс

Щелкнуть [Device Basic Configuration] → [QinQ] → [QinQ configuration] для входа на страницу настройки QinQ интерфейса, как показано на рисунке ниже.



- **Port**

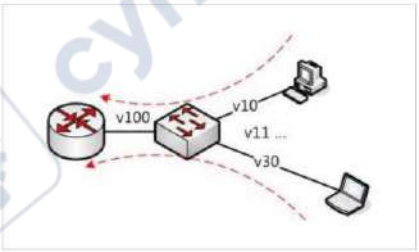
  Диапазон: все порты в коммутаторе

- **Port status**
  Опция: check / uncheck
  Функция: Выбор, следует ли включить порт QinQ.
- **TPID (hex)**
  Диапазон: 5dd-ffff
  Функция: конфигурирование TPID (hex)
  Описание: Когда интерфейс получает сообщение, устройство записывает тег VLAN для VLAN по умолчанию.

5.6. PVLAN конфигурация

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

Верхний VLAN — это VLAN с общим доменом, в которой порты являются восходящими портами. Нижний VLAN являются изолированными доменами, в которых порты являются портами нисходящей линии связи. Порты нисходящей линии связи могут быть назначены разным доменам изоляции, и они могут одновременно взаимодействовать с портом восходящей линии связи. Изолированные домены не могут взаимодействовать друг с другом.



Как показано на рисунке, общий домен — это VLAN100, а изолированные домены — это 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.

Функцию PVLAN можно реализовать с помощью специальной конфигурации портов.

- PVID восходящих портов совпадает с общим идентификатором VLAN домена; PVID нисходящих портов совпадает с их собственным идентификатором VLAN домена изоляции.
- Для восходящих портов не используются теги, и они назначаются VLAN общего домена и всем изолированным доменам; для портов нисходящей линии связи не используются теги, и они назначаются VLAN общего домена и собственному изолированному домену.

5.7. Зеркалирование

С функцией зеркального отображения портов коммутатор копирует все полученные или переданные кадры данных в одном порту (зеркальное отображение исходного порта)

на другой порт (зеркальное отображение порта назначения). Порт назначения зеркалирования может быть подключен к анализатору протокола или монитору RMON для мониторинга сети, управления и диагностики неисправностей.

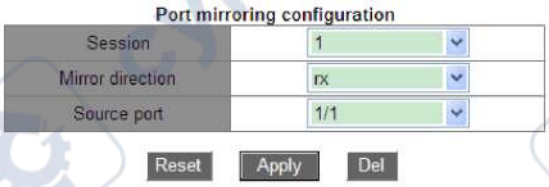
Коммутатор поддерживает только один порт назначения для зеркалирования, но несколько портов-источников. Несколько исходных портов могут находиться либо в одной VLAN, либо в разных VLAN. Порт источника и порт назначения зеркалирования могут находиться в одной и той же VLAN или в разных VLAN. Исходный порт и порт назначения не могут быть одним и тем же портом.

Порт назначения зеркалирования и port channel являются взаимоисключающими. Порт назначения зеркального отображения не может быть добавлен к port channel, и порт в port channel не может быть установлен в качестве порта назначения зеркального отображения.

5.7.1. Настройка через веб интерфейс

Выберите исходный порт зеркалирования и режим зеркалирования.

Щелкнуть [Device Basic Configuration] → [Port mirroring configuration] → [Mirror configuration] для входа на страницу конфигурации порта источника зеркалирования, как показано на рисунке ниже.



- **Session**
  Опция: 1~7
  По умолчанию: 1
  Функция: Выберите группу зеркалирования.
- **Mirror Direction**
  Опция: rx/tx/both
  По умолчанию: rx
  Функция: Выберите данные для зеркального отображения в исходном порту зеркального отображения.
  Описание: rx указывает, что в исходном порту зеркалируются только полученные пакеты;
  tx указывает, что в исходном порту зеркалируются только передаваемые пакеты.
  both указывает, что и переданные, и полученные пакеты зеркально отражены в исходном порту.
- **Source port**
  Опции: все порты коммутатора

Функция: Выберите исходный порт зеркалирования. Вы можете выбрать несколько исходных портов.

Выберите порт назначения зеркалирования, как показано на рисунке ниже.

- **Session**
  Опция: 1~7
  По умолчанию: 1
  Функция: Выбор группы зеркалирования
- **Destination port**
  Опция: все порты, кроме исходного порта.
  Функция: Выберите порт назначения зеркалирования.
  Описание: Установите порт в качестве порта назначения зеркалирования. Существует только один порт назначения зеркалирования. Порт назначения зеркального отображения не может быть членом канала порта. Лучше, чтобы пропускная способность порта назначения была больше или равна общей пропускной способности портов-источников.

5.8. Port Storm Control

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

5.8.1. Настройка через веб интерфейс

Настройте пороговое значение port storm control.

Щелкнуть [Device Basic Configuration] → [Port Storm Suppression configuration] → [Port Storm Suppression configuration] для входа на страницу конфигурации, как показано на рисунке ниже.

- **Port name**
  Опции: все порты коммутатора
  Функция: Выберите порты, для которых требуется ограничение скорости.

- **Rate Unit**
  Опции: bps/kbps/percent
  Функция: Выберите единицу порога.
- **Rate Value**
  Диапазон: 1~1000000kbps/1~1000000000bps/1~100 Percent
  По умолчанию: 0, когда значение равно 0, управление штормом портов отключено.
  Функция: Настройте пороговое значение для ограничения скорости порта, и пакеты, превышающие пороговое значение, будут отброшены. Диапазон значений зависит от фактической скорости порта. Подробнее смотри таблицу ниже.
  Описание: Пороговое значение порта Fast Ethernet находится в диапазоне 1~100000 кбит/с / 1~100000000 бит/с; порог порта Gigabit Ethernet находится в диапазоне 1~1000000кбит/с / 1~10000000000бит/с. Процент соответствует пропускной способности порта, например, если значение ограничения скорости порта 100M составляет 60%, порт начинает отбрасывать данные после получения трафика данных 60M.

Port Rate	Threshold Unit	Step	Value Range
10M	bps	512	512~10000000
	kbps	Not recommended	Not recommended
100M	bps	5120	5120~100000000
	kbps	5	5~100000
1000M	bps	51200	51200~1000000000
	kbps	50	50~1000000

Выберите тип управляемых пакетов, как показано на рисунке ниже.

- **Port name**
  Опции: все порты, на которых включено port storm control
- **Suppression Type**
  Опции: Multicast / broadcast / dlf
  Функция: Выберите тип пакетов для управления.
- **Function**
  Опции: Enable / Disable.
  По умолчанию: Disable
  Функция: Включение или выключение контроль над типом пакетов.

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

5.9. Port Isolation

Чтобы реализовать изоляцию пакетов на уровне 2, вы можете добавить порты в разные VLAN. Однако этот метод приведет к пустой трате ограниченных ресурсов VLAN. Используя функцию изоляции портов, вы можете 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.

- Порты группы изоляции могут быть только портами одного и того же коммутатора.
- Одно устройство поддерживает максимум 14 групп изоляции, и количество портов Ethernet в каждой группе не ограничено.
- После настройки группы изоляции только пакеты между портами группы изоляции не могли обмениваться друг с другом, связь между портами в группе изоляции и портами вне группы изоляции не пострадала бы.
- Изолированный порт и канал порта являются взаимоисключающими. Порт группы изоляции нельзя добавить в канал порта, а порт в канале порта нельзя добавить в группу изоляции.

5.9.1. Настройка через веб интерфейс

Щелкнуть [Device Basic Configuration] → [Port Isolate configuration] → [Port Isolate configuration] для входа на страницу конфигурации, как показано на рисунке ниже.

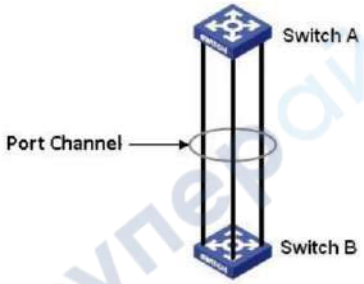
- **Port Isolate**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: Включите или отключите изоляцию порта.

Один порт добавляется только в одну группу изоляции.

5.10. Port Channel

Канал порта предназначен для привязки группы физических портов с одинаковой конфигурацией к логическому порту для увеличения пропускной способности и повышения скорости передачи. Порты-члены 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 канал порта и становиться независимым логическим портом, тем самым увеличивая пропускную способность сети и обеспечивая резервирование канала.

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



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

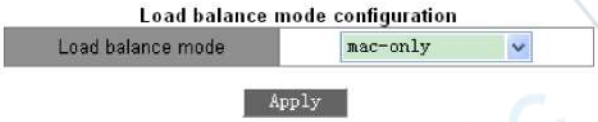
Коммутаторы серии поддерживают не более 8 групп портов, и каждая группа содержит не более 8 портов-членов.

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

5.10.1. Настройка через веб интерфейс

Настроить режим распределения нагрузки канала порта.

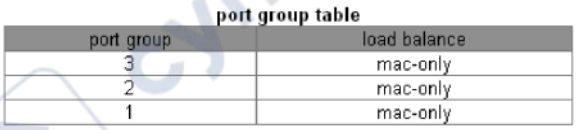
Щелкнуть [Device Basic Configuration] → [Port channel configuration] → [Port group configuration] для входа на страницу конфигурации, как показано на рисунке ниже.



- **Load balance mode**
  Опции: mac-only / ip-only / mac-ip / ip-l4 / mac-ip-l4
  По умолчанию: mac-only
  Функция: Установить режим распределения нагрузки канала порта.
  Описание: mac-only указывает на распределение нагрузки на основе MAC-адресов.
  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.
  Объяснение: Если режим распределения нагрузки необходимо изменить после формирования канала порта, изменение вступит в силу после следующей агрегации.

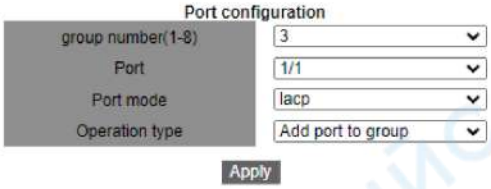
Создайте или удалите группу портов, как показано на рисунке ниже.

- **group number**
  Диапазон: 1~8
  Функция: Установите номер группы портов, максимум 8 групп портов.
- **Operation type**
  Опции: добавить группу портов/удалить группу портов
  По умолчанию: добавить группу портов
  Функция: создание или удаление группы портов.
  После завершения настройки на странице «Таблица групп портов» перечислены все созданные группы портов и режимы распределения нагрузки, как показано на рисунке ниже.



Настройка члена группы портов.

Щелкнуть [Device Basic Configuration] → [Port channel configuration] → [port configuration] для входа на страницу конфигурации, как показано на рисунке ниже.



- **group number**
  Опции: все созданные номера групп портов.
- **Port**
  Опции: все порты коммутатора
  По умолчанию: добавить группу портов
  Функция: Выберите порт, который необходимо добавить или удалить из группы портов.
  Описание: порты-участники одной группы портов имеют одинаковые атрибуты порта.
- **Operation type**
  Опции: Добавить порт в группу / Удалить порт из группы
  По умолчанию: добавить порт в группу
  Функция: добавить порт или удалить порт из группы портов.

5.11. Конфигурация Telnet Server

Telnet — это протокол для доступа к удаленным терминалам. Вы можете войти на удаленный хост, используя IP-адрес или имя хоста через Telnet. Telnet может передавать ваши команды на удаленный хост и возвращать вывод удаленного устройства на ваш дисплей через TCP.

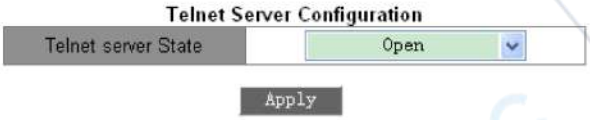
Telnet работает в режиме клиент / сервер. Локальная система является клиентом, а удаленный хост — сервером. Коммутаторы этой серии могут служить в качестве сервера или клиента Telnet.

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

Когда коммутатор служит клиентом Telnet, вы можете 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.

5.11.1. Настройка через веб интерфейс

Щелкнуть [Device Basic Configuration] → [Telnet server configuration] → [Telnet server configuration] для входа на страницу конфигурации, как показано на рисунке ниже.



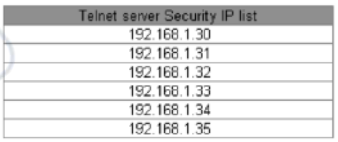
- **Telnet server state**
  Опции: open / close.
  По умолчанию: open
  Функция: включение или выключение функции сервера Telnet.
  Описание: Open означает, что клиенты Telnet могут входить в коммутатор. Close означает, что клиенты Telnet не могут войти в коммутатор.

➢ Коммутатор может работать как клиент Telnet для входа на удаленный хост независимо от того, включена ли эта функция.

Настройте безопасный IP-адрес для входа клиента Telnet.

Щелкнуть [Device Basic Configuration] → [Telnet server configuration] → [Telnet security IP] для входа на страницу конфигурации, как показано на рисунке ниже.

- **Security IP address**
  Формат: A.D.C.D
  Функция: Настройка безопасного IP-адрес для входа клиента Telnet, когда коммутатор работает как сервер Telnet.
  Описание: Если безопасный IP-адрес не установлен, ограничения на IP-адрес клиента Telnet отсутствуют.
  После установки безопасных IP-адресов только клиент с безопасным IP-адресом может войти в систему и настроить коммутатор с помощью Telnet.
  Коммутатор допускает до 32 безопасных IP-адресов. По умолчанию безопасный IP-адрес не настроен.
  После завершения настройки в «Списке IP-адресов безопасности сервера Telnet» отображаются IP-адреса клиентов Telnet, которые могут войти в коммутатор, как показано на рисунке ниже.



5.12. Конфигурация SSH Server

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

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

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 безопасности на основе ключей требует секретных ключей, и каждый конец 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 даты, чтобы гарантировать безопасность данных.

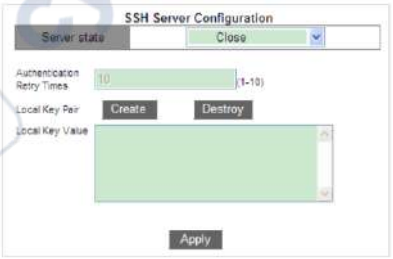
Чтобы реализовать безопасное соединение SSH в процессе связи, сервер и клиент проходят следующие пять этапов: Стадия согласования версии: в настоящее время SSH состоит из двух версий: SSH1 и SSH2. Две стороны договариваются об используемой версии. Этап согласования ключа и алгоритма: SSH поддерживает несколько типов алгоритмов шифрования. Две стороны согласовывают алгоритм для использования. Состояние аутентификации: клиент SSH отправляет запрос на аутентификацию на сервер, и сервер аутентифицирует клиента. Этап запроса сеанса: клиент отправляет запрос сеанса на сервер после прохождения аутентификации. Стадия сеанса: клиент и сервер начинают общение после передачи запроса сеанса.

5.12.1. Настройка через веб интерфейс

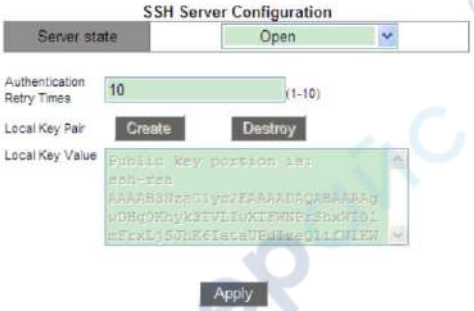
Этапы настройки SSH-сервера.

Щелкнуть [Device Basic Configuration] → [SSH Server Configuration] → [SSH server configuration] для входа на страницу конфигурации, как показано на рисунке ниже.

- Отключить статус SSH.
- Нажмите <Destroy>, чтобы уничтожить старую пару ключей, как показано на рисунке ниже.



- Нажмите <Create>, чтобы создать новую пару ключей.
- Включите протокол SSH и настройте сервер SSH, как показано на рисунке.



- **Server state**
  Опции: open / close.
  По умолчанию: close
  Функция: включить/отключить протокол SSH. Если он включен, коммутатор работает как SSH-сервер.
- **Authentication Retry Times**
  Диапазон конфигурации: 1~10
  По умолчанию: 10
  Функция: установить количество попыток входа на сервер SSH.
- **Local Key Pair**
  Опции: Создать / Удалить
  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. Нажмите <Create>, чтобы автоматически сгенерировать значение ключа.

Настройка безопасного IP-адреса для входа клиента SSH.

Щелкнуть [Device Basic Configuration] → [SSH Server Configuration] → [SSH security IP] для входа на страницу конфигурации, как показано на рисунке ниже.

- **Security IP Address**
  Формат: A.B.C.D.
  Функция: Настройте безопасный IP-адрес для входа клиента SSH, когда коммутатор работает как сервер SSH. Если безопасный IP-адрес не установлен, ограничения на IP-адрес SSH-клиента отсутствуют.
  После установки безопасных IP-адресов только клиент с безопасным IP-адресом может войти в систему и настроить коммутатор с помощью SSH.
  Объяснение: Коммутатор допускает использование максимум 6 IP-адресов безопасности. По умолчанию безопасный IP-адрес не настроен.

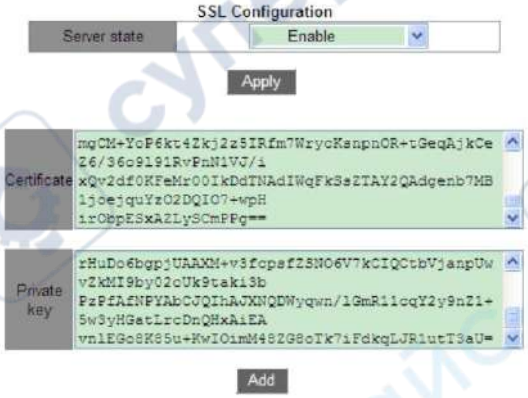
5.13. SSL конфигурация

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 в сети. Когда коммутатор включает SSL, пользователи должны использовать безопасную ссылку https, например https://192.168.0.2, для доступа к коммутатору.

5.13.1. Настройка через веб интерфейс

Включение HTTPS протокола.

Щелкнуть [Device Basic Configuration] → [SSL Server configuration] → [SSL Server Configuration] для входа на страницу конфигурации, как показано на рисунке ниже.



- **Server state**
  Опция: Enable / Disable
  По умолчанию: Disable
  Функция: включить или отключить протокол SSL.
  Объяснение: После включения SSL пользователи должны использовать безопасную ссылку https://ip-адрес для доступа к коммутатору.
- **Certificate/Private key**
  Функция: введите правильный сертификат и закрытый ключ, затем нажмите кнопку <Add>, чтобы импортировать их для переключения.

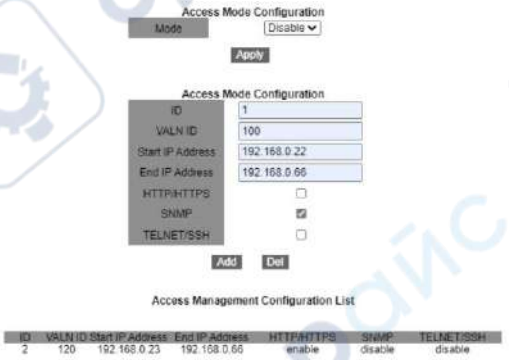
Сертификат по умолчанию и закрытый ключ, предоставленные компанией, уже импортированы в коммутатор. Пользователи могут напрямую включить протокол SSL и получить доступ к коммутатору в режиме HTTPS.

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

5.14. Управление доступом

5.14.1. Настройка через веб интерфейс

Включить ли управление доступом, включить ли метод доступа через веб / ftp / telnet, идентификатор управления доступом, идентификатор Vlan, начальный IP-адрес, конечный IP-адрес, тип службы и удалить метод управления доступом можно настроить на странице управления доступом, как показано на рисунке ниже.



- **Access management status**
  Опция: Enable / Disable
  По умолчанию: Disable
  Функция: Включить ли управление доступом, если включено, устройство будет управлять доступом к устройству.
- **ID**
  Диапазон: 1 ~ 16
  Функция: используется для подписи условия управления доступом к устройству.
- **Vlan ID**
  Диапазон конфигурации: 1~4093
  Функция: настройка VLAN, для которой требуется управление доступом.
- **Start IP address**
  Формат: A.B.C.D.
  Функция: Настройка диапазона IP-адресов, позволяющих конфигурировать 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, позволяющих 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: если выбран HTTP/HTTPS, хост, который соответствует идентификатору VLAN и IP-адресу в записи доступа, может получить доступ к коммутатору через HTTP/HTTPS.
- **SNMP**

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

- **TELNET/SSH**
  Функция: Если выбран TELNET/SSH, хост, который соответствует идентификатору VLAN и IP-адресу в записи доступа, может получить доступ к коммутатору через TELNET/SSH.
  Нажмите <Add New Entry>, чтобы настроить запись управления доступом, коммутатор поддерживает до 16 записей управления доступом.

5.15. Служба передачи файлов

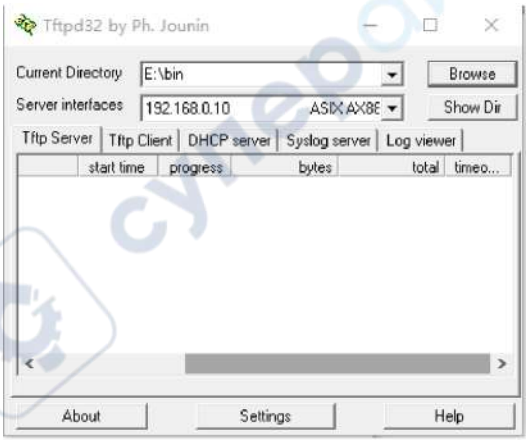
Служба передачи файлов обеспечивает взаимное резервное копирование файлов между сервером и клиентом. При изменении файла на сервере (или клиенте) вы можете получить файл резервной копии с клиента (или сервера) через FTP / TFTP / SFTP. Коммутатор может служить клиентом или сервером для загрузки и выгрузки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

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

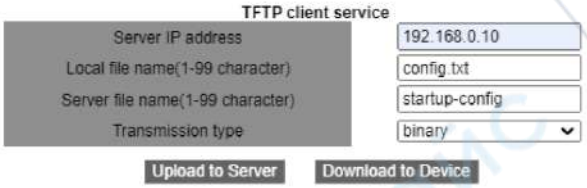
5.15.1. TFTP Service

Коммутатор работает как TFTP-клиент.

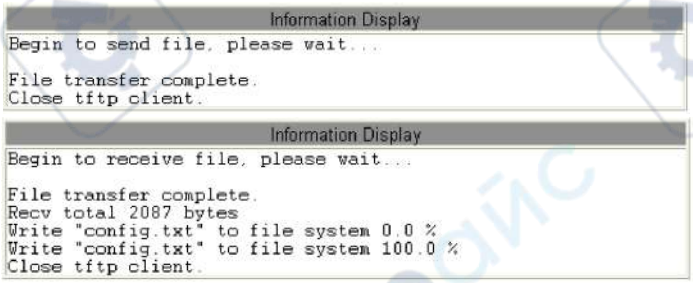
Сначала установите TFTP-сервер, как показано на рисунке ниже. В Current Directory найдите используемый путь к хранилищу файлов. Введите IP-адрес сервера в интерфейсе сервера.



Щелкнуть [Device Basic Configuration] → [File transmit] → [TFTP Service] → [TFTP client service] для входа на страницу конфигурации TFTP клиента, как показано на рисунке ниже.



- **Server IP address**
  Формат: A.D.C.D.
  Описание: Ввод IP адреса 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**
  Элементы конфигурации: binary / ascii
  По умолчанию: binary
  Функция: выбор стандарта передачи файлов.
  Объяснение: ascii означает использование стандарта ASCII для передачи файла; двоичный означает использование двоичного стандарта для передачи файла.
  Метод: Нажмите <Upload to PC>, чтобы загрузить файл с коммутатора на сервер, или <Download to Server>, чтобы загрузить файл с сервера на коммутатор.
  После успешной передачи файла в веб-интерфейсе появляется следующая информация, как показано на рисунках ниже.



- В процессе передачи файлов поддерживает работу TFTP-сервера.
- Файл версии программного обеспечения не является текстовым файлом и должен принимать двоичный стандарт для передачи.

Коммутатор работает как TFTP-сервер.

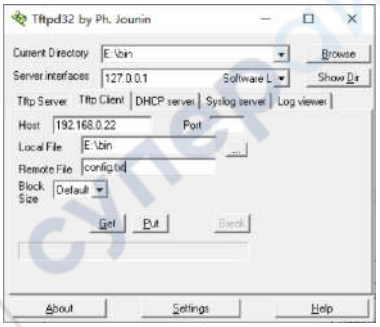
Щелкнуть [Device Basic Configuration] → [File transmit] → [TFTP Service] → [TFTP sever service] для входа на страницу конфигурации TFTP сервера, как показано на рисунке ниже.

- **Server state**

Элементы конфигурации: Close / Open
По умолчанию: Close
Функция: включение/выключение функции сервера TFTP.

- **TFTP Timeout**
  Диапазон: 5~3600 с
  По умолчанию: 20 с.
  Функция: Настройка тайм-аута подключения к серверу TFTP.
- **TFTP Retransmit times**
  Диапазон: 1~20
  По умолчанию: 5
  Функция: настройка времени повторной передачи сервера TFTP во время тайм-аута.

Установите клиентское программное обеспечение TFTP, как показано на рисунке ниже. Введите IP-адрес коммутатора в Host; выберите путь хранения файлов клиента в Local File; введите имя файла, сохраненного в переключателе в удаленном файле; нажмите <Get>, чтобы загрузить файл с коммутатора на клиента; нажмите <Put>, чтобы загрузить файл клиента для переключения.

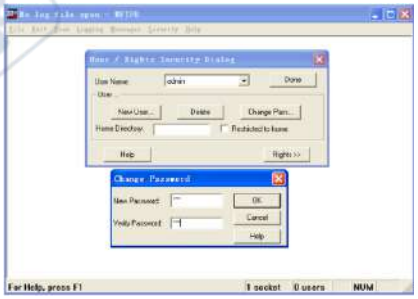


➢ Во время передачи файлов не отключайте программное обеспечение клиента TFTP.

5.15.2. FTP Service

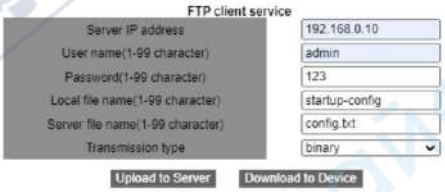
Коммутатор работает как FTP-клиент.

Сначала установите FTP-сервер. Щелкнуть [Security] → [users/rights] для открытия диалогового окна. Нажмите <новый пользователь>, чтобы создать нового пользователя FTP, как показано на рис. 96. Введите имя пользователя (username) и пароль (password), например, имя пользователя: admin; пароль: 123. Нажмите <OK>.



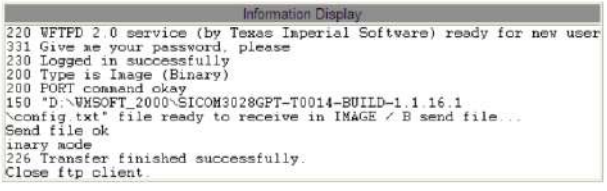
Введите путь к хранилищу файлов на сервере в домашнем каталоге, как показано на рисунке ниже. Нажмите <Done>.

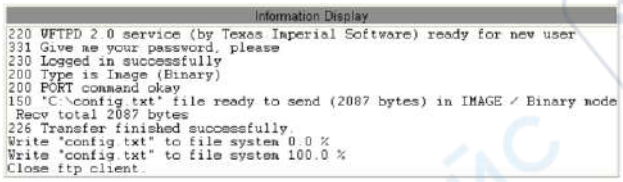
Щелкнуть [Device Basic Configuration] → [File transmit] → [FTP Service] → [FTP client] для входа на страницу конфигурации FTP клиента, как показано на рисунке ниже.



- **Server IP address**
  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 FTP-сервере.
- **Local file name.**
  Диапазон: 1~99 символов
  Описание: указывает имя файла в коммутаторе.
- **Server file name**
  Диапазон: 1~99 символов
  Описание: указывает имя файла на сервере.
- **Transmission type**
  Элементы конфигурации: binary / ascii
  По умолчанию: binary
  Функция: выбор стандарта передачи файлов.
  Объяснение: ascii означает использование стандарта ASCII для передачи файла; binary означает использование двоичного стандарта для передачи файла.
  Метод: Нажмите <Upload to PC>, чтобы загрузить файл с коммутатора на сервер. Нажмите <Download to device>, чтобы загрузить файл с сервера для переключения.

  После успешной передачи файла в веб-интерфейсе появляется следующая информация, как показано на рисунках ниже.



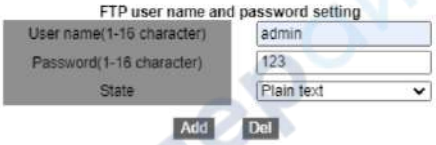


В процессе передачи файлов не отключайте программное обеспечение FTP-сервера. Файл версии программного обеспечения не является текстовым файлом, и для передачи он должен принимать двоичный стандарт.

Коммутатор работает как FTP-сервер.

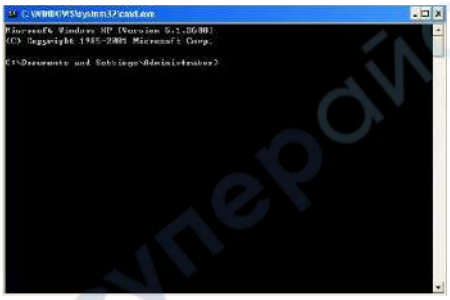
Щелкнуть [Device Basic Configuration] → [File transmit] → [FTP Service] → [FTP server] для входа на страницу конфигурации FTP сервера, как показано на рисунке ниже.

- **FTP Server state**
  Формат: Close / Open.
  По умолчанию: Close
  Функция: включение или отключение функции FTP-сервера.
- **FTP Timeout**
  Диапазон: 5~3600 с
  По умолчанию: 600 с
  Функция: настройка времени ожидания подключения к FTP-серверу.
  Описание: Если в течение тайм-аута 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 ниже.

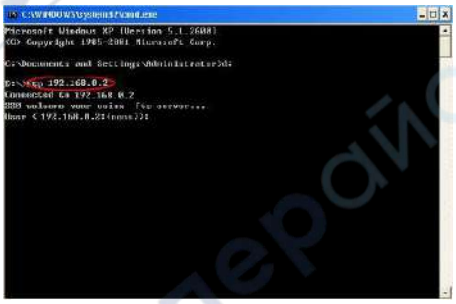


- **{Username, Password}**
  Диапазон: {1~16 символов, 1~16 символов}
  Функция: Настройка имени пользователя и пароля для входа на FTP-сервер.
  Описание: Когда коммутатор работает как FTP-сервер, он может одновременно подключаться к нескольким FTP-клиентам.
- **State**
  Опции: Простой текст / Зашифрованный текст
  По умолчанию: обычный текст
  Функция: Выберите режим отображения пароля.

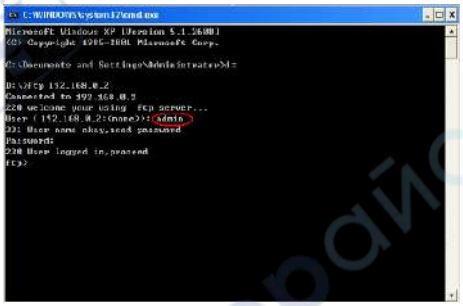
Щелкнуть [Пуск] → [Выполнить] в Windows. Отображается диалоговое окно «Выполнить». Введите «cmd» и нажмите Enter. Отображается следующая страница.



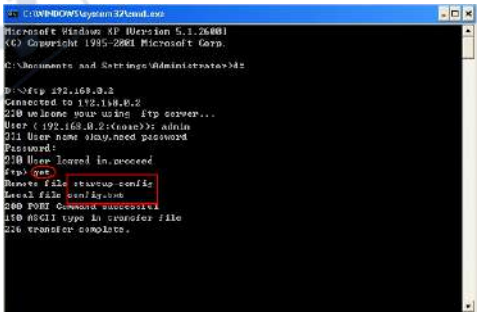
Путь передачи файла можно изменить. Войдите на FTP-сервер, как показано на рисунке:



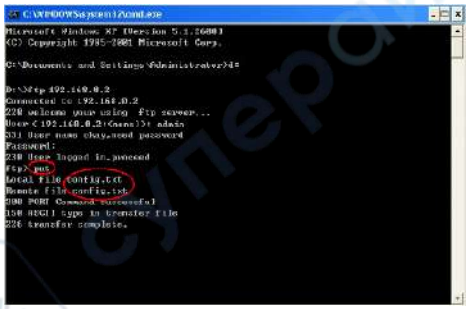
Используйте настроенное имя пользователя «admin» и пароль «123» для входа на FTP-сервер, как показано на рисунке ниже:



Используйте команду «get», чтобы загрузить файл по указанному пути на клиенте, как показано на рисунке. Введите команду «get» и нажмите Enter. Введите имя файла на коммутаторе для загрузки в удаленный файл и имя файла, сохраненного на клиенте, в локальный файл.



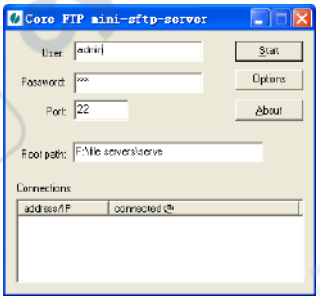
Используйте команду «put», чтобы загрузить файл по указанному пути в клиенте на сервер, как показано на рисунке ниже. Запустите команду «put» и нажмите Enter. Введите имя файла в переключатель в удаленном файле и имя файла в клиенте, который будет загружен в локальный файл.



5.15.3. SFTP Service

Коммутатор работает как SFTP-клиент.

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



Щелкнуть [Device Basic Configuration] → [File transmit] → [SFTP Service] → [SFTP client service] для входа на страницу конфигурации SFTP клиента, как показано на рисунке ниже.

- **Server IP address**
  Формат: A.B.C.D.
  Описание: Настройка IP-адреса SFTP-сервера.
- **{User name, Password}**
  Диапазон: {1~99 символов, 1~99 символов}
  Описание: Введите имя пользователя и пароль, созданные на SFTP-сервере.
- **Local file name**

Диапазон: 1~99 символов

Описание: указывает имя файла в коммутаторе.

- **Имя файла сервера**

  Диапазон: 1~99 символов

  Описание: указывает имя файла на сервере.

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

  После успешной передачи файла в веб-интерфейсе появляется следующая информация, как показано на рисунках ниже.

```
Upload file "config.txt" start, file size 1518 bytes.

Upload "config.txt" 100.0 %
File transfer finished, total 1518 bytes.
```

```
Download file "config.txt" start, file size 1518 bytes.

Download "config.txt" 100.0 %
Download "config.txt" 100.0 %
File transfer finished , total 1518 bytes.

Write "runconfig2.txt" 0.0 %
Write "runconfig2.txt" 100.0 %
write to flash success
```

В процессе передачи файлов не отключайте программное обеспечение SFTP-сервера.

5.16. Конфигурация MAC Address

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 узнаются коммутатором 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 фрейм 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 фрейм с MAC-адресом в течение времени устаревания, равного одному или двум, коммутатор удаляет запись MAC-адреса из таблицы адресов динамической пересылки. Статические MAC-адреса не включают понятие времени устаревания.

Коммутатор поддерживает не более 1024 статических одноадресных записей.

5.16.1. Веб конфигурирование

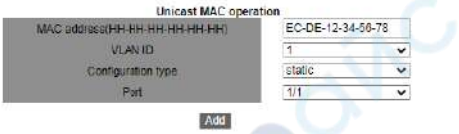
Настройка привязки по MAC-адресу.

Щелкнуть [Device Basic Configuration] → [MAC address table configuration] → [MAC bind Configuration] для входа на страницу конфигурации, как показано на рисунке ниже.

- **MAC bind state**
  Опция: Enable / Disable
  По умолчанию: Disable
  Функция: включение или отключение функции привязки MAC-адресов. Если выбрано значение enable, для пакета, исходный MAC-адрес и идентификатор VLAN которого соответствуют MAC-адресу и идентификатору VLAN записи статического индивидуального MAC-адреса, коммутатор проверяет, соответствует ли входной порт порту этого статического индивидуального MAC-адреса. Если да, коммутатор получает и пересылает пакет. Если нет, коммутатор отбрасывает пакет. При отключении предыдущая проверка не выполняется.

Добавление статического MAC-адрес индивидуальной рассылки.

Щелкнуть [Device Basic Configuration] → [MAC address table configuration] → [Unicast address configuration] для входа на страницу конфигурации, как показано на рисунке ниже.



- **MAC address**
  Формат: HH-HH-HH-HH-HH-HH (H — шестнадцатеричное число)
  Функция: Настройка одноадресного MAC-адреса. Младший бит в первом байте равен 0.
- **VLAN ID**
  Опции: все созданные идентификаторы VLAN.
  По умолчанию: VLAN1
- **Configuration type**
  Варианты: static / blackhole
  По умолчанию: static
  Функция: выберите тип записи MAC-адреса.
  Описание: Статический означает установление соответствия между назначенным MAC-адресом и номером порта или идентификатором VLAN. Blackhole должен отбросить пакет, исходный MAC-адрес которого или MAC-адрес назначения является назначенным MAC-адресом.

- **Port**
  Опции: все порты коммутатора
  Функция: выберите порт для пересылки пакетов с этим MAC-адресом назначения. Выбранный порт должен находиться в указанной сети VLAN.

Удаление статического MAC-адрес индивидуальной рассылки.

Щелкнуть [Device Basic Configuration] → [MAC address table configuration] → [Delete unicast address] для входа на страницу конфигурации, как показано на рисунке ниже.

Выберите критерий для удаления индивидуального адреса. Если выбрано несколько критериев, их взаимосвязь является логическим «И».

Настройка времени устаревания MAC-адреса.

Щелкнуть [Device Basic Configuration] → [MAC address table configuration] → [MAC address aging time setting] для входа на страницу конфигурации, как показано на рисунке ниже.

- **Aging time**
  Диапазон: 10~100000c
  По умолчанию: 300 с
  Функция: Установите время устаревания для записи динамического MAC-адреса.
  Описание: Когда время старения установлено на 0, старение запрещено. В этом случае адрес, полученный динамически, не устаревает со временем.

Запрос unicast MAC-адреса.

Щелкнуть [Device Basic Configuration] → [MAC address table configuration] → [MAC address query] для входа на страницу конфигурации, как показано на рисунке ниже.

Выберите критерий для unicast запроса MAC-адреса. Если выбрано несколько критериев, их взаимосвязь является логическим «И». Например: Если вы запрашиваете unicast адрес порта Ethernet 1/1, отображается следующая страница.

Просмотр unicast записей адресов

Щелкнуть [Device Basic Configuration] → [MAC address table configuration] → [Show mac-address table] для входа на страницу конфигурации, как показано на рисунке ниже.

5.17. Базовая информация по сопровождению конфигурации и отладке

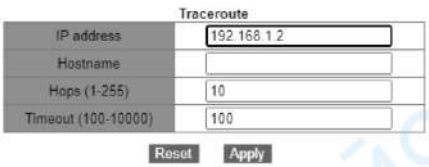
При настройке коммутатора может потребоваться проверка правильности различных конфигураций для обеспечения нормальной работы; или при возникновении определенных аномалий может потребоваться локализация неисправности. В этих случаях вы можете выполнить следующие операции для просмотра конфигурации системы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

Ping

Щелкнуть [Device Basic Configuration] → [Basic configuration debug] → [Ping and Traceroute] для входа на страницу конфигурации ping, как показано на рисунке ниже.

- **IP address**
  Формат: A.B.C.D.
  Описание: Введите IP-адрес удаленного устройства.
- **Hostname**
  Диапазон: 1~30 символов
  Функция: Если сопоставление между удаленным хостом и IP-адресом установлено, 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.

Traceroute



- **IP address**
  Формат: A.B.C.D.
  Описание: Введите IP-адрес удаленного устройства.
- **Hostname**
  Диапазон: 1~30 символов
  Функция: Если сопоставление между удаленным хостом и IP-адресом установлено, вам нужно ввести только имя удаленного хоста для выполнения операции Traceroute.
- **Hops**
  Опции: 1~255
  Функция: проверка количества шлюзов, через которые проходят пакеты от отправляющего устройства к целевому.
- **Timeout**
  Опции: 100~10000 мс
  Функция: Настройка тайм-аута. Если отправляющее устройство не получает ответный пакет от принимающего устройства в течение этого времени, считается, что связь не удалась.

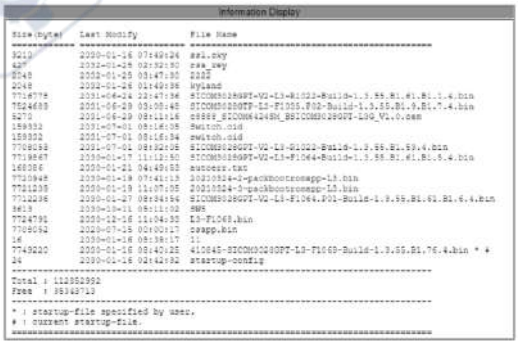
Просмотр системной даты и времени.

Коммутаторы этой серии поддерживают RTC. Даже питание отключено, хронометраж продолжается.

Щелкнуть [Device Basic Configuration] → [Basic configuration debug] → [show clock] для входа на страницу информации, как показано на рисунке ниже.

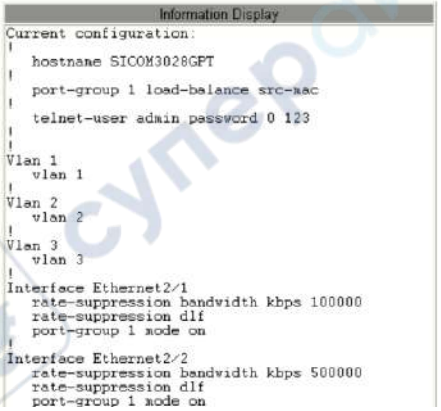
Просмотр информацию о файлах на flash.

Щелкнуть [Device Basic Configuration] → [Basic configuration debug] → [show flash] для входа на страницу информации, как показано на рисунке ниже.



Просмотр информации о конфигурации: running-config

Щелкнуть [Device Basic Configuration] → [Basic configuration debug] → [show running-config] для входа на страницу информации, как показано на рисунке ниже.



Просмотр информации о порте

Щелкнуть [Device Basic Configuration] → [Basic configuration debug] → [show switchport interface] для входа на страницу информации, как показано на рисунке ниже.

- **Type**
  Описание: тип VLAN.
- **Mode**
  Описание: режим порта. V
- **Port VID**
  Описание: порт PVID
- **Trunk allowed Vlan With TAG**
  Описание: Указывает VLAN для выбранного магистрального порта в виде тега.
- **Trunk allowed Vlan With UNTAG**
  Описание: указывает VLAN для выбранного транкового порта как неотмеченные.

Просмотр состояния TCP-соединения.

Щелкнуть [Device Basic Configuration] → [Basic configuration debug] → [show tcp] для входа на страницу информации, как показано на рисунке ниже.

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

- **Local Address**
  Описание: указывает локальный адрес TCP-соединения.
- **Local Port**
  Описание: указывает номер локального порта TCP-соединения.
- **Foreign Address**
  Описание: указывает адрес на другом конце TCP-соединения.
- **Foreign Port**
  Описание: указывает номер порта на другом конце соединения TCP.
- **State**
  Описание: указывает текущий статус TCP-соединения.

Просмотр состояния UDP-соединения.

Щелкнуть [Device Basic Configuration] → [Basic configuration debug] → [show udp] для входа на страницу информации, как показано на рисунке ниже.

Information Display

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

- **Local Address**
  Описание: указывает локальный адрес UDP-соединения.
- **Local Port**
  Описание: указывает номер локального порта UDP-соединения.
- **Foreign Address**
  Описание: указывает адрес на другом конце UDP-соединения.
- **Foreign Port**
  Описание: указывает номер порта на другом конце соединения UDP.
- **State**
  Описание: указывает текущий статус UDP-соединения.

Просмотр информации о залогининых пользователях.

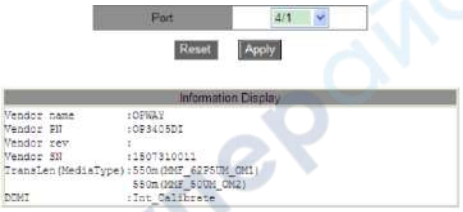
Щелкнуть [Device Basic Configuration] → [Basic configuration debug] → [show login] для входа на страницу информации, как показано на рисунке ниже.

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

Просмотр информации о модуле SFP.

Щелкнуть [Device Basic Configuration] → [Basic configuration debug] → [show transceiver information] для входа на страницу информации о модулях SFP, как показано на рисунке ниже.



6. Расширенная конфигурация

6.1. ARP конфигурация

Address Resolution Protocol (ARP, протокол разрешения адресов) разрешает сопоставление между IP-адресами и MAC-адресами с помощью механизма запроса и ответа адреса. Коммутатор может узнать сопоставление 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 фактическими 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.

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.

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

Процесс прокси-ARP выглядит следующим образом:

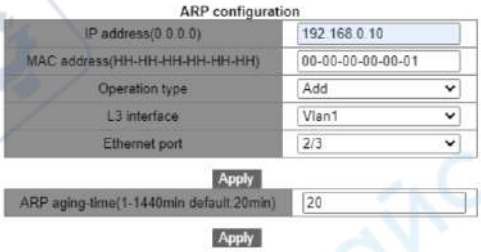
- Хост-источник отправляет запрос ARP на другой хост в другой физической сети.
- Функция proxy ARP на этом интерфейсе VLAN была включена на шлюзе в прямом соединении с хостом-источником.
- Если нормальный маршрут к целевому хосту существует, шлюз отвечает своим собственным MAC-адресом для целевого хоста.
- IP-пакеты, отправленные с исходного узла на узел назначения, отправляются на устройство с включенным прокси-ARP.
- Шлюз выполняет обычную IP-маршрутизацию и пересылку пакетов.
- IP-пакеты, которые должны быть отправлены на узел назначения, наконец достигают узла назначения через сеть.

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

6.1.1. Веб конфигурирование

Добавить или удалить статическую запись ARP.

Щелкнуть [Device Basic Configuration] → [ARP configuration] → [ARP configuration] для входа на страницу информации о ARP, как показано на рисунке ниже.



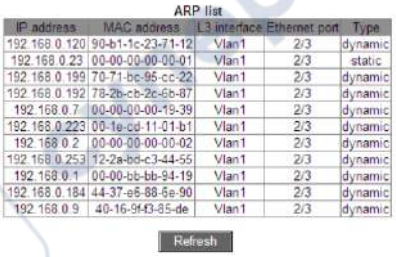
- **IP address**
  Формат: A.B.C.D.
  Функция: Настройка IP-адреса статической записи ARP.
- **MAC address**
  Формат: HH-HH-HH-HH-HH-HH (H — шестнадцатеричное число)
  Функция: Настройка MAC-адреса статической записи ARP.
- **Operation type**
  Опции: add / del
  По умолчанию: add
  Функция: добавить или удалить запись ARP.
- **L3 interface**
  Опции: все созданные интерфейсы VLAN уровня 3.
  По умолчанию: VLAN1
  Функция: выберите интерфейс VLAN уровня 3 для текущей записи ARP.
- **Ethernet Port**
  Опции: все порты в назначенной VLAN
  Функция: выберите выход, соответствующий текущей записи ARP.
- **ARP Aging time**
  Диапазон: 1 ~ 1440 мин.
  По умолчанию: 20 мин.
  Функция: Настройка времени устаревания ARP.
  Описание : Время устаревания ARP — это продолжительность с момента добавления динамической записи ARP в таблицу до момента удаления записи из таблицы.

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.

Просмотр записи адресов ARP.

Щелкнуть [Device Basic Configuration] → [ARP configuration] → [Show ARP] для входа на страницу информации о ARP, как показано на рисунке ниже.



- **ARP list**
  Портфолио: {IP-адрес, MAC-адрес, интерфейс L3, порт Ethernet, тип}
  Функция: просмотр записей ARP.
  Описание: Список ARP показывает все записи ARP, соответствующие портам LinkUp, включая статические записи и динамические записи.

Очистка кеша ARP.

Щелкнуть [Device Basic Configuration] → [ARP configuration] → [Clear ARP cache] для очистки кеша ARP, как показано на рисунке ниже.

Нажмите <Apply>, чтобы очистить динамические записи ARP в кэше.

Включить прокси-ARP.

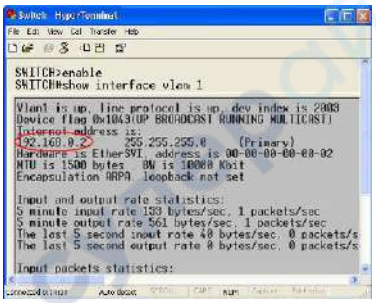
Щелкнуть [Device Basic Configuration] → [ARP configuration] → [Proxy ARP configuration] для конфигурирования кеша ARP, как показано на рисунке ниже.

- **VLAN interface**
  Функция: выберите 3-уровневый интерфейс VLAN для включения прокси-ARP.

6.2. Layer 3 конфигурация интерфейса

6.2.1. IP address коммутатора

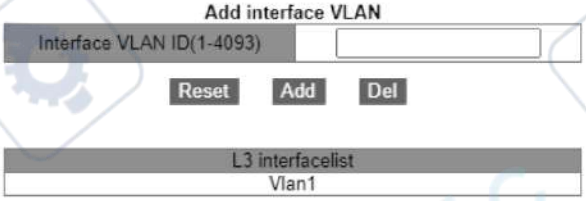
Войдите в CLI коммутатора через консольный порт. Запустите команду enable в общем виде, чтобы войти в привилегированный вид. Запустите команду show interface vlan 1, чтобы просмотреть IP-адрес коммутатора, как показано в красном круге на рисунке ниже.



6.2.2. Конфигурирование IP Address

Создайте интерфейс VLAN уровня 3.

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



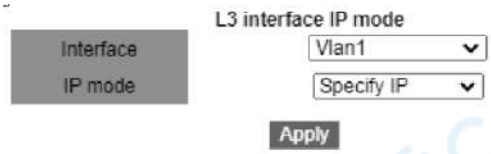
- **Interface vlan ID**
  Опции: все созданные номера VLAN.
  Функция: создание интерфейса VLAN уровня 3.

Коммутатор поддерживает максимум 16 интерфейсов VLAN уровня 3.
Перед созданием интерфейса VLAN убедитесь в наличии соответствующей VLAN. Если VLAN не существует, ее интерфейс VLAN не может быть создан.
Вы не можете удалить интерфейс VLAN, соответствующий IP-адрес которого используется для доступа к коммутатору через web.

Присвоение IP address.

IP-адрес коммутатора можно настроить вручную или получить автоматически.

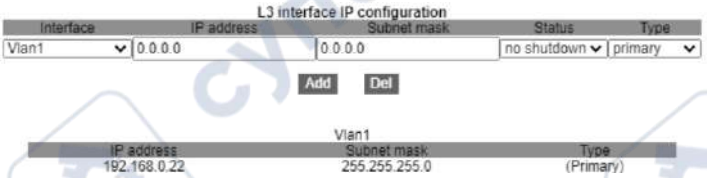
Щелкнуть [Device Basic Configuration] → [L3 interface configuration] → [L3 interface IP address mode configuration] для назначения IP Address для L3 интерфейса, как показано на рисунке ниже.



- **Interface**
  Опции: все созданные интерфейсы VLAN уровня 3.
  По умолчанию: VLAN1.
- **IP Mode**
  Опции: bootp-client / dhcp-client / Specify IP
  По умолчанию: Specify IP
  Функция: Выберите режим получения IP-адреса.
  Описание: Указать IP-адрес — настроить IP-адрес вручную; bootp-client / dhcp-client заключается в том, что коммутатор автоматически получает IP-адрес через DHCP / BOOTP. В сети должен быть сервер DHCP / BOOTP для назначения IP-адресов клиентам.

Ручная настройка IP address.

Щелкнуть [Device Basic Configuration] → [L3 interface configuration] → [Allocate IP address for L3 port]] для ручного назначения IP Address для L3 интерфейса, как показано на рисунке ниже.



- **IP Address**
  Формат конфигурации: A.B.C.D.
  Функция: Настройте IP-адрес для указанного интерфейса VLAN уровня 3.
- **Subnet 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. Обычно он настроен как 255.255.255.0.
- **Status**
  Опции: no shutdown / shutdown
  По умолчанию: no shutdown
  Функция: настройка состояния интерфейса VLAN уровня 3.
  Описание: без выключения: открывает интерфейс VLAN уровня 3. Завершение работы: закрывает интерфейс VLAN уровня 3.
- **Type**
  Опции: secondary / primary
  По умолчанию: primary
  Функция: В 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. Как правило, 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.

Нажмите <Add>, чтобы настроить IP-адрес для интерфейса VLAN; нажмите <Del>, чтобы удалить текущий IP-адрес, вы должны сначала удалить дополнительный IP-адрес, прежде чем удалять основной IP-адрес; нажмите <Update>, чтобы изменить основной IP-адрес интерфейса VLAN.

Каждый интерфейс VLAN уровня 3 поддерживает максимум 32 IP-адреса.
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

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

SNMP принимает 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 сетевого управления сетью SNMP.
- Агент — это процесс в управляемых сетевых устройствах. Он получает и обрабатывает пакеты запросов от NMS. Когда возникает тревога, агент заблаговременно сообщает об этом в NMS.

NMS является менеджером сети SNMP, а агент — управляемым устройством сети SNMP. NMS и агенты обмениваются пакетами управления через SNMP. SNMP включает в себя следующие основные операции:

- Get-Request
- Get-Response
- Get-Next-Request
- Set-Request
- Trap

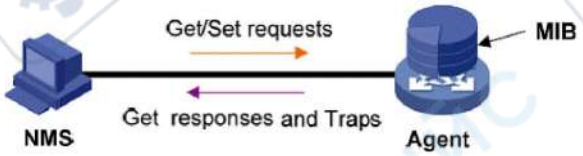
NMS отправляет пакеты Get-Request, Get-Next-Request и Set-Request агентам для запроса, настройки и управления переменными. После получения этих запросов агенты отвечают пакетами Get-Response. Когда возникает тревога, агент заранее сообщает об этом в NMS с помощью пакета ловушки.

Коммутаторы этой серии поддерживают SNMPv2 и SNMPv3. SNMPv2 совместим с SNMPv1. SNMPv1 использует community name для аутентификации. Community name действует как пароль, ограничивая доступ NMS к агентам. Если community name, переносимое пакетом SNMP, не подтверждается коммутатором, запрос завершается неудачно и возвращается сообщение об ошибке. SNMPv2 также использует community name для аутентификации. Он совместим с SNMPv1 и расширяет функции SNMPv1. Чтобы

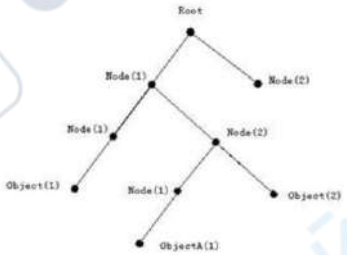
обеспечить связь между NMS и агентом, их версии SNMP должны совпадать. На агенте можно настроить разные версии SNMP, чтобы он мог использовать разные версии для связи с разными NMS.

6.3.1. MIB

Любой управляемый ресурс называется управляемым объектом. База управляющей информации (Management Information Base - MIB) хранит управляемые объекты. Он 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 ниже показаны взаимосвязи между NMS, агентом и MIB.



MIB определяет древовидную структуру. Узлы дерева являются управляемыми объектами. Каждый узел имеет уникальный идентификатор объекта (OID), указывающий расположение узла в структуре MIB. Как показано на рисунке ниже, OID объекта A равен 1.2.1.1.



6.3.2. Веб конфигурирование

Конфигурирование SNMPv2.

Щелкнуть [Device Basic Configuration] → [SNMP Configuration] → [SNMP Base Configuration] для конфигурирования SNMPv2, как показано на рисунке ниже.

- **Snmp Agent state**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включить / отключить SNMP.
- **V1/V2C/V3 state**
  Опции: Enable / Disable
  Функция: выберите версию SNMP.
- **Request Port**
  Диапазон: 1~65535
  По умолчанию: 161
  Функция: Настройка номера порта для приема SNMP-запросов.
- **Community**
  Диапазон: 4~16 символов
  Функция: Настройка сообщества коммутаторов.
  Описание: пакет может получить доступ к MIB коммутатора только в том случае, если имя сообщества, передаваемое в пакете SNMP, совпадает с этой строкой сообщества.
  Объяснение: Можно задать не более 5 строк сообщества.
- **Access Permission**
  Варианты: Read Only / Read And Write
  По умолчанию: Read Only
  Функция: Настройка режима доступа к MIB.
  Описание: Read Only: считывает только информацию MIB. Read And Write: чтение и запись информации MIB.

Настройка безопасных IP-адресов.

Щелкнуть [Device Basic Configuration] → [SNMP Configuration] → [IP Address of SNMP Manager] для конфигурирования безопасных IP-адресов, как показано на рисунке ниже.

- **Security IP Check**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включить или отключить проверку безопасности 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, вам необходимо установить IP-адрес безопасности, и только NMS с IP-адресом безопасности может получить доступ к информации MIB коммутатора.
- **IP Address**
  Формат: A.B.C.D.
  Функция: настроить безопасный IP-адрес NMS.
  Описание: Только NMS, чей IP-адрес соответствует IP-адресу безопасности, может получить доступ к информации MIB коммутатора. Коммутатор позволяет использовать максимум 6 IP-адресов безопасности NMS.

Конфигурирование trap.

Щелкнуть [Device Basic Configuration] → [SNMP Configuration] → [TRAP Configuration] для конфигурирования trap, как показано на рисунке ниже.

- **TRAP State**
  Опции: Open / Close
  По умолчанию: Close
  Функция: разрешить переключателю отправлять сообщение Trap или нет.
- **TRAP Port**
  Опции: 1~65535
  По умолчанию: 162
  Функция: Настройка номера порта для отправки сообщений-ловушек.
- **Version**
  Опция: V1 / V2C / V3
  Функция: V1 / V2C указывает, что коммутатор отправляет сообщения-ловушки версии 1 / версии 2C на сервер. V3 указывает, что коммутатор отправляет на сервер сообщения-ловушки версии 3. Если вы выберете V1 / V2C, необходимо настроить только IP-адрес назначения.
- **Destination IP Address**
  Формат: A.B.C.D.
  Функция: Настройка адреса сервера для получения сообщений-ловушек. Вы можете настроить максимум 8 серверов, то есть 8 записей-ловушек.

Просмотр SNMP статистики.

Щелкнуть [Device Basic Configuration] → [SNMP Configuration] → [SNMP Statistics] для просмотра SNMP, как показано на рисунке ниже.

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

6.4. SNMPv3

SNMPv3 обеспечивает механизм аутентификации модели безопасности на основе пользователей (User-Based Security Model - USM). Вы можете 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.

SNMPv3 предоставляет пять таблиц конфигурации. Каждая таблица может содержать 16 записей. Эти таблицы определяют, могут ли определенные пользователи получать доступ к информации MIB.

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

Групповая таблица — 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 представления относится к информации представления MIB, которая определяет информацию MIB, к которой могут обращаться пользователи. Представление MIB может содержать все узлы определенного поддерева MIB (т. е. пользователям разрешен доступ ко всем узлам поддерева MIB) или не содержать ни одного из узлов определенного поддерева MIB (т. е. узел поддерева MIB).

Вы можете определить права доступа MIB в таблице доступа по имени группы, имени контекста, модели безопасности и уровню безопасности.

6.4.1. Веб конфигурирование

Настройка таблицы пользователей.

Щелкнуть [Device Basic Configuration] → [SNMP Configuration] → [V3 User Table] для конфигурации пользователей для V3, как показано на рисунке ниже.

- **User Name**
  Диапазон: 4~16 символов
  Функция: Создать имя пользователя.
- **Authentication protocol**
  Опции: NONE / HMAC-MD5 / HMAC-SHA
  По умолчанию: NONE
  Функция: выбор алгоритма аутентификации.
- **Authentication password**
  Диапазон: 4~16 символов
  Функция: Создать пароль аутентификации.
- **Privacy protocol**
  Опции: NONE / CBC-DES
  По умолчанию: NONE
  Функция: выберите протокол шифрования пакетов.
- **Privacy password**
  Диапазон: 4~16 символов
  Функция: создание пароля для шифрования пакетов.

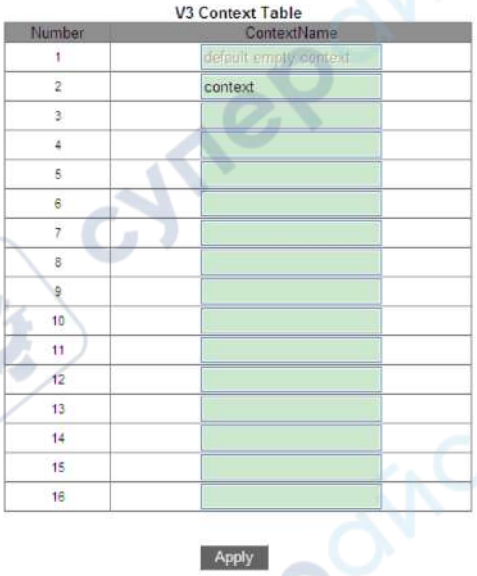
Настроить групповую таблицу.

Щелкнуть [Device Basic Configuration] → [SNMP Configuration] → [V3 Group Table] для конфигурации групп для V3, как показано на рисунке ниже.

- **Group Name**
  Диапазон: 4~16 символов
  Функция: Настройка имени групповой таблицы.
- **Security Name**
  Диапазон: все существующие имена пользователей, 4~16 символов.
  Функция: Настройка имени безопасности. Имя безопасности должно совпадать с именем пользователя в пользовательской таблице. Пользователи с одинаковым именем группы принадлежат к одной группе.
- **Security Model**
  По умолчанию: SNMPv3
  Описание: SNMPv3 указывает, что принята модель безопасности на основе пользователей (USM). В настоящее время значение должно быть SNMPv3.

Настройка контекстной таблицы.

Щелкнуть [Device Basic Configuration] → [SNMP Configuration] → [V3 Context Table] для конфигурации контекстной таблицы для V3, как показано на рисунке ниже.



- **Context Name**
  Диапазон: 4~16 символов
  Функция: настроить имя контекста.
  Описание: Имя первого контекста должно быть пустым.

Настройка таблицы просмотра.

Щелкнуть [Device Basic Configuration] → [SNMP Configuration] → [V3 View Table] для конфигурации таблицы просмотра для V3, как показано на рисунке ниже.

- **View Name**
  Диапазон: 4~16 символов
  Функция: Настройка имени представления.
- **Type**
  Опции: 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: MIB-дерево, обозначенное OID корневого узла дерева.
- **Mask**
  Функция: Маска дерева MIB. Oid-дерево и маска вместе определяют информацию об узле MIB текущего представления. Например, на рисунке имя представления «view1» может иметь 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.

Конфигурирование таблицы доступа.

Щелкнуть [Device Basic Configuration] → [SNMP Configuration] → [V3 Access Table] для конфигурации таблицы доступа для V3, как показано на рисунке ниже.

- **Group Name**
  Диапазон: все существующие имена групп, 4~16 символов
  Функция: Пользователи в группе имеют одинаковые права доступа.
- **Context Prefix**
  Диапазон: все существующие имена контекстов, 4~16 символов
  Функция: настроить имя 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**
  Опции: exact / prefix
  По умолчанию: exact

Функция: выберите режим соответствия имени контекста. Exact указывает, что значение префикса контекста должно совпадать с именем контекста. Префикс 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 версии 3.
  Описание: SNMPv3 указывает, что принята модель безопасности на основе пользователей (USM). В настоящее время значение должно быть SNMPv3.
- **Security Level**
  Опции: NoAuthNoPriv / AuthNoPriv / AuthPriv
  По умолчанию: NoAuthNoPriv
  Функция: Выберите права доступа к информации MIB.
  Описание: NoAuthNoPriv указывает, что не требуется ни аутентификация, ни шифрование пакетов. AuthNoPriv указывает, что требуется аутентификация, но не шифрование пакетов. AuthPriv указывает, что требуется как аутентификация, так и шифрование пакетов. 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**
  Опции: все существующие имена видов
  Функция: Выберите имя представления только для чтения
- **write View**
  Опции: все существующие имена видов
  Функция: Выберите имя представления записи.
- **notify View**
  Опции: все существующие имена видов
  Функция: Выберите имя представления, которое может отправлять сообщение-ловушку.

Настройка безопасных IP-адресов.

Щелкнуть [Device Basic Configuration] → [SNMP Configuration] → [IP Address of SNMP Manager] для конфигурации безопасных IP-адресов, как показано на рисунке ниже.

- **Security IP Check**
  Опция: Enable / Disable
  По умолчанию: Disable
  Функция: включить или отключить проверку безопасности 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, вам

необходимо установить IP-адрес безопасности, и только NMS с IP-адресом безопасности может получить доступ к информации MIB коммутатора.

- **IP Address**
  Формат: A.B.C.D.
  Функция: настроить безопасный IP-адрес NMS.
  Описание: Только NMS, чей IP-адрес соответствует IP-адресу безопасности, может получить доступ к информации MIB коммутатора. Коммутатор позволяет использовать максимум 6 IP-адресов безопасности NMS.

Конфигурирование trap.

Щелкнуть [Device Basic Configuration] → [SNMP Configuration] → [TRAP Configuration] для конфигурации trap, как показано на рисунке ниже.

- **TRAP State**
  Опции: Open / Close
  По умолчанию: Close
  Функция: Разрешить переключателю отправлять сообщение Trap или нет.
- **TRAP Port**
  Опции: 1~65535
  По умолчанию: 162
  Функция: Настройка номера порта для отправки сообщений-ловушек.
- **Version**
  Опция: V1 / V2C / V3
  Функция: V1 / V2C указывает, что коммутатор отправляет сообщения-ловушки версии 1 / версии 2C на сервер. V3 указывает, что коммутатор отправляет на сервер сообщения-ловушки версии 3.
- **Destination IP Address**
  Формат: A.B.C.D.
  Функция: Настройка адреса сервера для получения сообщений-ловушек. Вы можете настроить максимум 8 серверов, то есть 8 записей-ловушек.
- **{Security Level, Security Name, Context Name}**
  Опции: {NoAuthNoPriv / AuthNoPriv / AuthPriv, 4~16 символов, 4~16 символов}
  Функция: Эти три параметра необходимо настраивать только при выборе V3. Эти конфигурации должны соответствовать конфигурациям в таблице доступа. Уровень безопасности может быть равен или выше, чем в таблице доступа. Например, когда право доступа пользователя 1111 установлено на AuthNoPriv, коммутатор может отправлять ловушки на сервер только в том случае, если уровень безопасности имени безопасности 1111 — AuthNoPriv или AuthPriv. Имя контекста должно совпадать с префиксом контекста в таблице доступа.

6.5. ST-ring

ST-Ring и ST-Ring+ — это проприетарные протоколы резервирования ООО «СТЭЗ». Время восстановления сети в течение 20 - 50 мс при сбое канала, обеспечивая стабильную и надежную связь.

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

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

ST-Ring-Port и ST-Ring-VLAN не могут использоваться одновременно.

- Мастер: У одного кольца есть только один мастер. Мастер отправляет пакеты протокола ST-Ring и определяет состояние кольца. Когда кольцо закрыто, два кольцевых порта на ведущем устройстве находятся в состоянии пересылки и блокировки соответственно.

Первый порт, статус связи которого меняется на ир при закрытии кольца, находится в состоянии пересылки. Другой кольцевой порт находится в состоянии блокировки.

- Ведомый: Кольцо может включать в себя несколько ведомых устройств. Подчиненные устройства прослушивают и пересылают пакеты протокола ST-Ring и сообщают информацию об ошибках ведущему устройству.
- Резервный порт: Порт для связи между кольцами ST называется резервным портом.
- Основной резервный порт: если кольцо имеет несколько резервных портов, резервный порт с большим MAC-адресом является основным резервным портом. Он находится в состоянии пересылки.
- Подчиненный резервный порт: если в кольце имеется несколько резервных портов, все резервные порты, кроме основного резервного порта, являются подчиненными резервными портами. Они находятся в состоянии блокировки.
- Состояние пересылки: если порт находится в состоянии пересылки, порт может как получать, так и отправлять данные.
- Состояние блокировки: если порт находится в состоянии блокировки, порт может получать и пересылать только пакеты протокола ST-Ring, но не другие пакеты.

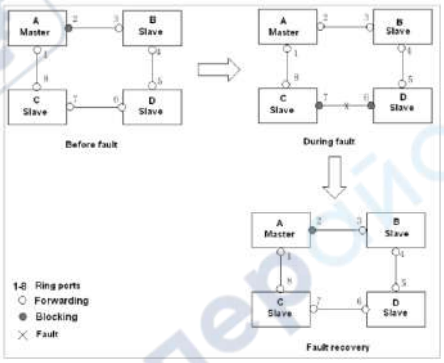
6.5.1. Реализация ST-Ring-Port

Порт пересылки на ведущем устройстве периодически отправляет пакеты протокола ST-Ring для определения состояния кольца. Если блокирующий порт мастера получает пакеты, кольцо замыкается; в противном случае кольцо разомкнуто.

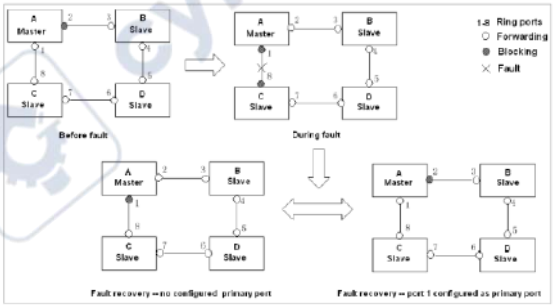
Рабочий процесс коммутатора A, коммутатора B, коммутатора C и коммутатора D:

- Настройте коммутатор A как ведущий, а остальные коммутаторы — как ведомые.

- Кольцевой порт 1 на ведущем устройстве находится в состоянии пересылки, а кольцевой порт 2 — в состоянии блокировки. Оба порта подчиненного устройства находятся в состоянии пересылки.
- Если линк CD неисправен, как показано на следующем рисунке:
  - Когда канал связи CD неисправен, порты 6 и 7 подчиненного устройства находятся в состоянии блокировки. Порт 2 на ведущем устройстве переходит в состояние пересылки, обеспечивая нормальную связь по каналу.
  - Когда неисправность устранена, порты 6 и 7 подчиненного устройства находятся в состоянии пересылки. Порт 2 на ведущем устройстве переходит в состояние блокировки. Происходит переключение каналов, и каналы восстанавливаются до состояния, предшествующего отказу CD.



- Если канал AC неисправен, как показано на следующем рисунке:
  - Когда канал AC неисправен, порт 1 находится в состоянии блокировки, а порт 2 переходит в состояние пересылки, обеспечивая нормальную связь по каналу.
  - После устранения неисправности,
    - Если на ведущем устройстве A не настроен основной порт, порт 1 все еще находится в состоянии блокировки, а порт 8 — в состоянии пересылки. Переключения не происходит.
    - Если порт 1 на мастере A настроен как основной порт. Когда кольцо замкнуто, основной порт должен находиться в состоянии пересылки. Поэтому порт 1 переходит в состояние пересылки. Порт 8 находится в состоянии пересылки, а порт 2 — в состоянии блокировки. Происходит переключение каналов.



Изменение статуса канала влияет на статус портов кольца

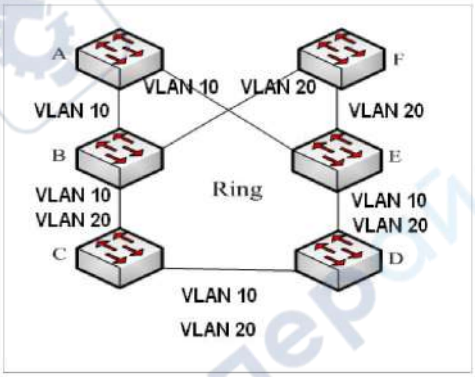
6.5.2. ST-RING-VLAN реализация

ST-Ring-VLAN позволяет пересылать пакеты из разных VLAN по разным путям. Каждый путь пересылки для VLAN образует ST-Ring-VLAN. У разных колец ST-VLAN-Ring могут быть разные мастера. Как показано на следующем рисунке, настроены две ST-Ring-VLAN.

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

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

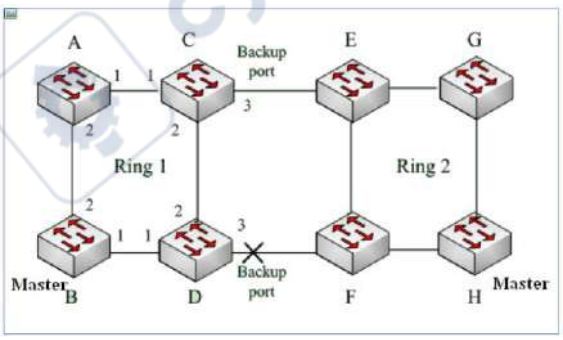
Два кольца касаются звеньев BC, CD и DE. Коммутатор C и коммутатор D используют одни и те же порты в двух кольцах, но используют разные логические каналы на основе VLAN.



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

6.5.3. ST-RING+ реализация

ST-Ring+ может обеспечить резервирование двух колец ST, как показано на следующем рисунке. Один резервный порт настроен соответственно на коммутаторе C и коммутаторе D. Какой порт является основным резервным портом, зависит от MAC-адресов двух портов. Если главный резервный порт или его канал выходят из строя, подчиненный резервный порт будет пересылать пакеты, предотвращая образование петель и обеспечивая нормальную связь между резервными кольцами.



Изменение статуса канала влияет на статус резервных портов.

Конфигурации ST-Ring должны соответствовать следующим условиям:

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

6.5.3.1. Веб конфигурирование

Конфигурирование кольцевой топологии.

Щелкнуть [Device Basic Configuration] → [ST-Ring Configuration] → [ST-Ring Mode] для конфигурации кольцевой топологии, как показано на рисунке ниже.

- **Redundancy Mode Set**
  Опции: ST-PORT / ST-VLAN
  По умолчанию: ST-PORT
  Функция: следует ли включить протокол ST-Ring и выбрать режим резервного звонка.

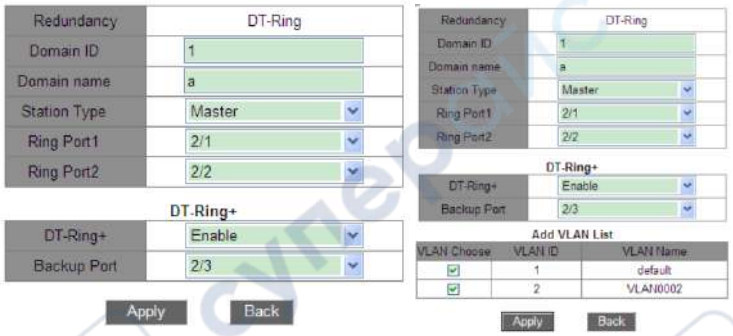
Кольцевые протоколы на основе портов включают RSTP, ST-Ring-Port и DRP-Port, а кольцевые протоколы на основе VLAN включают MSTP, ST-Ring-VLAN и DRP-VLAN. Кольцевые протоколы на основе VLAN являются взаимоисключающими, и для одного устройства можно настроить только тип кольцевого протокола на основе VLAN. Кольцевой протокол на основе портов и кольцевой протокол на основе VLAN являются взаимоисключающими, и для одного устройства можно выбрать только один режим кольцевого протокола.

Создание ST-ring.

Щелкнуть [Device Basic Configuration] → [ST-Ring Configuration] → [ST-Ring Configuration] для конфигурации ST-Ring, как показано на рисунке ниже.

Нажмите <Add>, чтобы создать ST-Ring.

Конфигурирование ST-ring и ST-VLAN-Ring, как показано на рисунке ниже.



- **Redundancy**
  Принудительная настройка: ST-Ring
- **Domain ID**
  Диапазон конфигурации: 1~32
  Функция: Идентификатор домена используется для различения различных колец. Один коммутатор поддерживает максимум 16 колец на основе портов или 8 колец на основе VLAN.
- **Domain name**
  Диапазон: 1~31 символ
  Функция: настроить доменное имя.
  Station Type
  Варианты: Master / Slave
  По умолчанию: Master
  Функция: выберите роль коммутатора в кольце.
- **Ring port 1/Ring port 2**
  Опции: все порты коммутатора
  Функция: выберите два кольцевых порта.

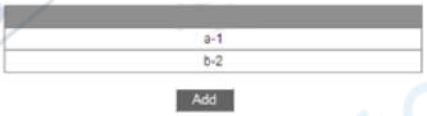
Кольцевой порт ST-Ring или резервный порт и канал порта являются взаимоисключающими. Кольцевой порт ST-Ring или резервный порт нельзя добавить к каналу порта; порт в канале порта не может быть настроен в качестве кольцевого порта ST-Ring или резервного порта.

Кольцевой порт ST-Ring или резервный порт и порт для зеркалирования являются взаимоисключающими. Кольцевой порт ST-Ring или резервный порт нельзя настроить в качестве зеркального порта назначения; порт назначения зеркалирования не может быть настроен в качестве кольцевого порта ST-Ring или резервного порта.

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

Не рекомендуется, чтобы порты в группе isolate настраивались одновременно как порты ST-Ring и резервные порты, а порты ST-Ring и резервные порты не могут быть добавлены в группу isolate.

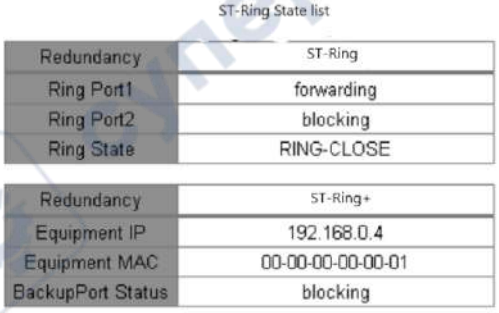
- **ST-RING+**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: Включить / выключить ST-Ring+.
- **Backup port**
  Опции: все порты коммутатора
  Функция: Установите порт в качестве резервного порта.
  Объяснение: Включите ST-Ring+ перед настройкой резервного порта.
- **Add VLAN list**
  Опции: все созданные VLAN
  Функция: выберите VLAN для кольцевого порта.
  После завершения настройки в списке ST-Ring List отображаются все созданные кольца, как показано на рисунке ниже.



Просмотр и изменение конфигурации ST-Ring.

Нажмите <Apply>, чтобы изменения вступили в силу после внесения изменений. Нажмите <Delete>, чтобы удалить запись конфигурации ST-Ring.

Просмотр ST-Ring и статус порта.



6.6. STP / RSTP

Стандартизированный в IEEE802.1D протокол связующего дерева (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 должен ждать в два раза больше задержки пересылки, чтобы перейти в состояние пересылки.

Чтобы преодолеть этот недостаток, IEEE создал стандарт 802.1w в дополнение к 802.1D. IEEE802.1w определяет протокол быстрого связующего дерева (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. Если корневой порт недействителен, альтернативный порт может быстро войти в состояние пересылки.

- Root bridge: служит root для сети. Сеть имеет только один root bridge. Root bridge меняется в зависимости от топологии сети. Root bridge периодически отправляет BPDU другим устройствам, которые пересылают BPDU для обеспечения стабильности топологии.
- Root bridge: указывает наилучший порт для передачи от некорневых мостов к корневому мосту. Лучший порт — это порт с наименьшей стоимостью для корневого моста. Non-root bridge взаимодействует с root bridge через root port. Non-root bridge имеет только один root port. Root bridge не имеет root port.
- Designated port: указывает порт для пересылки BPDU на другие устройства или локальные сети. Все порты root bridge являются designated port.
- Alternate port: указывает резервный порт root port. Если root port выходит из строя, alternate port становится новым root port.
- Backup port: указывает backup port назначенного порта. Когда designated port выходит из строя, backup port становится новым designated port и пересылает данные.

6.6.1. 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 ниже показана структура данных BPDU.

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

- Root bridge: приоритет корневого моста (2 байта) + MAC-адрес корневого моста (6 байт).
- Root path: стоимость пути к корневому мосту.
- Designation bridge ID: приоритет назначенного моста (2 байта) + MAC-адрес назначенного моста (6 байт).
- Designation port ID: приоритет порта + номер порта.
- Message age: время, в течение которого BPDU может распространяться по сети.
- Max age: максимальная продолжительность хранения BPDU на устройстве. Когда возраст сообщения превышает максимальный возраст, BPDU отбрасывается.

- Hello time: интервал для отправки BPDU.
- Forward delay: задержка изменения статуса (отбрасывание-обучение-пересылка).

Процесс для всех мостов, вычисляющий связующее дерево с помощью BPDU, выглядит следующим образом:

- Начальная фаза - каждый порт всех устройств генерирует BPDU с самим собой в качестве root bridge; оба root bridge ID и designated bridge ID являются идентификатором локального устройства; стоимость корневого пути равна 0; designated port является локальным портом.
- 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, назначенные идентификаторы моста, назначенные идентификаторы портов 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.
- Выбор root bridge - root bridge связующего дерева является мост с наименьшим идентификатором моста.
- Выбор root port - устройство без корневого моста выбирает порт, получающий лучший BPDU, в качестве корневого порта.
- Расчет BPDU designated port - на основе BPDU корневого порта и стоимости пути корневого порта устройство вычисляет BPDU designated port для каждого порта следующим образом:
    - Замените идентификатор корневого моста идентификатором корневого моста BPDU корневой порт.
    - Замените стоимость корневого пути на стоимость корневого пути BPDU корневого порта плюс стоимость пути корневого порта.
    - Замените назначенный идентификатор моста идентификатором локального устройства.
    - Замените назначенный идентификатор порта идентификатором локального порта.
- Выбор designated port - 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.

6.6.2. Веб конфигурирование

Включение RSTP.

Щелкнуть [Device Basic Configuration] → [RSTP configuration] → [RSTP configuration] для конфигурации RSTP, как показано на рисунке ниже.

- **Protocol Status**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: выключение или включение RSTP, или STP.

Кольцевые протоколы на основе портов включают RSTP, ST-Ring-Port и DRP-Port, а кольцевые протоколы на основе VLAN включают MSTP, ST-Ring-VLAN и DRP-VLAN. Кольцевой протокол на основе портов и кольцевой протокол на основе VLAN являются взаимоисключающими, и для одного устройства можно выбрать только один режим кольцевого протокола.

Установка временных параметров сетевого моста, как показано на рисунке ниже.

- **Bridge Priority**
  Диапазон: 0~65535. Шаг 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 отправки BPDU.
- **Max age time**
  Диапазон: 6~40 с
  По умолчанию: 20 с
  Описание: Если значение возраста сообщения в BPDU превышает указанное значение, то BPDU отбрасывается.
- **Forward Delay Time**
  Диапазон: 4~30 с
  По умолчанию: 15 с

Функция: настройка времени изменения статуса с «Discarding» на «Learning» или с «Learning» на «Forwarding».

- **Message-age Increment**
  Варианты: Compulsion / Default
  По умолчанию: Default
  Функция: Настройте значение, которое будет добавляться к возрасту сообщения, когда BPDU проходит через сетевой мост.
  Описание: В принудительном режиме значение равно 1.
  В режиме по умолчанию значение равно max (max age time / 16, 1).
  Forward Delay Time, Max Age Time и Hello Time должны соответствовать следующим требованиям: 2 x (Forward Delay Time — 1,0 секунды) ≥ Max Age Time;
  Max Age Time ≥ 2 x (Hello Time + 1,0 секунды).

Включение RSTP на портах, показана на рисунке ниже.

- **Protocol Status**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: Включение / выключение STP / RSTP на портах

Порт RSTP и channel порт являются взаимоисключающими. Порт RSTP нельзя добавить в channel порт; порт в channel порт не может быть настроен как порт RSTP.
Порт RSTP и порт назначения 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, ST-Ring-Port и DRP-Port являются взаимоисключающими, то есть порт RSTP нельзя настроить как кольцевой порт DRP-Port / ST-Ring-Port или DRP-Port / ST-Ring-Port резервный порт; Кольцевой порт DRP-Port / ST-Ring-Port и резервный порт DRP-Port / ST-Ring-Port нельзя настроить как порт RSTP.
Не рекомендуется одновременно настраивать порты в группе isolate как порты RSTP, а порты RSTP нельзя добавлять в группу isolate.

- **Port Priority**
  Диапазон: 0~255. Шаг 16.
  По умолчанию: 128
  Функция: Настройка приоритета порта, который определяет роли портов.
- **Path Cost**
  Диапазон: 1~200000000

По умолчанию: 2000000 (порт 10M), 200000 (порт 100M), 20000 (порт 1000M)
Описание: Стоимость пути порта используется для расчета наилучшего пути. Значение параметра зависит от пропускной способности. Чем больше значение, тем ниже стоимость. Вы можете изменить роль порта, изменив значение параметра стоимости пути. Чтобы настроить значение вручную, выберите No для счетчика затрат.

- **Auto Cost Count**
  Диапазон: Yes / No
  По умолчанию: Yes
  Описание: Yes указывает, что стоимость пути порта принимает значение по умолчанию. No означает, что вы можете настроить стоимость пути.

Просмотр RSTP статуса, показана на рисунке ниже.

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

6.7. DRP

ООО «СТЭЗ» использует в коммутаторах протокол распределенного резервирования (Distributed Redundancy Protocol - 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 мастера без фиксированного мастера. DRP предоставляет следующие возможности:

- 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 прерывания отчетов 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.

- Разнообразные функции обнаружения ссылок.
  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 надлежащую передачу данных.

- Применимо 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 несколько экземпляров 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.

DRP mode.

DRP включает 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 сети VLAN. Таким образом, на портах касательного кольца можно настроить несколько VLAN. Порт может принадлежать разным кольцам DRP в соответствии с конфигурациями VLAN.

Статусы портов DRP.

Forwarding state: если порт находится в состоянии пересылки, он может получать и пересылать пакеты данных.
Blocking state: если порт находится в состоянии блокировки, он может получать и пересылать пакеты DRP, но не другие пакеты данных.
Primary port: указывает кольцевой порт (в корневом каталоге), состояние которого настроено как принудительная переадресация пользователем, когда кольцо закрыто.

Если в корне не настроен первичный порт, первый порт, состояние канала которого меняется на up при закрытии кольца, находится в состоянии пересылки. Другой кольцевой порт находится в состоянии блокировки.
Порт в заблокированном состоянии на корне может активно отправлять пакеты DRP.

DRP Roles.

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

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

ROOT: указывает устройство, на котором включен DRP, и по крайней мере один кольцевой порт находится в состоянии соединения. 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. Статусы 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 соединения, а другой — в состоянии соединения, 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. Статусы портов кольца: Один порт кольца находится в состоянии пересылки.

Normal: указывает устройство, на котором включен DRP, и оба кольцевых порта находятся в состоянии соединения без ухудшения CRC, а приоритет выше 200. Нормальный только пересылает пакеты Announce, но не проверяет содержимое пакетов. Статусы кольцевых портов: Оба кольцевых порта находятся в состоянии пересылки.

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

Каждый коммутатор поддерживает свой собственный вектор пакета Announce. Коммутатор с большим вектором будет выбран корневым.

Вектор пакета Announce содержит следующую информацию для назначения роли.

Link status	CRC degradation		Role priority	IP address of the device	MAC address of the device
	CRC degradation status	CRC degradation rate			

Link status: 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.

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

Скорость деградации CRC: отношение количества пакетов CRC к порогу за 15 минут.

Role priority: значение можно установить в веб-интерфейсе.

Параметры в Таблице Вектор пакета оповещения сравниваются в следующей процедуре:

- Сначала проверяется значение статуса канала. Устройство с большим значением статуса канала считается имеющим больший вектор.

- Если два сравниваемых устройства имеют одинаковое значение состояния канала, сравниваются значения состояния ухудшения CRC. Устройство с большим значением статуса деградации CRC считается имеющим больший вектор.
- Если значение статуса деградации CRC всех сравниваемых устройств равно 1, считается, что устройство с большим значением скорости деградации CRC имеет больший вектор. Если два сравниваемых устройства имеют одинаковое значение состояния канала и значение деградации CRC, значения приоритета ролей, IP-адресов и MAC-адресов сравниваются последовательно. Устройство с большим значением считается имеющим больший вектор.
- Устройство с большим вектором выбирается корневым.

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

Реализация режима DRP-Port-Based.

Роли коммутаторов следующие:

- При запуске все коммутаторы находятся в состоянии INIT. Когда состояние одного порта изменяется на Link up, коммутатор становится корневым и отправляет пакеты Announce другим коммутаторам в кольце для выбора.
- Коммутатор с наибольшим вектором пакета Announce выбирается корневым. Среди других коммутаторов в кольце коммутатор с одним кольцевым портом в состоянии Link down или в состоянии ухудшения CRC является B-Root. Коммутатор с обоими кольцевыми портами в состоянии Link up и отсутствием ухудшения CRC является нормальным.

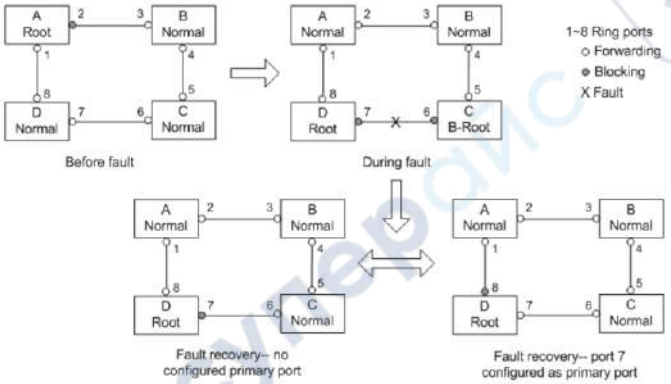
Процедура устранения неисправности следующая:

- В исходной топологии A является корнем; порт 1 находится в состоянии пересылки, а порт 2 в состоянии блокировки. B, C и D являются нормальными, и их кольцевые порты находятся в состоянии пересылки.
- Когда линк CD неисправен, DRP изменяет статусы портов 6 и 7 на блокировку. В результате C и D становятся корнями. Поскольку A, C и D в данный момент являются корневыми, 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 корня, а C становится корнем B. 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 изменяет статус порта 2 на переадресацию.

Когда связь CD восстанавливается, D по-прежнему является корнем, 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 изменяет состояние порта 6 на пересылку. В результате C становится Normal. Поэтому роли коммутаторов не меняются при восстановлении канала.



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.

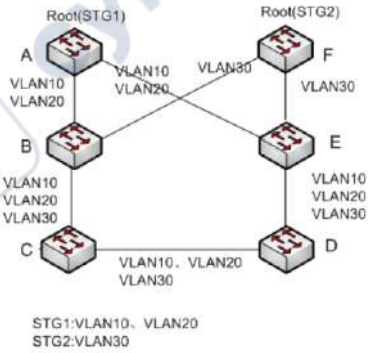
Экземпляр STG: каждый экземпляр STG соответствует одному кольцу на основе DRP-VLAN. С помощью DRP экземпляр STG записывает роли устройств и состояние порта. После получения пакета коммутатор определяет сопоставленный экземпляр STG на основе атрибута VLAN пакета. Коммутатор обрабатывает пакет в соответствии с ролями устройства и статусом порта экземпляра.

При настройке кольца на основе DRP-VLAN пакеты из разных VLAN могут пересылаться по разным путям. Как показано на рисунке ниже, сопоставление экземпляров STG и VLAN одинаково для всех устройств.

Кольцевая ссылка на базе STG1: AB-BC-CD-DE-EA. Пакеты VLAN10 и VLAN20 пересылаются по каналу. A — root.

Кольцевая ссылка на базе STG2: FB-BC-CD-DE-EF. Пакеты VLAN30 пересылаются по каналу. F — root.

Два кольца касаются звеньев 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.



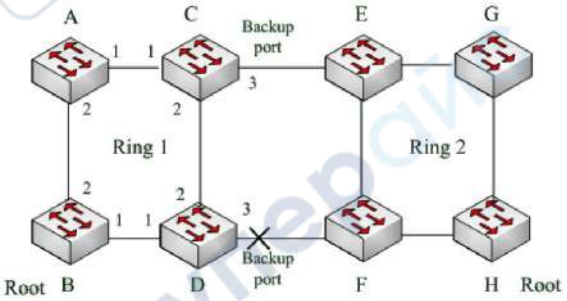
Состояние порта и назначение ролей для каждого кольца на основе DRP-VLAN такие же, как и для кольца на основе порта DRP.

DRP Backup

DRP также может обеспечивать резервирование двух колец DRP, предотвращая образование петель и обеспечивая нормальную связь между кольцами.

Backup port: указывает порт связи между кольцами DRP. Можно настроить несколько резервных портов, но они должны находиться в одном кольце. Первый резервный порт, который подключается, является основным резервным портом, который находится в состоянии пересылки. Все остальные резервные порты являются подчиненными. Они находятся в состоянии блокировки.

Как показано на следующем рисунке, на каждом коммутаторе можно настроить один резервный порт. Главный резервный порт находится в состоянии пересылки, а другие резервные порты — в состоянии блокировки. Если главный резервный порт или его канал неисправен, для пересылки данных будет выбран подчиненный резервный порт.

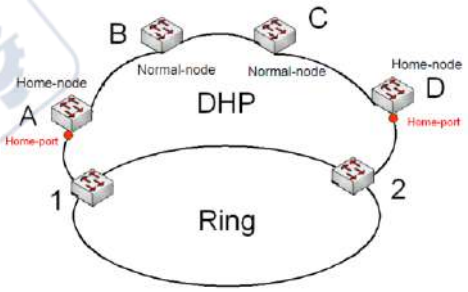


Изменение статуса канала влияет на статус резервных портов.

6.8. DHP

Как показано на следующем рисунке, A, B, C и D смонтированы на кольце. Протокол двойного подключения (DHP) реализует 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.

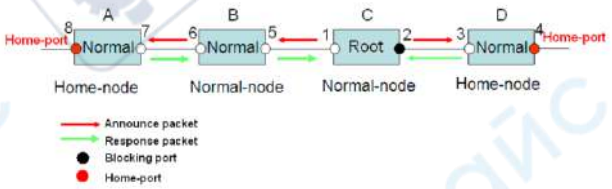


Реализация DHP основана на DRP. Механизм выбора и назначения ролей в DHP такой же, как и в DRP. DHP обеспечивает резервное копирование канала посредством конфигурации Home-node, Normal-node и Home-port.

Home-node: указывает устройства на обоих концах канала DHP и завершает пакеты DRP. Home-node: указывает порт, соединяющий домашний узел с внешней сетью. Домашний порт обеспечивает следующие функции:

- Отправка ответных пакетов в корневой узел после получения пакетов оповещения из корневого узла. Корень идентифицирует состояние кольца как закрытое, если он получает ответные пакеты. Если корень не получает ответные пакеты, он идентифицирует состояние кольца как открытое.
- 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.

Normal-node: указывает устройства в канале DHP, исключая устройства на обоих концах. Normal-node передают ответные пакеты домашних узлов.

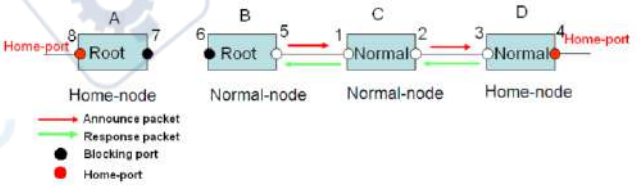


Как показано на предыдущем рисунке, конфигурации A, B, C и D на рисунке следующие:

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

Реализация:

- C, Root, отправляет пакеты Announce через два своих кольцевых порта. Домашний порт 8 и домашний порт 4 завершают полученные пакеты Announce и отправляют ответные пакеты на C. C идентифицирует состояние кольца как закрытое. Порт 2 находится в состоянии блокировки.
- Когда канал между A и B заблокирован, топология включает два канала: A и B-C-D. A избирается корнем. Порт 7 находится в состоянии блокировки.
- B ссылке B-C-D B выбран в качестве корня. Порт 6 находится в состоянии блокировки. C становится нормальным. Порт 2 находится в состоянии пересылки. A может связываться с B, C и D через устройство 1 и устройство 2, как показано на следующем рисунке.



6.8.1. Описание

Конфигурации DRP отвечают следующим требованиям:

- Все коммутаторы в одном кольце должны иметь одинаковый номер домена.
- Одно кольцо содержит только один корень, но может содержать несколько корней В или нормалей.
- На каждом коммутаторе можно настроить только два порта для кольца.
- Для двух связанных колец резервные порты можно настроить только в одном кольце.
- В одном кольце можно настроить несколько резервных портов.
- На коммутаторе для одного кольца можно настроить только один резервный порт.

6.8.2. Веб конфигурация

Конфигурирование DRP mode

Щелкнуть [Device Basic Configuration] → [DRP configuration] → [DRP Mode] для конфигурации DRP mode, как показано на рисунке ниже.

- **DRP Mode**
  Опции: Port Based / VLAN Based
  По умолчанию: Port Based
  Функция: Конфигурирование DRP mode

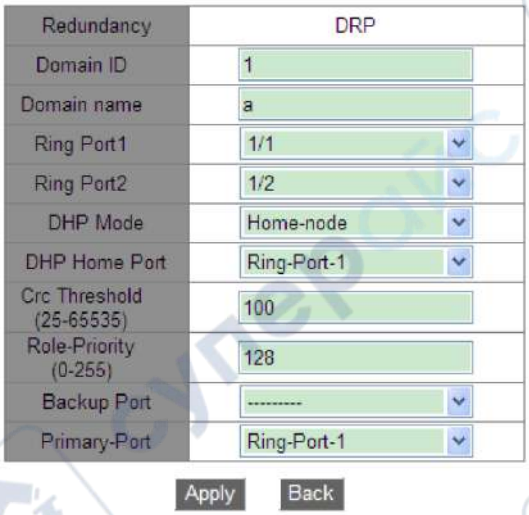
Кольцевые протоколы на основе портов включают RSTP, ST-Ring-Port и DRP-Port, а кольцевые протоколы на основе VLAN включают MSTP, ST-Ring-VLAN и DRP-VLAN.
Кольцевые протоколы на основе VLAN являются взаимоисключающими, и только тип кольцевого протокола на основе VLAN может быть настроен для одного устройства.
Кольцевой протокол на основе порта и кольцевой протокол на основе VLAN являются взаимоисключающими, и только один режим кольцевого протокола может быть выбран для одно устройство.

Создание DRP-Port-Based записи

Щелкнуть [Device Basic Configuration] → [DRP configuration] → [Port-Based DRP Configuration] для входа на страницу создание DRP-Port-Based записи, как показано на рисунке ниже.

Нажмите <Add>, чтобы создать запись DRP.

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

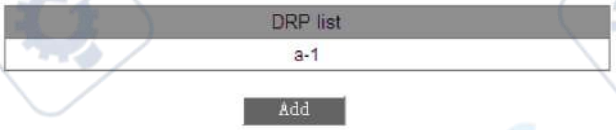


- **Redundancy**
  Обязательная конфигурация: DRP
- **Domain ID**
  Диапазон: 1~32
  Описание: Каждое кольцо имеет уникальный идентификатор домена. На одном коммутаторе можно настроить максимум 16 колец DRP.
- **Domain name**
  Диапазон: 1~31 символ
  Функция: настроить доменное имя.
- **Ring Port 1/Ring Port 2**
  Опции: все порты коммутатора
  Функция: выберите два кольцевых порта.
- **DHP Mode**
  Опции: Disable / Normal-node / Home-node
  По умолчанию: Disable
  Функция: отключить DHP или настроить режим DHP.
- **DHP Home Port**
  Варианты: Ring-Port-1 / Ring-Port-2 / Ring-Port-1-2
  Функция: настроить Home-port для Home-node DHP.
  Описание: Если в канале DHP есть только одно устройство, оба кольцевых порта домашнего узла должны быть настроены как домашние порты.
- **Crc Threshold**
  Диапазон: 25~65535
  По умолчанию: 100
  Функция: настроить пороговое значение CRC.
  Описание: Этот параметр используется при выборе root. Система подсчитывает количество полученных CRC. Если количество CRC одного кольцевого порта превышает пороговое значение, система считает, что порт имеет ухудшение CRC. В результате значение деградации CRC устанавливается равным 1 в векторе пакета Announce порта.
- **Role-Priority**
  Диапазон: 0~255
  По умолчанию: 128
  Функция: Настройка приоритета коммутатора.
- **Backup Port**

Опции: все порты коммутатора
Функция: Настройка резервного порта.

Не настраивайте кольцевой порт в качестве резервного порта.

- **Primary-Port**
  Опции: --/Ring-Port-1 / Ring-Port-2
  По умолчание: --
  Функция: Настройка основного порта. Когда кольцо замкнуто, основной порт root находится в состоянии пересылки.
  После завершения настройки параметров созданная запись будет отображаться в списке DRP, как показано на следующем рисунке.



Кольцевой порт DRP или резервный порт и канал порта являются взаимоисключающими. Кольцевой порт DRP или резервный порт нельзя добавить к каналу порта; порт в канале порта не может быть настроен в качестве кольцевого порта DRP или резервного порта.
Кольцевой или резервный порт DRP и пункт назначения зеркалирования являются взаимоисключающими. Кольцевой порт DRP или резервный порт нельзя настроить в качестве порта назначения зеркалирования; порт назначения зеркального отображения нельзя настроить в качестве кольцевого порта DRP или резервного порта.
Кольцевые порты между кольцевыми протоколами на основе портов RSTP, ST-Ring-Port и DRP-Port являются взаимоисключающими, то есть кольцевой порт и резервный порт DRP-Port не могут быть настроены как порт RSTP, кольцо ST-Ring-Port. порт или резервный порт ST-Ring-Port; Порт RSTP, кольцевой порт ST-Ring-Port и резервный порт ST-Ring-Port нельзя настроить как кольцевой порт DRP-Port или резервный порт.
Не рекомендуется, чтобы порты в группе изоляции настраивались одновременно как порты DRP и резервные порты, а порты DRP и резервные порты не могут быть добавлены в группу изоляции.

Просмотр настроек параметров записи DRP-Port-Based

Щелкнув запись DRP и можно просматривать, и изменять настройки параметров записи, как показано на следующем рисунке.

После завершения изменения нажмите <Apply>, чтобы изменение вступило в силу. Вы можете удалить запись DRP, нажав <Delete>.

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

Ring State List

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

Конфигурирование DRP-VLAN-Based записи

Щелкнуть [Device Basic Configuration] → [DRP configuration] → [DRP Mode] для входа на страницу конфигурации DRP mode. Выберете Vlan Based.

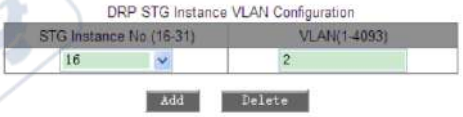
Конфигурация экземпляра DRP

Щелкнуть [Device Basic Configuration] → [DRP configuration] → [VLAN-Based DRP Configuration] → [DRP STG Instance] для входа на страницу конфигурации экземпляра DRP STG, как показано на следующем рисунке.

- **STG Instance No. (16-31)**
  Диапазон: 16 ~ 31
  Функция: Настройка идентификатора экземпляра DRP.

Конфигурация VLAN в экземпляре DRP

Щелкнуть [Device Basic Configuration] → [DRP configuration] → [VLAN-Based DRP Configuration] → [STG Instance Protocol VLAN Configuration] для входа на страницу конфигурации VLAN экземпляра DRP, как показано на следующем рисунке.

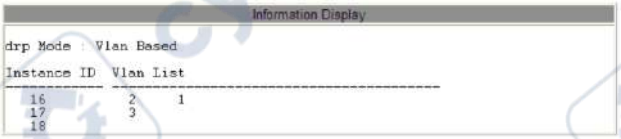


- **DRP STG Instance VLAN Configuration**
  Портфолио: {идентификатор экземпляра STG, идентификатор VLAN}
  Диапазон: {16~31, 1~4093}
  Функция: Настройте идентификатор VLAN для экземпляра DRP.

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

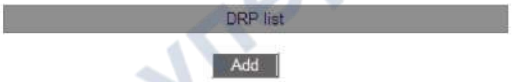
Просмотрите информацию об экземплярах DRP.

Щелкнуть [Device Basic Configuration] → [DRP configuration] → [VLAN-Based DRP Configuration] → [STG Instance Information] для входа на страницу информации об экземпляре DRP, как показано на следующем рисунке.

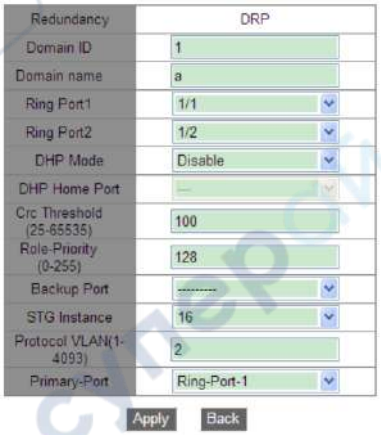


Конфигурация DRP-VLAN-Based.

Щелкнуть [Device Basic Configuration] → [DRP configuration] → [VLAN-Based DRP Configuration] → [Ring Configuration] для входа на страницу создания DRP-VLAN-Based, как показано на следующем рисунке.



Нажмите <Add>, чтобы создать запись DRP. Установите параметры для записи, как показано на следующем рисунке.



- **Redundancy**
  Обязательная настройка: DRP
- **Domain ID**
  Диапазон: 1~32
  Функция: Каждое кольцо имеет уникальный идентификатор домена. На одном коммутаторе можно настроить максимум 8 колец DRP.
- **Domain name**
  Диапазон: 1~31 символ
  Функция: настроить доменное имя.
- **Ring Port 1/Ring Port 2**
  Опции: все порты коммутатора

Функция: выберите два кольцевых порта.

- **DHP Mode**
  Опции: Disable / Normal-node / Home-node
  По умолчанию: Disable
  Функция: отключить DHP или настроить режим DHP.
- **DHP Home Port**
  Варианты: Ring-Port-1 / Ring-Port-2 / Ring-Port-1-2
  Функция: настроить домашний порт для домашнего узла DHP.
  Описание: Если в канале DHP есть только одно устройство, оба кольцевых порта домашнего узла должны быть настроены как домашние порты.
- **Crc Threshold**
  Диапазон: 25~65535
  По умолчанию: 100
  Функция: настроить пороговое значение CRC.
  Описание: Этот параметр используется при выборе root. Система подсчитывает количество полученных CRC. Если количество CRC одного кольцевого порта превышает пороговое значение, система считает, что порт имеет ухудшение CRC. В результате значение деградации CRC устанавливается равным 1 в векторе пакета Announce порта.
- **Role-Priority**
  Диапазон: 0~255
  По умолчанию: 128
  Функция: Настройка приоритета коммутатора.

Кольцевой порт DRP или резервный порт и канал порта являются взаимоисключающими. Кольцевой порт DRP или резервный порт нельзя добавить к каналу порта; порт в канале порта не может быть настроен в качестве кольцевого порта DRP или резервного порта.

Кольцевой или резервный порт DRP и пункт назначения зеркалирования являются взаимоисключающими. Кольцевой порт DRP или резервный порт нельзя настроить в качестве порта назначения зеркалирования; порт назначения зеркального отображения нельзя настроить в качестве кольцевого порта DRP или резервного порта.

Не рекомендуется, чтобы порты в группе изоляции настраивались одновременно как порты DRP и резервные порты, а порты DRP и резервные порты не могут быть добавлены в группу изоляции.

- **Backup Port**
  Опции: все порты коммутатора
  Функция: Конфигурирование резервного порта

Не настраивайте кольцевой порт в качестве резервного порта.

- **STG Instance**
  Опции: созданные экземпляры DRP
  Функция: настроить экземпляр для кольца.
  Описание: блокирующий порт в кольце будет блокировать пакеты данных всех VLAN, соответствующих экземпляру.
- **Protocol VLAN (1~4093)**

Диапазон: 1~4093

Описание: идентификатор VLAN должен быть одним из тех, которые соответствуют экземпляру STG. Функция: пакеты DRP с идентификатором VLAN служат основой для диагностики и обслуживания кольца на основе DRP-VLAN.

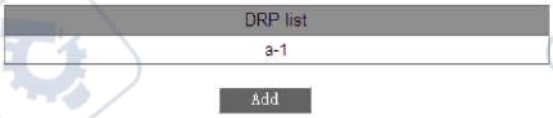
- **Primary-Port**

  Опции: -- / Ring-Port-1 / Ring-Port-2

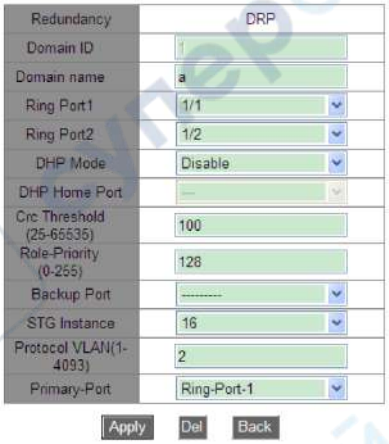
  По умолчанию: --

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

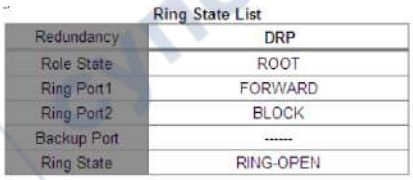
  После завершения настройки созданные кольца отображаются в списке DRP List, как показано на следующем рисунке.



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



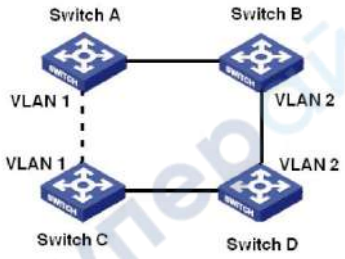
После завершения изменения нажмите <Apply>, чтобы изменение вступило в силу. Вы можете удалить запись DRP, нажав <Delete>. Просмотрите роли и статус порта кольца DRP, как показано на следующем рисунке.



6.9. Конфигурирование MSTP

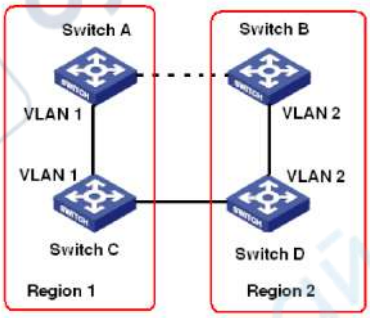
Хотя протокол RSTP обеспечивает быструю конвергенцию, у него, как и у STP, есть следующий недостаток: все мосты в локальной сети совместно используют одно связующее дерево, и пакеты всех VLAN пересылаются по связующему дереву. Как показано на рисунке ниже, некоторые конфигурации могут блокировать соединение 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 связаться с коммутатором C.

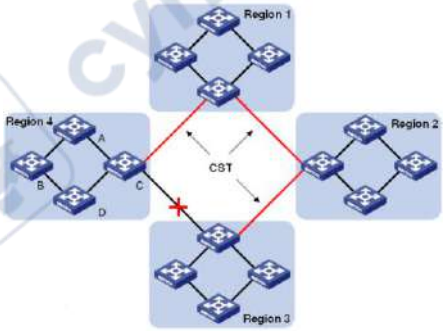


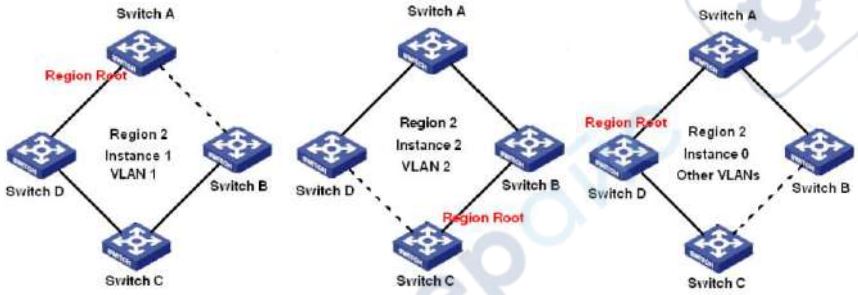
Чтобы решить эту проблему, появился протокол Multiple Spanning Tree Protocol (MSTP). Он обеспечивает как быструю конвергенцию, так и отдельные пути пересылки для трафика разных VLAN, обеспечивая лучший механизм распределения нагрузки для избыточных каналов.

MSTP отображает одну или несколько VLAN в один экземпляр. Коммутаторы с одинаковой конфигурацией образуют регион. Каждая область содержит несколько взаимно независимых остовных деревьев. Регион служит коммутационным узлом. Он участвует в расчете с другими областями на основе алгоритма связующего дерева, вычисляя общее связующее дерево. На основе этого алгоритма сеть на рисунке выше формирует топологию, показанную на рисунке ниже. И коммутатор A, и коммутатор C находятся в Region1. Ни одна ссылка не заблокирована, так как область не содержит циклов. То же самое и с Region2. Region1 и Region2 аналогичны узлам коммутатора. Эти два «переключателя» образуют петлю. Поэтому ссылка должна быть заблокирована.



Концепт MSTP представлен ниже:





Экземпляр: набор из нескольких VLAN. Один VLAN или несколько VLAN с одинаковой топологией могут быть сопоставлены с одним экземпляром; то есть один VLAN может образовывать связующее дерево, а несколько VLAN могут совместно использовать одно связующее дерево. Разные экземпляры сопоставляются с разными связующими деревьями. Экземпляр 0 является связующим деревом для устройств всех регионов, а остальные экземпляры — связующим деревом для устройств определенного региона. Множественный регион связующего дерева (регион MST): коммутаторы с одинаковым именем региона MSTP, уровнем версии и сопоставлением VLAN с экземпляром находятся в одном регионе MST. Как показано, Region1, Region2, Region3 и Region4 — это четыре разных региона MST. Таблица сопоставления VLAN: состоит из сопоставления между VLAN и связующими деревьями. Таблица сопоставления VLAN региона 2 представляет собой сопоставление между VLAN 1 и экземпляром 1, как показано на рис. 192; VLAN 2 сопоставляется с экземпляром 2, как показано на рис. 193. Другие VLAN сопоставляются с экземпляром 0, как показано на рис. 194. Общее и внутреннее связующее дерево (CIST): указывает экземпляр 0, то есть связующее дерево, охватывающее все устройства в коммутируемой сети. Как показано на рисунке, CIST состоит из IST и CST. Внутреннее связующее дерево (IST): указывает сегмент CIST в регионе MST, то есть экземпляр 0 каждого региона.

Общее связующее дерево (CST): указывает связующее дерево, соединяющее все регионы MST в сети коммутации. Если каждый регион MST является узлом устройства, CST является связующим деревом, вычисляемым на основе STP / RSTP этими узлами устройств. Как показано, красные линии обозначают остовное дерево. MST (множественный экземпляр связующего дерева): одна область MST может формировать несколько связующих деревьев, и они независимы друг от друга. Каждое связующее дерево является MSTI. IST также является специальным MSTI. Общий корень: указывает корневой мост CIST. Коммутатор с наименьшим идентификатором корневого моста в сети является общим корнем. В регионе MST остовные деревья имеют разную топологию, и их региональные корни также могут быть разными, три экземпляра имеют разные региональные корни. 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.

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

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

Discarding state: указывает, что порт не изучает MAC-адреса и не пересылает трафик.

Root port: 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 пересылки, обучения или сброса.

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 пересылки, обучения или сброса.

Главный порт: указывает порт, который соединяет регион MST с общим корнем. Порт находится на кратчайшем пути к общему корню. В CST главный порт является корневым портом региона (как узла). Мастер-порт — это специальный пограничный порт. Это корневой порт для CIST и главный порт для других экземпляров. Главный порт может находиться в состоянии пересылки, обучения или сброса.

Альтернативный порт: указывает резервный порт корневого порта или основного порта. При сбое корневого или главного порта альтернативный порт становится новым корневым или главным портом. Главный порт может находиться только в состоянии отбрасывания.

Резервный порт: указывает резервный порт назначенного порта. Когда назначенный порт выходит из строя, резервный порт становится назначенным портом и пересылает данные без каких-либо задержек. Резервный порт может находиться только в состоянии отбрасывания.

MSTP делит сеть на несколько регионов MST. CST рассчитывается между регионами. Несколько остовных деревьев рассчитываются в регионе. Каждое связующее дерево является MSTI. Экземпляр 0 — это IST, а остальные экземпляры — это MSTI.

- 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 рассчитывается в каждом регионе MST.
  - Каждый регион MST рассматривается как отдельное устройство, и CST рассчитывается между регионами.
  - CST и IST составляют CIST всей сети.
- Расчет MSTI

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

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

6.9.1. Веб конфигурирование

Включение MSTP протокола

Щелкнуть [Device Basic Configuration] → [MSTP configuration] → [Enable MSTP] для входа на страницу конфигурации протокола MSTP, как показано на рисунке ниже.

- **Mstp status**

Опции: Enable / Disable
По умолчанию: Disable
Функция: Включение / Выключение MSTP

Кольцевые протоколы на основе портов включают RSTP, ST-Ring-Port и DRP-Port, а кольцевые протоколы на основе VLAN включают MSTP, ST-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 портов и кольцевой протокол на основе VLAN являются взаимоисключающими, и для одного устройства можно выбрать только один режим кольцевого протокола.

Включение порт в режиме MSTP, как показано на рисунке ниже.

- **Port**
  Опции: все порты коммутатора
  По умолчанию: Disable
  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. Если вы хотите 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.

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

Конфигурирование MSTP state на порту

Щелкнуть [Device Basic Configuration] → [MSTP configuration] → [Enable Port MSTP] для входа на страницу конфигурации протокола MSTP, как показано на рисунке ниже.

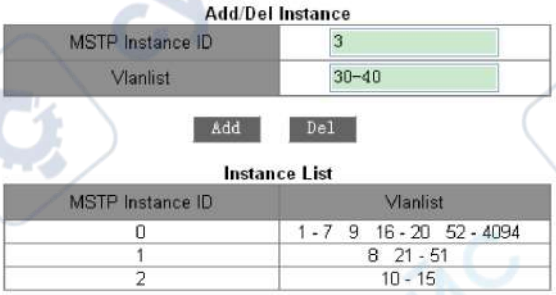
- **Port**
  Опции: все порты коммутатора
  По умолчанию: если включен глобальный протокол MSTP, состояние MSTP всех портов открыто.
  Функция: включить / отключить MSTP на порту.

Настройте параметр региона MST.

Щелкнуть [Device Basic Configuration] → [MSTP configuration] → [MSTP Region Config] для входа на страницу конфигурации параметров региона MST, как показано на рисунке ниже.

- **MSTP Region Name config**
  Диапазон: 1-32 символа
  По умолчанию: MAC-адрес устройства.
  Функция: Настройка имени региона MST.
- **MSTP Revision level config**
  Опции: 0~65535
  По умолчанию: 0
  Функция: Настройка параметра версии для региона MSTP.
  Описание: Параметр версии, имя региона MST и таблица сопоставления VLAN определяют регион MST, к которому принадлежит устройство. Когда все конфигурации одинаковы, устройства находятся в одном регионе MST.

Настройте таблицу сопоставления VLAN, как показано на рисунке ниже.



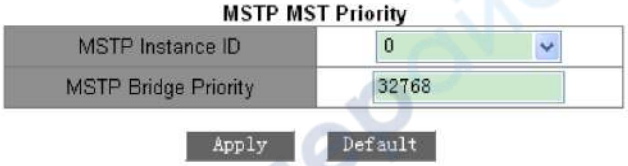
- **{MSTP Instance ID, VLAN list}**
  Диапазон: {0~16, 1~4094}
  По умолчанию: {0, 1~4094}.
  Функция: Настройте таблицу сопоставления VLAN в регионе MST.
  Описание. По умолчанию все VLAN сопоставляются с экземпляром 0. Одна VLAN сопоставляется только с одним экземпляром связующего дерева. Если VLAN с существующим сопоставлением сопоставляется с другим экземпляром, предыдущее сопоставление отменяется. Если сопоставление между назначенной VLAN и экземпляром удалено, эта VLAN будет сопоставлена с экземпляром 0.

<Del> не может удалить список VLAN экземпляра 0

После завершения настройки «Список экземпляров» покажет сопоставление между VLAN и экземпляром.

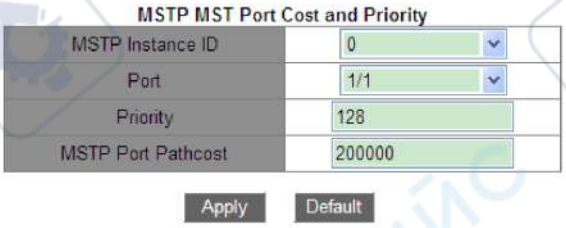
Настройте приоритет моста коммутатора в назначенном экземпляре.

Щелкнуть [Device Basic Configuration] → [MSTP configuration] → [MSTP Instance Config] для входа на страницу конфигурации параметров экземпляра MSTP, как показано на рисунке ниже.



- **MSTP Instance ID**
  Опции: все созданные экземпляры
- **MSTP Bridge Priority**
  Диапазон: 0~61440 с шагом 4096
  По умолчанию: 32768
  Функция: настроить приоритет 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, определенное устройство может быть назначено корневым мостом связующего дерева. Устройство с поддержкой MSTP можно настроить с разными приоритетами в разных экземплярах связующего дерева.

Настройка приоритета порта и стоимости пути в назначенном экземпляре, как показано на рисунке ниже.



- **MSTP Instance ID**
  Опции: все созданные экземпляры
- **Port**
  Опции: все порты коммутатора
- **Priority**
  Диапазон: 0~240 с шагом 16
  По умолчанию: 128
  Функция: настроить приоритет порта в назначенном экземпляре.
  Описание: Приоритет порта определяет, будет ли он выбран в качестве корневого порта. В том же состоянии порт с более низким приоритетом будет выбран в качестве корневого порта. Порты с поддержкой MSTP можно настроить 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 таблицах ниже.

Port Type	Default Path Cost	Recommended Range
10Mbps	2000000	2000000~20000000
100Mbps	200000	200000~2000000
1Gbps	20000	20000~200000

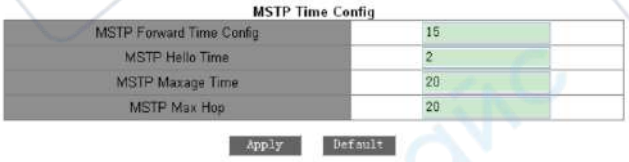
Port Type	Number of Aggregation Ports (in Allowed Aggregation Range)	Recommended Range
10Mbps	N	2000000/N
100Mbps	N	200000/N
1Gbps	N	20000/N

Функция: Настройка стоимости пути порта в назначенном экземпляре.

Описание: Стоимость пути порта используется для расчета оптимального пути. Этот параметр зависит от пропускной способности. Чем больше пропускная способность, тем ниже стоимость. Изменение стоимости пути порта может изменить путь передачи между устройством и корневым мостом, тем самым изменив роль порта. Порт с поддержкой MSTP можно настроить с различной стоимостью пути в разных экземплярах связующего дерева.

Конфигурирование параметров MSTP времени

Щелкнуть [Device Basic Configuration] → [MSTP configuration] → [MSTP Time Config] для входа на страницу настройки параметров времени MSTP, как показано на рисунке ниже.



- **MSTP Forward Time Config**
  Опции: 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 временного интервала для отправки BPDU.
- **MSTP Max Age Time**
  Диапазон: 6~40 с
  По умолчанию: 20 с
  Функция: Установите максимальный возраст пакетов BPDU.

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

- **MSTP Max Hop**
  Диапазон: 1~40
  По умолчанию: 20
  Функция: настроить максимальное количество переходов для региона MST. Максимальные прыжки области MST ограничивают масштаб области MST; максимальное количество переходов регионального корня равно максимальному количеству переходов региона MST.
  Описание: Начиная с корневого моста связующего дерева в регионе MST, номер перехода вычитает 1, когда BPDU проходит через устройство в регионе. Устройство отбрасывает BPDU с номером перехода 0.

Действительна только максимальная конфигурация переходов корневого моста в регионе MST. Устройство некорневого моста принимает конфигурацию максимального прыжка корневого моста.
Рекомендуется установка по умолчанию.

Настройка функции быстрого перехода состояния MSTP.

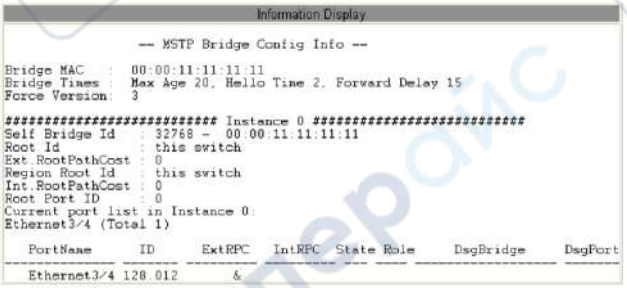
Щелкнуть [Device Basic Configuration] → [MSTP configuration] → [MSTP Fast Transfer Config] для входа на страницу конфигурации, как показано на рисунке ниже.

- **MSTP Port Link Type**
  Опции: AUTO / Force True / Force False
  По умолчанию: АВТО
  Функция: Установите тип соединения порта. Если порт подключен к каналу «точка-точка», состояние порта может быть быстро передано.
  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** означает, что ссылка, подключенная к локальному порту, является двухточечной. **Force False** означает, что ссылка, подключенная к локальному порту, является общей ссылкой.

- **Set/Cancel Edge Port**
  Варианты: Edge port / Ordinary port
  По умолчанию: Ordinary port
  Функция: Настройте порт как порт Edge или обычный порт.
  Описание: когда порт напрямую подключен к конечным устройствам, но не подключен к другим устройствам или общим сегментам, этот порт является граничным портом. Пограничный порт может быстро перейти от блокировки к пересылке без задержки. Как только пограничный порт получит сообщение BPDU, этот порт снова изменится на обычный порт.

Просмотр MSTP конфигурации

Щелкнуть [Device Basic Configuration] → [MSTP configuration] → [MSTP Information] для входа просмотра MSTP конфигурации, как показано на рисунке ниже.



6.10. Alarm

Коммутаторы этой серии поддерживают следующие типы аварийных сигналов:

- Аварийный сигнал конфликта IP/MAC: если включено, аварийный сигнал возникает при конфликте IP/MAC-адресов;
- Аварийный сигнал использования памяти / ЦП: Если эта функция включена, сигнал тревоги генерируется, когда использование ЦП / памяти превышает указанный порог.
- Аварийный сигнал порта: если эта функция включена, аварийный сигнал срабатывает, когда порт находится в состоянии отсутствия соединения.
- Аварийный сигнал питания: он применим к продуктам с двойным источником питания. Если эта функция включена, тревога срабатывает при отключении питания или отклонении от нормы.
- Тревога звонка: Если эта функция включена, тревога срабатывает, когда кольцо разомкнуто.
- Аварийный сигнал высокой температуры: если эта функция включена, аварийный сигнал срабатывает, когда температура переключателя превышает пороговое значение высокой температуры.

  Диапазон общего порога высокой температуры (T-high) составляет от 85 ℃ до 94 ℃ с настройкой по умолчанию 85 ℃.

  Диапазон опасного высокотемпературного порога (T-Max) составляет от 95℃ до 100℃ с настройкой по умолчанию 95℃.

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

Аварийный сигнал опасной высокой температуры срабатывает, когда температура переключателя равна или превышает пороговое значение T-Max (T-cur>=T-max).

- Аварийный сигнал низкой температуры: если эта функция включена, аварийный сигнал срабатывает, когда температура переключателя превышает пороговое значение низкой температуры.

  Диапазон порога низкой температуры (T-low) составляет от -40 ℃ до 10 ℃ с настройкой по умолчанию -40 ℃.

  Аварийный сигнал низкой температуры срабатывает, когда температура переключателя (T-cur) ниже порогового значения T-low (T-cur<T-low).
- Аварийный сигнал трафика порта: если эта функция включена, аварийный сигнал генерируется, когда скорость входящего/исходящего трафика порта превышает указанный порог.
- Аварийный сигнал ошибки CRC / потери пакета: Если эта функция включена, аварийный сигнал генерируется, когда количество ошибок CRC / потери пакета порта превышает указанный порог.

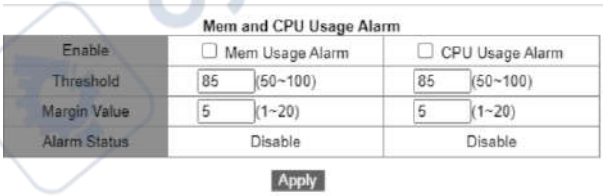
Когда функция тревоги включена, режимы тревоги включают запись в журнал, мигание светодиода тревоги на передней панели, срабатывание клеммного блока тревоги и отправку пакетов ловушек SNMP.

Только главная станция кольца ST и корень DRP поддерживают функцию кольцевой сигнализации.

6.10.1. Веб конфигурация

Настройка и отображения предупреждение об использовании памяти/ЦП.

Щелкнуть [Device Basic Configuration] → [Alarm] → [Basic Alarm] для входа на страницу конфигурации аварийного сигнала использования памяти/ЦП, как показано на рисунке ниже.



- **Mem Usage Alarm/CPU Usage Alarm**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включить / выключить сигнализацию использования памяти / процессора.
- **Threshold (%)**

Диапазон: 50~100
По умолчанию: 85
Функция: установка порога использования памяти/ЦП. Когда использование памяти/ЦП коммутатора превышает пороговое значение, генерируется аварийный сигнал.

- **Margin Value (%)**
  Диапазон: 1~20
  По умолчанию: 5
  Функция: Установите значение запаса использования памяти / ЦП.
  Описание: Если использование памяти / ЦП колеблется около порогового значения, аварийные сигналы могут генерироваться и сбрасываться неоднократно. Чтобы предотвратить это явление, вы можете указать значение маржи (по умолчанию 5%). Аварийный сигнал будет сброшен только в том случае, если использование памяти/ЦП ниже порогового значения на величину запаса или более. Например, порог использования памяти установлен на 60%, а значение поля установлено на 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**
  Опции: Disable / Disable
  Функция: просмотр состояния использования памяти / ЦП коммутатора. Тревога означает, что использование памяти / ЦП превышает пороговое значение и вызывает тревогу.

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

Настройка и отображение сигналов тревоги по мощности и температуре, как показано на рисунке ниже.

Power and Temperature Alarm

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

Apply

- **Power Alarm/High-Temperature Alarm/Low-Temperature Alarm**
  Опции: Disable / Enable
  По умолчанию: Disable
  Функция: включить / отключить сигнализацию питания / сигнализацию высокой температуры / сигнализацию низкой температуры.
- **Power Alarm Status**
  Варианты: Normal / Alarm
  Функция: просмотр состояния аварийного сигнала питания.
  Аварийный сигнал: для продуктов с резервным питанием один из модулей питания выходит из строя или работает ненормально, и срабатывает аварийный сигнал.

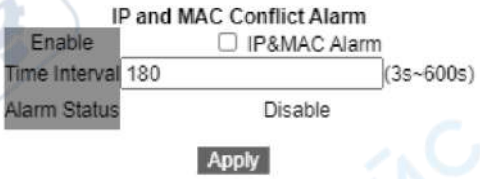
Нормальный: для продуктов с одним источником питания модуль питания подает питание в обычном режиме; для продукта с резервным питанием два силовых модуля обычно обеспечивают питание.

High-Temperature Alarm Status / Low-Temperature Alarm Status

Варианты: Normal / Alarm

Функция: просмотр рабочей температуры переключателя. Тревога означает, что температура переключателя превышает пороговое значение высокой/низкой температуры и вызывает тревогу. Нормальный означает, что рабочая температура переключателя нормальная.

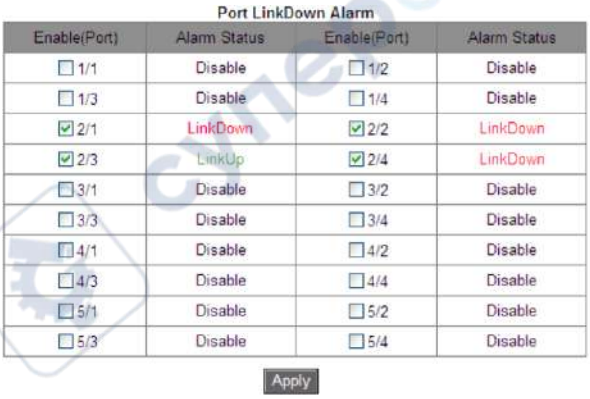
Настройка и отображение оповещения о конфликте IP, MAC, как показано на рисунке ниже.



- **IP and MAC conflict alarm**
  Опции: Enable / disable
  Конфигурация по умолчанию: disable
  Функция: включить ли сигнализацию о конфликте адресов.
- **Time Interval**
  Диапазон конфигурации: 3 с ~ 600 с
  По умолчанию: 180 с
  Функция: Настройка временного интервала для обнаружения конфликтов адресов.

Настройка и отображение тревоги порта

Щелкнуть [Device Basic Configuration] → [Alarm] → [Port LinkDown Alarm] для входа на страницу конфигурирования тревоги, как показано на рисунке ниже.



- **Port**
  Опции: Disable / Enable
  По умолчанию: Отключить
  Функция: включить / выключить тревогу порта.
- **Alarm Status**
  Опции: LinkDown / LinkUp

Функция: просмотр состояния подключения порта. LinkUp означает, что порт находится в состоянии подключения и поддерживает нормальную связь. LinkDown означает, что порт отключен или находится в ненормальном соединении (сбой связи).

Настройка и отображение аварийного сигнал трафика порта.

Щелкнуть [Device Basic Configuration] → [Alarm] → [Alarm about PortRate] для входа на страницу конфигурации оповещения о трафике портов, как показано на рисунке ниже.

- **input rate alarm/output rate alarm**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включить / отключить сигнализацию трафика порта.
- **Threshold**
  Диапазон: от 1 до 1000000000 бит/с или от 1 до 1000000 кбит/с.
  Функция: настроить пороговое значение для трафика порта.
- **Alarm Status**
  Варианты: Alarm / Normal
  Функция: просмотр состояния трафика порта. Тревога означает, что скорость входящего / исходящего трафика превышает пороговое значение и вызывает тревогу.

Настройка и отображение сигнала ошибки CRC / потери пакета.

Щелкнуть [Device Basic Configuration] → [Alarm] → [Alarm about CRC/ Pkt Loss] to enter] для входа на страницу конфигурации аварийного сигнала ошибки CRC / потери пакета, как показано на рисунке ниже.

- **CRC/Pkt Loss Alarm**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включение/отключение CRC/сигнала потери Pkt.
- **Threshold**
  Диапазон: от 1 до 1000000pps.
  Функция: Настройте пороговое значение для аварийного сигнала потери портов CRC/Pkt.
- **Alarm Status**
  Варианты: Alarm / Normal
  Функция: просмотр статуса потери портов CRC / Pkt. Аварийный сигнал означает, что потеря CRC / Pkt порта превышает пороговое значение и вызывает аварийный сигнал.

Настройка и отображение сигнала тревоги ST-Ring.

Щелкнуть [Device Basic Configuration] → [Alarm] → [Alarm about Ring] для входа на страницу конфигурации тревоги ST-Ring, как показано на рисунке ниже.

- **Alarm About ST-Ring**
  Опции: Disable / Enable
  По умолчанию: Disable
  Функция: включить / отключить сигнал DT-Ring.
- **Alarm Status**
  Варианты: Alarm / Normal
  Функция: просмотр состояния ST-Ring. Нормальный означает, что кольцо ST закрыто. Аварийный сигнал означает, что ST-Ring разомкнут или, находится в ненормальном состоянии.

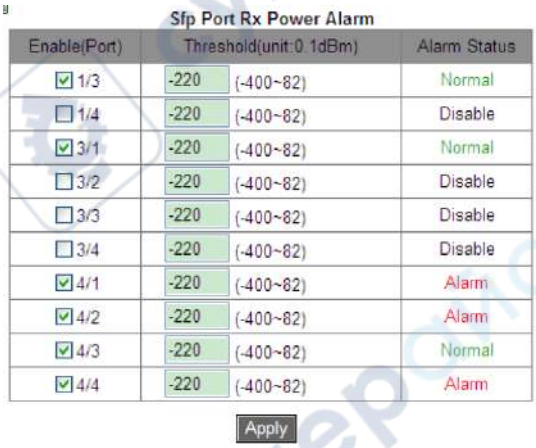
6.11. Цифровая диагностика

Цифровая диагностика является эффективным методом контроля важных рабочих параметров оптических приемопередатчиков. Параметры, подлежащие мониторингу, включают оптическую мощность передачи, оптическую мощность приема, температуру, рабочее напряжение, ток смещения и аварийные сигналы. Функция цифровой диагностики оптических трансиверов позволяет блоку NMS получать доступ к оптическим трансиверам через двухлинейные последовательные шины 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.

6.11.1. Веб конфигурирование

Конфигурирование и отображение SFP порт RX тревоги питания

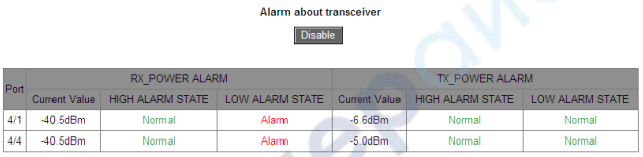
Щелкнуть [Device Basic Configuration] → [Alarm] → [Sfp Port Rx Power Alarm] для входа на страницу конфигурации аварийного сигнала питания порта SFP RX, как показано на рисунке ниже.



- **Sfp Port Rx Power Alarm**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включение / отключение сигнала тревоги питания RX порта SFP.
- **Threshold**
  Диапазон: -400~82 (единица измерения: 0,1 дБм)
  По умолчанию: -220 (-22,0 дБм)
  Функция: Настройка порога для сигнала тревоги мощности RX порта SFP.
- **Alarm Status**
  Варианты: Alarm / Normal
  Функция: после включения функции тревога означает, что мощность Rx для порта SFP меньше указанного порога и вызывает тревогу.

Настройка и отображение сигнала тревоги трансивера.

Щелкнуть [Device Basic Configuration] → [Alarm] → [Alarm about transceiver] для входа на страницу конфигурации тревог трансивера, как показано на рисунке ниже.



- **Alarm about transceiver**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включить / выключить сигнализацию 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 пороговое значение верхней тревоги.

Низкий и высокий порог оптической мощности зависят от аппаратного обеспечения и не могут быть настроены программно.

6.12. Конфигурация журнала

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.

Information Level	Value	Description
Critical	2	Serious system problem
Warning	4	Warning information
Information	6	Notification that needs to be recorded
Debugging	7	Information generated in the debugging process

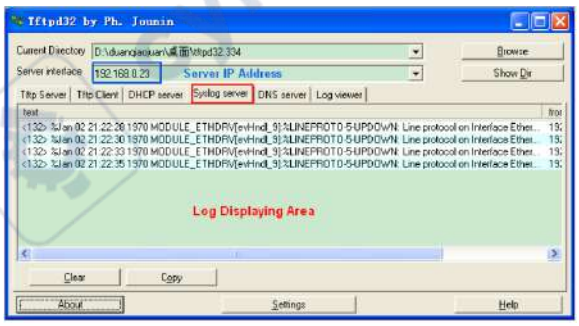
6.12.1. Веб конфигурирование

Настроика функции журнала

Щелкнуть [Device Basic Configuration] → [Log Configuration] → [Log Configuration] для входа на страницу конфигурирование журнала, как показано на рисунке ниже.

- **Log to flash enable**
  Опции: Enable / disable
  По умолчанию: disable
  Функция: сохранение журнала в службе включения флэш-памяти.
- **Log to flash interval**
  Варианты: 10~14400мин
  По умолчанию: 14400
  Функция: Настройка интервала времени для сохранения журналов во флэш-память.
- **IP Address of remote logging server**
  Настройте IP-адрес сервера, на который загружается информация журнала.
- **Facility**
  Опции: Local0 - Local7
  По умолчанию: Local0
  Описание: Средство используется для идентификации различных источников журналов на сервере журналов.
- **Level**
  Варианты: Critical / Warning / Information / Debugging
  По умолчанию: Warning
  Функция: Выберите уровень записываемой информации журнала.
  Описание: Информация журнала может быть отфильтрована по уровням. Правило фильтрации заключается в том, что запрещается вывод информации, значение которой больше значения выбранного информационного уровня. Например, если выбран уровень информации «Предупреждение» и соответствующее ему значение равно 4, система выводит только «Критическая информация» со значением 2 и «Предупреждение» со значением 4.

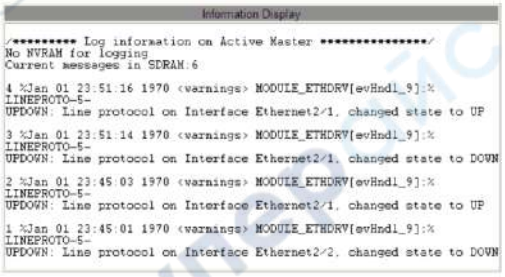
Вы можете установить программное обеспечение Syslog Server, например, Tftp32, на ПК для создания «Syslog Server». Информация журнала может отображаться в режиме реального времени на сервере Syslog, как показано на рисунке ниже.



Просмотр конфигурации журнала

Щелкнуть [Device Basic Configuration] → [Log Configuration] → [Show Log] для входа на страницу просмотра лога, как показано на рисунке ниже.

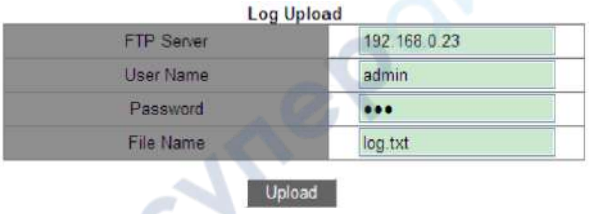
- **Level**
  Опции: Warning / Critical
  По умолчанию: Warning
  Функция: выберите самый низкий уровень отображаемой информации журнала.
- **Begin Index/End Index**
  Диапазон: 1~65535
  Функция: просмотр указанной информации журнала в буфере, и одна строка указывает на одну запись. На рисунке ниже показана указанная информация журнала в буфере.



В буфере сохраняется только критическая и предупредительная информация журнала без информации и информации журнала отладки.

Загрузка журнала

Щелкнуть [Device Basic Configuration] → [Log Configuration] → [Log Transmit] для входа на страницу загрузки журнала, как показано на рисунке ниже.



- **FTP Server**
  Формат: A.B.C.D.
  Функция: Установите IP-адрес FTP-сервера.
- **User Name**
  Функция: Настройка имени пользователя FTP.
- **Password**
  Функция: Настройка пароля пользователя FTP.
- **File Name**
  Диапазон: 1~32 символа
  Функция: установить имя файла, сохраненного на сервере.

FTP-сервер должен оставаться в онлайн-состоянии во время загрузки журналов.

Очистка информации в буфере журнала

Щелкнуть [Device Basic Configuration] → [Clear Log] для очистки журнала, как показано на рисунке ниже.

6.13. Конфигурация маршрутизации

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

6.13.1. Конфигурирование статической маршрутизации

Статические маршруты настраиваются вручную. Если топология сети проста, вам нужно только настроить статические маршруты для правильной работы сети. Статические маршруты просты в настройке и стабильны. Их можно использовать для балансировки нагрузки и резервного копирования 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 топологическое изменение, соответствующие маршруты станут недоступны, и сеть разорвется. В этом случае сетевой администратор должен изменить статические маршруты вручную.

6.13.1.1. Таблица маршрутов

Каждый коммутатор уровня 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:

Destination: указывает IP-адрес или сеть назначения.

Network mask: вместе с адресом назначения указывает сеть, в которой находится хост назначения или коммутатор уровня 3. Логическая операция И между адресом назначения и маской сети 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. Сетевая маска состоит из определенного количества последовательных единиц. Он может быть выражен в десятичном формате с точками или количеством единиц.

Egress: указывает интерфейс, через который должен быть перенаправлен соответствующий IP-пакет. IP-адрес следующего коммутатора уровня 3 (следующий переход): указывает новый коммутатор уровня 3, через который будет проходить IP-пакет.

Priority: 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 — тот, который имеет наивысший приоритет.

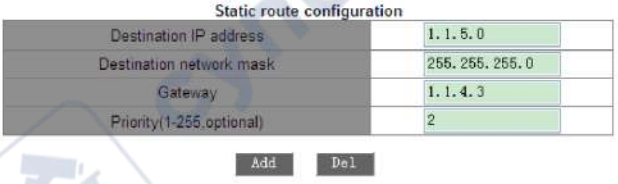
6.13.1.2. Маршрут по умолчанию

Чтобы предотвратить слишком много записей в таблице маршрутизации, вы можете 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.

6.13.1.3. Веб конфигурирование

Конфигурирование ститаческого мрашрута

Щелкнуть [Device Basic Configuration] → [Route configuration] → [Static route configuration] → [Static route configuration] для входа на страницу конфигурирования статического маршрута, как показано на рисунке ниже.



- **Destination IP address**
  Формат: A.B.C.D.
  Функция: Установите IP-адрес сети назначения.
- **Destination network mask**
  Функция: Установите маску подсети для сети, в которой находится целевой хост или коммутатор уровня 3.
- **Gateway**
  Формат: A.B.C.D.
  Функция: установка IP-адреса следующего перехода.

- **Priority**
  Диапазон: 1~255
  По умолчанию: 1
  Функция: Установить приоритет 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 ниже.

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

6.13.2. Настройка RIP

Протокол маршрутной информации (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 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 вводить 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 усовершенствован 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 3 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 прямым подключением равно 0. Количество переходов от маршрутизатора к маршрутизатору с прямым подключением равно 1. Чтобы ограничить время конвергенции, диапазон значений метрики RIP составляет от 0 до 15. Значение метрики равно 16. (или больше) считается

бесконечным, что означает, что сеть назначения недоступна. Именно поэтому RIP подходит для сетей небольшого размера.

6.13.2.1. Предотвращение петель маршрутизации

В сети с протоколом RIP, когда маршрут RIP становится недоступным, коммутатор L3 RIP 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 заметно влияет на время маршрутизации и время агрегации маршрутов.

Чтобы избежать бесконечного подсчета, RIP предоставляет механизмы разделения горизонта и триггерного обновления для решения проблемы петли маршрутизации. Разделение горизонта направлено на то, чтобы избежать отправки маршрутов на шлюз, из которого они были получены. Он содержит простой расщепленный горизонт и расщепленный горизонт с отравленным оборотом. Простой разделенный горизонт включает в себя удаление маршрутов, которые должны быть отправлены на соседний шлюз, от которого эти маршруты получены. Разделение горизонта с отравленным реверсом включает в себя удаление предыдущих маршрутов из пакета обновления маршрута и установку метрики этих маршрутов на 16. В механизме триггерного обновления всякий раз, когда шлюз изменяет метрику маршрута, пакет обновления маршрута будет транслироваться немедленно без учитывая состояние 30-секундного таймера обновления.

6.13.2.2. Операции

- После включения RIP маршрутизатор отправляет сообщения-запросы соседним маршрутизаторам.
  Соседние маршрутизаторы возвращают ответные сообщения, включая информацию о своих таблицах маршрутизации.
- 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, чтобы сохранить самую последнюю информацию о маршрутизации.
- По умолчанию локальная таблица маршрутизации будет отправляться 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 глобальным. Кроме того, RIP использует механизм истечения срока действия для обработки маршрутов с истекшим сроком действия. В частности, если коммутатор L3 не получает информацию об обновлении маршрута от соседа в течение указанного интервала времени (недопустимое значение таймера), все маршруты от этого соседа будут считаться недопустимыми маршрутами, и маршрут переходит в состояние подавления. Этот маршрут

имеет срок действия (значение таймера удержания) в таблице маршрутизации. Если в течение этого периода от этого соседа не будет получена информация об обновлении, эти маршруты будут удалены из таблицы маршрутизации.

6.13.2.3. Веб конфигурирование

Базовая конфигурация работы RIP в коммутаторе уровня 3 проста. Как правило, вам необходимо включить RIP и разрешить порту передавать и получать пакеты RIP, что означает передачу и получение пакетов RIP в соответствии с конфигурацией RIP по умолчанию (по умолчанию коммутатор уровня 3 передает RIP-2, принимает RIP-1 и RIP-1). 2).

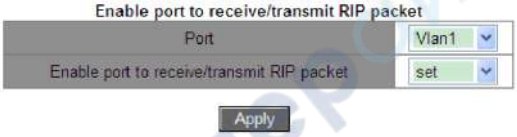
Включение RIP

Щелкнуть [Device Basic Configuration] → [Route configuration] → [RIP configuration] → [Enable RIP] → [Enable RIP] для включения RIP, как показано на рисунке ниже.

- **Enable RIP**
  Опции: Enable RIP / Disable RIP
  По умолчанию: Disable RIP
  Функция: Включение / выключение RIP

Включение RIP на интерфейсе

Щелкнуть [Device Basic Configuration] → [Route configuration] → [RIP configuration] → [Enable RIP] → [Enable port to receive/transmit RIP packet] для включения RIP на интерфейсе, как показано на рисунке ниже.



- **Enable port to receive/transmit RIP packet**
  Опции: set / cancel
  По умолчанию: set
  Function: Включение / выключение RIP на интерфейсе.

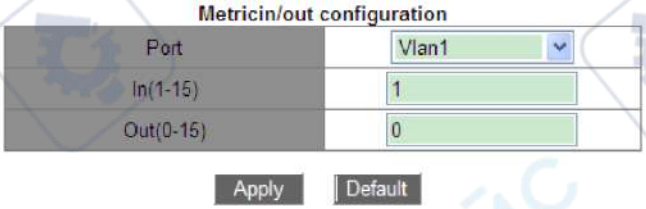
Настройка импортированного маршрута

Щелкнуть [Device Basic Configuration] → [Route configuration] → [RIP configuration] → [RIP parameter configuration] → [Enable imported route] для входа на страницу конфигурации импортированного маршрута, как показано на рисунке ниже.

- **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: перераспределить значение метрики импортированного маршрута. Этот параметр является необязательным. Если параметр не настроен, он будет перераспределен в соответствии со значением метрики по умолчанию.
- **Operation type**
  Опции: Add / Del
  Функция: добавить / отменить импорт другого протокола маршрутизации в RIP. По умолчанию никакие другие протоколы маршрутизации не импортируются в RIP.

Настройка дополнительной метрики маршрутизации

Щелкнуть [Device Basic Configuration] → [Route configuration] → [RIP configuration] → [RIP parameter configuration] → [Metricin/out configuration] для входа на страницу настройки дополнительной метрики маршрутизации, как показано на рисунке ниже.



- **In**
  Диапазон: 1~15
  По умолчанию: 1
  Функция: настроить входящую метрику дополнительной 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, а метрика маршрута в таблице маршрутизации не изменяется.

Конфигурирование RIP на порту

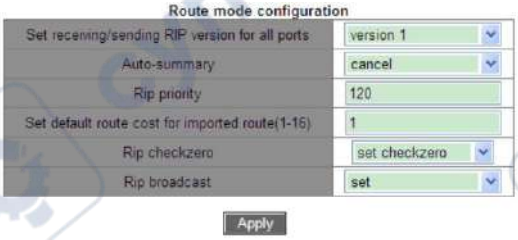
Щелкнуть [Device Basic Configuration] → [Route configuration] → [RIP configuration] → [RIP parameter configuration] → [RIP port configuration] для входа на страницу конфигурации порта RIP, как показано на рисунке ниже.

- **Receiving RIP version**
  Опция: version 1 / version 2 / version 1 и 2
  По умолчанию: version 1 и 2
  Функция: Установите версию сообщения RIP, полученного интерфейсом. Версия 1 означает сообщение RIP-1, полученное интерфейсом, версия 2 означает RIP-2, а версии 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: Установите версию сообщения RIP, передаваемого интерфейсом. Версия 1 означает сообщение RIP-1, передаваемое интерфейсом, версия 2 (BC) означает сообщение RIP-2, передаваемое интерфейсом в широковещательном режиме, версия 2 (MC) означает сообщение RIP-2, передаваемое интерфейсом в многоадресном режиме.
- **Receive packet**
  Варианты: Yes / No
  По умолчанию: Yes
  Функция: Разрешить интерфейсу получать RIP-сообщения или нет.
- **Send packet**
  Варианты: Yes / No
  По умолчанию: Yes
  Функция: разрешить интерфейсу передавать сообщение RIP или нет.
- **Split-horizon status**
  Варианты: permit / forbid
  По умолчанию: permit
  Функция: разрешить / запретить «расщепление горизонта». «Расщепление горизонта» позволяет избежать петель маршрутизации, т. е. избежать повторной передачи маршрутов, полученных от интерфейса, с этого интерфейса.
- **RIP authentication key**
  Диапазон: 1~16 символов
  Функция: Установите ключ аутентификации RIP.
- **RIP authentication type**
  Варианты: text / Cisco MD5 / MD5 / cancel
  По умолчанию: cansel
  Функция: Установите тип аутентификации RIP. текст означает текстовую аутентификацию; MD5 означает общую аутентификацию MD5; Cisco MD5 означает

аутентификацию Cisco MD5; отмена означает восстановление аутентификации по умолчанию: текстовая аутентификация. RIP-1 не поддерживает аутентификацию.

Конфигурирование RIP mode

Щелкнуть [Device Basic Configuration] → [Route configuration] → [RIP configuration] → [RIP parameter configuration] → [RIP mode configuration] для входа на страницу конфигурации RIP, как показано на рисунке ниже.



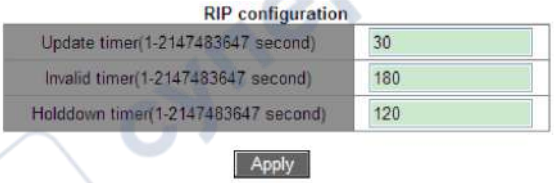
- **Set receiving/sending RIP version for all ports**
  Варианты: version 1 / version 2 / cancel
  По умолчанию: передача сообщения RIP-2, получение сообщения RIP 1 и RIP 2.
  Функция: Настройка версии сообщения RIP, передаваемого и принимаемого всеми интерфейсами маршрутизации. версия 1 означает, что сообщение RIP-1 передается и принимается всеми интерфейсами маршрутизации, версия 2 означает RIP-2, отмена означает восстановление конфигурации по умолчанию.
- **Auto-summary**
  Опции: cancel / set
  По умолчанию: cancel
  Функция: установить/отменить агрегацию маршрутов. Объединение 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 объединения маршрутов.
- **Rip priority**
  Диапазон: 0~255
  По умолчанию: 120
  Функция: Укажите приоритет RIP. Чем меньше значение, тем выше приоритет. Приоритет будет определять маршруты в базовой таблице маршрутизации, какой алгоритм маршрутизации будет использоваться для получения наилучшей маршрутизации.
- **Set default route cost for imported route**
  Диапазон: 1~16
  По умолчанию: 1
  Функция: настройка значения метрики по умолчанию для импортированного маршрута.
- **Rip checkzero**
  Опции: set checkzero / cancel checkzero
  По умолчанию: set checkzero

Функция: Проверить нулевое поле сообщения RIP-1 или нет. Некоторые поля в сообщении RIP-1 должны быть нулевыми. Эти поля называются нулевыми полями. Вы можете 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**
  Опции: set / cancel
  По умолчанию: set
  Функция: установка разрешает всем интерфейсам коммутатора уровня 3 передавать широковещательные пакеты RIP или многоадресные пакеты; Отменить — запретить всем интерфейсам коммутатора 3-го уровня передавать широковещательные или многоадресные пакеты RIP, а только передавать пакеты данных RIP между соседними коммутаторами 3-го уровня.

Конфигурирование времени RIP

Щелкнуть [Device Basic Configuration] → [Route configuration] → [RIP configuration] → [RIP parameter configuration] → [RIP timer configuration] для входа на страницу настройки таймеров RIP, как показано на рисунке ниже.



- **Update timer**
  Диапазон: 1～2147483647
  По умолчанию: 30
  Функция: Настройка интервала между обновлениями маршрутизации.
- **Invalid timer**
  Диапазон: 1～2147483647
  По умолчанию: 180
  Функция: Настройка диапазона времени объявления маршрутизации RIP недействительной. Если коммутатор L3 не получает информацию об обновлении маршрута от соседа в течение заданного интервала времени (недопустимое значение таймера), 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 таймера удержания) от этого соседа не будет получена информация об обновлении, эти маршруты будут удалены из таблицы маршрутизации. Holddown timer > Update timer.

6.13.3. Конфигурация OSPF

Open Shortest Path First (OSPF) — это протокол внутреннего шлюза состояния канала. Коммутаторы уровня 3 обмениваются информацией о состоянии канала для создания базы данных состояния канала (LSDB). Затем каждый коммутатор использует алгоритм поиска кратчайшего пути (SPF) на основе LSDB для создания таблицы маршрутизации. Коммутаторы этой серии поддерживают OSPF версии 2.

6.13.3.1. Базовый концепт

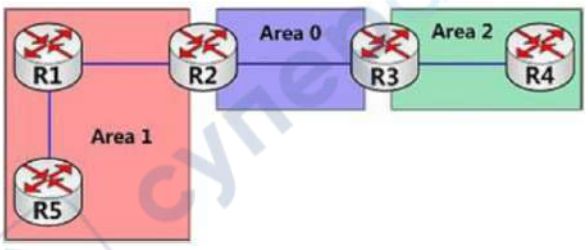
- AS
  Автономная система (AS) состоит из группы маршрутизаторов, использующих один и тот же протокол маршрутизации.
- Router ID
  Идентификатор маршрутизатора (RID). Маршрутизатор с поддержкой OSPF должен иметь собственный идентификатор маршрутизатора, который является уникальным идентификатором маршрутизатора в AS. RID можно настроить вручную или сгенерировать автоматически. Автоматически сгенерированный RID — это основной IP-адрес интерфейса VLAN с наименьшим идентификатором на коммутаторе.
- OSPF пакеты
  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 соседнему LSA для обновления. 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).
- Neighbor и adjacency
  Neighbor: Когда маршрутизатор OSPF запускается, он отправляет приветственный пакет через интерфейс OSPF, и маршрутизатор, который получает приветственный пакет, проверяет параметры, содержащиеся в пакете. Если параметры двух маршрутизаторов совпадают, они становятся соседями.
  Adjacency: Два соседа OSPF устанавливают отношения смежности для синхронизации своих LSDB. Следовательно, любые два соседа без обмена информацией о маршруте не устанавливают смежность.
- LSA тип
  Обмен LSA возможен только между соседними 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): генерируется 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 (тип 3): создается пограничными маршрутизаторами областей (ABR) и анонсируется в других областях. LSA описывает информацию о маршрутизации в области.
ASBR Summary LSA (тип 4): создается ABR и объявляется в соответствующих областях. LSA типа 4 описывают маршруты к граничному маршрутизатору автономной системы (ASBR).
AS External LSA (Type5): создается ASBR и рассылается по всей AS (за исключением тупиковых областей). Каждый LSA типа 5 описывает маршрут к другой AS.

6.13.3.2. Area и Router

Area partition

OSPF разбивает AS на несколько областей, которые идентифицируются идентификаторами областей. Области классифицируют маршрутизаторы в сети по различным логическим группам, как показано на рисунке ниже. Между областями происходит обмен сводной информацией о маршрутизации. Область 0, магистральная область, является основной областью всей сети OSPF. Все немагистральные области должны быть напрямую связаны с магистральной областью. Информация о маршрутизации немагистральных областей должна пересылаться магистральной областью. Чтобы уменьшить размер базы данных топологии, OSPF может разделить определенные области на тупиковые области. LSA типа 4 и типа 5 не могут входить в тупиковые области. 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 области.



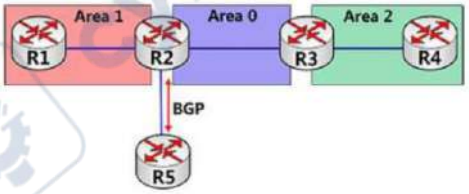
Разделение области основано на интерфейсах. Следовательно, маршрутизатор с несколькими интерфейсами может принадлежать нескольким областям, но каждый интерфейс принадлежит только одной области. Все маршрутизаторы в одной области поддерживают один и тот же LSDB. Если маршрутизатор принадлежит нескольким областям, он поддерживает LSDB для каждой области. Сетевой раздел имеет следующие преимущества:

- Маршрутизаторы в каждой области поддерживают только LSDB области, 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 областью может уменьшить объем данных OSPF.

Тип маршрутизатора

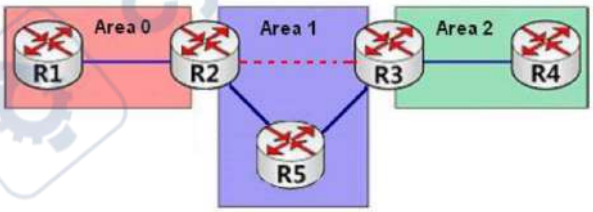
В зависимости от положения коммутатора уровня 3 в AS роль коммутатора может быть внутренним маршрутизатором, ABR, магистральным маршрутизатором или ASBR, как показано на рисунке ниже.



- Internal router: все интерфейсы внутреннего маршрутизатора принадлежат одной области OSPF. Например, R1 и R4 на рисунке.
- ABR: ABR соединяет одну или несколько областей с магистральной областью. В ABR хотя бы один интерфейс должен принадлежать магистральной области. Например, R2 и R3 на рисунке.
- Backbone router: по крайней мере один интерфейс магистрального маршрутизатора должен находиться в магистральной области. Все ABR и внутренние маршрутизаторы в области 0 являются магистральными маршрутизаторами. Например, R2 и R3 на рисунке.
- ASBR: Маршрутизатор, обменивающийся маршрутной информацией с другой AS, является ASBR. Например, R2 на рисунке.
- Один маршрутизатор может быть нескольких типов. Например, R2 на рисунке — это магистральный маршрутизатор, ABR и ASBR.

Virtual link

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



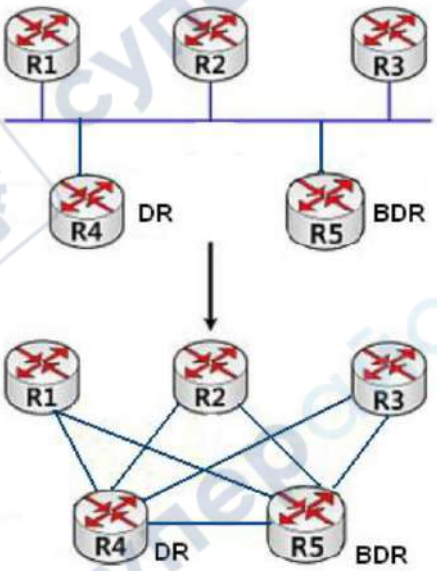
Виртуальный канал — это логическое соединение, установленное между двумя ABR через немагистральную область и настроенное на обоих ABR для вступления в силу. Немагистральная зона называется транзитной зоной. Например, красная пунктирная линия на рисеуrt — это виртуальный канал, а область 1 — транзитная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

Тип маршрута

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

6.13.3.3. 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 смежные отношения и обмениваются маршрутной информацией с DR. DR сообщает о состоянии сетевого канала другим маршрутизаторам. Чтобы предотвратить одноточечные сбои, вызванные сбоем DR, OSPF определяет резервный назначенный маршрутизатор (BDR). BDR также устанавливают соседние отношения с другими маршрутизаторами. BDR является резервной копией DR. Когда DR выходит из строя, BRD становится DR. Поскольку были установлены соседние отношения с другими маршрутизаторами, сбой DR оказывает незначительное влияние на сеть.



Как показано на Рисунке, на первом рисунке показаны физические соединения Ethernet, а на втором рисунке — установленные смежные отношения. После принятия 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 в качестве BDR выбирается другой маршрут.

- Концепция DR основана на интерфейсе. 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.

6.13.3.4. Веб конфигурирование

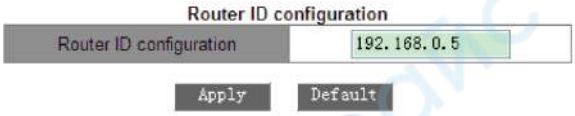
Включение OSPF

Щелкнуть [Device Basic Configuration] → [Route configuration] → [OSPF configuration] → [OSPF process configuration] → [OSPF Enable/Disable] для входа на страницу включения OSPF, как показано на рисунке ниже.

- **OSPF статус**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включение / выключение OSPF.

Установка RID

Щелкнуть [Device Basic Configuration] → [Route configuration] → [OSPF configuration] → [OSPF process configuration] → [Router-ID configuration] для входа на страницу конфигурации RID, как показано на рисунке ниже.

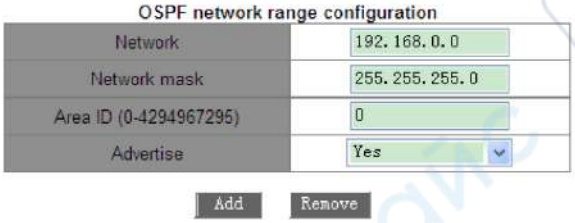


- **Router ID configuration (IP address)**
  Формат: A.B.C.D.
  По умолчанию: основной IP-адрес интерфейса VLAN с наименьшим идентификатором VLAN на коммутаторе.
  Функция: установка RID коммутаторов с поддержкой OSPF. Каждый коммутатор с поддержкой OSPF имеет уникальный RID в AS.

Изменение RID вступает в силу только после повторного включения OSPF.

Установка сетевого диапазона OSFP

Щелкнуть [Device Basic Configuration] → [Route configuration] → [OSPF configuration] → [OSPF process configuration] → [OSPF network range configuration] для входа на страницу конфигурации сетевого диапазона OSPF, как показано на рисунке ниже.



- **Network**
  Формат: A.B.C.D.
  Функция: Установите сетевой IP-адрес.
- **Network mask**
  Функция: установка маски подсети сети.
  Описание: Маска сети и IP-адрес определяют диапазон сети.
- **Area ID**
  Диапазон: 0~4294967295
  Функция: настроить область для сетевого диапазона.
  Описание: если в область добавляется сетевой диапазон, все внутренние маршруты сетевого диапазона не объявляются другим областям.
- **Advertise**
  Варианты: Да/Нет
  По умолчанию: Да
  Функция: настроить, следует ли объявлять дайджест-информацию о маршрутах в сетевом диапазоне.

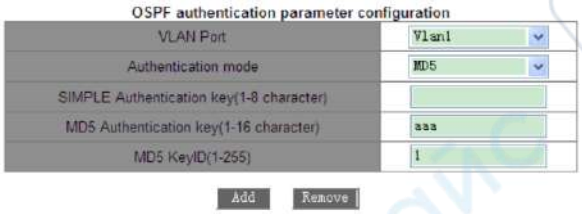
Установите область для интерфейса VLAN.

Щелкнуть [Device Basic Configuration] → [Route configuration] → [OSPF configuration] → [OSPF process configuration] → [OSPF area configuration for port (must)] для входа на страницу конфигурации области интерфейса VLAN, как показано на рисунке ниже.

- **Area ID**
  Диапазон: 0~4294967295
  Функция: Установите область для интерфейса VLAN.
  Описание: если интерфейс VLAN добавляется в область OSPF, OSPF включается на интерфейсе VLAN.

Установка параметров аутентификации OSPF.

Щелкнуть [Device Basic Configuration] → [Route configuration] → [OSPF configuration] → [OSPF TX-parameter configuration] → [OSPF authentication parameter configuration] для входа на страницу конфигурации аутентификации OSPF, как показано на рисунке ниже.

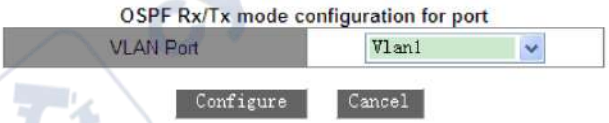


- **Authentication mode**
  Опции: SIMPLE / MD5
  Функция: настроить режим аутентификации для получения пакетов OSPF на указанном интерфейсе.
  Описание: SIMPLE указывает на аутентификацию в виде обычного текста. MD5 указывает зашифрованную аутентификацию.
- **SIMPLE Authentication key**
  Диапазон: 1~8 символов
  Функция: Установите ключ для SIMPLE аутентификации.
  Описание: Настройка этого параметра действует только в том случае, если в качестве режима аутентификации выбран SIMPLE.
- **MD5 Authentication key**
  Диапазон: 1~16 символов
  Функция: Установить ключ для аутентификации MD5.
  Описание: Установка этого параметра действует, только если в качестве режима аутентификации выбран MD5.
- **MD5 Key ID**
  Диапазон: 1~255
  Функция: Установите идентификатор ключа аутентификации MD5.

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

Настройка режим OSPF Rx/Tx для интерфейса VLAN.

Щелкнуть [Device Basic Configuration] → [Route configuration] → [OSPF configuration] → [OSPF TX-parameter configuration] → [Passive interface configuration] для входа на страницу конфигурации режима Rx/Tx OSPF, как показано на рисунке ниже.



- **VLAN Port**
  Опции: интерфейсы VLAN, на которых должен быть включен OSPF.
  Функция: настроить указанный интерфейс VLAN только для получения (но не для отправки) пакетов OSPF.
  Описание. По умолчанию все интерфейсы с поддержкой OSPF могут отправлять и получать пакеты OSPF.

Установка параметров таймера отправки пакетов OSPF.

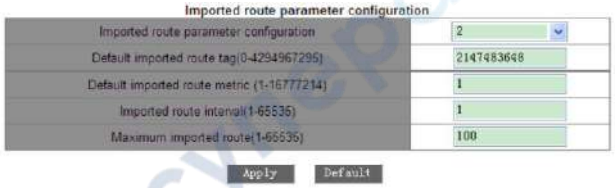
Щелкнуть [Device Basic Configuration] → [Route configuration] → [OSPF configuration] → [OSPF TX-parameter configuration] → [OSPF packet sending timer configuration] для входа на страницу настройки таймера отправки пакетов, как показано на рисунке ниже.

- **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 отправки приветственных пакетов на указанный интерфейс. Описание. Коммутатор периодически отправляет приветственные пакеты соседним устройствам для обнаружения и поддержания взаимосвязей между соседними устройствами и выбора DR и BDR.
- **Neighbour router invalid interval**
  Диапазон: 1~2147483647 с
  По умолчанию: 40 с
  Функция: Настройка интервала истечения маршрутов к соседним коммутаторам. Значение должно быть больше или равно четырехкратному интервалу приветственного пакета.
  Описание: Если коммутатор не получает приветственные пакеты от соседнего устройства в течение интервала, соседнее устройство считается недоступным и недействительным.
- **Sending link-state packet delay**
  Диапазон: 1~65535 с
  По умолчанию: 1 с
  Функция: настроить задержку отправки LSA на указанном интерфейсе.
- **Sending link-state packet retransmit interval**
  Диапазон: 1~65535 с
  По умолчанию: 5 с
  Функция: Установите интервал для повторной передачи LSA соседним коммутаторам на указанном интерфейсе.
  Описание: после отправки LSA соседнему устройству коммутатор сохраняет LSA до тех пор, пока не получит подтверждение от соседнего устройства. Если коммутатор не получает подтверждение в течение интервала, он повторно передает LSA.

Для обеспечения нормальной работы OSPF параметры таймера должны быть одинаковыми у соседей OSPF.

Задайте параметры для импорта маршрутов OSPF.

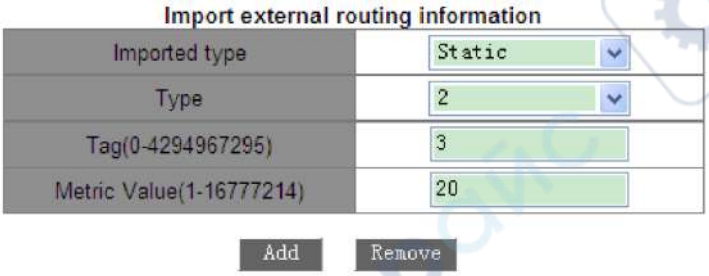
Щелкнуть [Device Basic Configuration] → [Route configuration] → [OSPF configuration] → [Imported route parameter configuration] → [Imported route parameter configuration] для входа на страницу конфигурации импорта маршрутов OSPF, как показано на рисунке ниже.



- **Imported route parameter configuration**
  Варианты: 1/2
  По умолчанию: 2
  Функция: Установить тип 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: Установить тег по умолчанию для импортированных маршрутов.
- **Default imported route cost**
  Диапазон: 1~16777214
  По умолчанию: 1
  Функция: Установить стоимость импортируемых маршрутов по умолчанию.
- **Imported route interval**
  Диапазон: 1~65535 с
  По умолчанию: 1 с
  Функция: Установите интервал для импорта внешних маршрутов. OSPF периодически импортирует информацию о внешнем маршруте и распространяет эту информацию по всей AS.
- **Maximum imported route**
  Диапазон: 1~65535
  По умолчанию: 100
  Функция: Установите максимальное количество маршрутов, которые могут быть одновременно импортированы OSPF.

Настройте импорт маршрутов других протоколов.

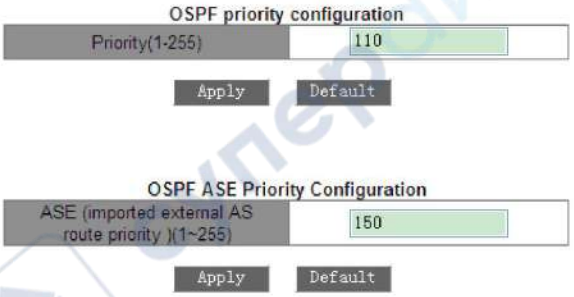
Щелкнуть [Device Basic Configuration] → [Route configuration] → [OSPF configuration] → [Imported route parameter configuration] → [Import external routing information для входа на страницу конфигурации импорта внешних маршрутов, как показано на рисунке ниже.



- **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 тега импортируемых маршрутов.
- **Metric Value**
  Диапазон: 1~16777214
  Функция: настроить значение метрики импортированных маршрутов.

Установка приоритетов для протоколов маршрутизации.

Щелкнуть [Device Basic Configuration] → [Route configuration] → [OSPF configuration] → [Other parameter configuration] → [OSPF priority configuration] для входа на страницу конфигурации приоритета протокола маршрутизации, как показано на рисунке ниже.



- **Priority**
  Диапазон: 1~255
  По умолчанию: 110
  Функция: установка приоритета OSPF.
- **ASE (imported external AS route priority)**
  Диапазон: 1~255
  По умолчанию: 150
  Функция: Установить приоритет импортируемых маршрутов.

Описание. Поскольку на коммутаторах уровня 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 обнаруживается несколькими протоколами маршрутизации, допустимым является протокол с наивысшим приоритетом (наименьшее число).

Конфигурирование stub area

Щелкнуть [Device Basic Configuration] → [Route configuration] → [OSPF configuration] → [Other parameter configuration] → [OSPF STUB area and default route cost] для входа на страницу конфигурации тупиковой области, как показано на рисунке ниже.

- **Default Route Cost**
  Диапазон: 1~65535
  Функция: Установить стоимость маршрута по умолчанию для тупиковой области.
- **Area ID**
  Диапазон: 1~4294967295
  Функция: Настройте указанную область в качестве тупиковой.

Магистральная область (backbone area), то есть область 0, не может быть настроена как тупиковая область (stub area).

Конфигурирование OSFP virtual link

Щелкнуть [Device Basic Configuration] → [Route configuration] → [OSPF configuration] → [Other parameter configuration] → [OSPF virtual link configurationle] для входа на страницу конфигурации виртуального канала OSPF, как показано на рисунке ниже.

- **Route ID**
  Формат: A.B.C.D.
  Функция: Установите RID для равноправного конца виртуального канала.
- **Transit Area ID**
  Диапазон: 1~4294967295
  Функция: укажите транзитную зону для виртуального канала.
- **Hello packet interval**
  Диапазон: 1~65535 с
  По умолчанию: 10 с

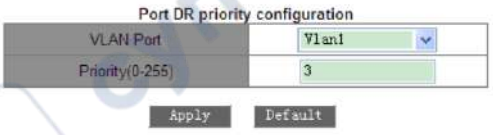
Функция: Настройка интервала отправки приветственных пакетов на указанный интерфейс. Описание: Коммутатор периодически отправляет приветственные пакеты соседним узлам для обнаружения и поддержания отношений между соседями и выбора DR и BDR.

- **Neighbour router invalid interval**
  Диапазон: 1~2147483647 с
  По умолчанию: 40 с
  Функция: Настройка интервала истечения маршрутов к соседним коммутаторам. Значение должно быть больше или равно четырехкратному интервалу приветственного пакета.
  Описание: Если коммутатор не получает приветственные пакеты от соседнего устройства в течение интервала, соседнее устройство считается недоступным и недействительным.
- **Sending link-state packet delay**
  Диапазон: 1~65535 с
  По умолчанию: 1 с
  Функция: настроить задержку отправки LSA на указанном интерфейсе.
- **Sending link-state packet retransmit interval**
  Диапазон: 1~65535 с
  По умолчанию: 5 с
  Функция: Установите интервал для повторной передачи LSA соседним коммутаторам на указанном интерфейсе.
  Описание: после отправки LSA соседнему устройству коммутатор сохраняет LSA до тех пор, пока не получит подтверждение от соседнего устройства. Если коммутатор не получает подтверждение в течение интервала, он повторно передает LSA.

Настройки параметров должны быть согласованы между обоими концами виртуального канала.

Установить приоритет интерфейса VLAN

Щелкнуть [Device Basic Configuration] → [Route configuration] → [OSPF configuration] → [Other parameter configuration] → [Port DR priority configuration] для входа на страницу настройки приоритета интерфейса VLAN, как показано на рисунке ниже.



- **Priority**
  Диапазон: 0~255
  По умолчанию: 1
  Функция: установка приоритета интерфейса VLAN с поддержкой OSPF.
  Описание: При выборе DR и BDR в качестве DR выбирается переключатель с наибольшим значением этого параметра.

Просмотрт OSPF информации

Щелкнуть [Device Basic Configuration] → [Route configuration] → [OSPF configuration] → [OSPF debug] → [show ip ospf] для входа на информационную страницу OSPF, как показано на рисунке ниже.

OSPF information

my router ID	192.168.0.22
preference	110
ase preference	150
export metric	1
export tag	2147483648

Просмотр информации о внешнем маршруте OSPF.

Щелкнуть [Device Basic Configuration] → [Route configuration] → [OSPF configuration] → [OSPF debug] → [show ip ospf ase] для входа на страницу информации о внешнем маршруте OSPF, как показано на рисунке ниже.

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

Просмотр OSPF статистики

Щелкнуть [Device Basic Configuration] → [Route configuration] → [OSPF configuration] → [OSPF debug] → [show ip ospf cumulative] для входа на страницу статистики OSPF, как показано на рисунке ниже.

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

Просмотр информации базы данных OSPF

Щелкнуть [Device Basic Configuration] → [Route configuration] → [OSPF configuration] → [OSPF debug] → [show ip ospf database] для входа на информационную страницу базы данных OSPF, как показано на рисунке ниже.

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	0x800001ee	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	0x80000229	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	0x80000020	1	64896

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	26614
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	748	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	8403
4.4.4.255	1.1.1.1	319	0x80000001	65535	63571
3.3.3.0	1.1.1.1	319	0x80000008	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	2896

AS External LSAs									
LS ID(ASBR's Rtr ID)	ADV rtr	Age	Sequence	Cost	Checksum	ls_type	metric	ase_type	forward	tag

Просмотрт соседей OSPF

Щелкнуть [Device Basic Configuration] → [Route configuration] → [OSPF configuration] → [OSPF debug] → [show ip ospf neighbor] для входа на страницу информации о соседнем OSPF, как показано на рисунке ниже.

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

Просмотр информации OSPF маршрутизации

Щелкнуть [Device Basic Configuration] → [Route configuration] → [OSPF configuration] → [OSPF debug] → [show ip ospf routing] для входа на страницу информации о маршрутизации OSPF, как показано на рисунке ниже.

OSPF routes information

AS internal routes

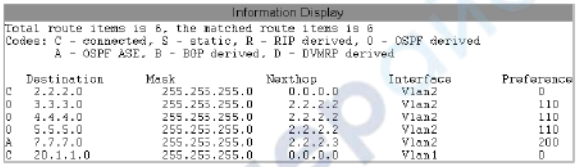
Destination	Area	Cost	Dest Type	Next Hop	ADV rtr
20.1.1.0	4	1	DTYPE_NET	20.1.1.1	1.1.1.1
2.2.2.0	0	1	DTYPE_NET	2.2.2.1	2.2.2.2
3.3.3.0	0	2	DTYPE_NET	2.2.2.2	2.2.2.2
5.5.5.0	0	4	DTYPE_NET	2.2.2.2	3.3.3.3
4.4.4.0	0	3	DTYPE_NET	2.2.2.2	3.3.3.3

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

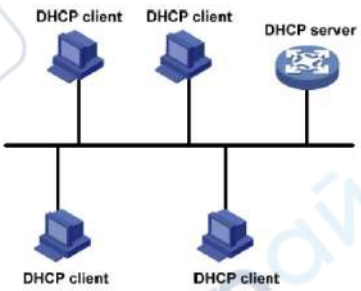
Просмотр записей маршрутов

Щелкнуть [Device Basic Configuration] → [Route configuration] → [OSPF configuration] → [show ip route] для входа на страницу информации о маршрутизации, как показано на рисунке ниже.



6.14. Конфигурация DHCP

С постоянным расширением масштаба сети и ростом сложности сети, в условиях частого перемещения компьютеров (таких как ноутбуки или беспроводная сеть) и количества компьютеров, превышающих выделяемые IP-адреса, протокол BootP, специально предназначенный для статического хоста. конфигурация становится все более неспособной 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. DHCP (протокол динамической конфигурации хоста) был введен для решения этих проблем. DHCP использует модель связи клиент-сервер. Клиент отправляет запрос конфигурации на сервер, а затем сервер отвечает на параметры конфигурации, такие как IP-адрес, клиенту, достигая динамической конфигурации IP-адресов. Структура типичного приложения DHCP показана на рисунке ниже.



В процессе динамического получения IP-адресов сообщения передаются способом 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 ретранслятор DHCP, чтобы получить IP-адреса и другие 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 связывающие IP-адреса клиентам по DHCP. Динамическое выделение: DHCP-сервер 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 применить IP-адрес. Сетевой администратор может выбрать механизм распределения DHCP для каждого клиента.

6.14.1. Конфигурация DHCP Server

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. В следующих случаях DHCP-сервер обычно используется для выделения IP-адресов.

- Большой масштаб сети. Рабочая нагрузка ручной настройки велика, и трудно управлять всей сетью.
- Количество хостов превышает количество назначаемых IP-адресов, и он не может выделить фиксированный IP-адрес каждому хосту.
- Только несколько хостов в сети нуждаются в фиксированных IP-адресах.

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

- IP-адрес статически привязан к MAC-адресу клиента.
- IP-адрес, записанный на DHCP-сервере, который когда-либо был выделен клиенту.
- IP-адрес, указанный в сообщении запроса, отправленном от клиента.
- Первый выделяемый IP-адрес, найденный в пуле адресов.
- Если нет доступного IP-адреса, проверьте IP-адрес, срок аренды которого истекает и который имел конфликты по порядку. Если найдено, выделите IP-адрес. Если нет, то нет процесса.

6.14.2. Веб конфигурирование

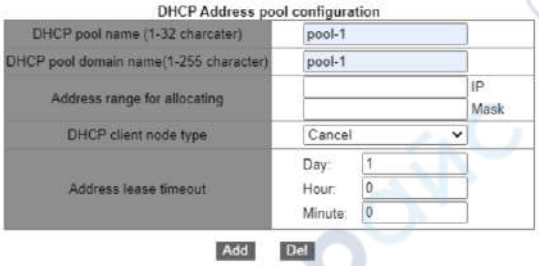
Включение DHCP сервера

Щелкнуть [Device Basic Configuration] → [DHCP configuration] → [DHCP server configuration] → [Enable DHCP] для входа на страницу включения DHCP сервера, как показано на рисунке ниже.

- **DHCP server status**
  Опция: Opne / Close
  По умолчанию: Close
  Функция: выберите текущий коммутатор для DHCP-сервера, чтобы выделить IP-адрес клиенту или нет.

Выделение статического IP адреса

Щелкнуть [Device Basic Configuration] → [DHCP configuration] → [DHCP server configuration] → [Address pool configuration] для создания DHCP адресного пула, как показано на рисунке ниже.



- **DHCP pool name**
  Диапазон: 1~32 символа
  Функция: настроить имя пула IP-адресов.
- **DHCP pool domain name**
  Диапазон: 1~255 символов
  Функция: настроить доменное имя пула IP-адресов. При назначении IP-адреса клиенту также отправьте клиенту суффикс доменного имени.
- **Address lease timeout**
  Диапазон: 0 дней 0 часов 0 минут ~ 365 дней 23 часов 59 минут
  Описание. Тайм-аут аренды статического выделения бесконечен. Конфигурация этого параметра недопустима для статического распределения.

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 перед статически выделенным IP-адресом.
Для каждого пула адресов DHCP можно настроить только один тип механизма распределения IP-адресов.

Щелкнуть [Device Basic Configuration] → [DHCP configuration] → [DHCP server configuration] → [Manual address pool configuration] для входа на страницу назначения статического адреса, как показано на рисунке ниже.

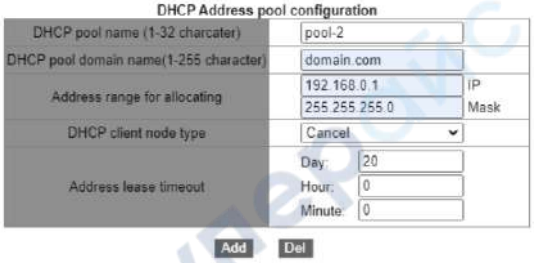
- **DHCP pool name**
  Функция: выбрать имя созданного пула.
- **Hardware address**
  Формат: HH-HH-HH-HH-HH-HH (H — шестнадцатеричное число)
  Функция: Настройка MAC-адреса клиента со статическим ограничением.
- **Client IP**
  Формат: A.B.C.D.
  Функция: Настройка IP-адреса клиента со статическим ограничением.
  Описание. Статическое выделение IP-адресов 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. Обычно он настроен на 255.255.255.0.
- **User name**
  Диапазон: 1~255 символов
  Функция: Настройка имени пользователя клиента.

Динамическое назначение IP адреса

Щелкнуть [Device Basic Configuration] → [DHCP configuration] → [DHCP server configuration] → [Address pool configuration] для входа на страницу конфигурации динамического распределения, как показано на рисунке ниже.



- **DHCP pool name**
  Диапазон: 1~32 символа
  Функция: настроить имя пула IP-адресов.
- **DHCP pool domain name**
  Диапазон: 1~255 символов
  Функция: настроить доменное имя пула IP-адресов. При назначении IP-адреса клиенту также отправьте клиенту суффикс доменного имени.
- **Address range of allocating {IP, MASK}**
  Функция: Настройте диапазон пула IP-адресов, а диапазон адресов определяется маской подсети. Маска подсети представляет собой число длиной 32 бита, состоящее из строки 1 и строки 0. «1» соответствует полям номера сети и полям номера подсети, а «0» соответствует полям номера хоста. Обычно он настроен на 255.255.255.0.

В каждом пуле адресов можно настроить только один сегмент адреса.

- **DHCP client node type**
  Опция: Cancel / Broadcast node / Peer-to-peer node / Mixed node / Hybrid node
  По умолчанию: Cancel
  Функция: Настройка типа клиентского узла NetBIOS, выделенного DHCP-сервером. Когда DHCP-клиент использует протокол NetBIOS для связи в сети, необходимо установить сопоставление между именем хоста и IP-адресом. Различные типы узлов получают отображение в разных режимах.
  Описание: Широковещательный узел получает отображение в широковещательном режиме. Одноранговый узел получает сопоставление,

отправляя одноадресный пакет для связи с WINS-сервером. Смешанный узел получает отображение, посылая широковещательный пакет в первый раз. Если смешанный узел не может получить сопоставление в первый раз, он получает сопоставление, отправляя 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 гибридному узлу не удается получить сопоставление в первый раз, он получает сопоставление, отправив широковещательный пакет во второй раз.

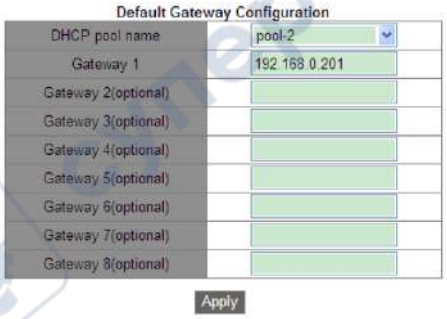
- **Address lease timeout**

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

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

Конфигурирование DHCP шлюза клинета

Щелкнуть [Device Basic Configuration] → [DHCP configuration] → [DHCP server configuration] → [Default Gateway Configuration] для входа на страницу конфигурации шлюза DHCP-клиента, как показано на рисунке ниже.



- **DHCP pool name**

  Функция: выбрать имя созданного пула.

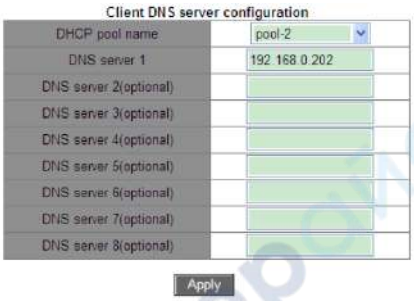
- **Gateway 1~Gateway 8**

  Функция: настроить адрес клиентского шлюза, выделенный DHCP-сервером.

  Объяснение: когда DHCP-клиент посещает хост, находящийся в другом сегменте, данные должны пересылаться через шлюзы. Когда DHCP-сервер выделяет IP-адреса клиентам, он может одновременно указывать адреса шлюза. Пул адресов DHCP может настроить до 8 шлюзов. Шлюз 1 имеет наивысший приоритет, а шлюз 8 — наименьший.

Конфигурирование DHCP-клиента DNS-сервера

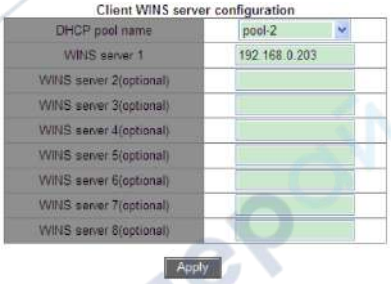
Щелкнуть [Device Basic Configuration] → [DHCP configuration] → [DHCP server configuration] → [Client DNS server configuration] для входа на страницу конфигурации DNS-сервера DHCP-клиента, как показано на рисунке ниже.



- **DHCP pool name**
  Функция: выбрать имя созданного пула.
- **DNS server 1~DNS server 8**
  Функция: Настройка адреса клиентского DNS-сервера, назначенного DHCP-сервером.
  Объяснение: При посещении сетевого узла через доменное имя доменное имя должно быть преобразовано в IP-адрес, который реализуется DNS (системой доменных имен). Чтобы DHCP-клиент мог посещать сетевой хост через доменное имя, когда DHCP-сервер выделяет IP-адреса клиентам, он может одновременно указывать IP-адреса серверов доменных имен. Пул адресов DHCP может настроить максимум 8 DNS-серверов. DNS-сервер 1 имеет наивысший приоритет, а DNS-сервер 8 — самый низкий приоритет.

Конфигурирование DHCP-клиента WINS-сервера

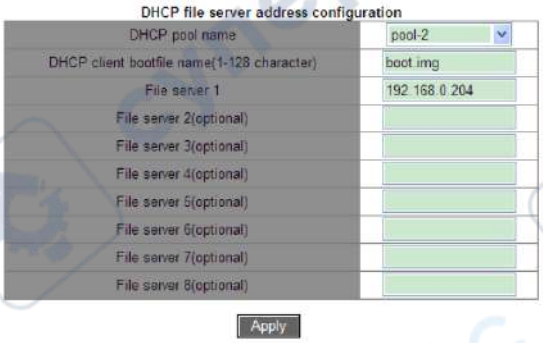
Щелкнуть [Device Basic Configuration] → [DHCP configuration] → [DHCP server configuration] → [Client WINS server configuration] для входа на страницу конфигурации WINS-сервера DHCP-клиента, как показано на рисунке ниже.



- **DHCP pool name**
  Функция: выбрать имя созданного пула.
- **WINS server 1~WINS server 8**
  Функция: Настройка адреса клиентского WINS-сервера, выделенного DHCP-сервером. Объяснение: 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 для связи протокол NetBIOS. Поэтому для большинства клиентов на базе ОС Windows требуется настройка WINS. Чтобы DHCP-клиент мог преобразовать имя хоста в IP-адрес, укажите адрес WINS-сервера, когда DHCP-сервер выделяет IP-адрес клиенту. Пул адресов DHCP может настроить до 8 серверов WINS. WINS-сервер 1 имеет наивысший приоритет, а WINS-сервер 8 — самый низкий приоритет.

Настройка DHCP-клиент, адрес TFTP-сервера и имя загрузочного файла.

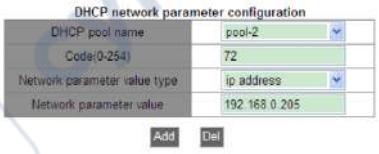
Щелкнуть [Device Basic Configuration] → [DHCP configuration] → [DHCP server configuration] → [DHCP file server address configuration] для ввода адреса DHCP-клиента TFTP-сервера и страницы конфигурации имени загрузочного файла, как показано на рисунке ниже.



- **DHCP pool name**
  Функция: выбрать имя созданного пула.
- **DHCP client bootfile name**
  Имя загрузочного файла DHCP-клиента
  Диапазон: 1~128 символов
  Функция: Настройка имени файла запуска клиента, назначенного DHCP-сервером. При запуске бездискового устройства файл запуска должен быть загружен с сервера, а затем импортирован.
- **File server 1~File server 8**
  Функция: Настройка адреса клиентского TFTP-сервера, выделенного DHCP-сервером. Пул адресов DHCP может настроить до 8 файловых серверов. Файловый сервер 1 имеет наивысший приоритет, а файловый сервер 8 — самый низкий.

Конфишурирование сетевых параметров DHCP.

Щелкнуть [Device Basic Configuration] → [DHCP configuration] → [DHCP server configuration] → [DHCP network parameter configuration] для входа на страницу конфигурации сетевых параметров DHCP, как показано на рисунке ниже.



- **DHCP pool name**
  Функция: выбрать имя созданного пула.
- **Code**
  Диапазон: 0~254
  Функция: настройка опции 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.

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 настроены как эти общие параметры.

- **Network parameter value type**
  Опции: ascii / hex / ip-адрес
  Функция: Настройка типа значения сетевого параметра. ascii — это строка символов ascii, и ее диапазон конфигурации составляет от 1 до 255 символов. Hex — это шестнадцатеричное число, и длина его конфигурации 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.

Запрос конфигурации пула адресов DHCP

Щелкнуть [Device Basic Configuration] → [DHCP configuration] → [DHCP server configuration] → [Query DHCP address pool information] для запроса конфигурации пула адресов DHCP, как показано на рисунке ниже.

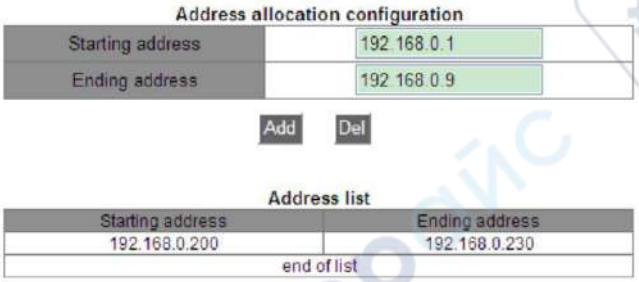
DHCP Adress Pool Information

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)

- **DHCP pool name**
  Функция: выбрать имя созданного пула.

Настройка диапазона IP-адресов, не выделяемых динамически в DHCP-адрес пуле.

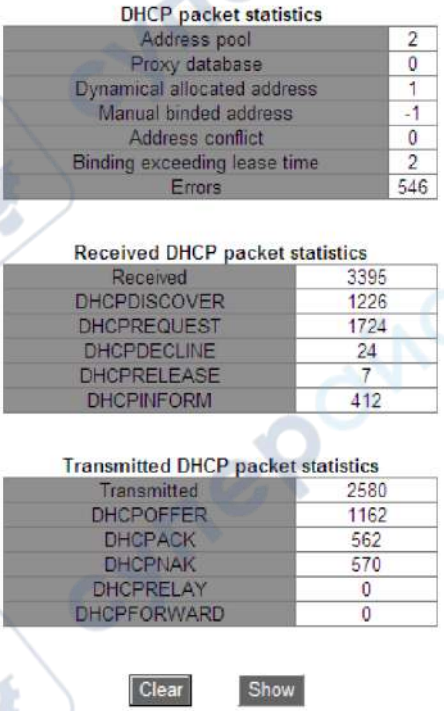
Щелкнуть [Device Basic Configuration] → [DHCP configuration] → [DHCP server configuration] → [Excluded address configuration] для входа в конфигурацию исключенного адреса на странице, как показано на рисунке ниже.



- **Starting address/Ending address**
  Функция: настроить диапазон IP-адресов, которые не распределяются динамически в DHCP. пул адресов. При распределении IP-адресов DHCP-сервер должен устранять занятые 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.

Просмотр статитстики DHCP пакетов.

Щелкнуть [Device Basic Configuration] → [DHCP configuration] → [DHCP server configuration] → [DHCP packet statistics] для просмотра DCHP статитстики, как показано на рисунке ниже.



Вы можете нажать кнопку <Show>, чтобы обновить статистику пакетов данных DHCP в режиме реального времени, и вы можете нажать кнопку <Clear>, чтобы очистить статистику полученных / отправленных пакетов данных DHCP.

Просмотр инфомрациии о привязке IP-MAC

Щелкнуть [Device Basic Configuration] → [DHCP configuration] → [DHCP debugging] → [Show IP-MAC binding] просмотеть информации о приязке IP-MAC можно, как показано на рисунке ниже.

6.15. Конфигурация ACL

Список управления доступом (Access Control List - ACL) позволяет пользователям настраивать правила сопоставления и режим обработки для пакетов во входящем направлении порта коммутатора для фильтрации пакетов. Он направлен на эффективное предотвращение доступа неавторизованных пользователей к сети, контроль трафика и экономию сетевых ресурсов.

Запись ACL может содержать несколько правил, и в каждом правиле можно указать параметры сопоставления пакетов и обработки пакетов. Перед настройкой правила необходимо создать запись ACL. В нескольких правилах в одной записи ACL правило с меньшим идентификатором правила предшествует правилу с большим идентификатором правила. Действие сопоставления пакетов начинается с первого правила до тех пор, пока пакеты не будут соответствовать правилу, а последующие правила не будут использоваться для сопоставления.

Записи ACL могут применяться к портам, виртуальным локальным сетям 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 глобальному ACL. 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.

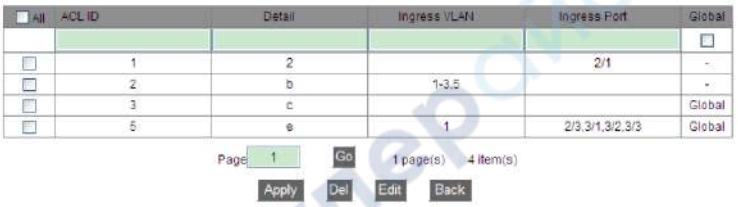
Запись ACL представляет собой набор из одного или нескольких правил. Следовательно, после применения записи ACL к порту / VLAN / глобально все правила, содержащиеся в этой записи ACL, будут применяться к порту / VLAN / глобально.

По умолчанию ACL, применяемый к порту / VLAN / глобально, вступает в силу раньше, чем ACL, который должен применяться к тому же порту / VLAN / глобально, но выдается позже. Пользователи могут настроить приоритет записей ACL по мере необходимости.

6.15.1. Веб конфигурирование

Конфигурирование записи ACL

Щелкнуть [Device Basic Configuration] → [ACL configuration] → [ACL Base Configuration] для конфигурирования записи ACL, как показано на рисунке ниже.



- **ACL ID**
  Диапазон: 1~1024
  Функция: Настройка идентификатора ACL. Данный тип коммутатора поддерживает до 512 записей ACL. Если запись ACL применяется к нескольким портам, она применяется к каждому из портов. Аналогичным образом, если запись ACL применяется к нескольким VLAN, она применяется к каждой из VLAN.
  Описание. Если запись ACL применяется к нескольким непрерывным портам или сетям VLAN, порты или сети VLAN могут быть разделены дефисом (-). Если запись ACL применяется к нескольким прерывистым портам или сетям VLAN, порты или сети VLAN могут быть разделены запятой (,).

Существуют некоторые системные записи ACL, и пользователи фактически могут 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.

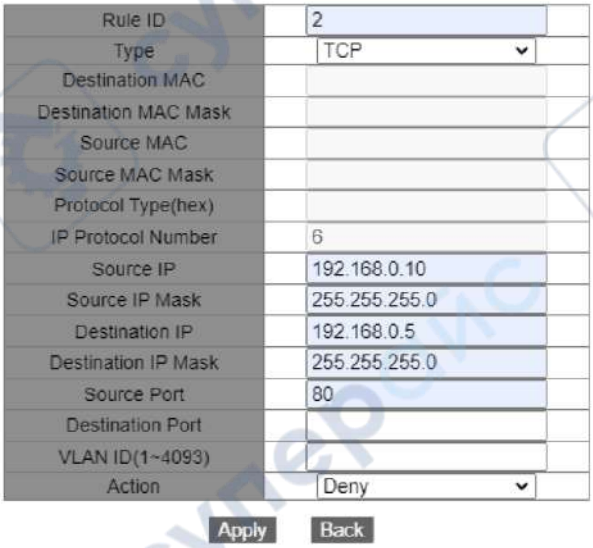
Редактирование ACL записи показано на рисунке ниже

Выберите запись ACL, нажмите <Del>, чтобы удалить запись ACL; щелкните <Изменить>, чтобы изменить конфигурацию записи ACL.

Добавление правила в ACL запись

Щелкните созданную запись ACL чтобы открыть возможность добавление правил (смотри рисунок ниже), нажмите <Добавить правило>, чтобы настроить правило для записи ACL.

Настройка правил для записи ACL, как показано на рисунке



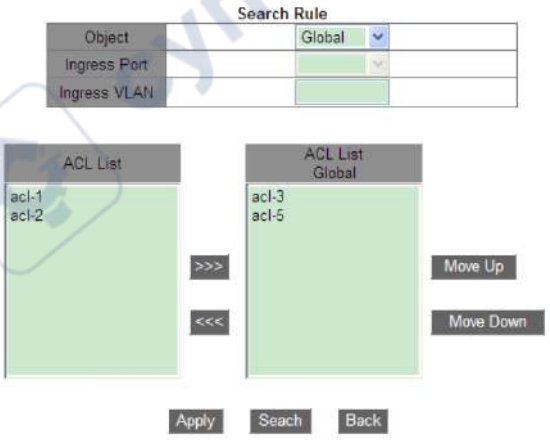
- **Rule ID**
  Диапазон: 1~1024
  Функция: Настройка идентификатора правила для записи ACL.
  Описание: Каждая запись ACL поддерживает максимум 512 правил, а общее количество правил во всех ACL не может превышать 512.
- **Type**
  Варианты: Customized/IGMP/ICMP/TCP/UDP/MAC
  По умолчанию: Customized
  Функция: Настройка типа пакета правила ACL.
- **Destination MAC/ Destination MAC Mask**
  Функция: Настройка MAC-адреса назначения. В маске MAC-адреса получателя **1** указывает на cared бит MAC-адреса получателя, а **0** указывает на игнорируемый бит MAC-адреса получателя.
- **Source MAC/ Source MAC Mask**
  Функция: Настройка исходного MAC-адреса. В маске MAC-адреса источника **1** указывает на cared 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 номера IP-протокола.
- **Source IP/ Source IP Mask**

Функция: настройка исходного IP-адреса. В маске исходного IP-адреса 1 указывает на заботливый бит IP-адреса источника, а 0 указывает на игнорируемый бит исходного IP-адреса.

- **Destination IP/ Destination IP Mask**
  Функция: настройка IP-адреса назначения. В маске IP-адреса назначения 1 указывает на заботливый 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 идентификатора VLAN.
- **Action**
  Опции: Permit / Deny / Mirror to CPU / Mirror to Port / Redirect to CPU / Redirect to Port
  По умолчанию: Permit
  Функция: настроить режим обработки пакетов для успешно сопоставленных пакетов.
  Описание: **Permit** указывает на получение успешно согласованных 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 сопоставленных 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.

Запрос записи ACL

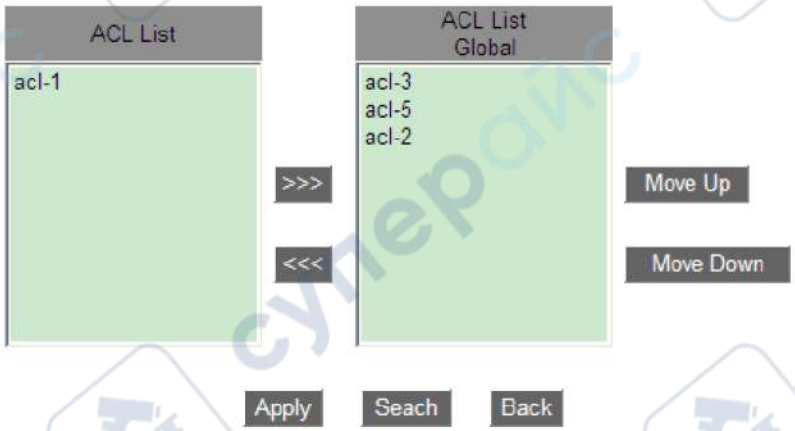
Щелкнуть [Device Basic Configuration] → [ACL configuration] → [ACL Search] для запроса записи ACL, как показано на рисунке ниже.



- **Object**
  Опции: Global / Port / VLAN
  Функция: выберите область применения запрашиваемых записей ACL.
- **Ingress Port**
  Функция: выберите порт приложения для записей ACL, которые будут запрашиваться, когда для параметра «**Object**» установлено значение «**Port**».
- **Ingress VLAN**
  Функция: выберите прикладную VLAN из записей ACL, которые будут запрашиваться, когда для параметра **Object** установлено значение **VLAN**.

Список ACL в нижней правой части показывает найденные записи ACL.

Доставьте записи ACL в объект и настройте приоритет для записей ACL. как показано на рисунке.



Переместите запись ACL, которую нужно применить к объекту, в список ACL справа. Выберите запись и нажмите <Переместить вверх> или <Переместить вниз>, чтобы изменить приоритет записей ACL, применяемых к объекту. Записи ACL сверху вниз в списке расположены в порядке убывания.

6.16. Конфигурация QoS

Качество обслуживания (Quality of Service - QoS) позволяет предоставлять дифференцированные услуги на основе различных требований при ограниченной пропускной способности посредством управления трафиком и распределения ресурсов в IP-сетях. QoS пытается удовлетворить передачу различных услуг, чтобы уменьшить перегрузку сети и свести к минимуму влияние перегрузки на услуги с высоким приоритетом.

QoS в основном включает в себя идентификацию услуг, управление перегрузками и предотвращение перегрузок.

Идентификация службы: объекты идентифицируются на основе определенных правил соответствия. Например, объекты могут быть тегами приоритета, переносимыми пакетами, приоритетом, отображаемым портами и виртуальными локальными сетями, или информацией о приоритете, отображаемой пятерками. Идентификация услуги является 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. Предотвращение перегрузки отслеживает использование сетевых ресурсов. При обнаружении увеличения перегрузки функция использует упреждающее отбрасывание пакетов и настраивает объем трафика для решения проблемы перегрузки.

6.16.1. QoS 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 (ширина и значение пакета), предусмотренного политикой QoS в пакете.

6.16.2. QoS Remark

QoS Remark цитирует правило ACL для идентификации потока и снова указывает приоритет (значение DSCP или COS) для соответствующего пакета.

6.16.3. Принципы

Каждый порт коммутаторов этой серии поддерживает 8 очередей кэширования, от 0 до 7 в порядке возрастания приоритета. Вы можете 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 отображения 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 (взвешенный циклический алгоритм) и очередь с приоритетом.

- WRR планирует потоки данных на основе коэффициента веса. Очереди получают свою пропускную способность на основе соотношения весов. WRR отдает приоритет очередям с высоким соотношением веса. Больше пропускной способности выделяется очередям с более высоким коэффициентом веса.
- Режим планирования очереди с приоритетом может строго гарантировать наивысший приоритет пересылки для пакета с наивысшим приоритетом, который в основном используется при передаче конфиденциального 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, она может начать обработку данных в очереди с более низким приоритетом.

6.16.4. Веб конфигурирование

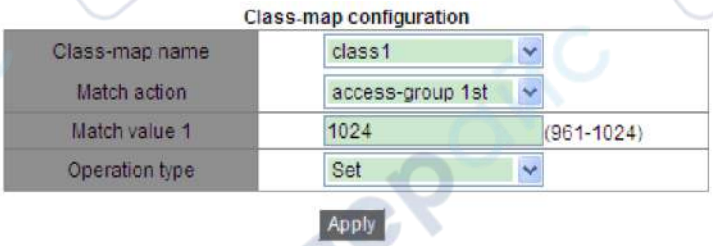
Включение QoS функции

Щелкнуть [Device Basic Configuration] → [QoS configuration] → [Enable QoS] -> [Enable/Disable QoS] для включяения QoS, как показано на рисунке ниже.

- **Class-map name**
  Диапазон: 1~16 символов
  Функция: Настройка имени карты классов. Нажмите <Add> / <Del>, чтобы создать/удалить таблицу классов.

Настройка действий сопоставления карты классов

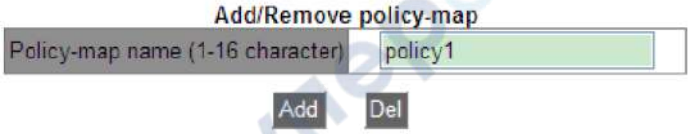
Щелкнуть [Device Basic Configuration] → [QoS configuration] → [Class-map configuration] –> [Class-map configuration] для входа на страницу конфигурации карты классов, как показано на рисунке ниже.



- **Class-map name**
  Параметры: Все созданные карты классов
- **Match action**
  По умолчанию: группа доступа 1st
  Функция: настроить действие сопоставления карты классов.
- **Match value 1**
  Диапазон: 961~1024
  Функция: соответствует указанной записи ACL. Для сопоставленной таблицы ACL действие должно быть разрешено.
- **Operation type**
  Опции: Set / Del
  Функция: установить / удалить действие сопоставления карты классов.

Добавить / удалить policy-map

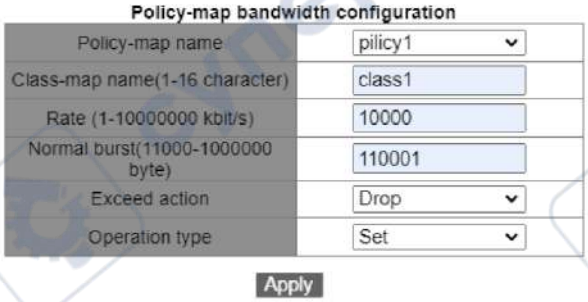
Щелкнуть [Device Basic Configuration] → [QoS configuration] → [Policy-map configuration] –> [Add/Remove policy-map] чтоб добавить / удалить police-map, как показано на рисунке ниже.



- **Policy-map name**
  Диапазон: 1~16 символов
  Функция: Настройка имени карты политик. Нажмите <Add>/<Del>, чтобы создать/удалить таблицу политик.

Конфигурирование пропускной способности policy-map

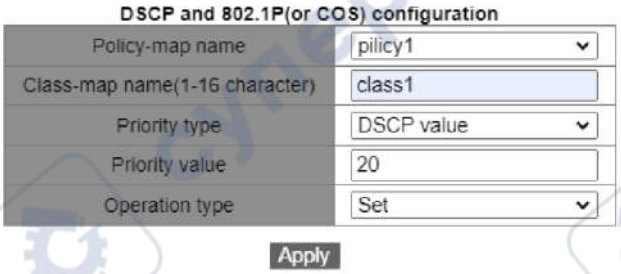
Щелкнуть [Device Basic Configuration] → [QoS configuration] → [Policy-map configuration] –> [Policy-map bandwidth configuration] для входа на страницу настройки пропускной способности policy-map, как показано на рисунке ниже.



- **Policy-map name**
  Опции: Все созданные карты политик.
- **Class-map name**
  Параметры: Все созданные карты классов
- **Rate**
  Диапазон: 1-10000000 кбит/с
  Функция: Настройка значения скорости.
- **Normal burst**
  Диапазон: 11000-1000000 байт
  Функция: Настройка нормального значения пакета.
- **Exceed action**
  Варианты: падение
  Функция: Выполнение политики отбрасывания пакетов для части, превышающей предельное значение скорости в действии сопоставления встречи пакетов в карте классов.
- **Operation type**
  Опции: Set / Del
  Функция: установка / удаление конфигурации пропускной способности карты политик.

Настройка приоритетной перемаркировки policy-map

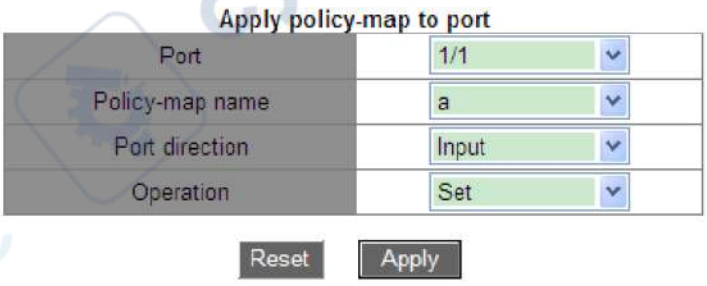
Щелкнуть [Device Basic Configuration] → [QoS configuration] → [Policy-map configuration] –> [Policy-map priority configuration] для входа на страницу настройки приоритета policy-map, как показано на рисунке ниже.



- **Policy-map name**
  Опции: Все созданные карты политик.
- **Class-map name**
  Опции: Все созданные карты классов.
- **Priority type**
  Опции: значение DSCP / значение COS
  Функция: выберите тип приоритета, который необходимо отметить.
- **Priority value**
  Опции: 0–63 (значение DSCP) / 0–7 (значение COS)
  Функция: Настройка значения перемаркировки приоритета.
  Описание: Выполнение политики перемаркировки для значения приоритета в действии сопоставления пакетов на карте классов.
- **Operation type**
  Опции: Установить/Удалить
  Функция: установка/удаление примечания приоритета карты политик.

Применение policy-map для порта

Щелкнуть [Device Basic Configuration] → [QoS configuration] → [Apply QoS to the port] –> [Apply policy-map to port] чтобы применить policy-map на порт, как показано на рисунке ниже.



- **Policy-map name**
  Опции: Все созданные карты политик.
- **Port direction**

Опции: ввод

Функция: Примените эту таблицу политик во входном направлении порта, чтобы реализовать ограничение скорости или перемаркировку приоритета для пакета, полученного через порт.

- **Operation type**
  Опции: Set / Del
  Функция: установить/удалить карту политик приложения на порт.

Примените к порту только одну карту политик.
Конфигурация режима доверия порта и сопоставление политики приложения с портом являются взаимоисключающими.

Конфигурирование trust mode на порту

Щелкнуть [Device Basic Configuration] → [QoS configuration] → [Apply QoS to port] –> [Port trust mode configurationion] для входа на страницу конфигурации режима доверия порта, как показано на рисунке ниже.

- **Port**
  Опции: все порты коммутатора
- **Port trust status**
  Варианты: cos / cos и pass through dscp / dscp / dscp и 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, а нетегированный пакет, порт не имеет режима доверия по умолчанию и сохранит пакет в очереди 0.
  Функция: настроить статус доверия портов коммутатора.
  Описание: **cos** и **cos** и **pass through dscp** означают значение CoS доверия порта. Очередь для сохранения полученного портом пакета определяется значением CoS и отображением очереди. Если пакет не имеет значения CoS, он сопоставляется с очередью в соответствии со значением CoS, равным 0. Различия между **cos** и **cos** и **pass through dscp** заключаются в том, что **cos** изменит значение DSCP пакета на значение, указанное в сопоставлении между CoS. и DSCP во время пересылки пакетов, но **cos** и **pass through dscp** не изменяют значение DSCP пакета во время пересылки пакетов.
  dscp и **dscp** и **pass through cos** означают значение DSCP доверия порта. Очередь для сохранения пакета, полученного портом, определяется значением DSCP и отображением очереди. Если пакет не имеет значения DSCP, он сопоставляется с очередью в соответствии со значением DSCP, равным 0. Различия между **dscp** и **dscp** и **pass through cos** заключаются в том, что dscp изменит значение CoS пакета на значение, указанное в сопоставлении между DSCP. и CoS во время пересылки

пакетов, но **dscp** и **pass through cos** не изменяют значение CoS пакета во время пересылки пакетов.

Port priority

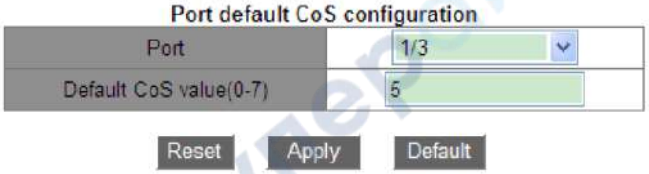
Варианты: 0~7

По умолчанию: 0

Функция: назначить приоритет физическому порту. Пакеты, полученные от порта, ставятся в очередь в соответствии с назначенным приоритетом, но 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 сделать таким же образом.

Настройте значение CoS порта по умолчанию

Щелкнуть [Device Basic Configuration] → [QoS configuration] → [Apply QoS to port] –> [Port default CoS configuration] для входа на страницу конфигурации CoS порта по умолчанию, как показано на рисунке ниже.



- **Port**

  Опции: все порты коммутатора

  Значение CoS по умолчанию

  Варианты: 0~7

  По умолчанию: 0

  Функция: Настройка значения CoS по умолчанию для порта.

  Объяснение: Когда пакет не помечен, приоритет в теге, добавленном к пакету, равен значению CoS по умолчанию для порта.

Настройте режим планирования очереди портов на приоритетную очередь

Щелкнуть [Device Basic Configuration] → [QoS configuration] → [Egress-queue configuration] –> [Port Egress-queue work mode configuration] для входа на страницу конфигурации режима приоритетной очереди, как показано на рисунке ниже.

- **Egress-queue Work Mode**

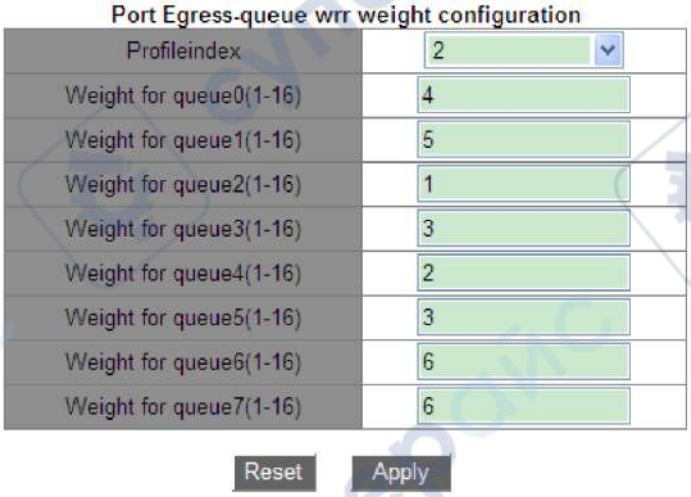
  Опции: PQ / WRR

  По умолчанию: PQ

  Функция: настроить режим исходящей очереди для выбранного порта.

Настройка веса WRR очереди порта

Щелкнуть [Device Basic Configuration] → [QoS configuration] → [Egress-queue configuration] –> [Port Egress-queue wrr weight configuration] для входа на страницу конфигурации веса WRR, как показано на рисунке ниже.



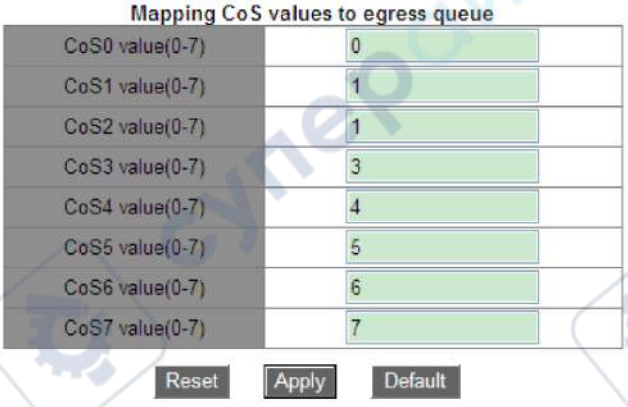
- **Profileindex**
  Варианты: 1~6
  По умолчанию: 1
  Функция: Настройка группы значений веса.
  Объяснение: Коммутатор поддерживает не более 6 групп значений веса.
- **{Weight for queue0, Weight for queue1, Weight for queue2, Weight for queue3, Weight for queue4, Weight for queue5, Weight for queue6, Weight for queue7}**
  Варианты: {0~15, 0~15, 0~15, 0~15, 0~15, 0~15, 0~15, 0~15}
  По умолчанию: {1, 2, 3, 4, 5, 6, 7, 8}
  Функция: Настройка значений веса. 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 со значением веса 0 и в очереди с высоким приоритетом, а второй приоритет отдается данным со значением веса 0 и в очереди с высоким приоритетом. очередь с низким приоритетом. Когда пересылаются все данные со значением веса 0, коммутатор начинает пересылать данные в другие очереди в соответствии с коэффициентом веса.

Установите режим планирования очереди портов на WRR и привяжите весовой коэффициент к порту, как показано на рисунке

- **Port name**
  Опции: все порты коммутатора
  Функция: выберите порт, чтобы установить для него режим планирования WRR.
  Profileindex
  Варианты: 1~6
  Функция: Выберите коэффициент веса WRR порта.

Настройка сопоставления между значением CoS и очередью.

Щелкнуть [Device Basic Configuration] → [QoS configuration] → [Egress-queue configuration] –> [Mapping CoS values to egress queue] для входа на страницу конфигурации CoS и сопоставления очередей, как показано на рисунке ниже.



- **{COS value, Queue-ID}**
  Варианты: {0~7, 0~7}
  По умолчанию: значение CoS 0 сопоставлено 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: настроить сопоставление между значением CoS и очередью.
  Объяснение: Каждое значение CoS можно сопоставить только с одной очередью. Несколько значений CoS могут быть сопоставлены с одной очередью.

Настройки сопоставления между значением DSCP и очередью.

Щелкнуть [Device Basic Configuration] → [QoS configuration] → [Egress-queue configuration] –> [Mapping DSCP values to egress queue] для входа на страницу конфигурации DSCP и сопоставления очередей, как показано на рисунке ниже.

Mapping DSCP values to egress queue

DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
0	0	8	0	16	0	24	0	32	0	40	0	48	0	56	0
1	0	9	0	17	0	25	0	33	0	41	0	49	0	57	0
2	0	10	0	18	0	26	0	34	0	42	0	50	0	58	0
3	0	11	0	19	0	27	0	35	0	43	0	51	0	59	0
4	0	12	0	20	0	28	0	36	0	44	0	52	0	60	0
5	0	13	0	21	0	29	0	37	0	45	0	53	0	61	0
6	0	14	0	22	0	30	0	38	0	46	0	54	0	62	0
7	0	15	0	23	0	31	0	39	0	47	0	55	0	63	0

Set Default

- **{DSCP, Queue value}**
  Опции: {0~63, 0~7}
  По умолчанию:
  Значение DSCP 0–7 отображается в очередь 0; Значение DSCP 8~15 сопоставляется с очередью 1;
  Значение DSCP 16~23 сопоставлено с очередью 2; Значение DSCP 24~31 сопоставляется с очередью 3; Значение DSCP 32~39 сопоставлено с очередью 4; Значение DSCP 40~47 сопоставлено с очередью 5; Значение DSCP 48~55 сопоставлено с очередью 6; Значение DSCP 56~63 сопоставляется с очередью 7.
  Функция: Настройка сопоставления между значением DSCP и очередью.
  Объяснение: Каждое значение DSCP можно сопоставить только с одной очередью. Несколько значений DSCP могут быть сопоставлены с одной очередью.
  Нажмите <Set>, чтобы установить новое сопоставление между значением DSCP и очередью, <Del>, чтобы восстановить сопоставление по умолчанию между значением DSCP и очередью.

Настройка сопоставление между значением CoS и значением DSCP.

Щелкнуть [Device Basic Configuration] → [QoS configuration] → [QoS mapping configuration] –> [CoS-to-DSCP mapping] для входа на страницу конфигурации сопоставления CoS и DSCP, как показано на рисунке ниже.

CoS-to-DSCP mapping

CoS value	0	1	2	3	4	5	6	7
DSCP value (0-63)	0	11	22	33	44	55	63	0

Set Del

- **DSCP value**
  Варианты: 0~63
  По умолчанию:
  Значение CoS 0 отображается на значение 0 DSCP; Значение CoS 1 отображается на значение 8 DSCP; Значение CoS 2 отображается на значение 16 DSCP; Значение CoS 3 отображается на значение DSCP 24; Значение CoS 4 отображается на значение DSCP 32; Значение CoS 5 отображается на значение DSCP 40; Значение CoS 6 отображается на значение 48 DSCP; Значение CoS 7 сопоставляется со значением DSCP 56.
  Функция: настроить отображение между CoS и DSCP. Когда режим доверия порта — CoS, значение DSCP пакета может быть изменено в соответствии с этим отображением.
  Объяснение: Одному значению DSCP можно сопоставить несколько значений CoS.

Нажмите <Set>, чтобы установить новое сопоставление между CoS и DSCP, <Del>, чтобы восстановить сопоставление по умолчанию между CoS и DSCP.

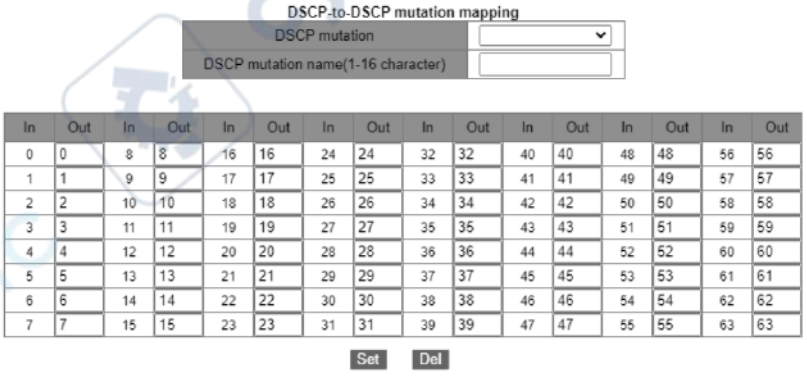
Настройка сопоставление между значением DSCP и значением CoS.

Щелкнуть [Device Basic Configuration] → [QoS configuration] → [QoS mapping configuration] –> [DSCP-to-CoS mapping] для входа на страницу конфигурации сопоставления DSCP с CoS, как показано на рисунке ниже.

- **{DSCP value, COS value}**
  Опции: {0~63, 0~7}
  По умолчанию: значение DSCP 0~7 отображается на значение CoS 0;
  Значение DSCP 8~15 отображается на значение CoS 1; Значение DSCP 16~23 отображается на значение CoS 2; Значение DSCP 24~31 отображается на значение CoS 3; Значение DSCP 32~39 отображается на значение CoS 4; Значение DSCP 40~47 отображается на значение CoS 5; Значение DSCP 48~55 отображается на значение CoS 6; Значение DSCP 56~63 отображается на значение CoS 7.
  Функция: настроить сопоставление между DSCP и CoS. Когда режим доверия порта — DSCP, значение CoS пакета может быть изменено в соответствии с этим отображением.
  Объяснение: Одному значению CoS можно сопоставить не более 8 значений DSCP.
  Нажмите <Set>, чтобы установить новое сопоставление между DSCP и CoS, <Del>, чтобы восстановить сопоставление по умолчанию между DSCP и CoS.

Настройка сопоставление между значением DSCP и значением DSCP.

Щелкнуть [Device Basic Configuration] → [QoS configuration] → [QoS mapping configuration] –> [DSCP-to-DSCP mutation mapping] для входа на страницу конфигурации сопоставления DSCP и DSCP, как показано на рисунке ниже.

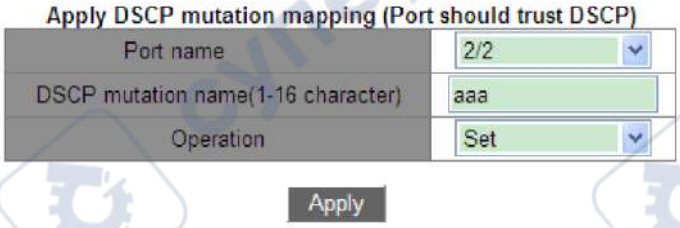


- **DSCP mutation name**
  Диапазон: 1~16 символов
  Функция: Установить имя для мутации DSCP.
- **{ In , Out }**
  Опции: {0~63, 0~63}
  Функция: настроить сопоставление между DSCP и DSCP. Чтобы изменить значение DSCP пакета, используйте это сопоставление, когда выход пересылает пакет.
  Объяснение: Одному значению DSCP можно сопоставить не более 8 значений DSCP. Нажмите <Set>, чтобы установить сопоставление между DSCP и DSCP, <Del>, чтобы удалить сопоставление между DSCP и DSCP. Коммутаторы этой серии поддерживают до 28 сопоставлений мутаций DSCP.

Очередь для сохранения пакетов определяется исходным сопоставлением между значением DSCP и очередью.

Применить сопоставление mutation DSCP на порту.

Щелкнуть [Device Basic Configuration] → [QoS configuration] → [Apply QoS to port] –> [Apply DSCP mutation mapping] для входа на страницу конфигурации, как показано на рисунке ниже.



- **Port name**
  Опции: все порты коммутатора
  Функция: выберите порт для использования картирования мутаций DSCP.
- **DSCP mutation name**
  Параметры: Имя DSCP для сопоставления DSCP.
  Функция: Настройка отображения mutation DSCP, используемого портом.
- **Operation**
  Опции: Set/Del
  Функция: добавление/удаление сопоставления мутаций DSCP, используемого портом.

6.17. Конфигурация IEC61850

В настоящее время коммутаторы прозрачны для других функциональных объектов в сетях подстанций. Для мониторинга коммутаторов необходимы инструменты, отличные от IEC61850, такие как EMS, Web, CLI 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 интеграции и управления, а также экономя строительство. и затраты на техническое обслуживание.

Файл моделирования по умолчанию switch.cid, предоставленный компанией, уже импортирован в коммутатор. Если заказчик хочет импортировать другие файлы моделирования, обратитесь к разделу «Служба передачи файлов».

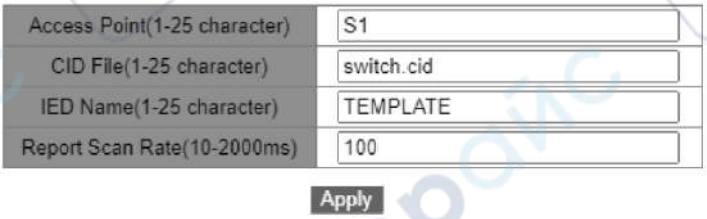
6.17.1. Веб конфигурирование

Включение IEC61850

Щелкнуть [Device Basic Configuration] → [IEC61850 Configuration] → [IEC61850 Configuration] для входа на страницу конфигурации IEC61850, как показано на рисунке ниже.

- **IEC61850 Function**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включение / выключение IEC61850 функции

Конфигурирование IEC61850



- **Access Point**
  Диапазон: 1~25 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 действительного 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.

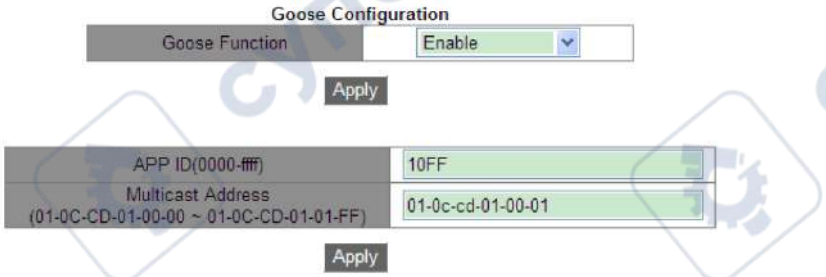
- **Report Scan Rate**
  Диапазон: 10~2000 мс
  По умолчанию: 100 мс
  Функция: настройка интервала сканирования информации об узле устройства.

Конфигурации имени точки доступа и устройства IED должны соответствовать имени точки доступа и устройства IED в указанном файле моделирования. В противном случае функция IEC61850 не может быть активирована.

6.18. Конфигурация GOOSE Trigger

GOOSE-Trigger определяет, следует ли подписываться на GOOSE-пакет, в соответствии с MAC-адресом получателя и идентификатором приложения GOOSE-пакета. Если устройство подписалось 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 переключается, он сообщает MMS REPORT).

Щелкните [Device Advanced Configuration] → [Goose configuration] → [Goose configuration] для входа на страницу конфигурации Goose, как показано на рисунке ниже.



- **Goose Function**
  Опции: Включить/Выключить
  По умолчанию: Отключить
  Функция: включение/выключение функции триггера GOOSE. Устройство может подписываться на пакеты GOOSE после включения функции Goose.
- **APP ID**
  Параметры: 0x0000~0xffff
  По умолчанию: 0x10ff
  Функция: Настройка идентификатора приложения GOOSE-пакетов, на которые необходимо подписаться. После включения триггера GOOSE устройство подпишется на пакеты GOOSE с идентификатором приложения, соответствующим конфигурации.
- **Multicast Address**
  Опции: 01-0C-CD-01-00-00~01-0C-CD-01-01-FF
  По умолчанию: 01-0C-CD-01-00-01
  Функция: настроить MAC-адрес GOOSE-пакетов, на которые следует подписаться. После включения триггера GOOSE устройство подпишется на пакеты GOOSE с MAC-адресом, соответствующим конфигурации.
  Диапазон: 64~1000000Кбит/с

6.19. IGMP Snooping

Отслеживание протокола группового управления Интернетом (Internet Group Management Protocol Snooping – IGMP Snooping) — 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.

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 запрашивающих, они автоматически выбирают тот, у которого наименьший IP-адрес, в качестве запрашивающего. Только выбранный запросчик периодически отправляет пакеты общего запроса IGMP. Другие запрашивающие только получают и пересылают пакеты запросов IGMP.

Router port: получает пакеты общего запроса (на коммутаторе с поддержкой IGMP) от запрашивающего. После получения отчета IGMP коммутатор устанавливает многоадресную запись и добавляет порт, который получает отчет IGMP, в список портов-членов. Если порт маршрутизатора существует, он также добавляется в список портов-членов. Затем коммутатор пересылает отчет IGMP другим устройствам через порт маршрутизатора, чтобы другие устройства установили ту же запись многоадресной рассылки.

IGMP Snooping управляет и поддерживает членов группы многоадресной рассылки путем обмена связанными пакетами между устройствами с поддержкой IGMP. Связанные пакеты следующие: Пакет общего запроса: запрашивающий периодически отправляет пакеты общего запроса (IP-адрес назначения: 224.0.0.1), чтобы подтвердить, есть ли в группе многоадресной рассылки порты-члены. После получения пакета запроса устройство, не являющееся запросчиком, пересылает пакет на все подключенные к нему порты.

Specific query packet: если устройство хочет выйти из группы многоадресной рассылки, оно отправляет пакет выхода IGMP. После получения пакета leave запрашивающий отправляет определенный пакет запроса (IP-адрес назначения: IP-адрес группы многоадресной рассылки), чтобы подтвердить, содержит ли группа другие порты-члены.

Membership report packet: если устройство хочет получить данные группы многоадресной рассылки, оно немедленно отправляет пакет отчета IGMP (IP-адрес назначения: IP-адрес группы многоадресной рассылки), чтобы ответить на пакет запроса IGMP группы. Пакет выхода: если устройство хочет покинуть группу многоадресной рассылки, оно отправит пакет выхода IGMP (IP-адрес назначения: 224.0.0.2).

6.19.1. Веб конфигурация

Включение IGMP Snooping

Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [IGMP Snooping configuration] –> [Enable IGMP Snooping] для входа на страницу глобальной конфигурации IGMP Snooping, как показано на рисунке ниже.

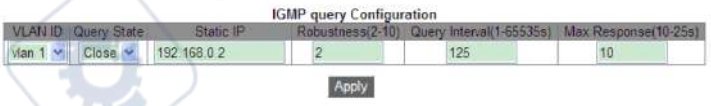
- **IGMP Snooping**
  Опции: Open / Close
  По умолчанию: Close
  Функция: Включить или отключить глобальный протокол IGMP Snooping. IGMP Snooping и GMRP нельзя включить одновременно.

Конфигурирование IGMP Snooping параметров

Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [IGMP Snooping configuration] –> [IGMP Snooping configuration] для входа на страницу конфигурации IGMP Snooping, как показано на рисунке ниже.

- **VLAN ID**
  Опции: все созданные идентификаторы VLAN.
- **Snooping state**
  Опции: Open / Close
  По умолчанию: Close
  Функция: включение или выключение функции отслеживания IGMP VLAN. Предпосылкой этого
  Функция состоит в том, чтобы включить глобальную функцию IGMP Snooping.
- **Static IP**
  Формат: A.B.C.D.
  По умолчанию: 192.168.0.2
  Функция: настроить исходный IP-адрес отправки пакетов.

Настройте параметры запроса IGMP, как показано на рисунке ниже.



- **VLAN ID**
  Опции: Все созданные идентификаторы VLAN.
  Функция: выберите идентификатор VLAN, чтобы включить функцию запроса IGMP.
- **Query State**
  Опции: Open / Close
  По умолчанию: Close
  Функция: включение или отключение функции запроса IGMP для выбранной VLAN.

предварительным условием этой функции является включение глобальной функции IGMP Snooping.

Описание: Если в сети есть несколько запрашивающих, они автоматически выберут тот, у которого наименьший IP-адрес, в качестве запрашивающего. Если есть только одно устройство, которое позволяет функцию запроса IGMP, это будет querier.

Функции Query и Snooping являются взаимоисключающими в VLAN. Это означает, что если запрос открыт, snooping должен быть закрыт в одном VLAN; если отслеживание открыто, запрос должен быть закрыт.

- **Static IP**
  Формат: A.B.C.D.
  По умолчанию: 192.168.0.2
  Функция: настроить исходный IP-адрес отправки пакета запроса.
- **Robustness**
  Диапазон: 2~10
  По умолчанию: 2
  Функция: укажите параметр надежности функции запроса IGMP.
  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: настроить максимальное время ответа на запрос пакета.
  Опции: Все созданные идентификаторы VLAN.

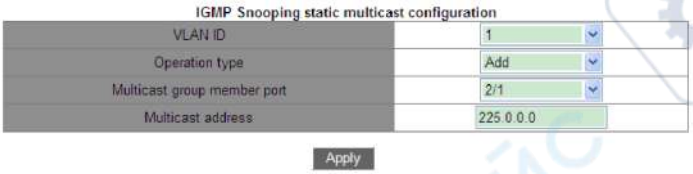
После завершения настройки в разделе «Конфигурация IGMP» отображается информация о конфигурации IGMP, показано на рисунке ниже.

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

Настройка статическиских параметров многоадресной рассылки IGMP Snooping.

Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [IGMP Snooping configuration] –> [IGMP Snooping static multicast configuration] для входа на страницу статической конфигурации IGMP Snooping, как показано на рисунке ниже.



- **VLAN ID**
  Опции: все созданные идентификаторы VLAN.
- **Operation type**
  Опции: Add / Del
  По умолчанию: Add
  Функция: Добавить / удалить порт участника группы многоадресной рассылки.
- **Multicast group member port**
  Опции: все порты коммутатора
  Функция: выберите порт-член, который необходимо добавить или удалить из группы многоадресной рассылки. Если
  порт подключен к хосту и хост получает данные определенной мультикаст-группы, этот порт
  может быть настроен для присоединения к статической группе многоадресной рассылки и становится статическим портом-участником.
- **Multicast address**
  Диапазон: 224.0.1.0~239.255.255.255
  Функция: Введите адрес группы многоадресной рассылки.
  Описание: при динамическом изучении вновь добавленного статического адреса многоадресной рассылки этот статический адрес многоадресной рассылки будет охватывать динамический адрес многоадресной рассылки.

Просмотр многоадресных записей.

Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [IGMP Snooping configuration] –> [Show IGMP Snooping information] для отображения многоадресных записей, как показано на рисунке ниже.

6.20. GMRP

Общий протокол регистрации атрибутов (Generic Attribute Registration Protocol - GARP) используется для распространения, регистрации и отмена определенной информации (VLAN, многоадресный адрес) среди коммутаторов на одном и том же сеть.

При использовании GARP информация о конфигурации члена GARP будет распространяться на всю коммутационную сеть. Член GARP инструктирует других членов GARP зарегистрироваться или отменить свою собственную информацию о конфигурации с помощью сообщения о присоединении/отключении соответственно. Участник также регистрирует или отменяет информацию о конфигурации других участников на основе в сообщениях о присоединении / выходе, отправленных другими участниками.

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

- Когда объект приложения GARP хочет зарегистрировать свою собственную информацию на других коммутаторах, объект отправляет сообщение о присоединении. Сообщения о присоединении делятся на два типа: JoinEmpty и JoinIn. Сообщение JoinIn отправляется для объявления зарегистрированного атрибута, а сообщение JoinEmpty отправляется для объявления атрибута, который еще не зарегистрирован.
- Когда объект приложения GARP хочет аннулировать свою собственную информацию о других коммутаторах, объект отправляет сообщение о выходе. Сообщения о выходе делятся на два типа: LeaveEmpty и LeaveIn. Сообщение LeaveIn отправляется для отмены зарегистрированного атрибута, а сообщение LeaveEmpty отправляется сообщение для отмены еще не зарегистрированного атрибута.
- После запуска объекта GARP он запускает таймер LeaveAll. Когда таймер истекает, объект отправляет сообщение LeaveAll.

Сущность приложения указывает на порт с поддержкой GARP.

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

Hold timer: при получении регистрационного сообщения объект GARP не отправляет сообщение о присоединении. сообщение немедленно, но запускает таймер удержания. Когда таймер истекает, объект отправляет все сообщений о регистрации, полученных в течение предшествующего периода, в одном сообщении о присоединении, отправка пакетов для лучшей стабильности сети.

Join time: чтобы убедиться, что сообщения о присоединении принимаются другими объектами приложения, Сущность приложения GARP запускает таймер присоединения после отправки сообщения присоединения. Если не получено JoinIn сообщения до истечения времени таймера присоединения объект снова отправляет сообщение о присоединении. Если вы получаете Сообщение JoinIn до истечения времени таймера объект не отправляет второе сообщение Join.

Leave timer: когда объект приложения GARP хочет отменить информацию о атрибут, объект отправляет сообщение о выходе. Сущность, получившая сообщение, начинает оставить таймер. Если сообщение о присоединении не получено до истечения таймера, объект, получивший сообщение, отменяет информацию об атрибуте.

LeaveAll timer: Когда объект приложения GARP запускается, он запускает таймер LeaveAll. Когда таймер истекает, объект отправляет сообщение LeaveAll, чтобы другие объекты приложения GARP перерегистрировать все атрибуты. Затем объект снова запускает таймер LeaveAll для нового цикла.

6.20.1. GMRP протокол

Протокол регистрации многоадресной рассылки GARP (GARP Multicast Registration Protocol - GMRP) — это протокол регистрации многоадресной рассылки, основанный на на ГАРП. 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 локальную многоадресную рассылку регистрационную информацию другим коммутаторам. Этот механизм обмена информацией обеспечивает непротиворечивость многоадресной информации, поддерживаемой всеми коммутаторами с поддержкой GMRP на сеть.

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.

Agent port: указывает порт, на котором включены GMRP и функция агента.

Propagation port: указывает порт, на котором включен только GMRP, но не прокси. функция.

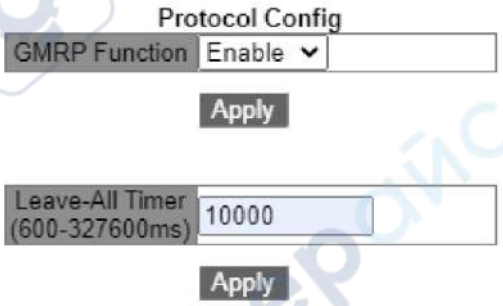
Динамически изученная многоадресная запись GMRP и запись агента пересылаются порт распространения к портам распространения устройств более низкого уровня.

Все таймеры GMRP в одной сети должны поддерживать согласованность во избежание взаимных помех. Таймеры должны соответствовать следующим правилам: Hold timer <Join timer, 2*Join timer < Leave timer, and Leave timer < LeaveAll timer.

6.20.2. Веб конфигурирование

Глобальное включение GMRP протокола

Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [GMRP configuration] –> [GMRP configuration] для входа на страницу конфигурации GMRP, как показано на рисунке ниже.



- **GMRP function**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включение / выключение глобальной функции GMRP. Функцию нельзя использовать вместе с функцией IGMP Snooping.
- **Leave-All timer**
  Диапазон: 600 мс~327600 мс
  По умолчанию: 10000 мс
  Функция: временной интервал для отправки пакетов LeaveAll. Значение должно быть кратно 100.
  Объяснение: если таймеры LeaveAll на разных устройствах истекают одновременно, они будут отправлять несколько сообщений LeaveAll одновременно, что увеличивает количество сообщений. Во избежание

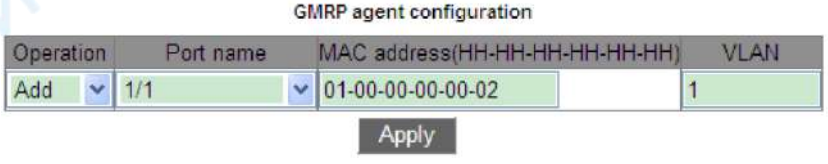
одновременного истечения срока действия таймеров LeaveAll на разных устройствах, фактическое время работы таймера LeaveAll представляет собой случайное значение, превышающее время одного таймера LeaveAll и менее чем в 1,5 раза превышающее время таймера LeaveAll.

Настройка функции GMPR на порту, как показано на рисунке.

- **Port name**
  Опции: все порты коммутатора
- **GMRP Function**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включить функцию GMRP на порту или отключить
- **GMRP Agent Function**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: Включить функцию агента GMRP на порту или нет.
- **Hold Timer**
  Диапазон: 100-163600 мс
  По умолчанию: 100 мс
  Описание: Это 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
  Это значение должно быть кратно 100. Лучше установить одинаковое время таймеров присоединения на всех портах с поддержкой GMRP.
- **Leave Timer**
  Диапазон: 500 мс~327500 мс
  По умолчанию: 3000 мс
  Это значение должно быть кратно 100. Лучше установить одинаковое время таймеров выхода на всех портах с поддержкой GMRP.

Добавление записи GMRP на порту

Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [GMRP configuration] –> [GMRP agent configuration] для входа на страницу конфигурации агента GMRP, как показано на рисунке ниже.



- **Operation**

Опции: Add / Del

По умолчанию: Del

Функция: добавить или удалить запись.

- **Port name**

  Параметры: все настроенные порты агента

- **MAC address**

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

  Функция: Настройка MAC-адреса группы многоадресной рассылки. Младший бит первого байта равен 1.

- **VLAN**

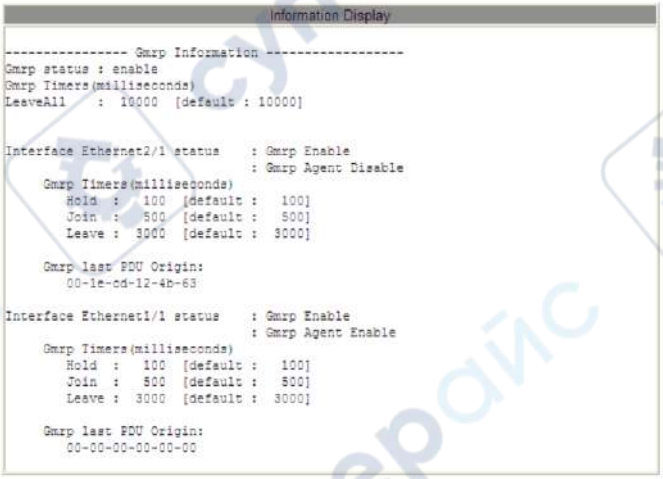
  Опции: все созданные номера VLAN

  Функция: Настройте идентификатор VLAN для записи агента GMRP.

  Описание: Запись агента GMRP может быть перенаправлена только из порта распространения с идентификатором VLAN, совпадающим с идентификатором VLAN этой записи.

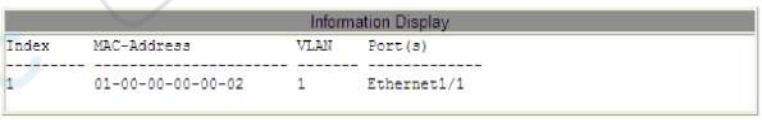
Просмотр GMRP конфигурации

Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [GMRP configuration] –> [Show GMRP configuration] для отображения информации о конфигурации GMRP, как показано на рисунке ниже.



Просмотр GMRP записи агента

Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [GMRP configuration] –> [Show GMRP agent configuration] для отображения записей агента GMRP, как показано на рисунке ниже.



Члены многоадресной рассылки этой записи агента на подключенном соседнем устройстве отображаются, как показано на рисунке ниже.

Он должен соответствовать следующим условиям:

- 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

- **GMRP dynamic multicast**
  Портфолио: {индекс, MAC-адрес многоадресной рассылки, идентификатор VLAN, членский порт}
  Функция: просмотр записей динамической многоадресной рассылки GMRP.

6.21. IGMP конфигурация

Протокол управления группами Интернета (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.

Существует три версии IGMP: IGMPv1, IGMPv2 и IGMPv3. Это устройство не поддерживает IGMPv3.

Основные различия между IGMPv1 и IGMPv2 заключаются 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 о выходе из группы. Когда хост покидает группу, хост активно отправляет пакет Leave Group. IGMPv1 не отправляет активно пакет выхода из группы.

(3) Max Resp Time: новое поле добавлено в пакеты запросов. Он указывает допустимое максимальное время ответа, установленное запрашивающим. 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.

Далее используется IGMPv2 в качестве примера для описания механизма реализации IGMP.

(1) Механизм выбора, запрашивающего: все маршрутизаторы IGMPv2 изначально считают себя запрашивающими и отправляют пакет запроса. 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 общего запроса: запрашивающий периодически отправляет пакет общего запроса, чтобы проверить, есть ли порты-члены в группе многоадресной рассылки. IP-адрес назначения пакета всегда 224.0.0.1.

Пакет отчета о членстве: когда хост в группе получает пакет запроса, он возвращает пакет ответа члена. Когда хост желает присоединиться к группе, он активно отправляет пакет отчета IGMP запрашивающему, чтобы присоединиться к группе многоадресной рассылки, в которой заинтересован хост.

(2) Механизм подавления участников: когда хост получает пакет запроса, 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 отчета о членстве. При получении пакета отчета о членстве другие хосты останавливают свои таймеры и не генерируют пакет отчета о членстве. Этот процесс называется механизмом подавления членов.

(3) Механизм выхода: когда хост намеревается покинуть группу многоадресной рассылки, он отправляет пакет выхода из группы с IP-адресом назначения 224.0.0.2.

Пакет Group-Specific Query: Хост отправляет пакет Leave Group при выходе из многоадресной группы. После получения от хоста пакета Leave Group запрашивающий отправляет пакет Group-Specific Query, чтобы проверить, является ли хост последним членом группы многоадресной рассылки. Если запрашивающий получает пакеты отчетов от других членов группы, он продолжает поддерживать группу многоадресной рассылки. В противном случае запросчик прекращает пересылку данных в группу многоадресной рассылки.

Querier

Интервал запроса: 125 с, указывающий интервал для отправки пакета общего запроса.

Интервал последнего запроса прослушивателя: максимальное время ответа в пакете группового запроса, то есть интервал передачи. Значение по умолчанию — 1 с.

Интервал ответа на запрос: максимальное время ответа в пакете общего запроса. Значение по умолчанию — 10 с. Хост, получивший пакет General Query, должен дать ответ в течение этого интервала. Значение должно быть меньше интервала запроса.

6.21.1. Веб конфигурирование

Включение IGMP протокола

IGMP запускается вместе с запуском независимой от протокола многоадресной рассылки (Protocol Independent Multicast - PIM). Его нельзя запустить отдельно.

По умолчанию: Disable

Настройка параметра группы IGMP

Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [IGMP configuration] –> [IGMP group parameter configuration], как показано на рисунке ниже.

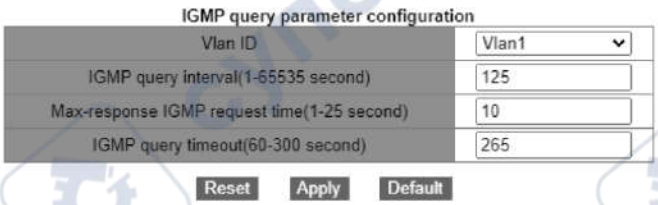
- **Vlan ID**

Опция: создан интерфейс VLAN уровня 3.
По умолчанию: VLAN 1
Функция: выберите интерфейс уровня 3 для добавления в группу многоадресной рассылки.

- **Add interface to IGMP group**
  Формат: A.B.C.D.
  Функция: укажите IP-адрес группы многоадресной рассылки, в которую должен быть добавлен коммутатор, и добавьте интерфейс коммутатора уровня 3 в группу многоадресной рассылки с указанным адресом многоадресной рассылки. По умолчанию для группы многоадресной рассылки не определен ни один член многоадресной рассылки.
- **Add IGMP static group to VLAN (A.B.C.D)**
  Формат: A.B.C.D.
  Функция: укажите IP-адрес группы многоадресной рассылки, к которой необходимо статически добавить интерфейс коммутатора уровня 3.

Настроить параметр запроса IGMP

Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [IGMP configuration] –> [IGMP query parameter configuration], как показано на рисунке ниже.



- **VLAN ID**
  Опции: Создан интерфейс VLAN уровня 3.
  По умолчанию: VLAN 1
  Функция: выберите интерфейс VLAN уровня 3, который необходимо настроить.
- **Configure the query interval for the IGMP querier to periodically send Query messages（1-65535s).**
  Диапазон：1c~65535c
  По умолчанию: 125 c
  Функция: Настройте интервал запроса для IGMP-запроса для периодической отправки сообщений Query.
- **Configure the maximum time of interface response to IGMP query packets（1-25s).**
  Диапазон: 1–25 c.
  По умолчанию: 10 c
  Функция: настроить максимальное время ответа интерфейса на пакеты запросов IGMP. Описание : Когда узлы желают присоединиться к группе многоадресной рассылки, узел, который первым отвечает на пакет запроса от запрашивающего и желает присоединиться к группе многоадресной рассылки, должен отправить запрашивающему пакет отчета о членстве в течение максимального времени ответа. Это максимальное время ответа является максимальным временем запроса. Если хосту не удается отправить пакет отчета о членстве в течение

максимального времени запроса, запрашивающий считает, что ветвь, в которой находится хост, не имеет члена, и эта ветвь будет удалена.

- **Configure the timeout time of IGMP query packets for an interface (60-300s).**
  Диапазон: 60–300 с.
  По умолчанию: 265 с
  Функция: настроить время ожидания пакетов запросов IGMP для интерфейса.
  Описание: Если не запрашивающему не удается получить пакет Query от запрашивающего в течение определенного интервала, интерфейс не запрашивающего автоматически становится запрашивающим. Этот интервал называется временем ожидания. Как правило, время ожидания равно удвоенному интервалу запроса плюс максимальное время ответа.

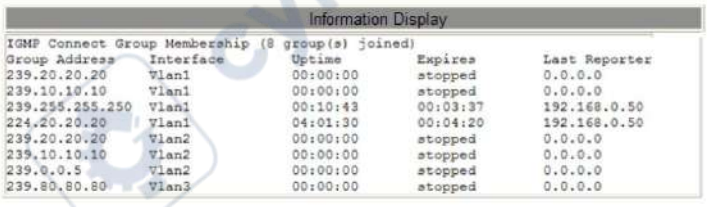
Конфигурирование IGMP протокола

Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [IGMP configuration] –> [IGMP version configuration], как показано на рисунке ниже.

- **VLAN ID**
  Опция: создан интерфейс VLAN уровня 3.
  По умолчанию: Влан 1
  Функция: выберите интерфейс уровня 3 для настройки.
- **IGMP version configuration(1 or 2)**
  Вариант: 1~2
  По умолчанию: версия 2
  Функция: настроить интерфейс уровня 3 для запуска версии 1 или версии 2.

Просмотр ip igmp групп

Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [IGMP configuration] –> [show ip igmp groups], как показано на рисунке ниже.

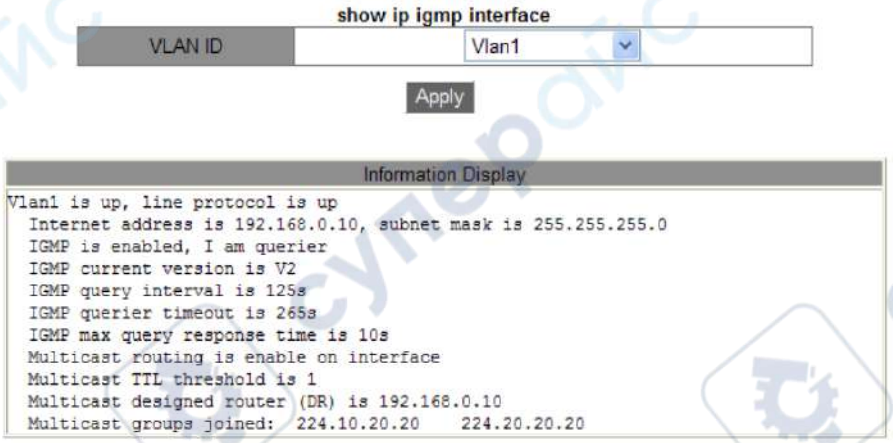


В таблице ниже описаны поля выходных сообщений.

Group Address	IP address of a multicast group
Interface	Layer-3 VLAN interface on the switch that a packet destined for a multicast group passes through
Uptime	Elapsed keepalive time of a multicast group, represented in the hh:mm:ss format
Expires	Remaining keepalive time of a multicast group, represented in the hh:mm:ss format. "Stopped" indicates that a multicast group never times out.
Last Reporter	IP address of the host that joins a multicast group last.

show ip igmp interface

Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [IGMP configuration] –> [show ip igmp interface], как показано на рисунке ниже.



- **VLAN ID**
  Опция: создан интерфейс VLAN уровня 3. По умолчанию: Vlan 1.
  Функция: выберите интерфейс Layer-3 для просмотра.
- **Information Display**
  информация об интерфейсе IP IGMP может отображаться после нажатия [Apply].

6.22. PIM конфигурирование

Многоадресная рассылка, независимая от протокола (Protocol Independent Multicast - PIM), выполняет проверку переадресации по обратному пути (RPF) для многоадресных пакетов с использованием существующей таблицы маршрутизации одноадресной рассылки, чтобы создать записи маршрутизации многоадресной рассылки и установить дерево переадресации многоадресной рассылки. PIM поддерживает два режима: PIM — плотный режим (PIM-DM) и PIM — разреженный режим (PIM-SM).

6.22.1. PIM-DM конфигурация

PIM-DM (PIM Dense Mode) использует режим Push для передачи многоадресных данных и обычно применяется к небольшим сетям с относительно плотными членами группы многоадресной рассылки.

Основные принципы PIM-DM следующие:

PIM-DM предполагает, что в каждой подсети сети существует по крайней мере один член 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 «затопления-отсечения» происходит периодически, и обрезанные ветки также могут периодически восстанавливаться до состояния пересылки.

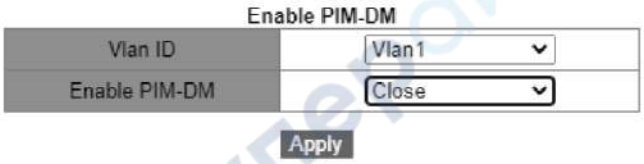
Когда член многоадресной группы появляется на узле, подлежащем удалению, PIM-DM использует механизм Graft для активного возобновления пересылки многоадресных данных, чтобы сократить время, необходимое узлу для возврата в состояние пересылки.

Как правило, путь пересылки пакета данных в плотном режиме представляет собой дерево источников (дерево пересылки, в котором источник многоадресной рассылки является «root», а член группы многоадресной рассылки — «leaf»). Поскольку исходное дерево использует кратчайший путь от источника многоадресной рассылки к получателю, оно также называется деревом кратчайшего пути (SPT).

6.22.2. Веб конфигурирование

Включение PIM-DM

Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [PIM-DM configurationn] –> [Enable PIM-DM], для входа на страницу конфигурации PIM-DM, как показано на рисунке ниже.



- **Vlan ID**
  Параметры: создан интерфейс VLAN уровня 3.
  По умолчанию: влан 1
- **Enable PIM-DM**
  Опции: включить/закрыть
  По умолчанию：Закрыть
  Функция: следует ли включить функцию PIM-DM интерфейса уровня 3.

6.22.3. PIM-SM конфигурация

PIM-SM использует режим «вытягивания» для установления дерева многоадресной пересылки между приемниками данных и передатчиком в соответствии с требованиями получателей данных.

Дерево переадресации PIM-SM устанавливается в два этапа: Шаг 1. Создание дерева переадресации, состоящего из дерева точек встречи (RPT) и дерева кратчайших точек (SPT) с центром в точке встречи (RP). Шаг 2: Переключитесь на SPT, установленный между приемниками данных и передатчиком.

Дерево пересылки PIM-SM устанавливается с центром RP. Источник многоадресной рассылки передает данные на RP по SPT, а RP пересылает данные многоадресной рассылки получателям по RPT.

RP — очень важный маршрутизатор в дереве пересылки PIM-SM. Он объединяет сообщения Prune/Join получателей, а также многоадресные данные источника многоадресной рассылки.

RPT: устанавливает дерево пересылки между получателями и RP, которое также называется деревом пересылки RPT.

Маршрутизатор начальной загрузки (BSR) в основном распространяет позицию RP и соответствующую информацию на маршрутизаторы в сети. Кандидаты BSR (C-BSR) и кандидаты RP (C-PR) настраиваются сетевыми администраторами, и можно настроить один или несколько C-BSR и C-PR. C-BSR с более высоким приоритетом, наконец, выбирается в качестве подлинного BSR.

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. Следовательно, RP отправляет пакет соединения (S,G) источнику многоадресной рассылки S. Когда пакет пересылается на назначенный маршрутизатор (DR) источника многоадресной рассылки шаг за шагом, запись (S,G) устанавливается на всех этапах. маршрутизаторы, через которые проходит пакет, и устанавливается дерево пересылки SPT от RP к источнику многоадресной рассылки S. 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.

Переключение 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. Механизм переключения SPT является решением этой проблемы.

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 соединения (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 устанавливается дерево пересылки SPT.

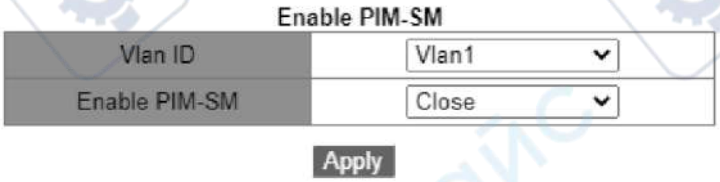
Когда получатель получает многоадресные данные, пересылаемые по дереву переадресации SPT, он отправляет пакет Prune на RP, чтобы уведомить RP о том, что многоадресные данные были перенаправлены от источника многоадресной рассылки к получателю по дереву переадресации SPT и дереву пересылки RPT. не требуется. Маршрутизаторы, через которые проходит пакет Prune, удаляют исходящий интерфейс, соответствующий записи (S,G), и обновляют запись (*,G).

Переключение SPT не является обязательным. То есть многоадресный маршрутизатор может выбрать, использовать ли SPT или RPT для пересылки данных.

6.22.4. Веб конфигурирование

Включение PIM-SM

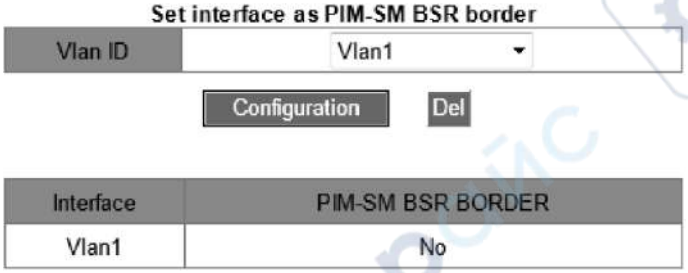
Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [PIM-SM configuration] –> [Enable PIM-SM], как показано на рисунке ниже.



- **VLAN ID**
  Параметры: создан интерфейс VLAN уровня 3.
  По умолчанию: влан 1
  Start PIM-SM
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: Включить ли функцию PIM-SM интерфейса Layer-3.

Назначить интерфейс как PIM-SM BSR border

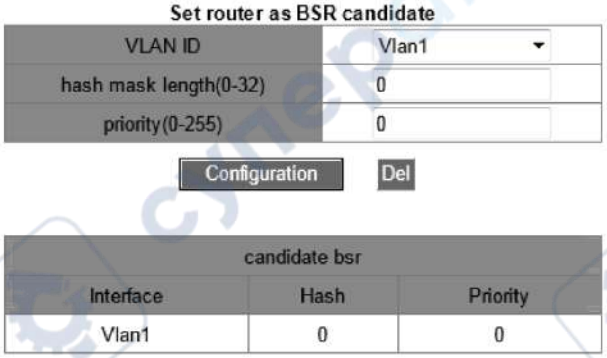
Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [PIM-SM configuration] –> [Set interface as PIM-SM BSR border], для входа на страницу настройки границы PIM-SM BSR, как показано на рисунке ниже.



- **VLAN ID**
  Опции: создан интерфейс VLAN уровня 3.
  По умолчанию: VLAN 1
  Функция: следует ли настраивать интерфейс уровня 3, присоединившийся к сети PIM-SM, в качестве границы PIM-SM BSR.

Установить маршрутизатор как кандидата BSR

Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [PIM-SM configuration] –> [Set router as BSR candidate], как показано на рисунке ниже.



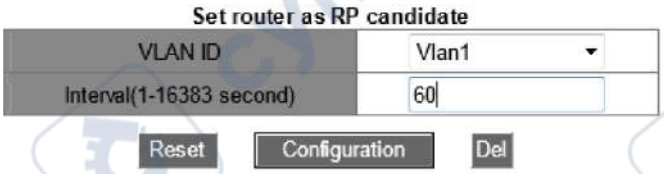
- **VLAN ID**
  Параметры: создан интерфейс VLAN уровня 3.
  По умолчанию: влан 1
  Функция: Настройте IP-адрес интерфейса VLAN уровня 3 в качестве IP-адреса C-BSR, чтобы отправлять сообщения BSR всем соседям PIM интерфейса.
- **hash mask length(0-32)**
  Диапазон：0~32
  По умолчанию: 0
  Функция: настроить длину хеш-маски. Длина хэш-маски — это число бывших битов в хэш-маске, которые будут использоваться в операции И с многоадресным адресом.
- **priority(0-255):**
  Диапазон: 0~255
  По умолчанию: 0
  Функция: настроить приоритет кандидата BSR

Все многоадресные группы с одинаковой длиной хэш-маски взаимодействуют с одним и тем же RP. Например, если длина хеш-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 наивысшим приоритетом является аутентичным BSR. Если C-BSR имеют одинаковый приоритет, C-BSR с наивысшим IP-адресом является аутентичным BSR.

Установить маршрутизатор как кандидата RP

Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [PIM-SM configuration] –> [Set router as RP candidate], как показано на рисунке ниже.



- **VLAN ID**
  Параметры: создан интерфейс VLAN уровня 3.
  По умолчанию: влан 1
  Функция: настроить IP-адрес интерфейса VLAN уровня 3 в качестве IP-адреса 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: 1c~16383c
  По умолчанию: 60 сек.
  Функция: Интервал, в течение которого C-BSR отправляет пакеты уведомлений в BSR.

6.23. Общая конфигурация многоадресной рассылки

6.23.1. Введение DR

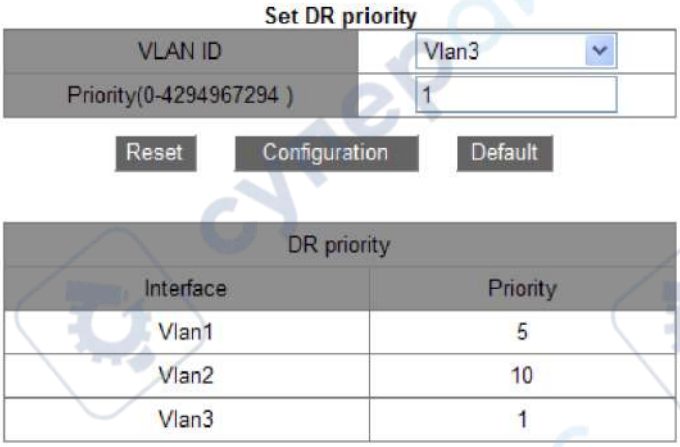
Назначенный маршрутизатор (Designated Router - DR) является единственным перенаправителем многоадресных данных в общей сети. DR должен быть выбран независимо от того, подключен ли он к источнику многоадресной рассылки или приемникам. В режиме PIM-SM пакеты приветствия маршрутизаторов PIM сравниваются 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 присоединения IGMP к RP.

6.23.2. Веб конфигурирование

Установка приоритета DR

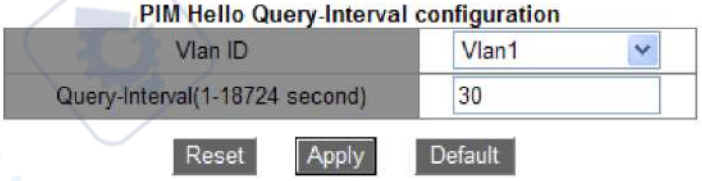
Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [Multicast common configuration] –> [Set DR priority], для входа на страницу конфигурации приоритета DR, как показано на рисунке ниже.



- **VLAN ID**
  Опция: создан интерфейс VLAN уровня 3.
  По умолчанию: Влан 1
  Функция: выберите интерфейс уровня 3 для настройки.
- **Priority（0-4294967294)**
  Опция: 0-4294967294
  По умолчанию: 1
  Функция: настроить приоритет выбранного интерфейса уровня 3.
- **Default**
  Нажмите **Default**, чтобы восстановить значение конфигурации приоритета по умолчанию.
- **DR priority**
  Отображение приоритета интерфейса Layer-3.

Конфигурирование PIM Hello Query-Interval

Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [Multicast common configuration] –> [PIM Hello Query-Interval configuration], для входа на страницу конфигурации PIM Hello Query-Interval, как показано на рисунке ниже.



- **VLAN ID**
  Опция: создан интерфейс VLAN уровня 3.
  По умолчанию: Влан 1
- **Query-Interval(1-18724)**

Опция: 1c~18724c

По умолчанию: 30 с

Функция: Настройте интервал для интерфейса уровня 3 для передачи пакетов Hello, чтобы обнаружить соседние маршрутизаторы PIM.

Показ IP Mroute

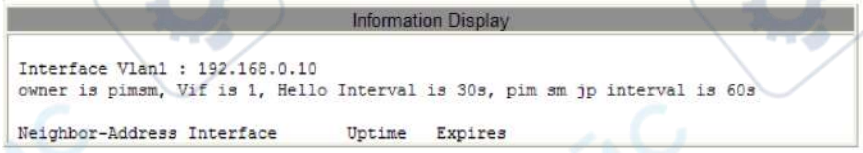
Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [Multicast common configuration] –> [show ip mroute], как показано на рисунке ниже.

6.24. Проверка и отладка

Команды проверки и отладки в основном используются для отображения конфигурации PIM коммутатора.

Show ip pim interface

Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [Inspect and debug] –> [show ip pim interface], как показано на рисунке ниже.

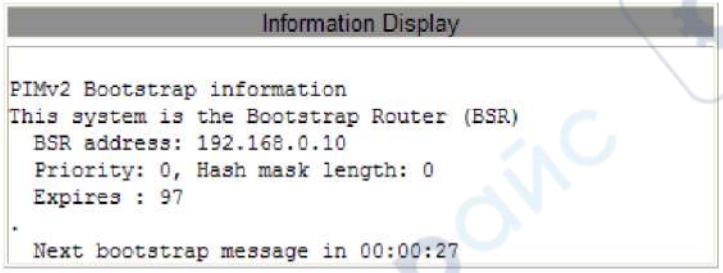


Show ip pim neighbor

Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [Inspect and debug] –> [show ip pim neighbor], как показано на рисунке ниже.

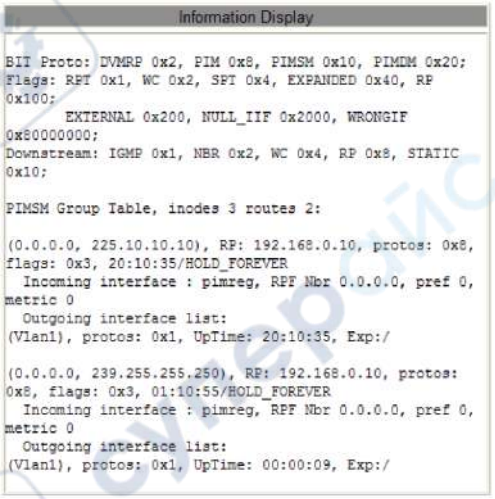
Show ip pim bsr-router

Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [Inspect and debug] –> [show ip pim bsr-router], как показано на рисунке ниже.



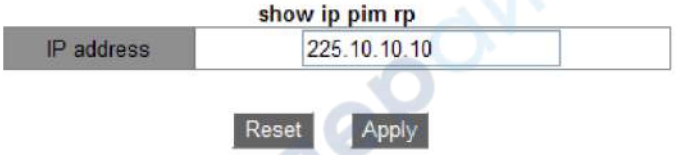
Show ip pim mroute sm

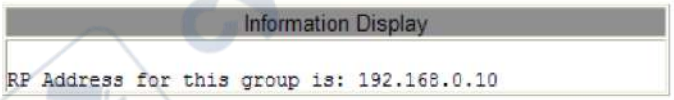
Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [Inspect and debug] –> [Show ip pim mroute sm], как показано на рисунке ниже.



Просмотр IP-адреса RP для группы многоадресной рассылки

Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [Inspect and debug] –> [Show ip pim rp], как показано на рисунке ниже.





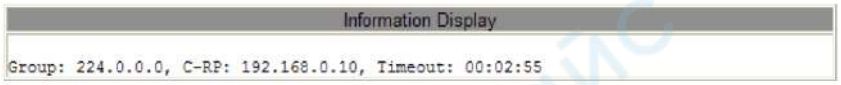
- **IP address**

  Опция: IP адрес мультикаст группы

  Функция: Введите IP-адрес группы многоадресной рассылки и нажмите [Apply], отобразится IP-адрес RP для этой группы многоадресной рассылки. Если многоадресная группа не существует, отображается информация о том, что эта группа недоступна.

Show ip pim rp mapping

Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [Inspect and debug] –> [Show ip pim rp mapping], как показано на рисунке ниже.



6.25. Незарегистрированная конфигурация multicast action

Незарегистрированные многоадресные пакеты относятся к многоадресным пакетам без соответствующих записей о пересылке на коммутаторе. При получении незарегистрированного многоадресного пакета коммутатор передает пакет в сети VLAN (все порты, кроме входного). Это займет большую полосу пропускания сети, что повлияет на скорость пересылки. В этом случае может быть включена функция отбрасывания незарегистрированных мультикастовых пакетов. Если эта функция включена, после получения незарегистрированного многоадресного пакета коммутатор отбрасывает его, а не пересылает.

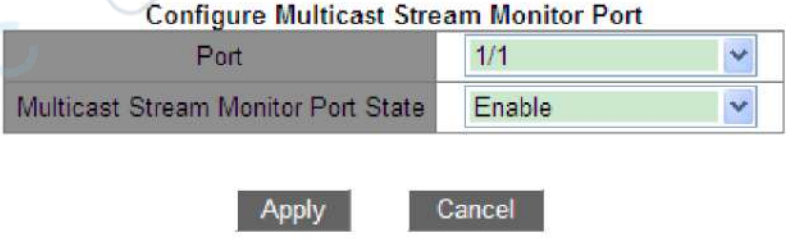
6.25.1. Веб конфигурирование

Настройка незарегистрированного многоадресного действия

Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [Unregistered multicast action configuration], как показано на рисунке ниже.

- **Unregistered multicast action**
  Опции: Forward / Discard
  По умолчанию: Forward
  Функция: Настройка незарегистрированного многоадресного действия.

Настройте порт монитора многоадресного потока, как показано на рисунке ниже



- **Multicast Stream Monitor Port**
  Опции: Disable / Enable
  По умолчанию: Disable
  Функция: настроить порт монитора многоадресного потока. Этот порт монитора 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 многоадресного мониторинга.

Когда для незарегистрированного действия многоадресной рассылки настроено отбрасывание, порт монитора многоадресного потока настроить нельзя.

Если порт монитора многоадресной рассылки доступен, незарегистрированный поток многоадресной рассылки перенаправляется только на порт монитора многоадресной рассылки.

Если порт монитора многоадресной рассылки недоступен, незарегистрированный поток многоадресной рассылки перенаправляется на все порты в VLAN. Порт монитора многоадресной рассылки не поддерживает протокол многоадресной рассылки; следовательно, его нельзя настроить как многоадресный порт-член.

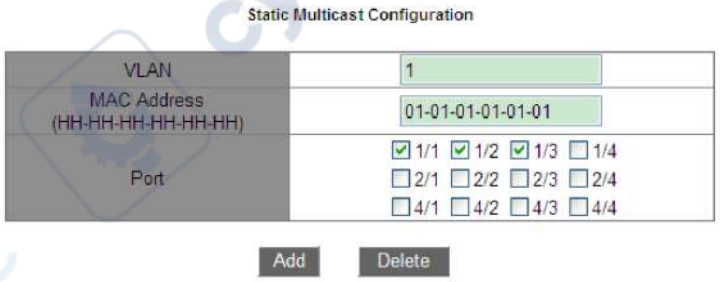
6.26. Конфигурация static multicast

Таблица многоадресных адресов может быть настроена статически. В таблицу многоадресных адресов добавляется запись в виде {VLAN ID, MAC-адрес многоадресной рассылки, порт-участник многоадресной рассылки}, и сообщение многоадресной рассылки будет перенаправлено на соответствующий порт-участник в соответствии с записью.

6.26.1. Веб конфигурирование

Добавление static multicast записи

Щелкнуть [Device Basic Configuration] → [Multicast protocol configuration] → [Static Multicast Configuration], для входа на страницу конфигурации статической многоадресной рассылки, как показано на рисунке ниже.



- **VLAN**
  Опции: Все существующие идентификаторы VLAN.

Функция: установить идентификатор VLAN для статической многоадресной записи. Только порты-члены VLAN могут пересылать это многоадресное сообщение.

- **MAC Address**
  Формат: HH-HH-HH-HH-HH-HH (H — шестнадцатеричное число)
  Функция: настройка группового адреса многоадресной рассылки. Младший бит старшего байта равен 1.
- **Port**
  Функция: выберите порты-члены многоадресного адреса. Если хост, подключенный к порту, хочет получать определенные данные группы многоадресной рассылки, статически добавьте этот порт в группу многоадресной рассылки и станьте статическим портом-участником.
  Нажмите кнопку <Add>, чтобы добавить статическую многоадресную запись; нажмите кнопку <Delete>, чтобы удалить статическую запись многоадресной рассылки.

Просмотр static multicast записи

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

6.27. LLDP

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.

6.27.1. Веб конфигуирование

Включение LLDP

Щелкнуть [Device Basic Configuration] → [LLDP configuration] → [LLDP configuration] для входа на страницу конфигурации LLDP, как показано на рисунке ниже.

- **LLDP configuration**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: Включение LLDP

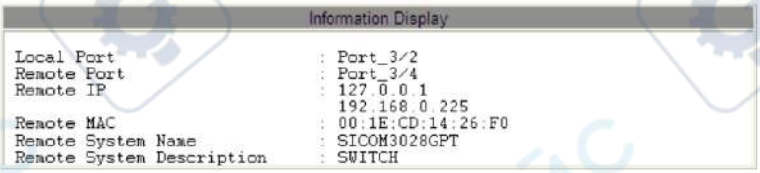
Включить функцию адреса управления TLV можно, как показано на рисунке ниже.

- **TLV Management Address**
  Опции: 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. Отправьте IP-адрес интерфейса и все IP-адреса, настроенные для текущего устройства, на подключенное устройство, когда эта функция включена. Можно отправить максимум 64 адреса управления TLV.

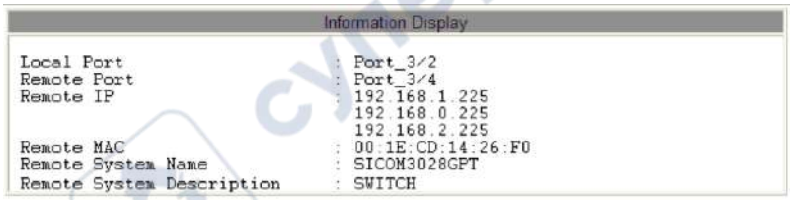
Когда на локальном устройстве включена функция управления адресом TLV и подключающееся соседнее устройство может анализировать функцию TLV, оно может правильно отображать все настроенные IP-адреса локального коммутатора.

Просмотр LLDP информации

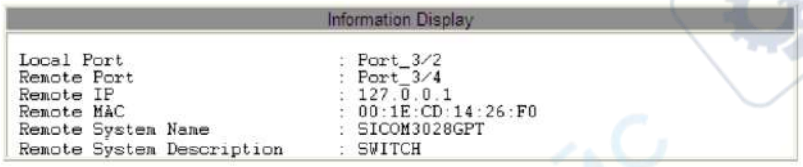
Щелкнуть [Device Basic Configuration] → [LLDP configuration] → [Show lldp] для отображения информации LLDP, как показано на рисунках ниже.



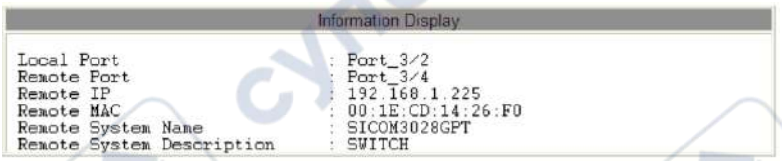
На предыдущем рисунке показано условие, при котором IP-адрес не настроен для первого интерфейса VLAN, где находится порт 3/4.



На предыдущем рисунке показано условие, при котором первичный IP-адрес первого интерфейса VLAN, в котором находится порт 3/4, равен 192.168.1.225. Когда адрес управления TLV включен, 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.



На предыдущем рисунке показано условие, при котором IP-адрес не настроен для первого интерфейса VLAN, где находится порт 3/4.



На предыдущем рисунке показано условие, при котором первичный IP-адрес первого интерфейса VLAN, в котором находится порт 3/4, равен 192.168.1.225. Когда адрес управления TLV отключен, 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.

Предпосылкой для отображения информации LLDP является то, что устройства с поддержкой LLDP подключены друг к другу.

6.28. RMON

Основанный на архитектуре SNMP, удаленный мониторинг сети (Remote Network Monitoring - 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.

6.28.1. 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.

- Statistics group

С помощью группы статистики система собирает статистику по всем типам трафика на портах и сохраняет статистику в таблице статистики Ethernet для дальнейшего запроса 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.

- History group

  Группа History 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.

- Event group

  Группа событий используется для определения индексов событий и методов обработки событий. События, определенные в группе событий, используются в элементе конфигурации группы тревог. Событие запускается, когда контролируемое устройство соответствует условию тревоги. События рассматриваются следующими способами:

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

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

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

  None: указывает на отсутствие действий.

- Alarm group

  Управление аварийными сигналами RMON может отслеживать указанные переменные аварийных сигналов. 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 нарастающее событие тревоги. Когда значение тревожной переменной меньше или равно нижнему пределу, запускается падающее тревожное событие. Аварийные сигналы будут обрабатываться в соответствии с определением события.

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

6.28.2. Веб конфигурирование

Щелкнуть [Device Basic Configuration] → [RMON configuration] → [RMON Statistics] для входа на страницу статистики RMON, как показано на рисунке ниже.

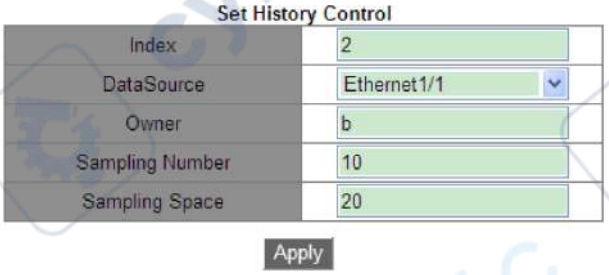
- **Index**

  Диапазон: 1~65535

Функция: Настройка номера записи статистики.

- **Ower**
  Диапазон: 1~32 символа
  Функция: Настройка имени записи статистики.
- **DataSource**
  Функция: Выберите порт, статистика которого должна быть собрана.

Щелкнуть [Device Basic Configuration] → [RMON configuration] → [RMON History] для входа на страницу RMON History, как показано на рисунке ниже.



- **Index**
  Диапазон: 1~65535
  Функция: Настройка номера записи истории.
- **DataSource**
  Функция: Выберите порт, информация которого должна быть запрошена.
- **Owner**
  Диапазон: 1~32 символа
  Функция: Настройка имени записи истории.
- **Sampling Number**
  Диапазон: 1~65535
  Функция: настроить время выборки порта.
- **Sampling Space**
  Диапазон: 1~3600 с
  Функция: Настройка периода выборки порта.

Щелкнуть [Device Basic Configuration] → [RMON configuration] → [RMON Event] для входа на страницу RMON Event, как показано на рисунке ниже.

- **Index**
  Диапазон: 1~65535
  Функция: Настройка порядкового номера записи события.
- **Owner**

Диапазон: 1~30 символов
Функция: Настройка имени записи события.

- **Event Type**
  Варианты: NONE / LOG / Snmp-Trap/ Log and Trap
  По умолчанию: NONE
  Функция: Настроить тип события для аварийных сигналов, то есть режим обработки аварийных сигналов.
- **Event Description**
  Диапазон: 1~126 символов
  Функция: Опишите событие.
- **Event Community**
  Диапазон: 1~126 символов
  Функция: настроить имя сообщества для отправки события ловушки. Значение должно быть таким же, как в SNMP.

Щелкнуть [Device Basic Configuration] → [RMON configuration] → [RMON Alarm] для входа на страницу RMON Alarm, как показано на рисунке ниже.

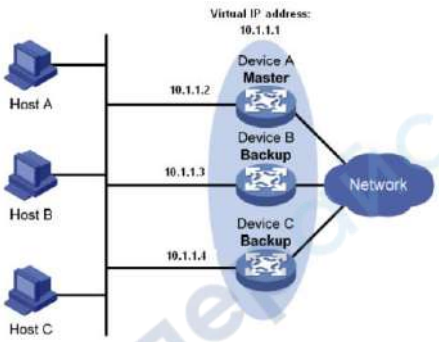
- **Index**
  Диапазон: 1~65535
  Функция: Настройка номера записи тревоги.
- **Counter Type**
  Опции: Счетчик 1213/ Счетчик RMON
  Функция: Выберите тип узла MIB.
- **1213 Counter/RMON Counter**
  Функция: Установите тип тревоги RMON.
- **Owner**
  Диапазон: 1~31 символ
  Функция: Настройка имени записи тревоги.
- **1213 DataSource**
  Функция: Выберите порт, информация о котором должна отслеживаться.
- **RMON DataSource**
  Параметры: Идентификатор индекса записи статистики в таблице статистики RMON.

Функция: контролировать информацию о порте в таблице статистики RMON.

- **Sampling Type**
  Опции: Абсолют/Дельта
  По умолчанию: Абсолютный
  Функция: Absolute указывает на выборку на основе абсолютного значения. Значение переменной извлекается напрямую, когда приближается конец периода выборки. Дельта указывает выборку на основе изменения значения. Значение изменения переменной в периоде выборки извлекается, когда приближается конец периода.
- **Alarm Type**
  Опции: RisingAlarm / FallingAlarm / RisOrFallAlarm
  По умолчанию: RisingAlarm
  Функция: Выберите тип тревоги, включая тревогу по нарастающему фронту, тревогу по заднему фронту, а также тревогу по нарастающему и заднему фронту.
- **Sampling Space**
  Диапазон: 1~65535
  Функция: Настройка периода выборки.
- **Rising Threshold**
  Диапазон: 0~65535
  Функция: Настройка порога нарастания фронта. Когда значение выборки превышает пороговое значение, а тип сигнала тревоги установлен на RisingAlarm или RisOrFallAlarm, генерируется сигнал тревоги и запускается индекс события нарастания.
- **Falling Threshold**
  Диапазон: 0~65535
  Функция: Настройка порога заднего фронта. Когда значение выборки ниже порогового значения, а тип сигнала тревоги установлен на FallingAlarm или RisOrFallAlarm, генерируется сигнал тревоги и запускается индекс события падения.
- **Rising EventIndex**
  Диапазон: 0~65535
  Функция: Настройте индекс нарастающего события, т. е. режим обработки сигналов тревоги нарастающего фронта.
- **Falling EventIndex**
  Диапазон: 0~65535
  Функция: Сконфигурируйте индекс падающего события, т. е. режим обработки аварийных сигналов заднего фронта.

6.29. VRRP

Протокол резервирования виртуальных маршрутизаторов (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 главного с помощью механизма выбора VRRP, а другие маршрутизаторы в группе становятся резервными. Когда мастер выходит из строя, резервные копии выбирают нового мастера, который берет на себя ответственность вышедшего из строя мастера. Это обеспечивает бесперебойную передачу данных без изменения конфигурации.



Как показано на рисунке выше, устройство A, устройство B и устройство 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. Мастер действует как шлюз. В случае сбоя один из резервных маршрутизаторов возьмет на себя ответственность вышедшего из строя главного маршрутизатора и будет выступать в качестве шлюза.

IP-адрес виртуального маршрутизатора может быть либо неиспользуемым IP-адресом в сегменте, где 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.
Каждая группа VRRP содержит только одного владельца IP-адреса.

6.29.1. Выбор мастера

Выбор мастера VRRP происходит:

1. Маршрутизатор с наивысшим приоритетом в группе VRRP выбирается ведущим. Мастер периодически отправляет объявления VRRP, чтобы информировать другие маршрутизаторы в группе VRRP о том, что он работает правильно.

Приоритет VRRP находится в диапазоне от 0 до 255. Чем больше число, 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 мастера в объявлении выше его собственного приоритета, маршрутизатор остается резервным.
   - Если приоритет ведущего в объявлении ниже, чем собственный приоритет маршрутизатора, маршрутизатор берет на себя ведущее устройство в вытесняющем режиме и остается резервным в невытесняющем режиме.
   - Если в течение определенного периода времени объявления VRRP не поступают, маршрутизатор считает, что мастер выходит из строя, и отправляет объявления VRRP, чтобы начать новый выбор мастера.

Невытесняющий режим: когда маршрутизатор в группе VRRP становится ведущим, он остается ведущим до тех пор, пока работает нормально, даже если резервному маршрутизатору позже будет присвоен более высокий приоритет. Упреждающий режим: когда резервная копия обнаруживает, что ее приоритет выше, чем у ведущей, резервная копия отправляет объявления VRRP, чтобы начать новый выбор ведущего в группе VRRP.

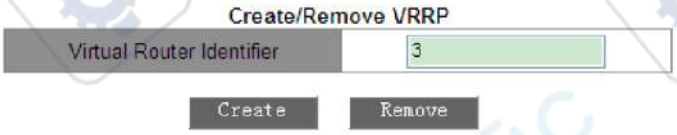
6.29.2. Мониторинг указанного интерфейса

Если интерфейс восходящей линии связи маршрутизатора в группе VRRP выходит из строя, обычно группа VRRP не может знать об отказе интерфейса восходящей линии связи. Если маршрутизатор является ведущим, узлы в локальной сети не могут получить доступ к внешним сетям. Эту проблему можно решить, отслеживая указанный интерфейс восходящей линии связи. В случае сбоя восходящего интерфейса приоритет ведущего устройства автоматически снижается на указанное значение, и маршрутизатор с более высоким приоритетом в группе VRRP становится ведущим.

6.29.3. Веб конфигурирование

Создание / удаление VRRP группы

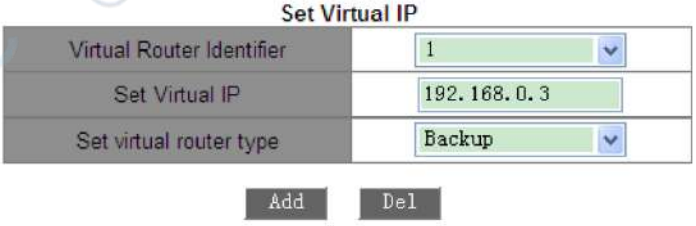
Щелкнуть [Device Basic Configuration] → [VRRP Configuration] → [Create/Remove VRRPs] для входа на страницу конфигурации VRRP group, как показано на рисунке ниже.



- **Virtual Router Identifier**
  Диапазон: 1~255
  Функция: Установите идентификатор группы VRRP.
  Примечание. Коммутаторы этой серии поддерживают не более 10 групп VRRP.

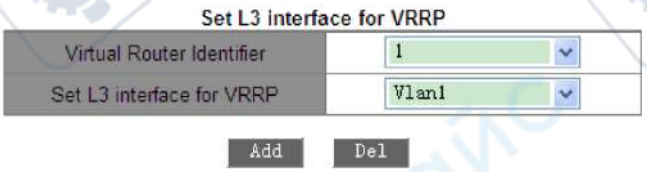
Установка IP-адреса виртуального маршрутизатора.

Щелкнуть [Device Basic Configuration] → [VRRP Configuration] → [VRRP Initialization] для входа на страницу инициализации VRRP, как показано на рисунке ниже.



- **Set Virtual IP**
  Формат: A.B.C.D.
  Функция: Установите IP-адрес виртуального маршрутизатора.
  Примечание. IP-адрес виртуального маршрутизатора должен находиться в том же сегменте сети, что и IP-адрес интерфейса.
- **Set virtual router type**
  Варианты: Основной/Резервный
  Описание: Master указывает, что текущее устройство является владельцем IP-адреса виртуального маршрутизатора. Backup указывает, что текущее устройство не является владельцем IP-адреса виртуального маршрутизатора.

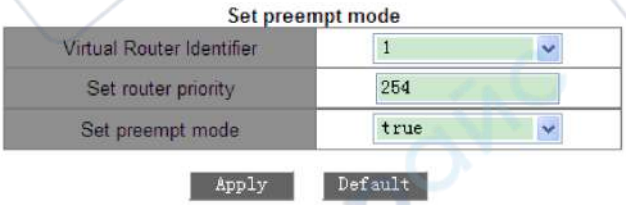
Настройте интерфейс уровня 3 для VRRP, как показано на рисунке ниже.



Функция: настроить интерфейс уровня 3 для указанной группы VRRP.

Настройте режим работы группы VRRP.

Щелкнуть [Device Basic Configuration] → [VRRP Configuration] → [Set preempt mode] для входа на страницу конфигурации рабочего режима VRRP, как показано на рисунке ниже.



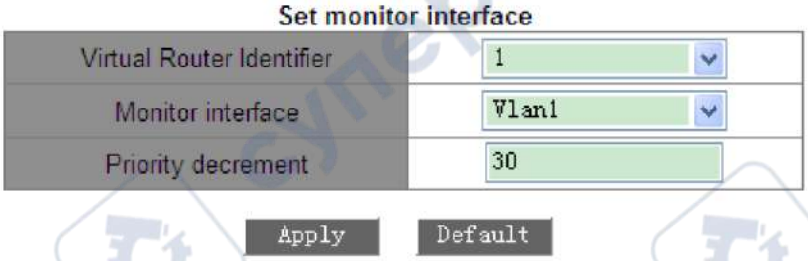
- **Set router priority**
  Диапазон: 1~254
  По умолчанию: 100 (для владельцев не-IP-адресов)
  Функция: Установить приоритет маршрутизатора в группе VRRP.
- **Set preempt mode**
  Варианты: правда/ложь
  По умолчанию: правда
  Функция: Установите режим работы виртуального маршрутизатора.
  Описание: True указывает на вытесняющий режим, а false указывает на невытесняющий режим.

Установка интервал оповещения.

Щелкнуть [Device Basic Configuration] → [VRRP Configuration] → [Set advertisement interval, monitor interface and connectivity check] для входа на страницу конфигурации, как показано на рисунке ниже.

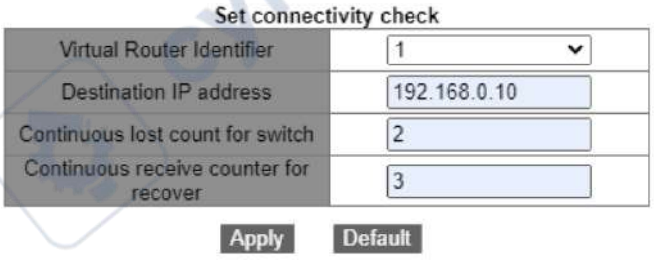
- **Set advertisement interval**
  Диапазон: 1~50 (единица измерения: 200 мс)
  По умолчанию: 5×200 мс
  Функция: установите интервал, через который главный маршрутизатор будет отправлять объявления VRRP.

Настройте контролируемый интерфейс, как показано на рисунке ниже.



- **Monitor Interface**
  Функция: выберите интерфейс VLAN для мониторинга.
- **Priority decrement**
  Диапазон: 1~253
  Функция: Установите значение уменьшения приоритета.

Установите проверку подключения, как показано на рисунке ниже.



- **Destination IP address**
  Формат: A.B.C.D.
  Функция: восходящий канал можно контролировать, установив IP-адрес назначения. Когда происходит сбой восходящей линии связи и хост в локальной сети не может получить доступ к внешней сети через маршрутизатор, уведомите

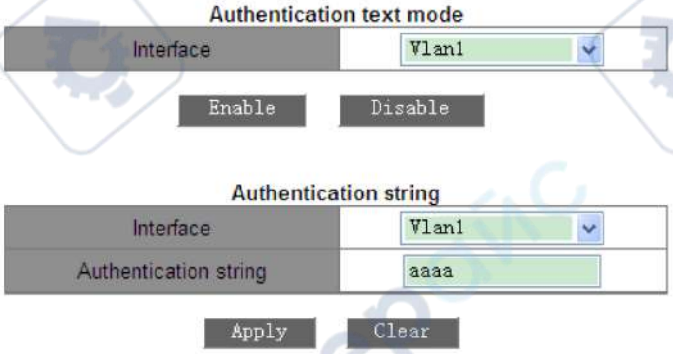
VRRP о снижении приоритета маршрутизатора до указанного значения. Следовательно, приоритет других маршрутизаторов в резервной группе выше, чем приоритет этого маршрутизатора, и он становится главным маршрутизатором, гарантируя, что связь между хостом и внешней сетью в локальной сети не прерывается. После восстановления восходящего канала уведомите VRRP о приоритете восстановления маршрутизатора.

- **Continuous lost count for switch**
  Диапазон: 2-100 (с)
  Функция: настроить время непрерывного прерывания перед переключением. Счетчик непрерывного приема для восстановления
  Диапазон: 2-100 (с)
  Функция: диапазон времени восстановления восходящего канала.
  Функция: выберите интерфейс VLAN для мониторинга.

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.

Установите параметры аутентификации VRRP

Щелкнуть [Device Basic Configuration] → [VRRP Configuration] → [VRRP Authentication] для входа на страницу конфигурации аутентификации VRRP, как показано на рисунке ниже.



- **Authentication text mode**
  Функция: включить интерфейс, требующий 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: настроить строку аутентификации.

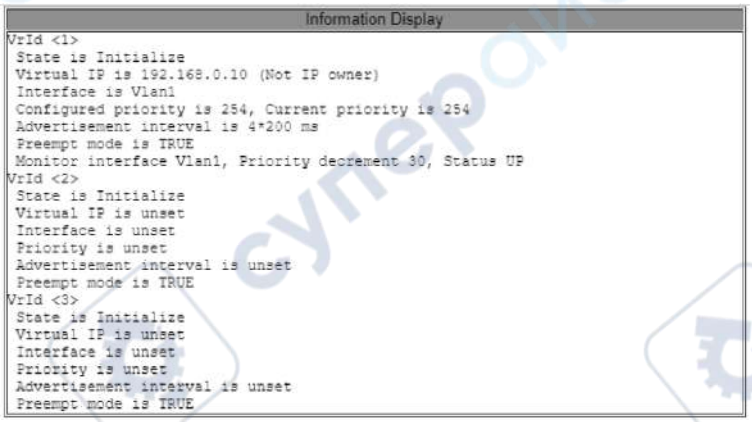
Включение группы VRRP.

Щелкнуть [Device Basic Configuration] → [VRRP Configuration] → [VRRP Initialization] для входа на страницу конфигурации VRRP initialization, как показано на рисунке ниже.

Функция: Включите функцию группы VRRP.

VRRP информация.

Щелкнуть [Device Basic Configuration] → [VRRP Configuration] → [VRRP information] для входа на страницу конфигурации VRRP information, как показано на рисунке ниже.



6.30. SNTP конфигурация

Простой протокол сетевого времени (Simple Network Time Protocol - 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 только один из них может быть активен одновременно. 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.

Для синхронизации времени по SNTP должен быть активный SNTP-сервер.
Вся информация о времени, передаваемая в протоколе SNTP, является стандартной информацией о времени для часового пояса 0.

6.30.1. Веб конфигурация

Включение SNTP протокола

Щелкнуть [Device Basic Configuration] → [SNTP configuration] → [SNTP server configuration] для входа на страницу конфигурации SNTP, как показано на рисунке ниже.

- **SNTP State**
  Параметры: Enable / Disable
  По умолчанию: Disable
  Функция: включить / отключить SNTP

Протоколы SNTP и NTP являются взаимоисключающими. Поскольку NTP и SNTP используют один и тот же номер порта UDP, их нельзя использовать одновременно.

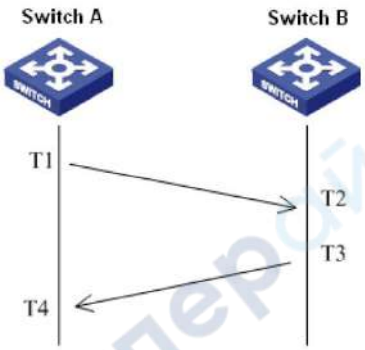
Просмотр информации о конфигурации SNTP.

Щелкнуть [Device Basic Configuration] → [SNTP configuration] → [SNTP information] для входа на страницу конфигурации SNTP, как показано на рисунке ниже.

6.31. NTP конфигурация

Протокол сетевого времени (Network Time Protocol - 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 ниже, двусторонняя задержка «(T4-T1)-(T3-T2)» и смещение часов «((T2-T1) + (T3-T4))/2» могут быть рассчитаны на основе обмен NTP-пакетами, благодаря чему достигается высокоточная синхронизация часов между устройствами.



6.31.1. Режимы работы NTP

NTP может использовать следующие рабочие режимы для синхронизации времени. При необходимости вы можете выбрать соответствующий режим работы.

Client/Server mode: 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.

Peer mode: в этом режиме активный одноранговый узел отправляет пакеты синхронизации часов (активный одноранговый режим) 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 равноправный 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 большей стратой часов синхронизирует время с одноранговым узлом с меньшей стратой часов.

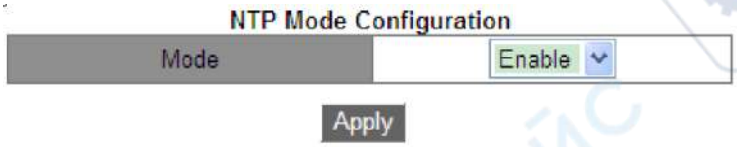
Broadcast mode: в этом режиме широковещательный сервер периодически рассылает пакеты синхронизации часов (широковещательный режим). После получения пакетов широковещательный клиент отправляет на сервер пакеты синхронизации часов (режим клиента). После получения пакетов запроса сервер отправляет пакеты ответа (режим сервера). Сервер и клиент выполняют синхронизацию часов, обмениваясь восемью пакетами запросов и ответов.

Multicast mode: 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.

6.31.2. Веб конфигурирование

Включение NTP

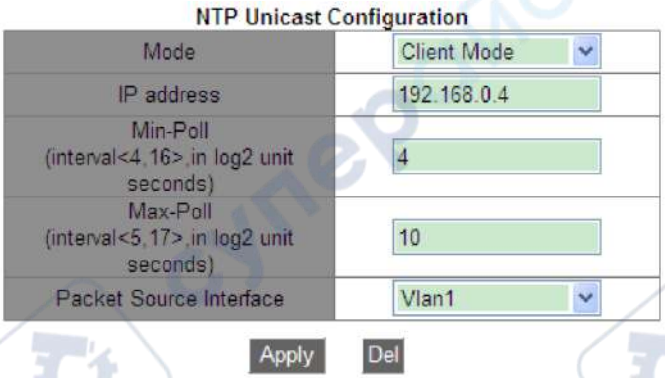
Щелкнуть [Device Basic Configuration] → [NTP configuration] → [NTP Global Configuration] для входа на страницу конфигурации NTP, как показано на рисунке ниже.



- **Mode**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включение или отключение функции глобальной службы NTP.

NTP и SNTP не могут использоваться одновременно, поскольку они используют один и тот же номер порта UDP.
Вы также можете настроить службу NTP и сохранить конфигурацию, когда служба NTP отключена. Включение службы NTP не влияет на конфигурацию службы NTP.

Настройка одноадресной рассылки NTP, как показано на рисунке ниже.



- **NTP State**
  Варианты: Client Mode / Peer Mode
  Функция: выберите режим работы NTP.
  Описание: Режим клиента указывает, что рабочий режим NTP является режимом клиент/сервер; одноранговый режим указывает, что рабочий режим NTP является одноранговым режимом.
- **IP address**
  Формат: A.B.C.D.
  Описание: При использовании режима клиент/сервер IP-адрес совпадает с адресом NTP-сервера. Когда принимается одноранговый режим, IP-адрес является адресом пассивного однорангового узла.
- **Min-Poll**
  Диапазон: от 4 до 16. Интервал=2n с («n» — значение этого параметра)
  По умолчанию: 4. В этом случае интервал равен 16 с (24).
  Функция: Настройка минимального интервала запросов для обмена пакетами NTP между локальным устройством и сервером.
- **Max-Poll**
  Диапазон: от 5 до 17. Интервал=2n с («n» — значение этого параметра)
  По умолчанию: 10. В данном случае интервал равен 1024 с (210).
  Функция: Настройка максимального интервала запросов для обмена пакетами NTP между локальным устройством и сервером.
- **Packet source interface**

Функция: укажите порт для отправки пакетов NTP.

Описание: Когда используется режим клиент/сервер, локальное устройство отправляет пакеты NTP на сервер. IP-адрес источника в пакетах является основным IP-адресом порта. Когда принимается одноранговый режим, локальное устройство отправляет пакеты NTP одноранговому узлу. IP-адрес источника в пакетах является основным IP-адресом порта.

Если принят режим клиент/сервер, вам нужно только выполнить предыдущую настройку на клиенте.

Настроенные часы сервера NTP должны быть синхронизированы, прежде чем обеспечивать синхронизацию времени для других устройств.

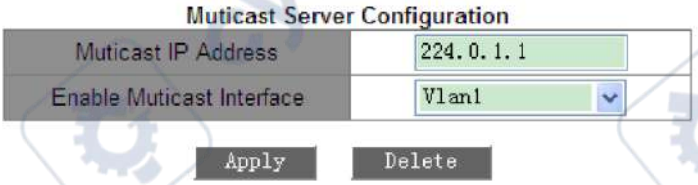
Если принят одноранговый режим, вам нужно только выполнить предыдущую настройку на активном одноранговом устройстве.

Min-Poll ≤ Max-Poll.

Значения Min-Poll одноранговых узлов NTP должны быть одинаковыми.

Настройка многоадресный сервер NTP.

Щелкнуть [Device Basic Configuration] → [NTP configuration] → [Multicast Server Configuration] для входа на страницу конфигурации сервера многоадресной рассылки, как показано на рисунке ниже.



- **Multicast IP Address**

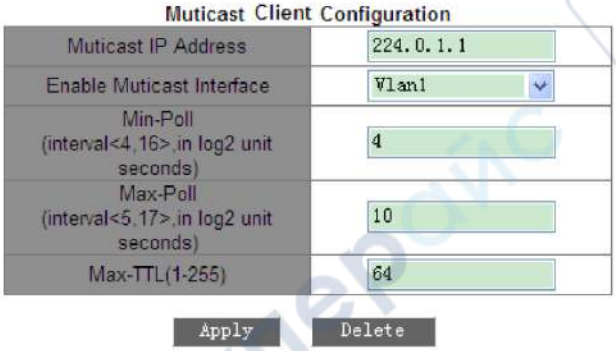
  Формат: A.B.C.D.

  Функция: Настройка многоадресного IP-адреса. Если указанный многоадресный IP-адрес недоступен, по умолчанию используется 224.0.1.1.

  Включить функцию интерфейса многоадресной рассылки: укажите порт многоадресной рассылки.

Настройка многоадресного клиента NTP.

Щелкнуть [Device Basic Configuration] → [NTP configuration] → [Multicast Client Configuration] для входа на страницу конфигурации многоадресного клиента, как показано на рисунке ниже.



- **Multicast IP Address**
  Формат: A.B.C.D.
  Функция: Настройка IP-адреса, используемого в многоадресном режиме. Если указанный многоадресный IP-адрес недоступен, по умолчанию используется 224.0.1.1.
- **Enable Multicast Interface**
  Функция: укажите многоадресный порт.
- **Min-Poll**
  Диапазон: от 4 до 16. Интервал=2n с («n» — значение этого параметра)
  По умолчанию: 4. В этом случае интервал равен 16 с (24).
  Функция: Настройка минимального интервала запросов для обмена пакетами NTP между локальным устройством и сервером.
- **Max-Poll**
  Диапазон: от 5 до 17. Интервал=2n с («n» — значение этого параметра)
  По умолчанию: 10. В данном случае интервал равен 1024 с (210).
  Функция: Настройка максимального интервала запросов 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.

Настройка широковещательного сервера NTP.

Щелкнуть [Device Basic Configuration] → [NTP configuration] → [Broadcast Server Configuration] для входа на страницу конфигурации сервера вещания, как показано на рисунке ниже.

- **Enable Broadcast Interface**
  Функция: Укажите широковещательный порт.

Настройка широковещательного клиента NTP.

Щелкнуть [Device Basic Configuration] → [NTP configuration] → [Broadcast Client Configuration] для входа на страницу настройки широковещательного клиента, как показано на рисунке ниже.

- **Broadcast Client Configuration**
  Функция: Укажите широковещательный порт.

Настройка эталонных часов

Щелкнуть [Device Basic Configuration] → [NTP configuration] → [Reference Clock Configuration] для входа на страницу конфигурации эталонных часов, как показано на рисунке ниже.

- **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: Настройте уровень эталонных часов.
  Описание: Stratum часов указывает на точность часов. Чем больше число, тем ниже точность. Если Stratum равна 16, часы не синхронизированы и, следовательно, не могут служить эталонными часами.
  Функция: Укажите широковещательный порт.

В настоящее время только сам коммутатор может служить эталонным тактовым генератором. Перед настройкой этого элемента необходимо подтвердить требования системы к синхронизации времени.

6.32. PTP конфигурирование

Протокол точного времени (Precision Time Protocol - PTP) синхронизирует независимые часы на распределенных узлах системы измерения и управления с высокой точностью. Протокол синхронизирует фазу и частоту с точностью до ±100 нс.

6.32.1. Концепт

- PTP domain
  Сеть, в которой применяется PTP, является доменом PTP. Домен PTP имеет только одни главные часы. Все остальные устройства синхронизируют время с ним.
- PTP port
  Порт с поддержкой PTP называется портом PTP.
- Clock node
  Узлы в домене PTP являются узлами часов. PTP определяет следующие узлы часов:
  - Ordinary Clock(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.
  - Boundary Clock (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 синхронизации восходящей линии связи или с узлом синхронизации нисходящей линии связи. Если несколько портов PTP участвуют в синхронизации часов, один из этих портов синхронизирует время с тактовым узлом восходящей линии связи, а другие порты синхронизируют время с тактовыми узлами нисходящей линии связи. Когда BC служит источником синхронизации, он может доставлять время на узлы синхронизации нисходящей линии связи через несколько портов PTP.
  - Transparent Clock (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:
    End-to-End Transparent Clock (E2ETC): напрямую пересылают не-PTP-пакеты и участвуют в расчете задержки для всего канала.
    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.

Связь между парой узлов синхронных часов

Узел, отправляющий информацию о часах синхронизации, находится в ведущем режиме, а узлы, получающие информацию, являются подчиненными узлами.

Часы главного узла являются ведущими часами, а часы подчиненного узла — подчиненными часами. Порт, отправляющий информацию о часах синхронизации, является главным портом, а порты, получающие информацию, являются подчиненными портами.

6.32.2. Принципы синхронизации

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 ведомые часы не получают пакеты Announce от главных часов в течение периода, главные часы считаются недействительными и начинается новый выбор. Пакеты объявлений содержат следующую информацию для выбора гроссмейстерских часов: гроссмейстерский приоритет 1, тактовая страта, точность часов, гроссмейстерский приоритет 2 и идентификатор часов. Информация сравнивается в следующей процедуре: часы с самым низким гроссмейстерским приоритетом 1 выбираются в качестве гроссмейстерских часов; если часы имеют одинаковое значение гроссмейстерского приоритета 1, часы с наименьшим часовым слоем выбираются гроссмейстерскими часами; аналогично, если часы имеют одинаковые значения для гроссмейстерского приоритета 1, страты часов, точности часов, гроссмейстерского приоритета 2, часы с наименьшим идентификатором часов выбираются в качестве гроссмейстерских часов.

Принцип синхронизации

Ведущие и ведомые часы обмениваются пакетами синхронизации, записывают время отправки и получения пакетов и вычисляют общую задержку между ведущими и ведомыми часами на основе разницы во времени. Если сетевой путь симметричен, однонаправленная задержка составляет половину общей задержки. Ведомые часы настраивают местное время в соответствии с разницей во времени между ведущими и ведомыми часами и однонаправленной задержкой, реализуя синхронизацию времени с ведущими часами.

PTP поддерживает два механизма измерения задержки:

Механизм запрос-ответ: используется для сквозного измерения задержки всего канала.

Механизм одноранговой связи: используется для измерения задержки между точками. По сравнению с механизмом request_response, одноранговый механизм измеряет задержку каждого сегмента ссылки.

6.32.3. Веб конфигурирование

Включение PTP на порту

Щелкнуть [Device Basic Configuration] → [PTP configuration] → [PTP configuration для входа на страницу конфигурации PTP, как показано на рисунке ниже.

- **Status**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включение / отключение функции порта PTP.
- **Pdelay Correction**
  Диапазон: -65535~65535 нс
  По умолчанию: 0 нс
  Функция: Настройка компенсации задержки канала PTP.
  Описание: При наличии фиксированного смещения между ведущими и ведомыми часами необходимо настроить параметр на ведомых часах для синхронизации фазы.
- **Master-allow**
  Опции: включить/отключить
  По умолчанию: Включить
  Функция: Этот параметр определяет, разрешено ли использовать текущий порт в качестве главного порта для запуска синхронизирующих часов. Когда выбрано **Enable**, узел часов может синхронизировать другие сетевые часы через этот порт. Когда выбрано **Disable**, узел часов не может синхронизировать другие сетевые часы через этот порт. Это предотвращает влияние узла часов на другую информацию о сетевых часах.
- **Limit Class**
  Диапазон: 0~255
  По умолчанию: 0
  Функция: Чтобы предотвратить влияние внешних источников синхронизации на текущую информацию о системных часах, настройте предельное значение слоя часов, чтобы ограничить слой часов в пакете Announce, полученном этим портом. Если уровень синхронизации в пакете Announce, полученном этим портом, превышает предельное значение (то есть значение уровня синхронизации меньше предельного значения), измените уровень синхронизации в пакете, чтобы он соответствовал предельному значению. В противном случае страта часов в пакете не обрабатывается. Когда предельное значение равно 0, страта часов в пакете Announce не ограничена.
- **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 ограничивается.

Установка параметров PTP, как показано на рисунке ниже

PTP Configuration

PTP Profile	None-Power-Profile
PTP Current Time	1970-01-02 08:02:07 sec: 115327 nsec: 119998500
Clock Stratum	248 (128~255)
Version	version2
UTC To TAI Offset(s)	35 (0~255)
Clock Type	Boundary
Delay Mechanism	request-response
Grandmaster Priority1	128 (0~255)
Grandmaster Priority2	128 (0~255)
Set Local Clock	Disable
PTP to NTP	Disable
TLV	Enable

Apply

- **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 коммутатора PTP. Время PTP отображается в формате TAI.
- **Clock Stratum**
  Диапазон: 128~255
  По умолчанию: 248
  Функция: Выберите stratum часов.
  Описание: Когда часы имеют одинаковое значение гроссмейстерского приоритета 1, в качестве гроссмейстерских часов выбираются часы с самой низкой стратой часов. Если часы получают время из часов GPS, слой часов может быть автоматически настроен как 6, 7, 52 или 187, чтобы улучшить возможность быть избранными в качестве часов гроссмейстера.
  Объяснение: Stratum часов можно настроить как 255, если тип часов — только подчиненные. В противном случае stratum часов не может быть настроен как 255.

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 составляет 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**
  Опции: virsion2
  По умолчанию: virsion 2

Функция: Выберите версию PTP.

- **UTC To TAI Offset**
  Диапазон: 0~255 с
  По умолчанию: 35 с
  Функция: настроить смещение UTC-TAI. Значение может быть перезаписано значением UTCOffSet, полученным из пакетов GPS или Announce основных часов. Связь между UTC, TAI и смещением следующая: UTC=TAI-Offset.
- **Clock Type**
  Варианты: Boundary / E2E / P2P / Slave-only
  По умолчанию: Boundary
  Функция: выберите тип часов PTP.
  Описание: Slave-only указывает, что часы OC могут быть только подчиненными часами.
- **Delay Mechanism**
  Варианты: запрос-ответ/одноранговая связь
  По умолчанию: запрос-ответ
  Функция: настройка механизма измерения задержки PTP.

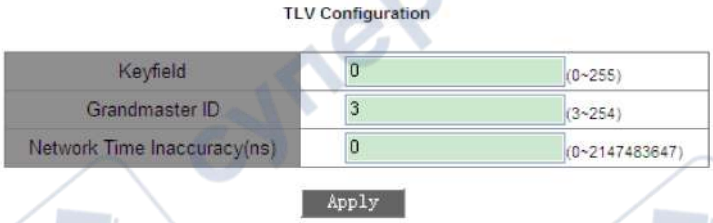
Узел часов, имеющий несколько доменов, должен быть настроен на граничный тип часов.
Механизм задержки тактового узла BC/OC может быть установлен на режим запрос-ответ или одноранговый.
Если тип узла синхронизации TC — E2ETC, механизм измерения задержки должен быть установлен в режим запрос-ответ.

Если тип узла синхронизации 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 узлов синхронизации TC в домене PTP должны быть одинаковыми.

- **Grandmaster priority1/Grandmaster priority2**
  Диапазон: 0~255
  По умолчанию: 128
  Функция: Настройте Grandmaster priority1 и Grandmaster priority2.
  Описание: Grandmaster priority1 и Grandmaster priority2 используются для выбора часов гроссмейстера. Часы с наименьшим гроссмейстерским приоритетом выбираются в качестве гроссмейстерских часов.
- **Set Local Clock**
  Опции: 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 в NTP**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: обновлять ли время NTP временем PTP
- **TLV**

Опции: Enable / Disable
По умолчанию: Disable
Функция: Включение TLV означает, что пакеты Announce содержат поле TLV. Отключение TLV означает, что пакеты Announce не содержат поле TLV.

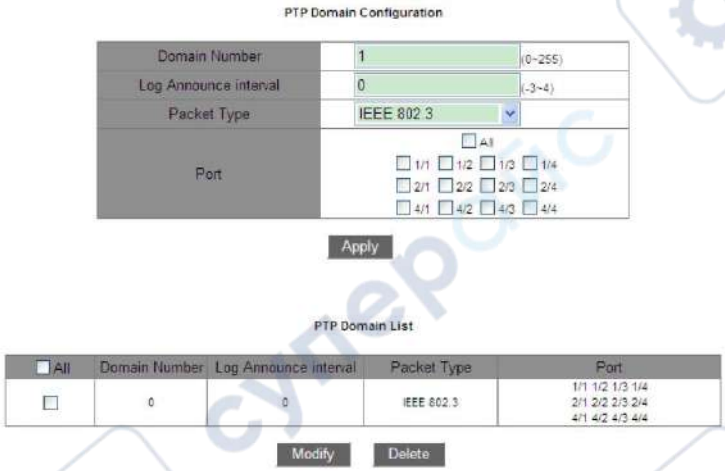
Установите параметры TLV, как показано на рисунке ниже.



- **Keyfield**
  Диапазон: 0~255
  По умолчанию: 0
  Функция: настроить гроссмейстерские часы Keyfield. 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 гроссмейстера. 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 неточности сетевого времени PTP. Если тип поля TLV, переносимого пакетами Announce, — ORGANIZATION_EXTENSION, параметр необходимо настроить как неточность времени, накопленную в наихудшем сетевом пути.

Конфигурирование PTP domain

Щелкнуть [Device Basic Configuration] → [PTP configuration] → [PTP Domain Configuration] для входа на страницу конфигурации домена PTP, как показано на рисунке ниже.

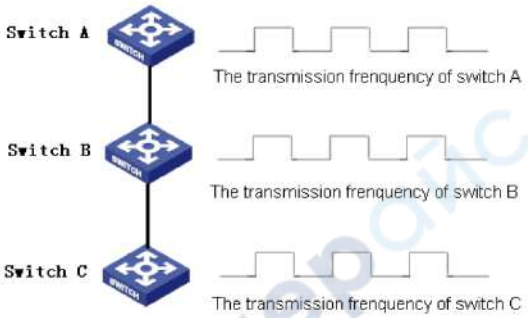


- **Domain Number**
  Диапазон: 0~255
  По умолчанию: 0
  Функция: Настройка идентификатора домена PTP.
- **Log Announce interval**
  Диапазон: -3~4
  По умолчанию: 0
  Функция: Настройка показателя интервала объявления.
  Описание: Каждый узел отправляет пакеты Announce с интервалом 2n с (n — показатель степени).
- **Packey Type**
  Опции: IEEE802.3 / IPv4 UDP
  По умолчанию: IEEE802.3.
  Функция: Выберите тип пакетов, несущих информацию PTP.
- **Port**
  Функция: выберите порт устройства в текущем домене PTP.

Домен 0 — это PTP-домен системы по умолчанию, который нельзя удалить.
Конфигурации типов пакетов всех устройств в одном домене PTP должны быть согласованными.
Один порт можно добавить только к одному домену.

6.33. SyncE конфигурация

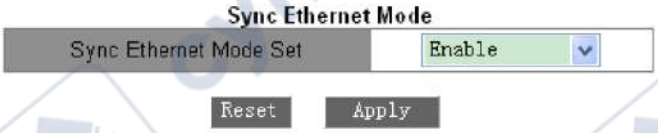
Synchronous Ethernet (SyncE) синхронизирует физические функции коммутаторов. Это может обеспечить постоянную частоту между переключателями разных уровней. Если SyncE включен, PTP может обеспечить точность синхронизации ±50 нс. Как показано на рисунке ниже, коммутатор B использует SyncE для синхронизации 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.



Коммутатор с поддержкой SyncE должен быть подключен к синхронизированному коммутатору восходящей линии связи или к главным часам. Поскольку SyncE синхронизирует только частоту, его необходимо использовать вместе с PTP. Когда PTP используется вместе с SyncE, рекомендуется сначала включить SyncE, а затем включить и настроить PTP.

6.33.1. Веб конфигурирование

Щелкнуть [Device Basic Configuration] → [Sync Ethernet Configuration] → [Sync Ethernet Mode] для входа на страницу конфигурации SyncE, как показано на рисунке ниже.



- **Sync Ethernet Mode Set**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включение/выключение функции синхронизации Ethernet.
  Описание: После включения функции коммутатор будет синхронизировать частоту с подключенным коммутатором восходящей линии связи.

6.34. GPS конфигурация

Глобальная система позиционирования (Global Positioning System - GPS) — это передовая и сложная спутниковая система 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, выдает второй импульсный сигнал, точно синхронизированный с международным стандартным временем, и синхронизирует информацию о точном времени со всей системой для обеспечения синхронного хронометража.

6.34.1. Веб конфигурирование

Щелкнуть [Device Basic Configuration] → [GPS Configuration] → [GPS Configuration] для входа на страницу конфигурации GPS, как показано на рисунке ниже.

- **GPS Latency Compensation**
  Диапазон: -32768~32767 нс
  По умолчанию: 0 нс
  Функция: настроить компенсацию задержки GPS.
- **GPS PPS Width**
  Диапазон: 20~255 мс
  По умолчанию: 200 мс
  Функция: Настройка ширины GPS PPS.
- **Set Local Clock**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включение или отключение функции синхронизации локального системного времени RTC с часами GPS. Местное системное время RTC отображается в формате UTC.
- **Set PTP Info**
  Опции: 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**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: разрешать ли текущим часам снижаться до ведомых часов при возникновении сбоев GPS.
- **Hold Over Time**
  Диапазон: 0~65535 ч
  По умолчанию: 1 час
  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 после сбоев GPS, уровень часов устройства будет автоматически настроен на 187, и будет запущен повторный выбор основных часов, если включена функция понижения до подчиненных; тактовая частота устройства будет автоматически настроена на 52, и будет запущен повторный выбор ведущих часов, если функция понижения до ведомого не включена.

6.35. IRIG-B конфигурация

Код Inter Range Instrumentation Group (IRIG) - это стандарт времени, установленный Американским советом командиров полигонов (RRC). Код IRIG широко применяется в различных областях, включая военный, коммерческий и промышленный секторы. Коды IRIG подразделяются 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 фрейм данных содержит информацию о дне года (1~366), часах, минутах и секундах.

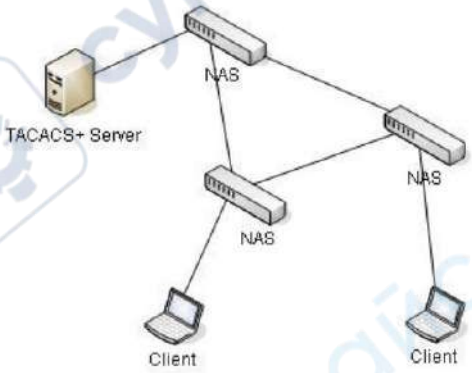
6.35.1. Веб конфигурирование

Щелкнуть [Device Basic Configuration] → [IRIG B configuration] → [IRIG B configuration] для входа на страницу конфигурации IRIG-B, как показано на рисунке ниже.

- **IRIG-B Slot ID**
  Функция: выберите конфигурируемый модуль IRIG-B.
- **PPS width**
  Диапазон: 20~255 мс
  По умолчанию: 200 мс
  Функция: Настройка ширины PPS.
- **IRIG-B format**
  Опции: Irig-b000~Irig-b007
  По умолчанию: Irig-b004
  Функция: Выберите выходной формат IRIG-B.
- **VPP**
  Варианты: 3/4/4,5/5/6/7/8/9/10Vp-p
  По умолчанию: 4,5 Впик-пик
  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: Выберите режим четности для IRIG-B.

6.36. TACACS+

Система управления доступом к контроллеру доступа к терминалу (Terminal Access Controller Access Control System - TACACS+) представляет собой приложение на основе TCP. Он принимает 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. Рисунок ниже показывает структуру.



Протокол аутентифицирует, авторизует и логирует 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 операций.

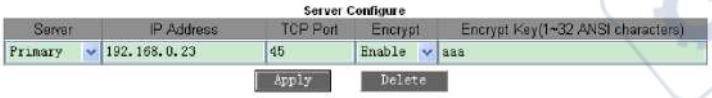
6.36.1. Веб конфигурация

Включение TACACS+

Щелкнуть [Device Basic Configuration] → [TACACS-PLUS Configuration] → [TACACS-PLUS configuration] для входа на страницу конфигурации TACACS+, как показано на рисунке ниже.

- **TACACS-PLUS State**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: Включение / выключение TACACS+.

Конфигурирование сервер TACACS+, как показано на рисунке.

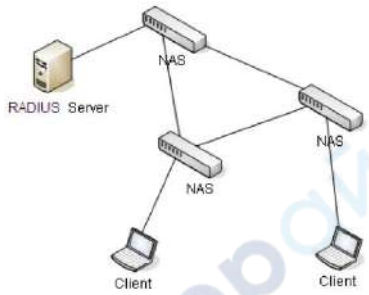


- **Server**
  Опции: Primary / Secondary
  По умолчанию: Primary
  Функция: выберите тип сервера.
- **IP Address**
  Формат: A.B.C.D.
  Функция: введите IP-адрес сервера.
- **TCP port**
  Диапазон: 1~65535
  По умолчанию: 49
  Функция: Установите количество портов, которые получают запросы аутентификации NAS.
- **Encrypt**
  Опции: включить/отключить
  По умолчанию: Отключить
  Функция: Шифровать пакет или нет. Если он включен, требуется ключ.
- **Encrypt Key**
  Диапазон: 1~32 символа
  Описание: Установите ключ 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 убедитесь, что настроенный ключ совпадает с ключом на сервере TACACS+.
  После завершения настройки в следующем разделе «Sever Configured» отображается информация о конфигурации сервера, как показано на рисунке ниже.

Server Configured			
Primary Server	192.168.0.23	49	Encrypt
Secondary Server	192.168.0.32	45	Unencrypt

6.37. RADIUS конфигурирование

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 является сервером для пользователей, но клиентом для сервера RADIUS. Рисунок ниже показывает структуру.

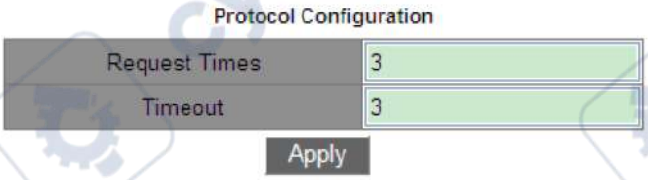


Протокол аутентифицирует пользователей терминалов, которым для работы необходимо войти в систему. Выступая в качестве клиента RADIUS, устройство отправляет информацию о пользователе на сервер RADIUS для аутентификации и разрешает или запрещает пользователям входить в систему в соответствии с результатами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

6.37.1. Веб конфигурирование

Настроить параметры RADIUS

Щелкнуть [Device Basic Configuration] → [RADIUS configuration] → [RADIUS configuration] для входа на страницу конфигурации RADIUS, как показано на рисунке ниже.



- **Request Times**
  Диапазон: 1~3
  По умолчанию: 3
  Функция: Установите максимальное количество попыток повторной передачи для пакетов запросов RADIUS. Если устройство по-прежнему не получает ответные пакеты от сервера RADIUS после максимального количества попыток повторной передачи, устройство считает, что аутентификация не удалась.
- **Timeout**
  Диапазон: 1~3
  По умолчанию: 3
  Функция: Установите дополнительное время для ответа 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.

Настроить сервер RADIUS, как показано на рисунке ниже.

- **Server Type**
  Опции: Authentication Primary Server / Authentication Secondary Server
  Функция: настроить первичный или вторичный сервер RADIUS. Если первичный сервер недоступен, для аутентификации будет использоваться вторичный сервер.
- **Server IP**
  Формат: A.B.C.D.
  Функция: Установите IP-адрес сервера RADIUS.
- **Port**
  Диапазон: 1~65535
  По умолчанию: 1812
  Функция: Установите UDP-порт RADIUS-сервера.
- **Password**
  Диапазон: 1~32 символа
  Функция: Настройка пароля сервера RADIUS.
  Диапазон: 64~1000000Кбит/с

6.38. IEEE802.1x конфигурирование

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 может пройти аутентификацию, он не может получить доступ к ресурсам в локальной сети. Системы 802.1x используют структуру клиент/сервер. Аутентификация пользователя и авторизация управления 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 отправит запрос на соединение.

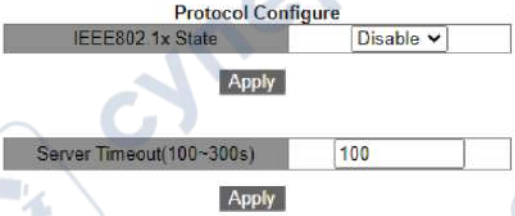
Устройство: указывает коммутатор аутентификации в системе Ethernet. Он загружает и доставляет информацию об аутентификации пользователя, а также включает или отключает порт в зависимости от результата аутентификации.

Сервер аутентификации: указывает объект, предоставляющий сервис 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.

6.38.1. Веб конфигурирование

Включение IEEE802.1x протокола

Щелкнуть [Device Basic Configuration] → [IEEE802.1x configuration] → [IEEE802.1x configuration] для входа на страницу конфигурации IEEE802.1x, как показано на рисунке ниже.



- **IEEE802.1x State**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включение / отключение глобальной функции 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.

Настройка порта, на котором включен IEEE802.1x, как показано на рисунке ниже

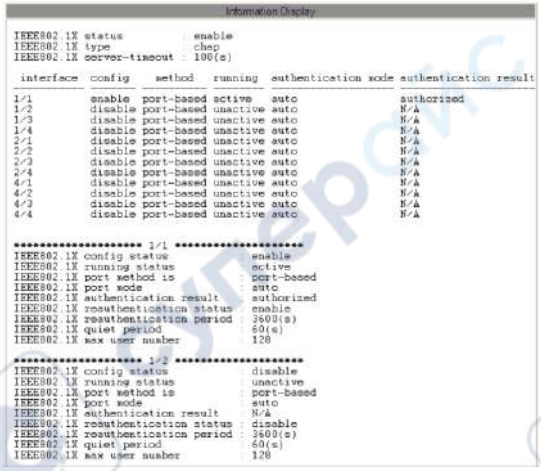
- **PortId**
  Опции: все порты коммутатора
- **IEEE802.1x State**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включение/отключение IEEE802.1x на порту.
  Описание: Когда эта функция включена, связь пользователей через порт зависит от режима порта IEEE802.1x.
- **Port Mode**
  Варианты: Unauthorized-force / Auto / Authorized-force
  По умолчанию: Авто
  Функция: выберите режим аутентификации 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 с этого порта. **Auto** означает, что начальное состояние порта неавторизовано, 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**
  Опции: включить/отключить
  По умолчанию: Отключить
  Функция: Настройка необходимости регулярной повторной аутентификации при успешном выполнении аутентификации.
- **ReAuth Timer**
  Диапазон: 60~7200 с
  По умолчанию: 3600 с
  Функция: при успешной аутентификации установите временной интервал для повторной аутентификации.
- **Quiet Timer**
  Диапазон: 10~120 с
  По умолчанию: 60 сек.
  Функция: если аутентификация не удалась, начинается период молчания (QuietPeriod). В течение периода молчания сервер не отвечает на запросы аутентификации от клиента. После окончания периода молчания сервер снова начинает принимать запросы аутентификации.
- **Port-Method**
  Варианты: на основе порта / на основе MAC-адреса
  По умолчанию: на основе порта
  Функция: настройка режима управления доступом к портам с поддержкой IEEE802.1x.
  Описание: MAC_Based указывает, что пользователи, использующие порт, должны пройти аутентификацию соответственно. Когда пользователь находится в автономном режиме, только пользователь не может использовать сеть. Port_Based указывает, что пользователи аутентифицируются 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: настроить максимальное количество пользователей доступа, использующих порт с поддержкой IEEE802.1x.
  Описание: Конфигурация действительна только для портов с управлением доступом на основе MAC-адресов.
  Диапазон: 100 ~ 300 с

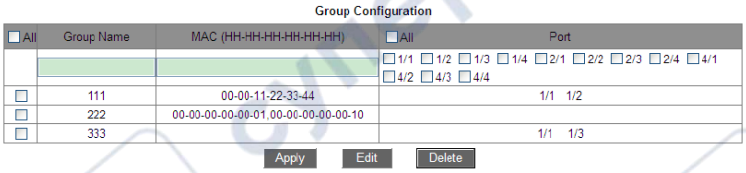
Просмотр IEEE802.1x конфигурации

Щелкнуть [Device Basic Configuration] → [IEEE802.1x configuration] → [EEE802.1x information] для просмотра конфигурации EEE802.1x, как показано на рисунке ниже.



Настройка группы IEEE802.1x

Щелкнуть [Device Basic Configuration] → [IEEE802.1x configuration] → [IEEE802.1x Group configuration] для входа на страницу конфигурации группы IEEE802.1x, как показано на рисунке ниже.

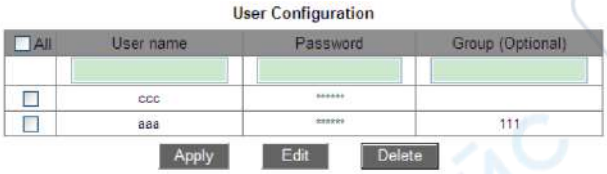


- **Group Name**
  Диапазон: 1~16 символов
  Функция: Настройка имени группы.
- **MAC**
  Формат: HH-HH-HH-HH-HH-HH (H — шестнадцатеричное число)
  Функция: Настройка MAC-адреса для группы. В одну группу можно добавить несколько MAC-адресов, при этом MAC-адреса разделяются однобайтовыми запятыми.
- **Port**
  Функция: Добавить порты для группы.

Группа аутентификации пользователя позволяет настраивать только MAC-адрес или номер порта.

Конфигурирование IEEE802.1x user информации

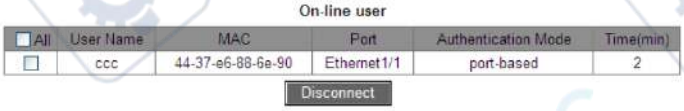
Щелкнуть [Device Basic Configuration] → [IEEE802.1x configuration] → [IEEE802.1x User configuration] для входа на страницу конфигурации IEEE802.1x User, как показано на рисунке ниже.



- **User Name**
  Диапазон: 1~16 символов
  Функция: Настройка имени пользователя IEEE802.1x.
- **Password**
  Диапазон: 1~16 символов
  Функция: Настройка пароля IEEE802.1x.
- **Group**
  Функция: привязать 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 к какой-либо группе проверки подлинности пользователя. В этом случае пользователи могут проводить аутентификацию, используя любой MAC-адрес и номер порта.

Просмотр информации о пользователе IEEE802.1x в режиме онлайн

Щелкнуть [Device Basic Configuration] → [IEEE802.1x configuration] → [IEEE802.1x On-line user] для входа на страницу просмотра IEEE802.1x пользователей онлайн, как показано на рисунке ниже.

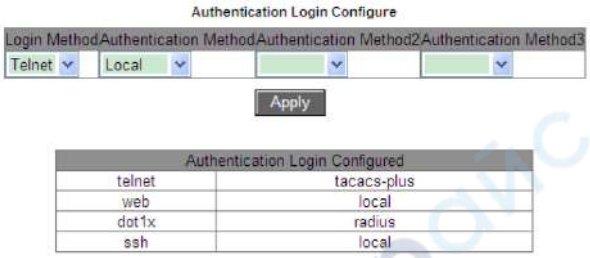


Вы можете выбрать одного или нескольких пользователей и нажать <Disconnect>, чтобы отключить выбранных пользователей от коммутатора.

6.39. Конфигурация авторизации входа

Настройте режим доступа для переключения, режим аутентификации и порядок аутентификации.

Щелкнуть [Device Basic Configuration] → [Authentication login configuration] для входа на страницу конфигурации входа в систему аутентификации, как показано на рисунке ниже.



- **Login Method**
  Опции: Telnet / Web / dot1x / SSH
  Функция: выберите режим доступа для переключения.
- **Authentication Method/Authentication Method 2/Authentication Method 3**
  Опции: Local / TACACS+ / RADIUS / RADIUS + Local / TACACS Plus+ Local
  По умолчанию: Local
  Функция: выберите порядок аутентификации. Сначала выполняется метод аутентификации 1. Если аутентификация не удалась, выполняется метод аутентификации 2. Если и метод аутентификации 1, и метод аутентификации 2 терпят неудачу, выполняется метод аутентификации 3.
  Описание: **Local** означает использование имени пользователя и пароля, установленных локально, для выполнения аутентификации. **TACACS+** означает использование имени пользователя и пароля, установленных на сервере TACACS+ для аутентификации. **RADIUS** означает использование имени пользователя и пароля, установленных на сервере RADIUS, для аутентификации.

Если для доступа к коммутатору используется dot1x, можно выбрать только один режим аутентификации.

6.40. Конфигурация диагностики

6.40.1. Link check (диагностика канала)

Проверка канала использует периодическое взаимодействие протокольных пакетов 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 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 в течение периода ожидания приема (5 с), порт отображает состояние ошибки Tx. Если связь с портом не работает, порт отображает состояние связи.

Порт, для которого отключена проверка состояния линка, работает в пассивном режиме. То есть он не отправляет пакет проверки связи в активном режиме. Однако после получения пакета проверки канала от удаленного узла этот порт немедленно возвращает

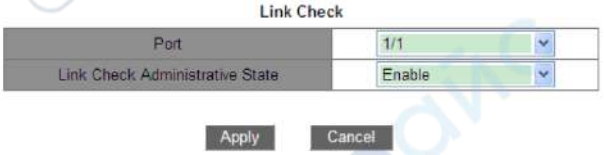
пакет проверки канала, чтобы информировать удаленный узел о том, что он получил пакет проверки канала.

Если кольцевой / резервный порт DRP, для которого включена проверка канала, неисправен (например, ненормальный прием, ненормальная отправка или отключение), кольцевой протокол DRP заблокирует этот кольцевой / резервный порт.

6.40.1.1. Веб конфигурирование

Включение link chaeck на порту

Щелкнуть [Device Basic Configuration] → [Diagnosis Configuration] → [Link Check] для входа на страницу конфигурации диагностики канала, как показано на рисунке ниже.



- **Link Check Administrative State**
  Опции: Disable / Enable
  По умолчанию: Disable
  Функция: включить / отключить проверку связи на порту.

Если одноранговое устройство не поддерживает эту функцию, функция должна быть отключена на подключенном порту локального устройства.

Просмотр диагностики канала на порту, как показано на рисунке ниже

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

- **Link Check State**
  Варианты: Normal / Rx Fault / Disable / Tx Fault/ Link Down
  Описание: если для порта включена проверка канала и порт нормально отправляет и принимает данные, отображается Normal. Если одноранговая сторона не получает пакеты обнаружения от устройства, отображается ошибка отправки. Если устройство не получает пакеты обнаружения от одноранговой стороны,

отображается ошибка приема. Если порт отключен, отображается Link Down. Если Link Check не включен для порта, отображается Disable.

6.40.2. Virtual Cable Tester

VCT (Virtual Cable Tester) использует рефлектометрию во временной области (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 месте повреждения. точка 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:

Короткое: это означает короткое замыкание. Это замыкание двух и более проводов.

Открытый: это означает открытую цепь. На кабеле могут быть оборваны провода.

Нормальный: это означает нормальное кабельное соединение.

Imped: это 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: это означает, что тест VCT не пройден.

6.40.2.1. Веб конфигурирование

Детектирование кабеля

Щелкнуть [Device Basic Configuration] → [Diagnosis Configuration] → [Virtual Cable Tester] для входа на страницу конфигурации виртуального кабельного тестера, как показано на рисунке ниже.

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

6.41. Конфигурация обнаружения петли

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. CPU периодически отправляет пакеты для обнаружения петель на порт. Если какой-либо порт коммутатора принимает 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.

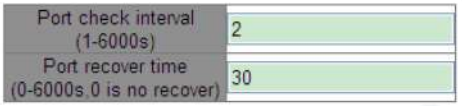
NOTE

Обнаружение петель и ST-Ring / DRP / RSTP / MSTP являются взаимоисключающими. Обнаружение петель на порту нельзя настроить как резервный порт; резервный порт не может быть включен для обнаружения петель.

6.41.1. Веб конфигурирование

Настройка функцию обнаружения петель порта

Щелкнуть [Device Basic Configuration] → [Loop Detect configuration] → [Loop Detect configuration] для входа на страницу Loop detect, как показано на рисунке ниже.



Port	LoopDetect Enable	LoopDetect Status
1/1	☐	-
1/2	☐	-
1/3	☐	-
1/4	☐	-
2/1	☑	No
2/2	☑	No
2/3	☑	Yes
2/4	☐	-
3/1	☐	-
3/2	☐	-
3/3	☐	-
3/4	☐	-
4/1	☐	-
4/2	☐	-
4/3	☐	-
4/4	☐	-
5/1	☐	-
5/2	☐	-
5/3	☐	-
5/4	☐	-

Apply

- **Port check interval**
  Диапазон: 1~6000 с
  По умолчанию: 2 с
  Функция: Настройка временного интервала для отправки пакетов обнаружения петель.
- **Port recovery time**
  Диапазон: 0~6000 с
  По умолчанию: 30 с
  Функция: Настройте время восстановления порта, 0 указывает, что порт не может быть подключен автоматически.
- **Loop Detect Enable**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включение или отключение функции обнаружения петли порта.
- **Loop Detect Status**
  Варианты: Yes / No
  Функция: Статус обнаружения петель показывает наличие петель в сети, в которой включена функция обнаружения петель порта. Yes указывает на наличие петель, а No указывает на отсутствие петли.

6.42. Port CRC Protect

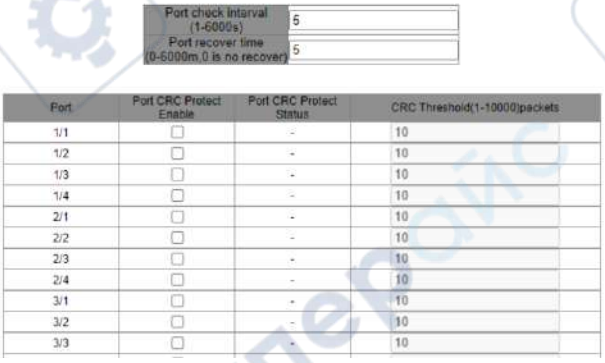
После того, как функция защиты портов CRC включена, может быть реализовано периодическое обнаружение пакетов с ошибками CRC. Если количество пакетов ошибок CRC превышает ожидаемый порог во время обнаружения, выключите порт. Подключите

порт через некоторое время и продолжайте обнаружение. Время обнаружения пакетов ошибок CRC и время восстановления порта можно настроить в программном обеспечении.

6.42.1. Веб конфигурирование

Настройка функцию защиты порта CRC.

Щелкнуть [Device Basic Configuration] → [CRC Protect configuration] → [CRC Protect configuration] для входа на страницу конфигурации CRC Protect, как показано на рисунке ниже.



- **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 пороговое значение, выключите порт.
  Диапазон: 0~6000 м
  По умолчанию: 5 м
  Функция: Настройте время восстановления порта, 0 указывает, что порт не может быть подключен автоматически.
- **Port CRC Protect Enable**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: Включить или отключить функцию защиты портов 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 порта CRC включена, а состояние порта — соединение. --: функция защиты порта CRC не включена.
- **CRC Threshold**
  Диапазон: 1~10000 пакетов
  По умолчанию: 10 пакетов
  Функция: настроить пороговое значение CRC.