Промышленный управляемый

Коммутатор STEZ32xx

Руководство пользователя

Оглавление

1. Описание устройства

1.1. Введение

Коммутаторы серии STEZ32xx включает в себя серию высокопроизводительных управляемых промышленных Ethernet-коммутаторов. STEZ32xx соответствует EN50155, EN50121 и другим промышленным стандартам. Коммутатор представляет собой коммутатор уровня 2, а также протоколы резервирования MSTP, RSTP, IS-Ring, IEC62439-6, гарантируя надежную работу системы. Коммутаторы также поддерживает оптический модуль SFP с функцией цифровой диагностики, который может контролировать мощность передачи и мощность приема оптического модуля приемопередатчика в режиме реального времени. Кроме того, коммутаторы соответствуют стандартам электроэнергетики IEC61850-3 и IEEE1613.

1.2. Модели серии

В портфолио серии STEZ32xx входят следующие коммутаторы:

- **STEZ3208G-4GSFP** (артикул 70110005) – 4 порта 100/1000Base-X SFP, 8 портов 10/100/1000Base-T(X) RJ45, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания;
- **STEZ3208G-2GSFP** (артикул 70110006) - 2 порта 100/1000Base-X SFP, 8 портов 10/100/1000Base-T(X) RJ45, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания;
- **STEZ3208** (артикул 70110007) – 8 портов 10/100Base-TX, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания;
- **STEZ3208-2GSFP** (артикул 70110008) – 2 порта 100/1000Base-X SFP, 8 портов 10/100Base-TX, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания;
- **STEZ3208-4GSFP** (артикул 70110009) – 4 порта 100/1000Base-X SFP, 8 портов 10/100Base-TX, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания;
- **STEZ3208G** (артикул 70110010) – 8 портов 10/100/1000Base-T(X) RJ45, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания;

- **STEZ3216** (артикул 70110011) - 16 портов 10/100Base-TX, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания;
- **STEZ3216G** (артикул 70110012) - 16 портов 10/100/1000Base-T(X) RJ45, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания;
- **STEZ3216-2GSFP** (артикул 70110013) - 2 порта 100/1000Base-X SFP, 16 порта 10/100Base-T(X) RJ45, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания;
- **STEZ3216G-2GSFP** (артикул 70110014) - 2 порта 100/1000Base-X SFP, 16 портов 10/100/1000Base-T(X) RJ45, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания;
- **STEZ3216-4GSFP** (артикул 70110015) - 4 порта 100/1000Base-X SFP, 16 портов 10/100Base-T(X) RJ45, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания;
- **STEZ3216G-4GSFP** (артикул 70110016) - 4 порта 100/1000Base-X SFP, 16 портов 10/100/1000Base-T(X) RJ45, Console Port RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания;
- **STEZ3208G-8GSFP** (артикул 70110017) - 8 портов 100/1000Base-X SFP, 8 портов 10/100/1000Base-T(X) RJ45, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания;
- **STEZ3208G-12GSFP** (артикул 70110018) - 12 портов 100/1000Base-X SFP, 8 портов 10/100/1000Base-T(X) RJ45, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания;
- **STEZ3208-2SFP** (артикул 70110019) - 2 порта 100Base-X SFP, 8 портов 10/100Base-TX, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания;
- **STEZ3208-4SFP** (артикул 70110020) - 4 порта 100Base-X SFP, 8 портов 10/100Base-TX, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания;
- **STEZ3216-4SFP** (артикул 70110021) - 4 порта 100Base-X SFP, 16 портов 10/100Base-T(X) RJ45, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания;
- **STEZ3208-8SFP** (артикул 70110022) - 8 портов 100Base-X SFP, 8 портов10/100Base-T(X) RJ45, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания.
- **STEZ3208G-4GSFP-PN** (артикул 70110034) – 4 порта 100/1000Base-X SFP, 8 портов 10/100/1000Base-T(X) RJ45, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания, PROFINET;
- **STEZ3208G-2GSFP-PN** (артикул 70110035) - 2 порта 100/1000Base-X SFP, 8 портов 10/100/1000Base-T(X) RJ45, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания, PROFINET;
- **STEZ3208-PN** (артикул 70110036) – 8 портов 10/100Base-TX, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания, PROFINET;
- **STEZ3208-2GSFP-PN** (артикул 70110037) – 2 порта 100/1000Base-X SFP, 8 портов 10/100Base-TX, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания, PROFINET;
- **STEZ3208-4GSFP-PN** (артикул 70110038) – 4 порта 100/1000Base-X SFP, 8 портов 10/100Base-TX, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания, PROFINET;

- **STEZ3208G-PN** (артикул 70110039) – 8 портов 10/100/1000Base-T(X) RJ45, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания, PROFINET;
- **STEZ3216-PN** (артикул 70110040) - 16 портов 10/100Base-TX, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания, PROFINET;
- **STEZ3216G-PN** (артикул 70110041) - 16 портов 10/100/1000Base-T(X) RJ45, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания, PROFINET;
- **STEZ3216-2GSFP-PN** (артикул 70110042) - 2 порта 100/1000Base-X SFP, 16 порта 10/100Base-T(X) RJ45, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания, PROFINET;
- **STEZ3216G-2GSFP-PN** (артикул 70110043) - 2 порта 100/1000Base-X SFP, 16 портов 10/100/1000Base-T(X) RJ45, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания, PROFINET;
- **STEZ3216-4GSFP-PN** (артикул 70110044) - 4 порта 100/1000Base-X SFP, 16 портов 10/100Base-T(X) RJ45, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания, PROFINET;
- **STEZ3216G-4GSFP-PN** (артикул 70110045) - 4 порта 100/1000Base-X SFP, 16 портов 10/100/1000Base-T(X) RJ45, Console Port RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания, PROFINET;
- **STEZ3208G-8GSFP-PN** (артикул 70110046) - 8 портов 100/1000Base-X SFP, 8 портов 10/100/1000Base-T(X) RJ45, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания, PROFINET;
- **STEZ3208G-12GSFP-PN** (артикул 70110047) - 12 портов 100/1000Base-X SFP, 8 портов 10/100/1000Base-T(X) RJ45, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания, PROFINET;
- **STEZ3208-2SFP-PN** (артикул 70110048) - 2 порта 100Base-X SFP, 8 портов 10/100Base-TX, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания, PROFINET;
- **STEZ3208-4SFP-PN** (артикул 70110049) - 4 порта 100Base-X SFP, 8 портов 10/100Base-TX, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания, PROFINET;
- **STEZ3216-4SFP-PN** (артикул 70110050) - 4 порта 100Base-X SFP, 16 портов 10/100Base-T(X) RJ45, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания, PROFINET;
- **STEZ3208-8SFP-PN** (артикул 70110051) - 8 портов 100Base-X SFP, 8 портов10/100Base-T(X) RJ45, Консольный порт RS232 RJ45, 12-24VDC(9-36VDC) резервированный источник питания, PROFINET.

1.3. Функции программного обеспечения

Коммутаторы серии STEZ32xx предоставляют множество программных функций, удовлетворяющих различные требования клиентов.

- Протоколы резервирования: RSTP/STP, MSTP, IS-Ring, DRP
- Поддержка мультикаст протоколов: IGMP Snooping, GMRP и static multicast
- VLAN, PVLAN, GVRP, QoS и ARP
- Управление шириной канала: port trunk, port rate limiting

- Протоколы синхронизации времени: PTP, SNTP
- Безопасность: ACL, port isolate, IEEE802.1x, TACACS+, RADIUS, SSH, SSL
- Диагностика: port mirroring, LLDP, контроль линии, loop detect
- 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, SNMP v1/v2c/v3
- Поддержка промышленный протоколов EtherNet/IP, ModbusTCP, Profinet.

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 response information for ping operation. Restart the switch. Save current configuration. Display current configuration. Update software.	Input "configure terminal" to enter the Configuration mode from the Privileged mode. 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.

Таблица 1. Типы просмотра

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

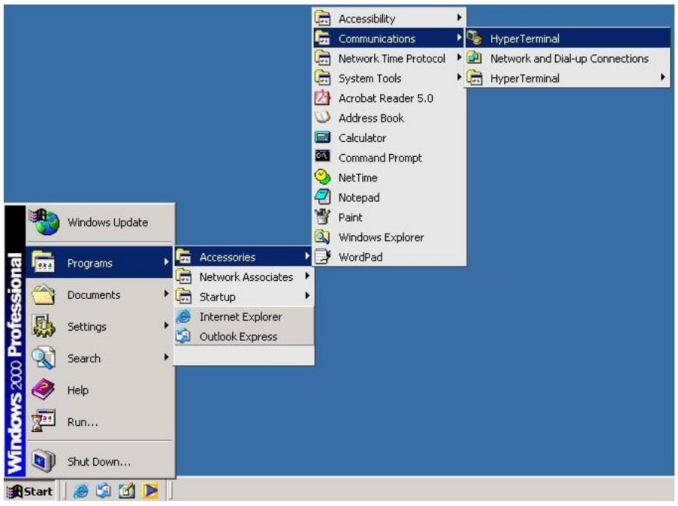


Рисунок 1. Запуск Hyper Terminal

Можно использовать любой другой эмулятор терминала, такой как Putty.

- Введите имя для нового соединения

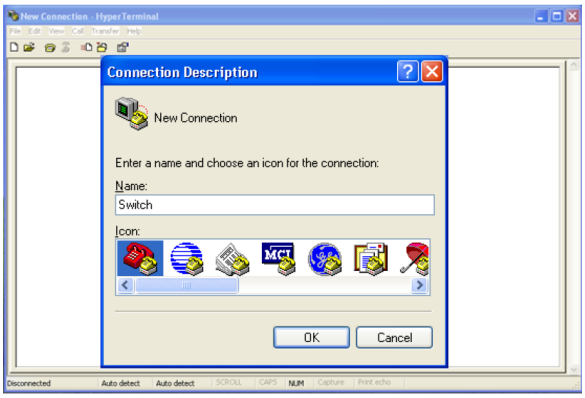


Рисунок 2. Создание нового соединения

- Выберите номер COM порта для его использования

Рисунок 3. Выбор коммутационного порта

- 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.

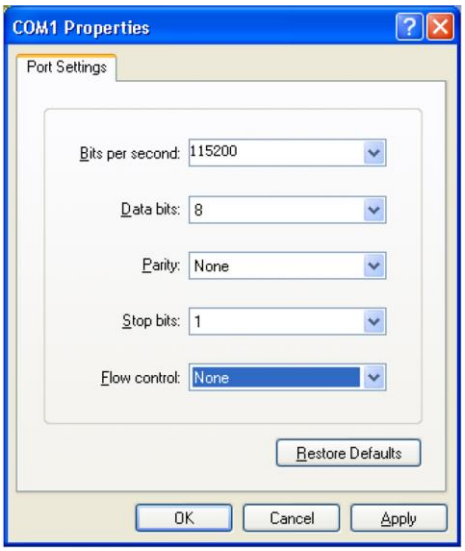


Рисунок 4. Выбор параметров порта

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

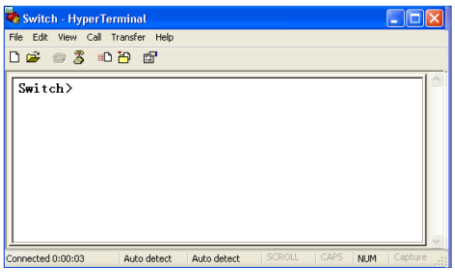


Рисунок 5. CLI

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.

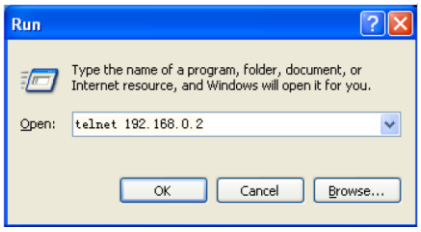


Рисунок 6. Подключение к telnet

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

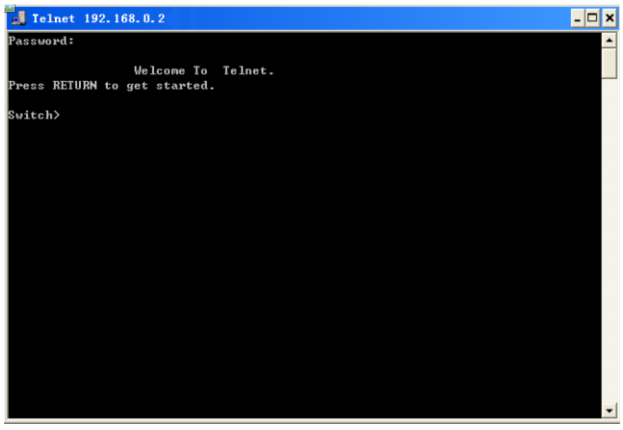


Рисунок 7. Интерфейс telnet

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. Обслуживание коммутатора

Презагрузка может быть выполнена, как показано на русунке 8:

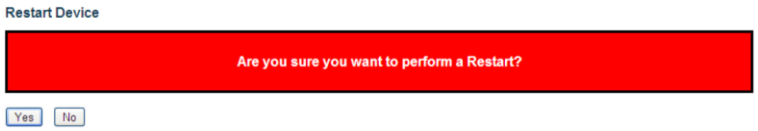


Рисунок 8. Перезагрузка

Перед перезагрузкой подтвердите сохранение текущей конфигурации. Если вы выберете «Да», коммутатор запустит текущую конфигурацию после перезагрузки. Если вы выберете «Нет», коммутатор использует предыдущую сохраненную конфигурацию. Если конфигурация не была сохранена, коммутатор восстановит конфигурацию по умолчанию после перезагрузки.

Восстановление конфигурацию по умолчанию, как показано на рисунке 9:

Рисунок 9. Восстановление конфигурации по умолчанию

После восстановления настроек по умолчанию необходимо перезагрузить устройство, чтобы настройки вступили в силу.

Сохранение текущей running-congif, как показано на рисунке 10.

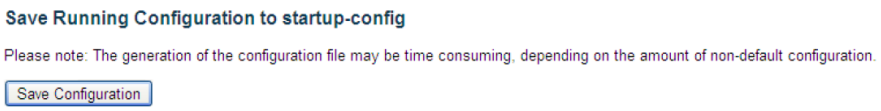


Рисунок 10. Сохранение текущей конфигурации

Загрузить файл с коммутатора на сервер можно, как показано на рисунках 11 и 12.

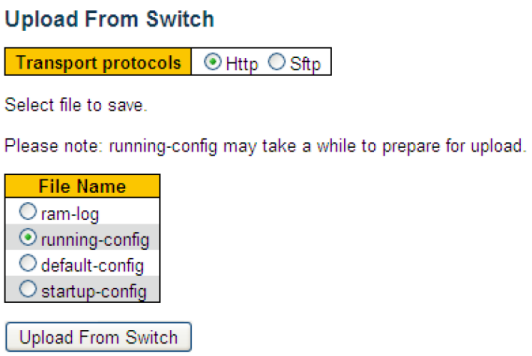


Рисунок 11. Скачивания файла с коммутатора – через HTTP

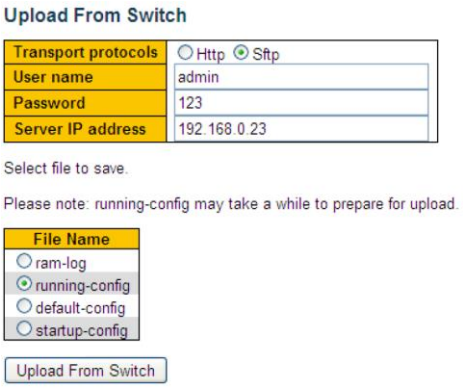


Рисунок 12. Скачивания файла с коммутатора – через SFTP

- **{User name, Password }**
  Диапазон: {1~63 символа, 1~63 символа}
  Описание: Введите имя пользователя и пароль, созданные на SFTP-сервере.
- **Server IP address**
  Формат: A.B.C.D.
  Описание: Настройка IP-адреса SFTP-сервера.

Для передачи файла по SFTP вам необходимо настроить имя пользователя SFTP, пароль и IP-адрес сервера SFTP.
В процессе передачи файлов поддерживает работу SFTP-сервера.

Вы можете сохранить файл в коммутаторе на локальном / сервере. **ram-log** записывает информацию журнала, **running-config** — это текущий рабочий файл конфигурации коммутатора, **default-config** — это файл конфигурации по умолчанию, а **startup-config** — это файл запуска коммутатора. Выберите файл и нажмите <Upload from switch>, чтобы сохранить файл на локальном компьютере / сервере.

Скачать файл с сервера на коммутатор можно, как показано на рисунках 13 и 14.

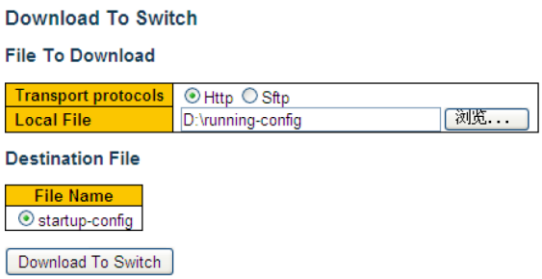


Рисунок 12. Загрузка файла на кммутатора – через HTTP

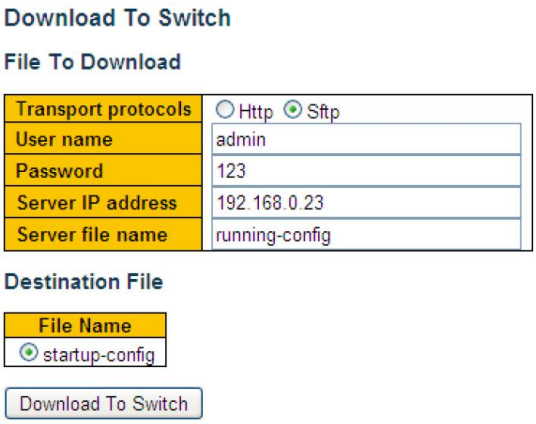


Рисунок 13. Загрузка файла на кммутатора – через SFTP

- **Local File**
  Функция: Выберите файл конфигурации, хранящийся в локальном.
- **{ User name, Password }**
  Диапазон: {1~63 символа, 1~63 символа}
  Описание: Введите имя пользователя и пароль, созданные на SFTP-сервере.
- **Server IP address**
  Формат: A.B.C.D.
  Описание: Настройка IP-адреса SFTP-сервера.
- **Server file name**
  Диапазон: 1~63 символа
  Описание: Настройте имя файла конфигурации, хранящегося на сервере SFTP.

Для передачи файла по SFTP вам необходимо настроить имя пользователя SFTP, пароль и IP-адрес сервера SFTP.
В процессе передачи файлов поддерживает работу SFTP-сервера.

Вы можете загрузить файл конфигурации с сервера для коммутатора в качестве нового файла запуска для коммутатора. Новый файл запуска заменит исходный файл конфигурации запуска. Нажмите <Download To Switch>, чтобы загрузить файл конфигурации с сервера на коммутатор.

Загрузка и скачивание файлов конфигурации через USB-накопитель, как показано на рисунке.

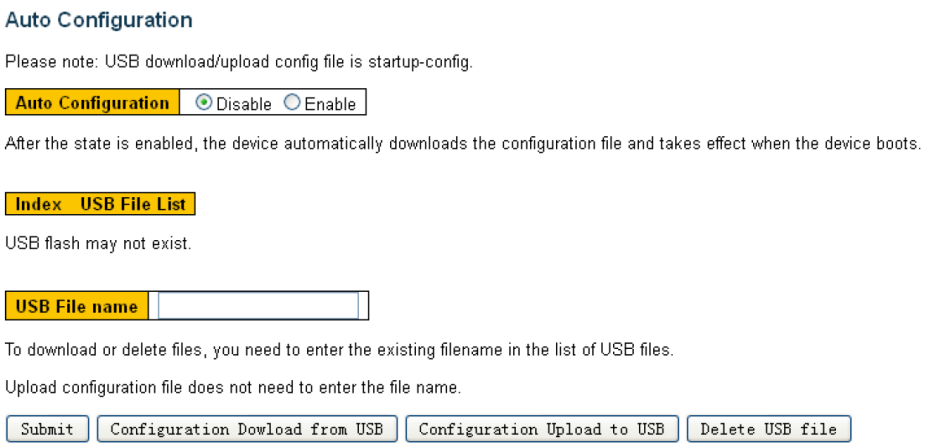


Рисунок 14. USB конфигурация

4. Базовая конфигурация

4.1. Информация о системе

Системная информация включает контакты, имя системы, тип устройства, MAC-адрес, серийный номер, системное время и информацию о версии, как показано на рисунке 15.

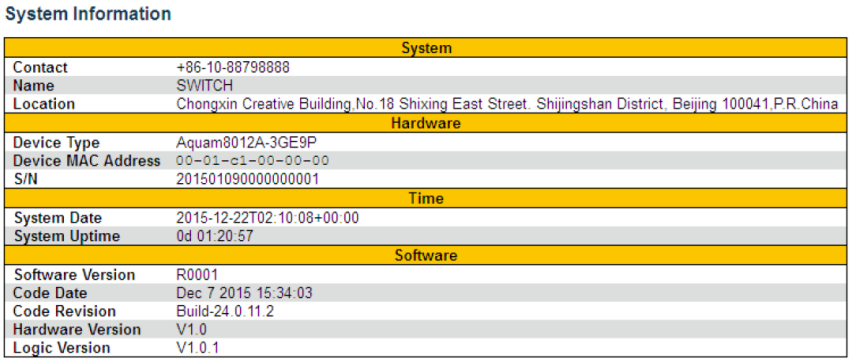


Рисунок 15. Информация о системе

4.2. Конфигурация системы

Конфигурация системы включает контакт, имя системы и конфигурацию местоположения, как показано на рисунке 16.

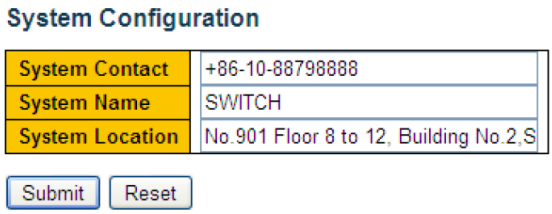


Рисунок 16. Конфигурация системы

- **System Contact**
  Диапазон: 0~255 символов (символы ASCII от 32 до 126)
- **System Name**
  Диапазон: 0~255 символов (алфавит A~Z / a~z, цифры 0~9, знак минус -. Первый символ должен быть буквой, а первый или последний символ не должен быть знаком минус.
- **System Location**
  Диапазон: 0~255 символов (символы ASCII от 32 до 126)

4.3. Загрузка CPU

Нагрузка измеряется как усредненная за последние 100 мс, 1 с и 10 с, как показано на рисунке ниже.

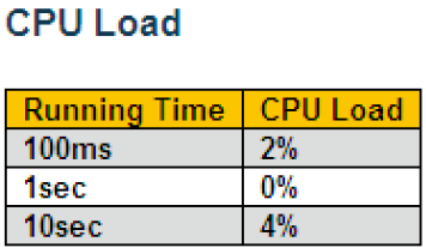


Рисунок 17. Загрузка CPU

4.4. Обновление внутреннего ПО (firmware)

Обновление микропрограммы может помочь коммутатору повысить его производительность. Для коммутаторов этой серии обновление микропрограммы включает обновление версии загрузочной версии и обновление версии системного программного обеспечения. Версия Boot должна быть обновлена до версии системного программного обеспечения. Если версия Boot не меняется, можно обновить только версию системного ПО. Для обновления прошивки требуется помощь HTTP/SFTP.

4.4.1. Обновление прошивки через HTTP

Обновить firmware можно, как показано на рисунке ниже:

Рисунок 18. Обновление прошивки - HTTP

- **Upgrade Target**
  Опции: Application / Bootloader
  Функция: выберите цель обновления.
- **Upgrade Mode**
  Варианты: Первый / Второй / Все
  Описание: На коммутатор можно загрузить две версии программного обеспечения, они могут быть одинаковыми или разными. Инфикаторы на версию 1 и версию 2.
- **Local File**
  Функция: выберите файл обновления, хранящийся на локальном компьютере.

Когда обновление будет завершено, как показано на рисунке 19, активируйте версию программного обеспечения и перезагрузите устройство, откройте страницу «Информация о системе», чтобы проверить, успешно ли выполнено обновление и активна ли новая версия.

Рисунок 19. Обовление прошло успешно

4.4.2. Обновление прошивки 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 пользователя SFTP, как показано на рисунке 20. Введите пользователя и пароль, например, admin и 123. Установите номер порта 22. Введите путь для сохранения файла версии прошивки в поле Root path.

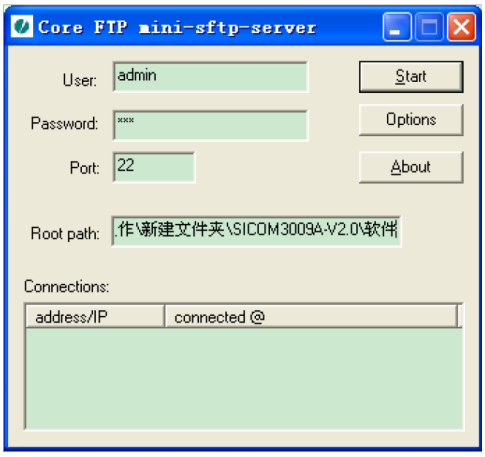


Рисунок 20. Добавление SFTP пользователя

Обновить прошивку как показано на рисунке ниже:

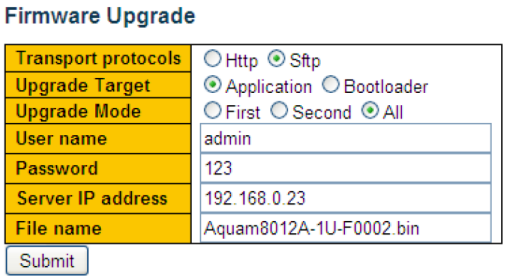


Рисунок 21. Обновление прошивки - SFTP

- **Upgrade Target**
  Опции: Application / Bootloader
  Функция: выберите цель обновления.
- **Upgrade Mode**
  Варианты: Первый/Второй/Все
  Описание: В коммутатор можно загрузить две версии прошивки, они могут быть одинаковыми или разными. Индикаторы на версию 1 и версию 2.
- **{ User name, Password }**
  Диапазон: {1~63 символа, 1~63 символа}
  Описание: Введите имя пользователя и пароль, созданные на SFTP-сервере.
- **Server IP address**
  Формат: A.B.C.D.
  Описание: Настройка IP-адреса SFTP-сервера.
- **File name**
  Диапазон: 1~63 символа
  Описание: Настройка имени файла обновления микропрограммы, хранящегося на SFTP-сервере.

Когда обновление будет завершено, как показано на рисунке 22, активируйте версию программного обеспечения и перезагрузите устройство, откройте страницу «Информация о системе», чтобы проверить, успешно ли выполнено обновление и активна ли новая версия.

Рисунок 22. Обовление прошло успешно

4.5. Активация Firmware

Активируйте приложение прошивки, как показано на рисунке ниже.

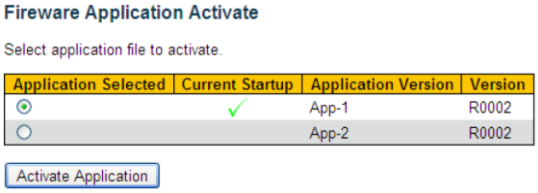


Рисунок 23. Активирование прошивки

Выберите одну версию и нажмите кнопку <Activate Application>, настроив версию как активную версию, которая будет следующей версией запуска. Одновременно может быть активна только одна версия. Текущий запуск указывает, что версия является текущей рабочей версией.

5. IP конфигурация

5.1. IP address конфигурация

Просмотрите IP-адрес коммутатора с помощью консольного порта.

Войдите в интерфейс командной строки коммутатора через консольный порт. Запустите команду «**show interface vlan 1**» в привилегированном режиме, чтобы просмотреть IP-адрес коммутатора, как показано в красном круге на рисунке 24.

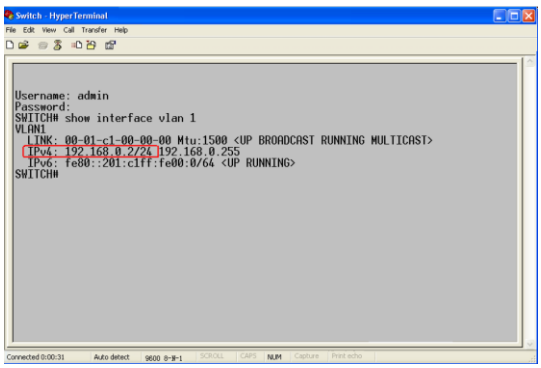


Рисунок 24. Просмотр IP адреса

Создание IP-интерфейса.

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

Конфигурирование IP address.

IP-адрес коммутатора можно настроить вручную или получить автоматически, как показано на рисенке ниже.

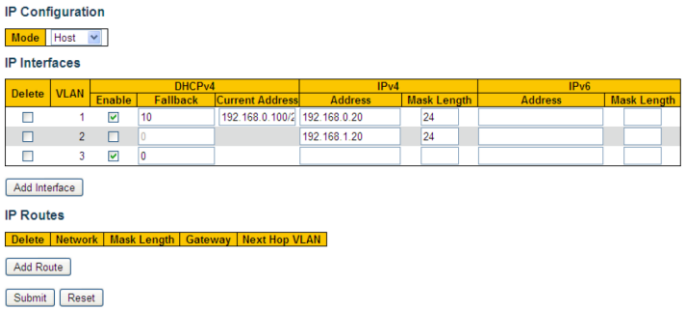


Рисунок 25. Конфигурирование IP адреса

- **VLAN**
  Функция: Настройте атрибут VLAN для IP-интерфейса, только порты в этой VLAN смогут получить доступ к IP-интерфейсу.
- **DHCPv4-Enable**
  Опции: Enable / Disable
  Функция: отключить DHCPv4, настроить IP-адрес и маску вручную; включить DHCPv4, коммутатор (как DHCP-клиент) автоматически получает IP-адрес через DHCP. В сети должен быть DHCP-сервер для назначения IP-адресов и масок клиентам.
- **DHCPv4-Fallback**
  Диапазон: 0~4294967295 с
  Функция: если значение не равно нулю, коммутатор получает время попытки IP-адреса по протоколу динамической конфигурации хоста (DHCP). В этом случае IP-адрес необходимо настроить вручную. По истечении времени попытки IP-адрес, настроенный вручную, вступает в силу. Если значение равно 0, коммутатор неоднократно пытается получить IP-адрес, пока не получит IP-адрес через DHCP. В этом случае IP-адрес не нужно настраивать вручную.
- **DHCPv4-Current Address**
  Функция: отображение IP-адреса и длины маски, которые автоматически получаются с DHCP-сервера. Если коммутатору не удается получить IP-адрес через DHCP в течение времени попытки, IP-адрес и длина маски, настроенные вручную, отображаются в поле **Current Address**.
- **IPv4-Address**
  Формат: A.B.C.D.
  Функция: вручную настроить IP-адрес.
- **IPv4-Mask Length**

Функция: 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. Длина маски — это число «1» в маске подсети. Нажмите <Добавить интерфейс>, чтобы добавить новый IP-интерфейс, поддерживается не более 8 интерфейсов.

Каждый IP-интерфейс поддерживает один IP-адрес.
IP-адреса разных сегментов сети должны быть настроены для разных IP-интерфейсов.

Просмотр IP-интерфейсов, как показано на рисунке 26.

IP Interfaces

Interface	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	::1/128	
OS:lo	IPv6	fe80::1/64	
VLAN1	LINK	00-01-c1-00-00-00	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.0.100/24	
VLAN1	IPv6	fe80::201:c1ff:fe00:0/64	
VLAN2	LINK	00-01-c1-00-00-00	<BROADCAST MULTICAST>
VLAN2	IPv4	192.168.1.20/24	
VLAN2	IPv6	fe80::201:c1ff:fe00:0/64	
VLAN3	LINK	00-01-c1-00-00-00	<BROADCAST RUNNING MULTICAST>
VLAN3	IPv6	fe80::201:c1ff:fe00:0/64	

IP Routes

Network	Gateway	Status
127.0.0.1/32	127.0.0.1	<UP HOST>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

Neighbour Cache

IP Address	Link Address
192.168.0.184	VLAN1:44-37-e6-88-6e-90
fe80::201:c1ff:fe00:0	VLAN1:00-01-c1-00-00-00
fe80::201:c1ff:fe00:0	VLAN2:00-01-c1-00-00-00
fe80::201:c1ff:fe00:0	VLAN3:00-01-c1-00-00-00

Рисунок 25. Просмотр IP-интерфейсов

5.2. ARP

Протокол разрешения адресов (Address Resolution Protocol - ARP) 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.

5.2.1. Веб конфигурирование

Конфигурировние ARP aging time, как показано на рисунке 26.

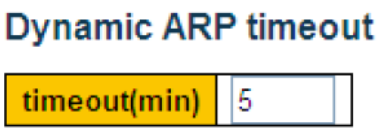


Рисунок 26. Конфигурировние ARP aging time

- **timeout**
  Диапазон: 0 ~ 60 мин.
  По умолчанию: 5 мин.
  Функция: настроить время устаревания ARP, когда время устаревания установлено на 0, устаревание запрещено. Описание. Время устаревания ARP — это время с момента добавления динамической записи ARP в таблицу до момента удаления записи из таблицы.

Добавление статитческой записи ARP, как показано на рисунке 27

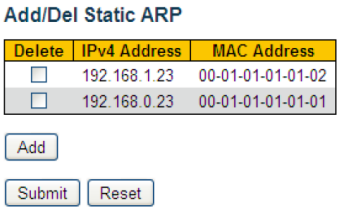


Рисунок 27. Добавление статитческой записи ARP

- **ARP**
  Портфолио: {IP-адрес, MAC-адрес}
  Формат: {A.B.C.D, HHHHHHHHHHHH} (H — шестнадцатеричное число).
  Функция: настройка статической записи ARP.

Как правило, коммутатор автоматически запоминает записи ARP. Ручная настройка не требуется.

Нажмите <Add>, чтобы добавить новую статическую запись ARP, поддерживается не более 128 статических записей ARP.

5.3. DHCP конфигурация

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 28.

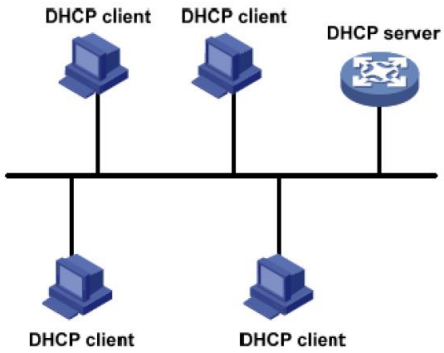


Рисунок 28. Добавление статитческой записи ARP

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. Срок аренды для статического размещения является постоянным.

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.

5.3.1. Конфигурирование DHCP сервера

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.

5.3.1.1. DHCP Address Pool

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.

5.3.1.1.1. Веб конфигурирование

Включение DHCP сервера, как показано на рисунке 29.

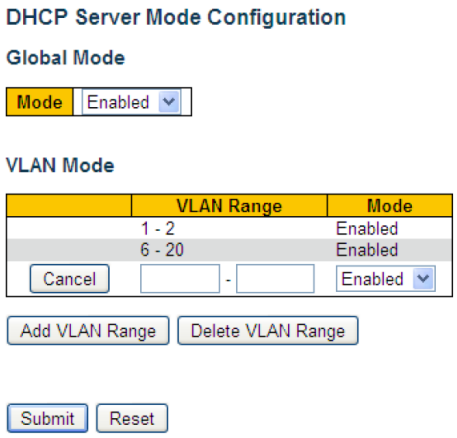


Рисунок 29 Включение DHCP сервера

- **Global Mode**
  Опции: Disabled / Enabled
  По умолчанию: Disabled
  Функция: выберите текущий коммутатор для DHCP-сервера, чтобы выделить IP-адрес клиенту или нет.
- **{VLAN Range, Mode}**
  Диапазон: {1~4095, отключено/включено}
  Функция: если для VLAN клиента, подающего заявку на получение IP-адреса, установлено значение Enabled, DHCP-сервер выделяет IP-адрес клиенту. В противном случае DHCP-сервер не выделяет IP-адрес клиенту.
  Значения: binary/ascii

Создание DHCP address pool, как показано на рисунке 30.

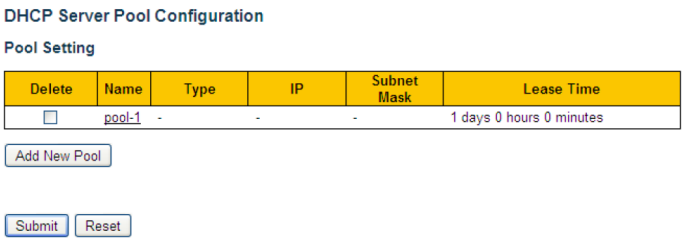


Рисунок 30 Создание DHCP address pool

- **Name**
  Диапазон: 1~32 символа
  Функция: настроить имя пула IP-адресов.
  Нажмите <Добавить новый пул>, чтобы создать новый пул адресов DHCP.

Настройте пул адресов DHCP, щелкните <Name>, чтобы настроить пул адресов DHCP, как показано на рисунке 31.

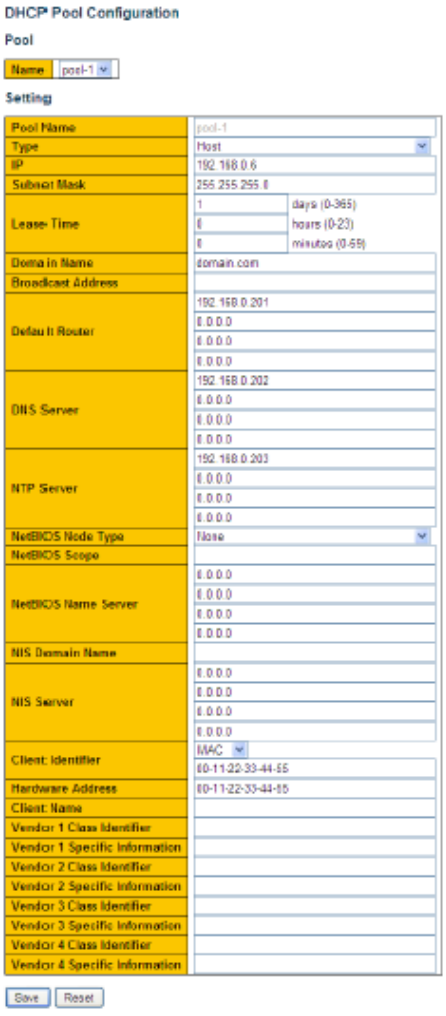


Рисунок 31 Конфигурирование пула адресов DHCP

- **Name**
  Функция: выбрать имя созданного пула.
- **Type**
  Варианты: Нет/Сеть/Хост
  По умолчанию: Нет
  Функция: Настройка типа пула адресов. Сеть: коммутатор динамически выделяет IP-адреса нескольким DHCP-клиентам. Хост: коммутатор поддерживает статическое выделение IP-адресов специальным DHCP-клиентам.
- **{IP, Subnet Mask}**
  Функция: Сеть указывает, что вы можете настроить диапазон пула IP-адресов, а диапазон адресов определяется маской подсети. Маска подсети представляет собой число длиной 32 бита, 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.
  Хост указывает, что вы можете настроить статически ограниченный IP-адрес клиента. Назначение статического IP-адреса реализовано путем ограничения MAC-адреса и IP-адреса клиента. Когда клиент с этим MAC-адресом запрашивает IP-адрес, DHCP-сервер находит IP-адрес, соответствующий MAC-адресу клиента, и выделяет IP-адрес клиенту. Приоритет этого режима выделения выше, чем у динамического выделения IP-адресов, а срок аренды является постоянным.
- **Lease Time**
  Диапазон: 0 дней 0 часов 0 минут~365 дней 23 часа 59 минут
  По умолчанию: 1 день 0 час 0 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.
- **Domain Name**
  Диапазон: 1~36 символов
  Функция: настроить доменное имя пула IP-адресов. При назначении IP-адреса клиенту также отправьте клиенту суффикс доменного имени.
- **Broadcast Address**
  Формат: A.B.C.D.
  Функция: настроить широковещательный адрес клиента, выделенный DHCP-сервером.
- **Default Router**
  Формат: A.B.C.D.
  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 максимум 4 шлюза.
- **DNS Server**
  Формат: A.B.C.D.
  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 4 DNS-сервера.

- **NTP Server**
  Формат: A.B.C.D.
  Функция: Настройка адреса клиентского NTP-сервера, выделенного DHCP-сервером.
- **NetBIOS Node Type**
  Варианты: None / B-node / P-node / M-node / H-node
  По умолчанию: Нет
  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: B-узел получает отображение в широковещательном режиме. P-узел получает сопоставление, отправляя одноадресный пакет для связи с WINS-сервером. M-узел получает отображение, отправив широковещательный пакет в первый раз. Если M-узел не может получить сопоставление в первый раз, он получает сопоставление, отправляя одноадресный пакет для связи с WINS-сервером во второй раз. H-узел получает сопоставление, отправляя одноадресный пакет для связи с WINS-сервером в первый раз. Если H-узел не может получить отображение в первый раз, он получает отображение, отправив широковещательный пакет во второй раз.
- **NetBIOS Scope**
  Диапазон: 1~36 символов
  Функция: Настройка имени NetBIOS.
- **NetBIOS Name Server**
  Формат: A.B.C.D.
  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 4 серверов WINS.
- **NIS Domain Name**
  Диапазон: 1~36 символов
  Функция: Настройте доменное имя клиента NIS, выделенное DHCP-сервером.
- **NIS Server**
  Формат: A.B.C.D.
  Функция: настроить адрес клиентского NIS-сервера, выделенный DHCP-сервером.
- **Client Identifier**
  Варианты: None / FQDN / MAC
  По умолчанию: Нет
  Функция: если тип пула — хост, укажите уникальный идентификатор клиента.
- **Hardware Address**
  Формат: ЧЧ-ЧЧ-ЧЧ-ЧЧ-ЧЧ-ЧЧ (Н — шестнадцатеричное число)

Функция: если тип пула — хост, настройте статически ограниченный MAC-адрес клиента.

- **Client Name**
  Диапазон: 1~32 символа
  Функция: Настройка имени пользователя клиента. Настройка имени пользователя клиента.
- **Vendor i Class Identifier**
  Диапазон: 1~64 символа
  Функция: Настройка идентификатора класса поставщика клиента, назначенного DHCP-сервером.
- **Vendor i Specific Information**
  Диапазон: 1~64 шестнадцатеричных числа
  Функция: Настройка информации о поставщике клиента, выделяемой DHCP-сервером.

Настройка исключенных IP-адреса (IP-адреса не выделяются динамически в пуле адресов DHCP), как показано на рисунке 32.

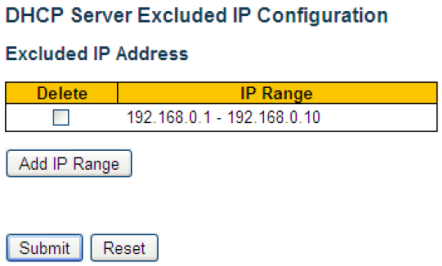


Рисунок 32 Конфигурирование исключаемых IP-адресов

- **IP Range**
  Функция: настроить диапазон IP-адресов, которые не распределяются динамически в пуле адресов DHCP. При распределении IP-адресов DHCP-сервер должен исключить занятый IP-адрес (например, IP-адреса шлюза и DNS-сервера). В противном случае один и тот же IP-адрес может быть назначен двум клиентам, что приведет к конфликту IP-адресов.
  Нажмите <Add IP Range>, чтобы настроить диапазон IP-адресов, которые не выделяются динамически.

Просмотр статистики DHCP-сервера, как показано на рисунке 33.

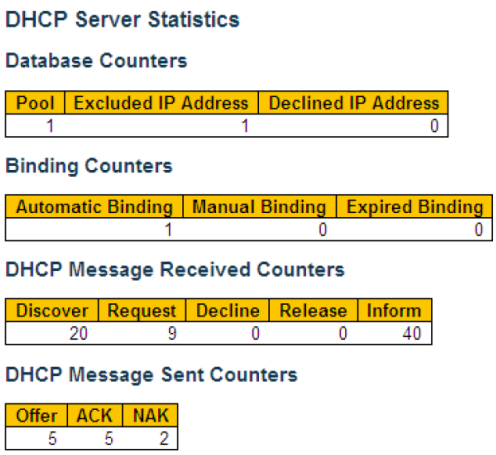


Рисунок 33 Просмотр статистики DHCP-сервера

Просмотр информации об IP-адресах, выделенных DHCP-сервером, как показано на рисунке 34.

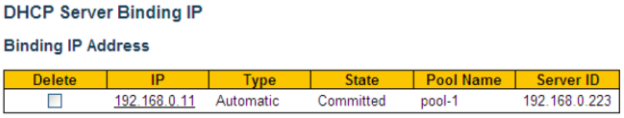


Рисунок 34 Просмотр информации об IP-адресах

Просмотр IP-адреса, отклоненный DHCP-клиентами, как показано на рисунке 35.

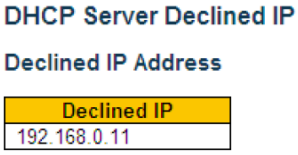


Рисунок 34 Просмотр IP-адреса, отклоненный DHCP-клиентами

Когда клиент обнаруживает, что IP-адрес, выделенный сервером, конфликтует со статическим IP-адресом в том же сегменте сети, он отправляет на сервер пакет отклонения, чтобы отклонить этот IP-адрес. Сервер записывает IP-адрес, отклоненный клиентом, и не будет выделять этот IP-адрес другим клиентам в течение определенного периода времени.

5.3.2. DHCP Snooping

Отслеживание DHCP — это функция мониторинга служб DHCP на уровне 2 и функция безопасности DHCP, обеспечивающая дополнительную безопасность клиента. Механизм безопасности DHCP Snooping может контролировать, что только доверенный порт может пересылать сообщение запроса DHCP-клиента на легальный сервер, в то же время он может контролировать источник ответного сообщения DHCP-сервера, гарантируя, что

клиент получит IP-адрес. с действительного сервера и предотвращение выделения IP-адресов или других параметров конфигурации другим хостам поддельным или недействительным DHCP-сервером.

Механизм безопасности DHCP Snooping делит порт на доверенный порт и ненадежный порт. Доверенный порт: это порт, который прямо или косвенно подключается к действительному DHCP-серверу. Доверенный порт обычно пересылает сообщения запросов DHCP-клиентов и ответные сообщения DHCP-серверов, чтобы гарантировать, что DHCP-клиенты могут получить допустимые IP-адреса. Ненадежный порт: это порт, который подключается к недействительному DHCP-серверу. Ненадежный порт не пересылает сообщения запросов DHCP-клиентов и ответные сообщения DHCP-серверов, чтобы предотвратить получение DHCP-клиентами недопустимых IP-адресов.

5.3.2.1. Веб конфигурирование

Включите функцию DHCP Snooping, как показано на рисунке 35.

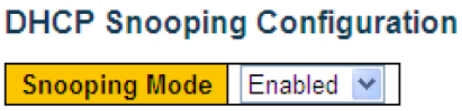


Рисунок 35 Включение функции DHCP Snooping

- **DHCP Snooping Mode**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включение / выключение функции DHCP Snooping.

Коммутатор, работающий как DHCP-сервер и клиент, не может включить функцию DHCP Snooping.

Настройка доверенного порта, как показано на рисунке 36.

Рисунок 36 Настройка доверенного порта

- **Mode**
  Опции: Trusted / Untrusted
  По умолчанию: Untrusted
  Функция: установите порт как доверенный или ненадежный порт. Порты, которые прямо или косвенно подключаются к действующим DHCP-серверам, являются доверенными портами.

Конфигурация доверенного порта и магистральный порт являются взаимоисключающими. Порт, входящий в группу соединительных линий, не может быть установлен в качестве доверенного порта. Доверенный порт не может присоединиться к группе соединительных линий.

6. Система часов

6.1. Конфигурация часов

Настройте часовой пояс, как показано на рисунке 37.

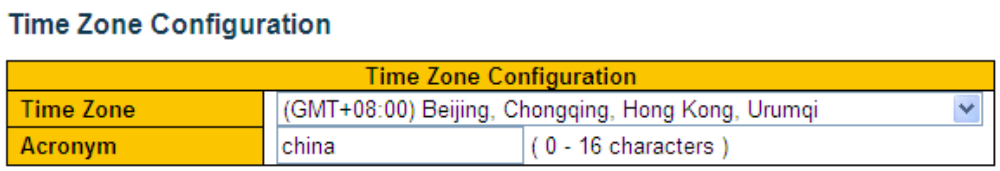


Рисунок 37 Конфигурирование часового пояса

- **Часовой пояс**
  Функция: Выберите местный часовой пояс
- **Acronym**
  Функция: Описание часового пояса.

Настройте летнее время, как показано на рисунке 38.

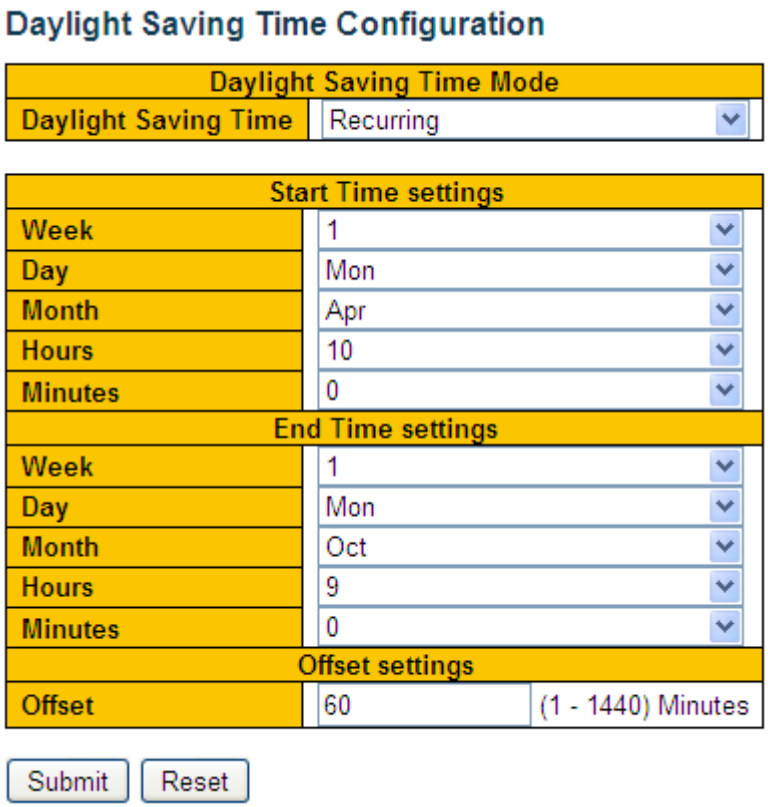


Рисунок 38 Конфигурирование летнего время

- **Daylight Saving Time**
  Варианты: Отключено / Повторяющееся / Неповторяющееся
  По умолчанию: отключено
  Функция: включить или выключить DST.
- **Start Time setting /End Time setting**
  Функция: после включения перехода на летнее время настройте временной сегмент для перехода на летнее время. В неповторяющемся режиме вам необходимо настроить год, месяц, дату, час и минуту, чтобы указать временной сегмент для перехода на летнее время. Как показано на рис. 50, летнее время настроено на выполнение в период с 10:00 1 апреля 2015 г. до 9:00 1 октября 2015 г. Вы можете установить месяц, неделю, день, час и минуту в цикле. режим для указания диапазона времени выполнения летнего времени каждый год. Например, вы можете настроить выполнение летнего времени с 10:00 утра первого понедельника апреля до 9:00 утра первого понедельника октября каждого года, как показано.
- **Offset**
  Диапазон: 1~1440мин
  По умолчанию: 1 мин.

Функция: Установите смещение часов DST, то есть продолжительность времени, на которое часы переводятся вперед для выполнения DST.

Например, запустите летнее время с 10:00:00 1 апреля до 9:00:00 1 октября. Смещение составляет 60 мин. Время без летнего времени будет работать до 10:00:00 1 апреля. Затем часы переходят на 11:00:00, чтобы начать летнее время. Летнее время работает до 9:00:00 1 октября. Затем часы возвращаются к 8:00:00, чтобы перейти к времени, отличному от летнего времени.

6.2. SNTP

Простой протокол сетевого времени (SNTP) синхронизирует время между сервером и клиентом с помощью запросов и ответов. Как клиент коммутатор синхронизирует время с сервером по пакетам сервера.

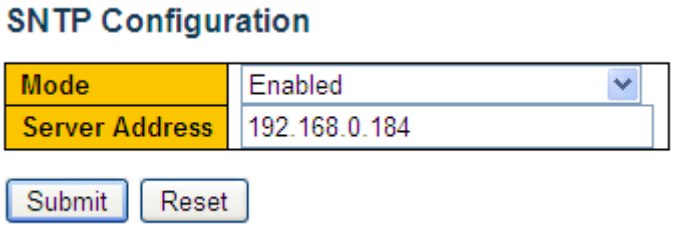


Рисунок 39 Включение SNTP

- **Mode**
  Параметры: Включено/Выключено
  По умолчанию: отключено
  Функция: включить/отключить SNTP.
- **Адрес сервера**
  Формат: A.B.C.D.
  Функция: Настройка IP-адреса сервера SNTP. Клиенты будут синхронизировать время в соответствии с пакетами сервера.
  Проверьте, синхронизируются ли часы с сервера.

Щелкните [Basic Configuration] → [System Information] для просмотра информации о часах, как показано на риceurt 40.

System Information

System	
Contact	+86-10-88798888
Name	SWITCH
Location	No.901 Floor 8 to 12, Building No.2,Shixing Avenue 30#, Shijingshan District, Beijing, P. R. China 100144
Hardware	
Device Type	SICOM3000A-2GX8GE
Device MAC Address	00-1e-cd-1c-e8-e0
S/N	S30U0035Axxxxxxxxx
Time	
System Date	1970-01-02T00:30:08+00:00
System Uptime	1d 00:30:08
Software	
Software Version	R3001
Code Date	Jul 25 2018 09:02:04
Code Revision	Build-24.0.44.2.B1.4.3
Hardware Version	V1.0
Logic Version	V1.0.0

Рисунок 40 Просмотр информации о часах

6.3. PTP

Протокол точного времени (PTP) синхронизирует независимые часы на распределенных узлах системы измерения и управления с высокой точностью. Протокол синхронизирует фазу и частоту с точностью до ±100 нс.

6.3.1. Веб конфигурование

Конфигурация часов PTP показано на рисунке 41.

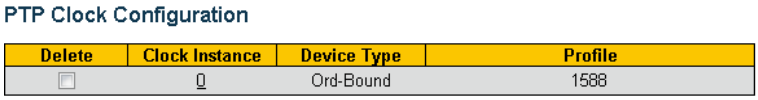


Рисунок 41 Конфигурация часов PTP

- **Clock Instance:**
  Диапазон: 0~3
  Функция: Настройка экземпляра PTP
- **Тип устройства:**
  Диапазон: Ord-Bound/P2pTransp/E2eTransp/Masteronly/Slaveonly
  Функция: Настройка типа часов PTP
- **Профиль:**
  Диапазон: Нет профиля/1588
  Функция: Выбрать файл описания PTP

  Щелкните Instance No., чтобы войти в подробную конфигурацию ptp, как показано на 42.

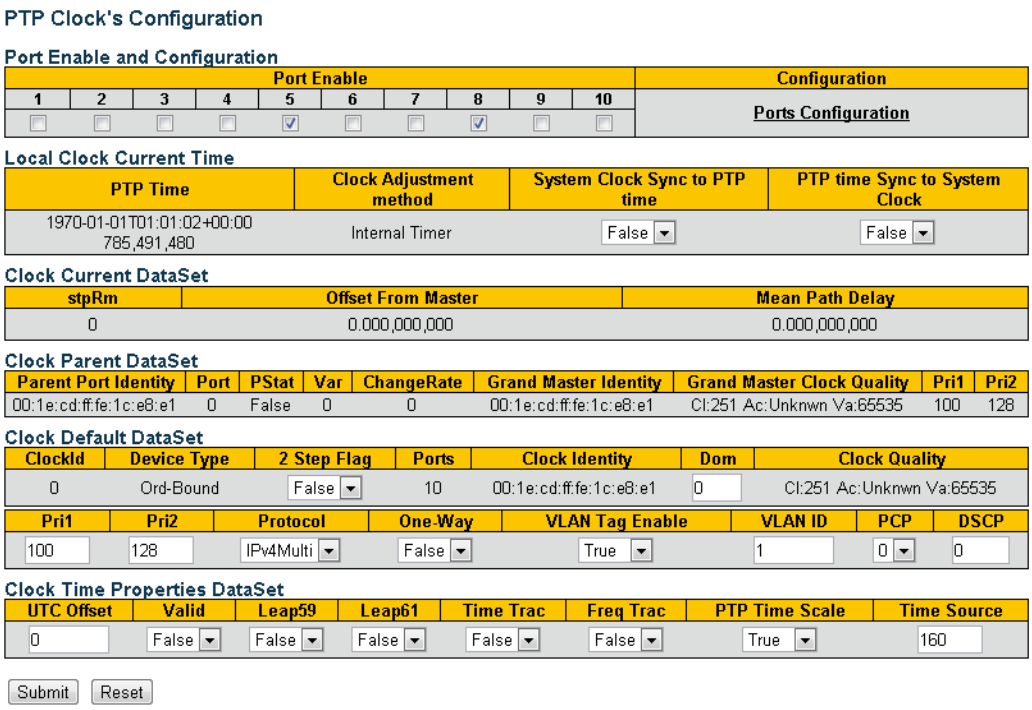


Рисунок 42 Конфигурация часов PTP

- **Port enable and configuration**
  Port Enable:
  Функция: выбор одного пота для включения PTP

  Нажмите «Конфигурация портов», как показано на рисунке 43.

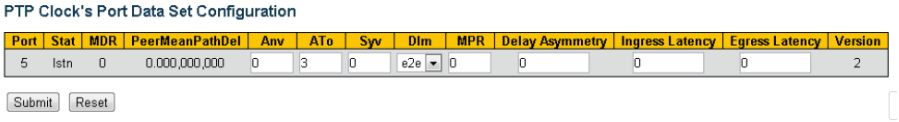


Рисунок 43 Конфигурация портов

- **Anv:**
  Диапазон: -3~4
  Функция: Интервал для выдачи сообщений-уведомлений в ведущем состоянии.
- **ATo:**
  Диапазон: 1~10
  Функция: Тайм-аут для получения анонсирующих сообщений на порт.
- **Syv:**
  Диапазон: -7~4
  Функция: интервал для выдачи сообщений синхронизации в мастере.
- **Dlm:**
  Диапазон: p2p/e2e
  Функция: настраиваемый элемент delayMechanism. Механизм задержки, используемый для порта: сквозное измерение задержки e2e.
  p2p одноранговое измерение задержки.
  Может быть определен для каждого порта в обычных/граничных часах.

В прозрачных часах все порты используют один и тот же механизм задержки, определяемый типом часов.

- **MPR:**
  Диапазон：-7~5
  Функция: Интервал выдачи сообщений Delay_Req для порта в режиме E2e. Это значение объявляется от ведущего к ведомому в сообщении объявления. Значение отражается в поле MDR в Slave.
  Интервал выдачи сообщений Pdelay_Req для порта в режиме P2P.
- **Delay Asymmetry:**
  Диапазон: -100000~100000нс
  Функция: если задержка передачи для канала несимметрична, здесь можно настроить асимметрию.
- **Ingress latency:**
  Диапазон: -100000~100000нс
  Функция: задержка входящего трафика, измеренная в нс, как определено в IEEE 1588, раздел 7.3.4.2.
- **Egress Latency:**
  Диапазон: -100000~100000нс
  Функция: исходящая задержка, измеренная в нс, как определено в IEEE 1588, раздел 7.3.4.2.

Часы Текущий набор данных

Показывает фактическое время PTP с разрешением в наносекундах. Существует два метода: синхронизировать системные часы с временем PTP или синхронизировать время PTP с системными часами.

Набор данных часов по умолчанию

- **2 Step Flag:**
  включить двухшаговый флаг
- **Domain:**
  настроить идентификатор домена экземпляра ptp
- **Pri 1:**
  Тактовый приоритет 1 [0..255], используемый алгоритмом выбора главного устройства BMC.
- **Pri 2:**
  Тактовый приоритет 2 [0..255], используемый алгоритмом выбора главного устройства BMC.
- **Protocol:**
  Диапазон: Ethernet/IPv4Multi
  Функция: Транспортный протокол, используемый механизмом протокола PTP.
  Описание: Ethernet PTP через многоадресную передачу Ethernet/IPv4Multi PTP через многоадресную рассылку IPv4
- **One-Way:**
  Если true, используются односторонние измерения. Этот параметр применяется только к ведомому устройству. В одностороннем режиме измерения задержки не выполняются, т. е. это применимо только в том случае, если необходима частотная синхронизация. Мастер всегда отвечает на запросы задержки.

- **VLAN Tag Enable:**
  Включает маркировку VLAN для кадров PTP.
  Примечание. Пакеты помечаются только в том случае, если порт настроен для тегирования vlan для настроенной VLAN.
- **VlanID:**
  Диапазон: 1-4094
- **PCP:**
  Диапазон：0~7
  Описание: значение Priority Code Point, используемое для кадров PTP.
- **DSCP:**
  Диапазон: 0~63
  Описание: значение кода дифференцированных услуг, используемое для кадров PTP.

Набор данных свойств времени часов:

- **UTC Offset:**
  Диапазон: 0-10000
- **Valid:**
  Диапазон: ИСТИНА/ЛОЖЬ
- **Leap59, Leap61:**
  Описание: дополнительная секунда
- **Time Trac、Freq Trac:**
  Диапазон: ИСТИНА/ЛОЖЬ
- **PTP Time Scale:**
  Диапазон: ИСТИНА/ЛОЖЬ
- **Time Source:**
  Набор данных свойств времени часов определен в стандарте IEEE 1588. Набор данных является как настраиваемым, так и динамическим, т.е. параметры могут быть настроены для гроссмейстера. В ведомых часах параметры перезаписываются временными свойствами гроссмейстеров. Параметры не используются в текущей реализации PTP.
  Допустимые значения параметра «Источник времени»:
  16 (0x10) ATOMIC_CLOCK
  32 (0x20) GPS
  48 (0x30) TERRESTRIAL_RADIO
  64 (0x40) PTP
  80 (0x50) NTP
  96 (0x60) HAND_SET
  144 (0x90) OTHER
  160 (0xA0) INTERNAL_OSCILLATOR

Просмотр конфигурацию часов ptp, можно как показано на рисунке 44

PTP Clock Configuration

		Port List								
Clock Instance	Device Type	1	2	3	4	5	6	7	8	9	10
0	Ord-Bound					✓					

Рисунок 44 Просмотр конфигурацию часов ptp

PTP Clock's Configuration

Auto-refresh

Local Clock Current Time

PTP Time	Clock Adjustment method	Ports Page
1970-01-01T04:50:22+00:00 152,387,820	Internal Timer	Ports

Clock Default DataSet

ClockId	Device Type	2 Step Flag	Ports	Clock Identity	Dom	Clock Quality	Pri1	Pri2	Protocol	One-Way	VLAN Tag Enable	VID	PCP	DSCP
0	Ord-Bound	False	10	00:1e:cd:ff:fe:1c:e8:e1	0	Cl:251 Ac:Unknwn Va:65535	100	128	IPv4Multi	False	True	1	0	0

Clock Current DataSet

stpRm	Offset From Master	Mean Path Delay	Slave Port	Slave State	Holdover(ppb)
0	0.000,000,000	0.000,000,000	0	FREERUN	N.A.

Clock Parent DataSet

Parent Port Identity	Port	PStat	Var	ChangeRate	Grand Master Identity	Grand Master Clock Quality	Pri1	Pri2
00:1e:cd:ff:fe:1c:e8:e1	0	False	0	0	00:1e:cd:ff:fe:1c:e8:e1	Cl:251 Ac:Unknwn Va:65535	100	128

Clock Time Properties DataSet

UTC Offset	Valid	Leap59	Leap61	Time Trac	Freq Trac	PTP Time Scale	Time Source
0	False	False	False	False	False	True	160

Рисунок 45 Детализованный просмотр конфигурацию часов ptp

7. Конфигурация портов

Настройте состояние порта, скорость порта, управление потоком и другую информацию, как показано на рисунке 46.

Port Configuration

Port	Link	Speed		Adv Duplex		Adv Speed			Flow Control			Maximum	Excessive	Reset
		Current	Configured	Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx	Frame Size	Collision Mode	
*			<>	☑	☑	☑	☑	☑	☑			9600	<>	☐
1		100fdx	Auto	☑	☑	☑	☑	☑	☑	✓	✓	9600	Discard	☐
2		100fdx	Auto	☑	☑	☑	☑	☑	☑	✓	✓	9600	Discard	☐
3		100fdx	Auto	☑	☑	☑	☑	☑	☑	✓	✓	9600	Discard	☐
4		Down	10Mbps HDX	☐	☐	☐	☐	☐	☐	✗	✗	9600	Discard	☐
5		Down	10Mbps FDX	☐	☐	☐	☐	☐	☑	✓	✓	9600	Discard	☐
6		Down	100Mbps HDX	☐	☐	☐	☐	☐	☑	✓	✓	9600	Discard	☐
7		Down	100Mbps FDX	☐	☐	☐	☐	☐	☑	✓	✓	9600	Discard	☐
8		Down	Auto	☑	☑	☑	☑	☑	☑	✓	✓	9600	Discard	☐
9		Down	Auto	☑	☑	☑	☑	☑	☑	✓	✓	9600	Discard	☐
10		Down	Auto	☑	☑	☑	☑	☑	☐	✗	✗	9600	Discard	☐
11		Down	Auto	☑	☑	☑	☑	☑	☑	✓	✓	9600	Discard	☐
12		Down	Auto	☑	☑	☑	☑	☑	☑	✓	✓	9600	Discard	☐

Submit Reset

Рисунок 46 Конфигурирование порта

- **Link**
  Отображение состояния соединения портов.
  Зеленый: порт находится в состоянии соединения и может нормально обмениваться данными.
  Красный: порт находится в состоянии Linkdown и не может нормально обмениваться данными.
- **Speed-Current**
  Отображение скорости связи и дуплексного режима портов.
- **Speed-Configured**
  Варианты: Отключено/Авто/10 Мбит/с HDX/10 Мбит/с FDX/100 Мбит/с HDX/100 Мбит/с FDX//1 Гбит/с FDX
  По умолчанию: Авто
  Функция: Настройка скорости и дуплексного режима портов. Disabled указывает на то, что порт отключен и запрещает передачу данных. Эта опция напрямую влияет на аппаратное состояние порта и запускает аварийные сигналы порта.
  Описание: скорость и дуплексный режим портов могут быть автоматически согласованы или установлены принудительно. Если установлено значение Auto, скорость порта и режим дуплекса будут автоматически согласовываться в соответствии со статусом соединения порта. Рекомендуется включить автосогласование для каждого порта, чтобы избежать проблем с подключением,

вызванных несоответствием конфигурации порта. Если вы хотите принудительно включить режим скорости/дуплекса порта, убедитесь, что конфигурация скорости/режима дуплекса одинакова для подключенных портов на обоих концах.

- **Adv Duplex**
  Варианты: FDX/HDX
  Функция: Настройка дуплексного режима автоматического согласования портов.
  Описание: Fdx указывает, что порт может одновременно принимать и передавать данные; Hdx указывает, что порт одновременно принимает или передает данные. Когда для режима порта установлено значение Auto, дуплексный режим порта по умолчанию определяется путем согласования с одноранговым узлом. Согласованный дуплексный режим может быть либо Fdx, либо Hdx. Параметр может быть настроен для порта на согласование только одного дуплексного режима, тем самым управляя согласованием дуплексного режима.
- **Adv Speed**
  Варианты: 10М / 100М / 1Г
  Функция: настройка скорости автоматического согласования портов.
  Описание: Когда для режима порта установлено значение «Авто», скорость порта по умолчанию определяется путем согласования с узлом. Согласованная скорость может быть любой в пределах допустимого диапазона скоростей порта. Параметр может быть настроен для порта на согласование только некоторых скоростей, тем самым контролируя согласование скорости.
- **Flow Control**
  Параметры: Включено/Выключено
  По умолчанию: отключено
  Функция: включение/отключение функции управления потоком на назначенном порту.
  Описание: как только функция управления потоком включена, порт сообщит отправителю о снижении скорости передачи, чтобы избежать потери пакетов по алгоритму или протоколу, когда поток, полученный портом, превышает размер кэша порта. Если устройства работают в разных дуплексных режимах (полу/полный), управление потоком у них реализуется по-разному. Если устройства работают в полнодуплексном режиме, принимающая сторона отправит специальный кадр (Пауза), чтобы проинформировать отправляющую сторону о прекращении отправки пакетов. Когда отправитель получает кадр паузы, он прекращает отправку пакетов на период «времени ожидания», указанный в кадре паузы, и продолжает отправлять пакеты после окончания «времени ожидания». Если устройства работают в полудуплексном режиме, они поддерживают управление потоком обратного давления. Принимающая сторона создает конфликт или несущий сигнал. Когда отправитель обнаруживает конфликт или несущую, он делает отсрочку, чтобы отложить передачу данных.
- **Curr Rx/Curr Tx**
  Функция: отображение состояния управления потоком портов.
- **Maximum Frame Size**
  Диапазон: 1518~9600 байт
  По умолчанию: 9600 байт.
  Функция: установить максимальный размер пакета, принимаемого портом. Пакеты с размером больше указанного значения отбрасываются.
- **Reset**
  Параметры: Включено/Выключено

По умолчанию: отключено
Функция: сбросить порт или нет.

Просмотр статистики порта, как показано на рисунке 47.

Port Statistics Overview

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	1275387	11523	98799397	2629185	0	0	869612	0	609
2	184535	1092883	17294542	80989316	0	0	1226	0	125257
3	227	183345	26332	16672027	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0

Рисунок 47 Статистика по порту

- **Port**
  Нажмите <порт>, чтобы перейти на страницу «подробной статистики порта».
- **Packets**
  Отображение количества пакетов, которые каждый порт отправляет/получает.
- **Bytes**
  Отображение количества байтов, которые каждый порт отправляет/получает.
- **Errors**
  Отображение количества пакетов ошибок, которые каждый порт отправляет/получает.
- **Drops**
  Отображение количества пакетов, отброшенных из-за конфликтов передачи/получения.
- **Filtered Received**
  Отображение количества пакетов, отфильтрованных принимающей стороной.
  Нажмите <порт>, чтобы перейти на страницу «подробной статистики порта».

Просмотр подробной статистики порта, как показано на рисунке 48.

Detailed Port Statistics Port 2

Port 2 Auto-refresh Refresh Clear

Receive Total		Transmit Total	
Rx Packets	11065	Tx Packets	11
Rx Octets	1034290	Tx Octets	1276
Rx Unicast	10	Tx Unicast	0
Rx Multicast	1110	Tx Multicast	11
Rx Broadcast	9945	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	3043	Tx 64 Bytes	0
Rx 65-127 Bytes	7529	Tx 65-127 Bytes	11
Rx 128-255 Bytes	365	Tx 128-255 Bytes	0
Rx 256-511 Bytes	83	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	45	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	11065	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	11
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	8073		

Рисунок 48 Детальная статистика по порту

8. QoS

Качество обслуживания (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. Классификация трафика, контроль трафика, формирование трафика, управление перегрузками и предотвращение перегрузок являются основными концепциями развертывания QoS. В основном они выполняют следующие функции:

- Классификация трафика: идентифицирует объект на основе определенных правил сопоставления. Это основа и предпосылка QoS.
- Контроль трафика: контролирует скорость трафика пакетов, которые передаются на устройство. Когда скорость трафика превышает указанную скорость трафика, устройство принимает меры ограничения или наказания для защиты сетевых ресурсов от повреждения. Контроль трафика подразделяется на контроль трафика на основе портов и контроль трафика на основе очередей.
- Формирование трафика: проактивно регулирует скорость вывода трафика. Он направлен на адаптацию трафика к доступным сетевым ресурсам нисходящего устройства, чтобы предотвратить ненужное отбрасывание пакетов и перегрузку. Формирование трафика подразделяется на формирование трафика на основе портов и формирование трафика на основе очередей.
- Управление перегрузками: это обязательно для решения проблемы конкуренции за ресурсы. Управление перегрузками кэширует пакеты в очередях и определяет последовательность пересылки пакетов на основе определенного алгоритма планирования, обеспечивая приоритетную пересылку для ключевых служб. Предотвращение перегрузки: Чрезмерная перегрузка может привести к повреждению сетевых ресурсов. Предотвращение перегрузки отслеживает использование сетевых ресурсов. При обнаружении увеличения перегрузки функция использует упреждающее отбрасывание пакетов и настраивает объем трафика для устранения перегрузки.

Контроль трафика, формирование трафика, управление перегрузками и предотвращение перегрузок контролируют сетевой трафик и выделенные ресурсы с разных сторон. Они являются конкретным воплощением QoS. Например, коммутатор контролирует пакеты, которые передаются в сеть, на основе установленной скорости. Он формирует пакеты до того, как пакеты покинут коммутатор. Он управляет планированием очереди в случае перегрузки и принимает меры по предотвращению перегрузки, когда перегрузка усиливается.

Каждый порт коммутаторов этой серии поддерживает 8 очередей кэширования, от 0 до 7 в порядке возрастания приоритета.

Когда кадр достигает порта, коммутатор определяет очередь для кадра в соответствии с информацией о кадре и портом. Коммутаторы этой серии поддерживают классификацию трафика в следующих режимах сопоставления очередей: порт, информация заголовка 802.1Q, кодовая точка дифференцированного обслуживания (DSCP) и контрольный список QoS (QCL) с приоритетом в порядке возрастания. При пересылке данных порт использует режим планирования для планирования данных в 8 очередях и

пропускной способности каждой очереди. Коммутаторы этой серии поддерживают два режима планирования: 6 взвешенных очередей и SP (строгий приоритет).

WRR (Weighted Round Robin) 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.

В режиме SP преимущественно пересылаются высокоприоритетные пакеты. Он в основном используется для передачи чувствительных сигналов. Если кадр поступает в очередь с высоким приоритетом, коммутатор прекращает планирование очередей с низким приоритетом и начинает обрабатывать данные очереди с высоким приоритетом. Когда очередь с высоким приоритетом не содержит данных, коммутатор начинает обрабатывать данные из очереди с более низким приоритетом.

6 Queues Weighted указывает, что очередь 6 и очередь 7 используют режим планирования Strict Priority, а очередь 0 ~ очередь 5 используют режим планирования WRR. Данные в очереди 7 обрабатываются до данных в очереди 6. Когда и очередь 7, и очередь 6 пусты, данные в очереди 0 ~ очереди 5 планируются на основе соотношения весов.

8.1. Веб конфигурирование

Настройте режим сопоставления очередей на основе портов, как показано на рис. 49.

Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based	Address Mode
*	<>	<>	<>	<>			<>
1	2	0	1	0	Disabled		Source
2	0	0	0	0	Disabled		Source
3	0	0	0	0	Disabled		Source
4	0	0	0	0	Disabled		Source
5	0	0	0	0	Disabled		Source
6	0	0	0	0	Disabled		Source
7	0	0	0	0	Disabled		Source
8	0	0	0	0	Disabled		Source
9	0	0	0	0	Disabled		Source
10	0	0	0	0	Disabled		Source
11	0	0	0	0	Disabled		Source
12	0	0	0	0	Disabled		Source

Submit Reset

Рисунок 49 Настройка режима сопоставления очередей на основе портов

- **COS**
  Диапазон: 0~7
  По умолчанию: 0
  Функция: Настройка значения CoS порта по умолчанию.
  Описание: значение CoS определяет очередь для хранения пакетов. Значение CoS находится в диапазоне от 0 до 7, что соответствует очереди от 0 до очереди 7 соответственно. После того, как пакет передан коммутатору, коммутатор выделяет значение CoS пакету. Если полученный пакет относится к типу тегов, а классификация тегов отключена, или полученный пакет относится к типу без тегов,

значением CoS в пакете является значение CoS по умолчанию для порта, принимающего пакет.

- **PCP**
  Диапазон: 0~7
  По умолчанию: 0
  Функция: Настройка значения PCP (приоритетного кода) по умолчанию для порта.
  Объяснение: Когда пакет не помечен, приоритет в теге, добавленном к пакету, равен значению PCP по умолчанию для порта.
- **DEI**
  Диапазон: 0~1
  По умолчанию: 0
  Функция: Настройте значение DEI по умолчанию (Индикатор допустимости сброса) для порта.
  Объяснение: Когда пакет не помечен, CFI в теге, добавленном к пакету, является значением DEI по умолчанию для порта.

Настройте режим отображения очереди на основе заголовка кадра 802.1Q.

Нажмите <Tag Cliass> на рисунке 49, чтобы открыть страницу конфигурации режима сопоставления очереди заголовков кадров 802.1Q, как показано на рис. 50.

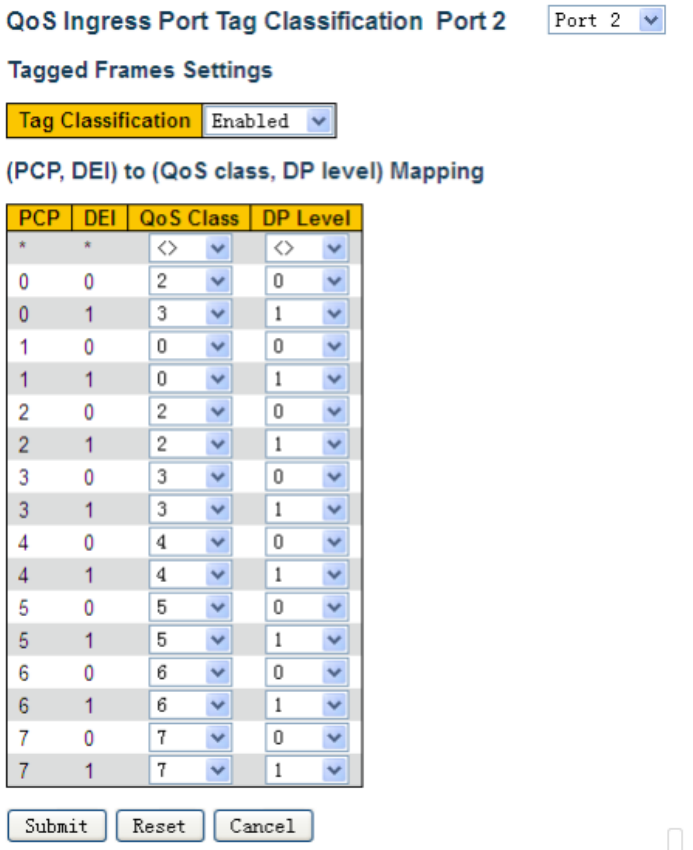


Рисунок 50 Настройка режима сопоставления очередей на основе портов

- **Tag Classification**
  Опции: Enable / Disable
  По умолчанию: Disable

Функция: следует ли включить режим сопоставления очередей на основе информации заголовка 802.1Q. Этот режим сопоставления очередей имеет более высокий приоритет по сравнению с режимом сопоставления очередей на основе портов.

- **(PCP, DEI) to (QoS class, DP level) Mapping**
  Диапазон: 0~7 (класс QoS) 0~1 (уровень DP)
  По умолчанию: диапазон значений PCP — 0, 1, 2, 3, 4, 5, 6 и 7, которые соответственно сопоставлены с классами QoS 1, 0, 2, 3, 4, 5, 6 и 7. Диапазон значений DEI составляет 0 и 1, которые соответственно отображаются на уровни DP 0 и 1.
  Функция: Установите отображение с (PCP, DEI) на (CoS, DPL) на основе значений PCP и DEI в пакетах.
  Описание: Класс QoS эквивалентен значению CoS. Значение CoS определяет очередь для хранения пакетов, а значения CoS 0-7 соответственно соответствуют очередям 0-7. После того, как пакет передан коммутатору, коммутатор выделяет пакету значение CoS и значение DPL. Значение CoS и значение DPL пакета (CoS, DPL) сопоставляются с (PCP, DEI), если полученный пакет представляет собой тип тега и включена классификация тегов.
  Вы можете выбрать порт для настройки режима сопоставления очереди на основе информации заголовка 802.1Q в правом верхнем углу страницы.

Настройте перемаркировку 802.1p, как показано на рисунке 51.

Port	Mode
1	Classified
2	Mapped
3	Default
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified
11	Classified
12	Classified

Рисунок 51 Настройка перемаркировки 802.1p

- **Mode**
  Опция: Classified / Mapped / Default
  Функция: Отображает режим перемаркировки 802.1p, когда выходной порт пересылает пакеты. Перемаркировка 802.1p используется для обновления значения PCP и значения DEI в пакетах, когда выходной порт пересылает пакеты.

Нажмите <Port>, чтобы открыть страницу конфигурации перемаркировки 802.1p.

- Настройте режим перемаркировки 802.1p на Classified, как показано на рисунке 52.

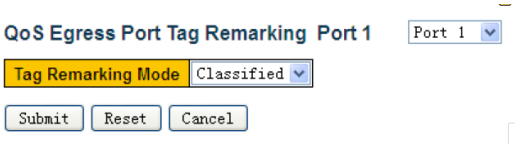


Рисунок 52 Настройка режим перемаркировки 802.1p на Classified

- **Tag Remarking Mode**
  Опции: Classified / Mapped / Default
  По умолчанию: Classified
  Функция: Настройка режима перемаркировки 802.1p. Классифицировано: значение PCP и значение DEI в пакетах не обновляются, когда выходной порт пересылает пакеты.
  Вы можете выбрать порт для настройки режима перемаркировки 802.1p в правом верхнем углу страницы.

  Настройте режим перемаркировки 802.1p по умолчанию, как показано на рисунке 53.

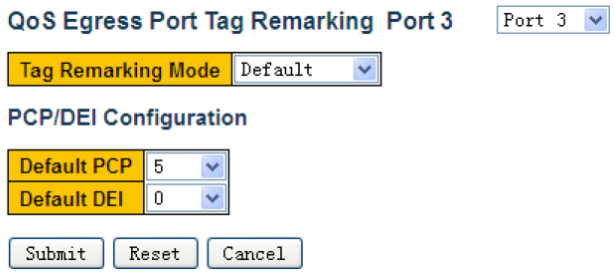


Рисунок 53 Настройка режим перемаркировки 802.1p по умолчанию

- **Tag Remarking Mode**
  Опции: Classified / Mapped / Default
  По умолчанию: Classified
  Функция: Настройка режима перемаркировки 802.1p. По умолчанию: значение PCP и значение DEI в пакетах обновляются до значений по умолчанию (установленных в нижней части страницы) выходного порта, когда исходящий порт пересылает пакеты.
- **Default PCP**
  Диапазон: 0~7
  По умолчанию: 0
  Функция: Установите значение PCP по умолчанию для выходного порта.
- **Default DEI**
  Диапазон: 0~1
  По умолчанию: 0
  Функция: Установите значение DEI по умолчанию для выходного порта.
  Вы можете выбрать порт для настройки режима перемаркировки 802.1p в правом верхнем углу страницы.

  Настройте режим перемаркировки 802.1p на Mapped, как показано на рисунке 54.

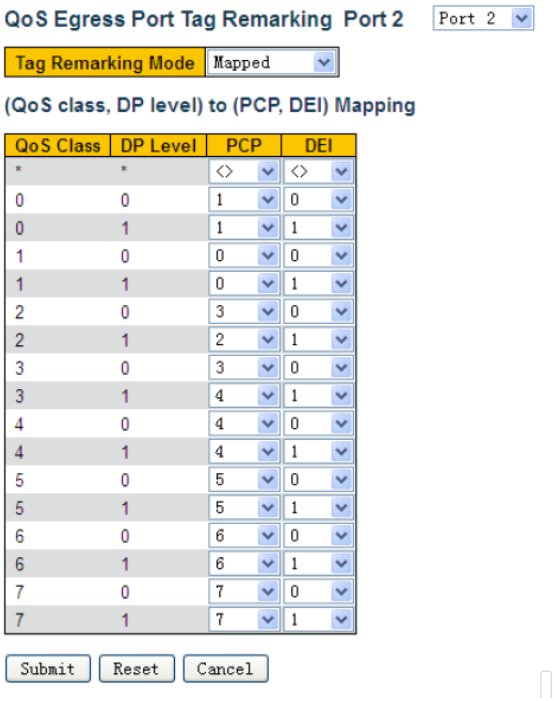


Рисунок 54 Настройка режим перемаркировки 802.1p по Mapped

- **Tag Remarking Mode**
  Опции: Classified / Mapped / Default
  По умолчанию: Classified
  Функция: Настройка режима перемаркировки 802.1p. Сопоставление: значение PCP и значение DEI в пакетах обновляются до (PCP, DEI), сопоставленного с (CoS, DPL), когда выходной порт пересылает пакеты. Отображение настраивается в нижней части страницы.
- **(QoS class, DP level) to (PCP, DEI) Mapping**
  Диапазон: 0~7 (PCP) 0~1 (DEI)
  По умолчанию: диапазон классов QoS — 0, 1, 2, 3, 4, 5, 6 и 7, которые соответственно отображаются на значения PCP 1, 0, 2, 3, 4, 5, 6 и 7. Диапазон значений уровня DP составляет 0 и 1, которые соответственно отображаются на значения DEI 0 и 1.
  Функция: Настройте отображение из (CoS, DPL) в (PCP, DEI) на основе значений CoS и DPL в пакетах.
  Вы можете выбрать порт для настройки режима перемаркировки 802.1p в правом верхнем углу страницы.

  Включите режим сопоставления очередей на основе DSCP, как показано на рисунке 55.

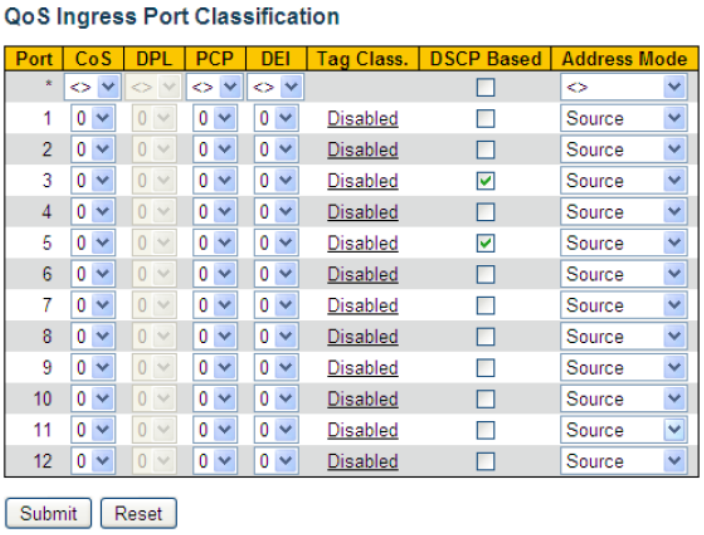


Рисунок 55 Включение режима сопоставления очередей на основе DSCP

- **DSCP Based**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: следует ли включить режим сопоставления очередей на основе DSCP. Этот режим отображения очереди имеет более высокий приоритет по сравнению с режимом отображения очереди на основе информации заголовка 802.1Q. 5.

  Включите трансляцию DSCP для входного порта и функцию перезаписи DSCP для выходного порта, как показано на рисугке 56.

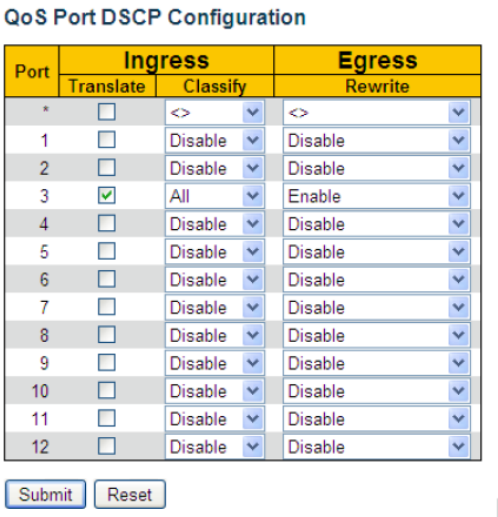


Рисунок 56 Включение трансляцию DSCP для входного порта и функцию перезаписи DSCP

- **Translate**
  Опции: Enable / Disable
  По умолчанию: Disable

Функция: следует ли преобразовывать значение DSCP в пакет, полученный входным портом. Если установлено значение Enable, значение DSCP преобразуется в соответствии с таблицей преобразования DSCP (столбец Translate на рисунке 58).

- **Classify**
  Опции: Отключить/DSCP=0/Выбрано/Все
  По умолчанию: Отключить
  Функция: выбирает перезаписанное значение DSCP для выходного порта, когда для параметра Rewrite установлено значение Enable. Disable: значение DSCP в пакетах не перезаписывается, когда выходной порт пересылает пакеты.
  DSCP=0: Когда выходной порт пересылает пакеты, если значения DSCP в пакетах равны 0, значения DSCP в пакетах перезаписываются в соответствии с классификацией на рисунке 59. Выбрано: Когда выходной порт пересылает пакеты, если значения DSCP в пакетах выбранное значение (столбец «Классификация» на рисунке 58), значения DSCP в пакетах переписываются в соответствии с классификацией на рисунке 59.
  Все: Когда выход пересылает пакеты, значения DSCP в пакетах записываются в соответствии с классификацией на рисунке 59.
- **Rewrite**
  Опции: Disable / Enable / Remap DP Unaware / Remap DP Aware
  По умолчанию: Disable
  Функция: Установите режим перезаписи значения DSCP в пакетах, когда выходной порт пересылает пакеты.
  Disable: значения DSCP в пакетах не перезаписываются, когда выходной порт пересылает пакеты.
  Включить: Перезаписываются ли значения DSCP в пакетах, определяется на основе конфигурации классификации, когда выходной порт пересылает пакеты.
  Remap DP Unaware: значения DSCP в пакетах перезаписываются на основе отображения (столбец Remap DP0 на рисунок 58) из (DSCP, DPL=0) в DSCP, когда выход пересылает пакеты.
  Remap DP Aware: значения DSCP в пакетах перезаписываются на основе отображения (столбцы Remap DP0 и «Remap DP1» на рисунке 58) из (DSCP, DPL) в DSCP, когда выход пересылает пакеты.

Настройте режим сопоставления очередей на основе DSCP, как показано на рисунке 57.

Рисунок 57 Настройка режима сопоставления очередей на основе DSCP

- **Trust**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: доверять ли значению DSCP
- **QoS Class**
  Диапазон: 0~7 По умолчанию: 0
  Функция: Установите отображение от DSCP до CoS.
  Описание: Класс QoS эквивалентен значению CoS. Значение CoS определяет очередь для хранения пакетов, а значения CoS 0~7 соответственно соответствуют очередям 0~7. После того как пакет со значением DSCP, являющимся доверенным значением, передан коммутатору, коммутатор выделяет значение CoS пакету в соответствии с преобразованием DSCP в CoS.

  Настройка трансляции и перезаписи DSCP, как показано на рисунке 58.

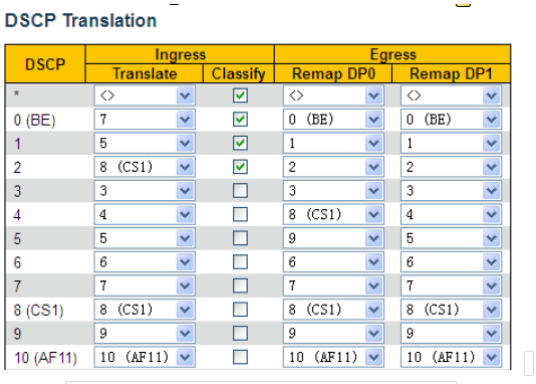


Рисунок 57 Настройка режима сопоставления очередей на основе DSCP

- **Translate**
  Диапазон: 0~63
  Функция: Установите таблицу перевода значений DSCP.
- **Classify**
  Параметры: Включено / Выключено

По умолчанию: отключено

Функция: Когда для параметра Classify установлено значение Selected на рисунке 56, этот параметр используется для установки выбранного значения DSCP.

- **Remap DP0/ Remap DP1**

  Диапазон: 0~63

  Функция: Установите отображение из (DSCP, DPL) в значения DSCP.

Настройте классификацию DSCP, как показано на рисунке 59.

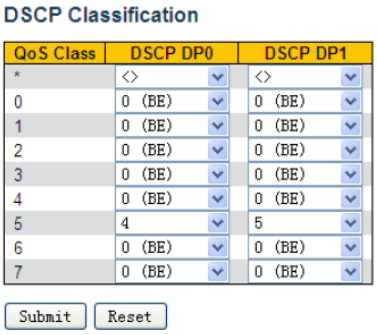


Рисунок 59 Настройка классификацию DSCP

- **Remap DP0/ Remap DP1**

  Диапазон: 0~63

  Функция: Установите отображение из (CoS, DPL) в значения DSCP. Класс QoS эквивалентен значению CoS. Значение CoS определяет очередь для хранения пакетов, а значения CoS 0-7 соответственно соответствуют очередям 0-7.

Настройте запись QCL, как показано на рисунке 60.

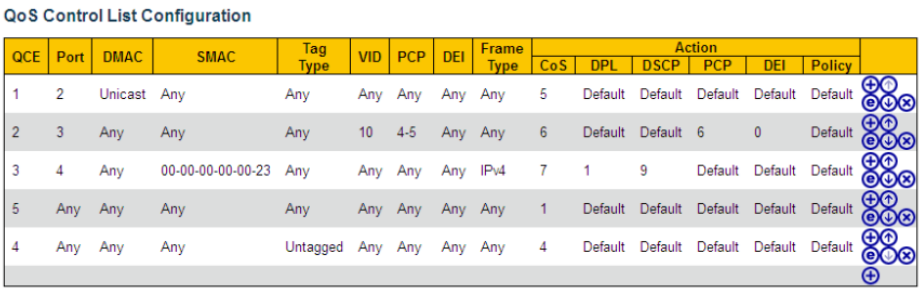


Рисунок 60 Настройка запись QCL

Отображение очереди пакетов реализуется путем сопоставления записей QCL. Каждая запись состоит из нескольких условий в логической связи И. Считается, что пакет, полученный портом-участником, соответствует записи QCL только тогда, когда пакет удовлетворяет всем условиям. Записи QCL не зависят друг от друга. При наличии нескольких записей QCL устройство сравнивает пакет с записями QCL одну за другой (сверху вниз). Как только совпадение найдено, предпринимаются действия, и дальнейшее сравнение не проводится. Нажмите <o+>, чтобы добавить новую запись QCL; нажмите <oe>, чтобы отредактировать запись QCL; нажмите <ox>, чтобы удалить запись QCL, нажмите <o↑>, чтобы переместить текущую запись вверх; нажмите <o↓> для перемещения вниз по текущей записи. QCE — это идентификатор записи QCL, который

нумеруется на основе временной последовательности создания записи. 10. Параметры входа QCL конфигурации.

Выберите порт, на котором действует текущая запись QCL, как показано на рисунке 61.

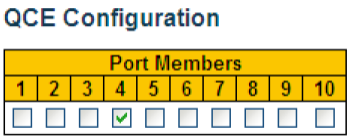


Рисунок 61 Настройка запись QCL

- **Port members**
  Функция: выберите порт, на котором действует текущая запись QCL. Все порты по умолчанию являются портами-участниками.

  Настройте параметры записи QCL, как показано на рисунке 62.

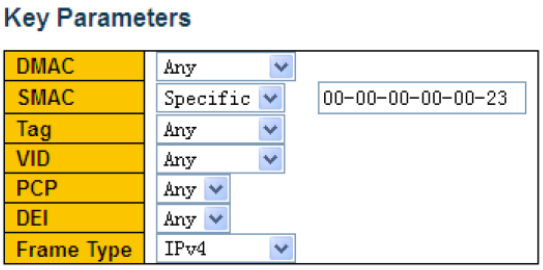


Рисунок 62 Настройка параметры записи QCL

- **DMAC**
  Опция: Any/ Unicast/ Multicast / Broadcast
  По умолчанию: Any
  Функция: Установите условие — MAC-адрес назначения. Когда MAC-адрес назначения в пакете, полученном портом-членом, соответствует настройкам этого параметра, условие успешно выполнено.
- **SMAC**
  Варианты: любой/конкретный
  По умолчанию: любой
  Функция: Установите условие — MAC-адрес источника. Если для него установлено значение «Специфический», необходимо установить MAC-адрес. Когда исходный MAC-адрес в пакете, полученном портом-участником, соответствует настройкам этого параметра, условие выполняется успешно.
- **Tag**
  Варианты: любой/ без тега/ с тегом
  По умолчанию: любой
  Функция: Установить условие-тег. Когда пакет, полученный портом-участником, соответствует настройкам этого параметра, условие выполняется успешно.
- **VID**
  Варианты: любой/конкретный（1~4095）/диапазон（1~4095）
  По умолчанию: любой

Функция: Установить условие--VID. Если установлено значение «Специфический», необходимо установить значение VID. Когда он установлен на Range, необходимо установить диапазон VID. Когда VID в пакете, полученном портом-членом, соответствует настройкам этого параметра, условие успешно соблюдено. Этот параметр недоступен, если для параметра «Тег» задано значение «Без тега».

- **PCP**
  Варианты: Любой/0/1/2/3/4/5/6/7/0-1/2-3/4-5/6-7/0-3/4-7
  По умолчанию: любой
  Функция: Установите условие — PCP. Когда значение PCP в пакете, полученном портом-членом, соответствует настройкам этого параметра, условие успешно соблюдено. Этот параметр недоступен, если для параметра «Тег» задано значение «Без тега».
- **DEI**
  Варианты: Любой/0/1
  По умолчанию: любой
  Функция: Установить условие — DEI. Когда значение DEI в пакете, полученном портом-членом, соответствует настройкам этого параметра, условие успешно соблюдено. Этот параметр недоступен, если для параметра «Тег» задано значение «Без тега».
- **Frame Type**
  Варианты: Any/ EtherType/ LLC/ SNAP/ IPv4/ IPv6
  По умолчанию: Any
  Функция: выбор типа рамки.

  Настройте параметры кадра EtherType, как показано на рисунке 63.

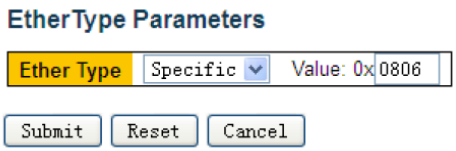


Рисунок 63 Настройка параметров кадра EtherType

- **Ether Type**
  Варианты: Any/ Specific (0x0600~0xFFFF)
  По умолчанию: Any
  Функция: Установите условие — тип Ethernet. Если для него установлено значение «Специфический», необходимо указать тип Ethernet.
  устанавливать. Когда пакет Ethernet, полученный портом-участником, соответствует настройкам этого параметра, условие успешно выполнено.

  Настройте параметры кадра LLC, как показано на рисунке 64.

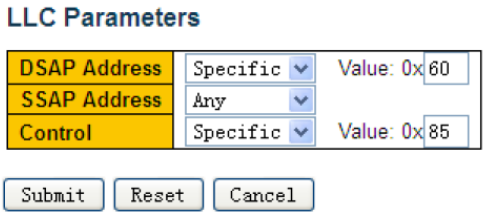


Рисунок 64 Настройка параметров кадра LLC

- **DSAP Address/SSAP Address/Control**
  Варианты: Any/ Specific (0x0600~0xFFFF)
  По умолчанию: Any
  Функция: Установить условие -- параметры пакета LLC. Если для параметра Адрес DSAP, Адрес SSAP или Управление установлено значение Особый, необходимо ввести конкретное значение. Когда пакет LLC, полученный портом-участником, соответствует настройкам параметров, условие успешно выполняется.

  Настройте параметры кадра SNAP, как показано на рисунке 65.

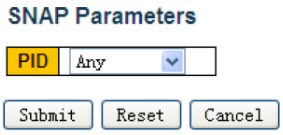


Рисунок 64 Настройка параметров кадра SNAP

- **PID**
  Варианты: Any/ Specific (0x0600~0xFFFF)
  По умолчанию: Any
  Функция: Установите условие — параметр пакета SNAP. Если установлено значение «Специфический», необходимо ввести значение PID. Когда PID в пакете SNAP, полученном портом-членом, соответствует настройкам этого параметра, условие успешно соблюдено.

  Настройте параметры кадра IPv4/IPv6, как показано на рисунке 65.

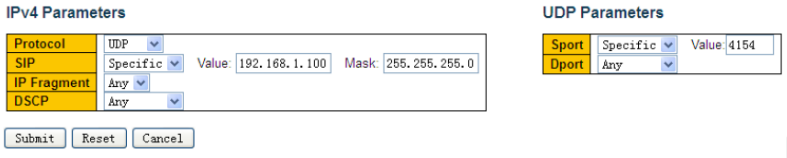


Рисунок 65 Настройка параметров кадра IPv4

- **Protocol**
  Варианты: Any/ UDP/ TCP/ Other（0~255）
  По умолчанию: Any
  Функция: Установите условие — тип протокола пакета IPv4. Если установлено значение UDP или TCP, необходимо установить идентификатор исходного порта и

идентификатор порта назначения. Если для него установлено значение «Другой», необходимо установить идентификатор протокола. Когда тип протокола в пакете, полученном портом-членом, соответствует настройкам этого параметра, условие успешно соблюдено.

- **Sport/ Dport**
  Варианты: Any/ Specific（0~65535）/ Range（0~65535）
  По умолчанию: Any
  Функция: Установите условие — идентификатор исходного порта TCP/UDP и идентификатор порта назначения. Если для них установлено значение «Специфический», необходимо установить идентификатор порта. Когда для них установлено значение Range, необходимо установить диапазон идентификаторов портов. Когда идентификаторы портов в IP-пакете, полученном портом-участником, соответствуют настройкам этого параметра, условие успешно выполняется.
- **SIP**
  Варианты: Any/ Specific
  По умолчанию: Any
  Функция: Установите условие — исходный IP-адрес и исходную маску IP-адреса. Если установлено значение «Специфический», необходимо установить IP-адрес и маску IP-адреса. Когда SIP в IP-пакете, полученном портом-членом, соответствует настройкам этого параметра, условие выполняется успешно.
- **IP Fragment**
  Варианты: Any/ Yes/ No
  По умолчанию: Any
  Функция: Установите условие - пакет IP-фрагментов. Когда фрагмент в пакете IPv4, полученном портом-членом, соответствует настройкам этого параметра, условие выполняется успешно.
- **DSCP**
  Варианты: Any/ Specific（0~63）/ Range（0~63）
  По умолчанию: Any
  Функция: Установите условие — значение DSCP. Если установлено значение «Специфический», необходимо ввести значение DSCP. Когда он установлен на Range, необходимо установить диапазон DSCP. Когда DSCP в IP-пакете, полученном портом-членом, соответствует настройкам этого параметра, условие выполняется успешно.

Настройте действие QCL, как показано на рисунке 66.

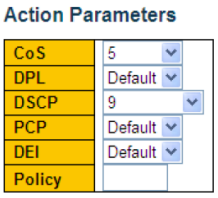


Рисунок 66 Настройка QCL

- **CoS**
  Варианты: 0~7/ по умолчанию
  По умолчанию: 0

Функция: значение CoS определяет очередь для хранения пакетов. Значение CoS находится в диапазоне от 0 до 7, что соответствует очереди от 0 до очереди 7. Значение по умолчанию указывает, что значение CoS равно 0. Когда пакет, полученный портом-участником, соответствует записи QCL, коммутатор назначает значение CoS для пакета.

- **DPL**
  Варианты: По умолчанию/ 0/ 1
  По умолчанию: По умолчанию
  Функция: изменить значение DPL в пакете, полученном портом-участником, на значение этого параметра, когда пакет соответствует записи QCL. Значение по умолчанию указывает, что значение DPL в пакете не изменяется.
- **DSCP**
  Варианты: По умолчанию/ 0~63
  По умолчанию: По умолчанию
  Функция: изменить значение DSCP в пакете, полученном портом-членом, на значение этого параметра, когда пакет соответствует записи QCL. Значение по умолчанию указывает, что значение DSCP в пакете не изменяется.
- **PCP**
  Варианты: По умолчанию/ 0~7
  По умолчанию: По умолчанию
  Функция: изменить значение PCP в пакете, полученном портом-участником, на значение этого параметра, когда пакет соответствует записи QCL. Значение по умолчанию указывает, что значение PCP в пакете не изменяется.
- **DEI**
  Варианты: По умолчанию/ 0/ 1
  По умолчанию: По умолчанию
  Функция: изменить значение DEI в пакете, полученном портом-членом, на значение этого параметра, когда пакет соответствует записи QCL. Значение по умолчанию указывает, что значение DEI в пакете не изменяется.

Просмотр записи QCL, как показано на рисунке 67.

QoS Control List Status

User	QCE	Port	Frame Type	Action						Conflict
				CoS	DPL	DSCP	PCP	DEI	Policy	
Static	1	2	Any	5	Default	Default	Default	Default	Default	No
Static	2	3	Any	6	Default	Default	6	0	Default	No
Static	3	4	IPv4	7	1	9	Default	Default	Default	No
Static	5	Any	Any	1	Default	Default	Default	Default	Default	No
Static	4	Any	Any	2	Default	Default	Default	Default	Default	No

Рисунок 67 Просмотр записи QCL

- **Conflict**
  Варианты: No/YES
- Функция: Отображает состояние конфликта записи QCL. Если ресурсов для создания записи QCL недостаточно, для параметра **Conflict** для этой записи устанавливается значение **YES**. В противном случае для параметра «**Conflict**» для этой записи установлено значение «**NO**».
  Щелкните <Resolve Confilct>, чтобы освободить ресурсы, необходимые для конфликтующей записи QCL, чтобы разрешить конфликт ресурсов.

Настройте ограничители входящего порта, как показано на рисунке 68.

QoS Ingress Port Policers

Port	Enable	Rate	Unit	Flow Control
*	☐	500	<>	☐
1	☐	500	kbps	☐
2	☑	2	Mbps	☑
3	☑	200	fps	☐
4	☐	500	kbps	☐
5	☐	500	kbps	☐
6	☐	500	kbps	☐
7	☐	500	kbps	☐
8	☐	500	kbps	☐
9	☐	500	kbps	☐
10	☐	500	kbps	☐
11	☐	500	kbps	☐
12	☐	500	kbps	☐

Submit Reset

Рисунок 68 Настройка ограничителей входящего порта

- **Enable**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включение или отключение ограничителей входящего порта. Контроль трафика порта реализуется путем ограничения скорости порта или управления потоком порта.
- **Rate, Unit**
  Диапазон: 100~3276700 кбит/с/ 1~3276 Мбит/с/ 100~3276700 кадров/с/ 1~3276 кбит/с
  По умолчанию: 500 кбит/с
  Функция: ограничение скорости пакетов, принимаемых портом. Пакеты со скоростью, превышающей значение, отбрасываются.
- **Flow Control**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включить ли управление потоком портов. После включения управления потоком для порта, когда трафик, полученный портом, превышает предельное значение, отправитель получает указание замедлить передачу, чтобы предотвратить потерю пакетов с помощью алгоритмов или протоколов.

Настройте ограничители входной очереди, как показано на рис. 69.

QoS Ingress Queue Policers

Port	Queue 0 Enable	Queue 1 Enable	Queue 2 E	Queue 2 Rate	Queue 2 Unit	Queue 3 Enable	Queue 4 Enable	Queue 5 Enable	Queue 6 Enable	Queue 7 Enable
*	☐	☐	☐	500	<>	☐	☐	☐	☐	☐
1	☐	☐	☐	500	kbps	☐	☐	☐	☐	☐
2	☐	☐	☑	20	Mbps	☐	☐	☐	☐	☐
3	☐	☐	☐	500	kbps	☐	☐	☐	☐	☐
4	☐	☐	☐	500	kbps	☐	☐	☐	☐	☐
5	☐	☐	☐	500	kbps	☐	☐	☐	☐	☐
6	☐	☐	☐	500	kbps	☐	☐	☐	☐	☐
7	☐	☐	☐	500	kbps	☐	☐	☐	☐	☐
8	☐	☐	☐	500	kbps	☐	☐	☐	☐	☐
9	☐	☐	☐	500	kbps	☐	☐	☐	☐	☐
10	☐	☐	☐	500	kbps	☐	☐	☐	☐	☐
11	☐	☐	☐	500	kbps	☐	☐	☐	☐	☐
12	☐	☐	☐	500	kbps	☐	☐	☐	☐	☐

Submit Reset

Рисунок 69 Настройка ограничителей входной очереди

- **E**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включение или отключение ограничителей входящей очереди. Вам необходимо установить скорость и единицу измерения после включения ограничения трафика для очереди.
- **Rate, Unit**
  Диапазон: 100~3276700 кбит/с/ 1~3276 Мбит/с
  По умолчанию: 500 кбит/с
  Функция: ограничение скорости пакетов, полученных очередью порта. Пакеты со скоростью, превышающей значение, отбрасываются.

Настройте режим планирования очереди портов, как показано на рисунке 70 и рисунке 71.

QoS Egress Port Schedulers

Port	Mode	Weight Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	6 Queues Weighted	13%	25%	25%	13%	13%	13%
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-
10	Strict Priority	-	-	-	-	-	-
11	Strict Priority	-	-	-	-	-	-
12	Strict Priority	-	-	-	-	-	-

Рисунок 70 Просмотр режима планирования очереди портов

Нажмите <Port>, чтобы перейти на страницу конфигурации «режим планирования очереди портов».

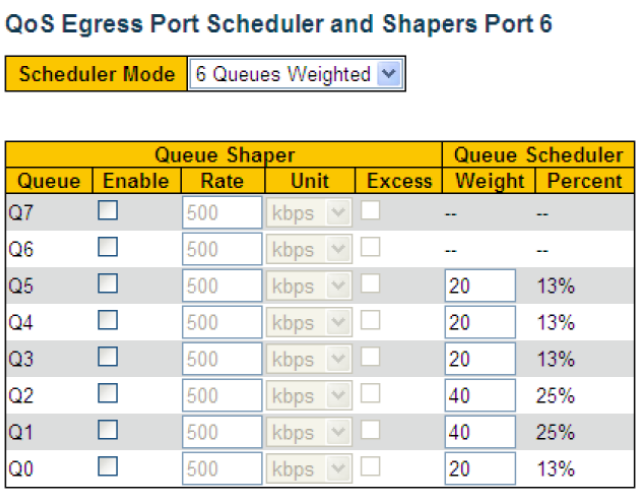


Рисунок 71 Настройка режима планирования очереди портов

- **Scheduler Mode**
  Опции: Строгий приоритет/6 взвешенных очередей
  По умолчанию: Строгий приоритет
  Функция: настроить режим исходящей очереди для выбранного порта.
- **Queue Weight**
  Диапазон: 1~100
  По умолчанию: 17
  Функция: Настройка значений веса очереди.
  Вы можете выбрать порт для настройки режима планирования очереди в правом верхнем углу страницы.

  Настройте формирователи выходного порта, как показано на рисунке 72.

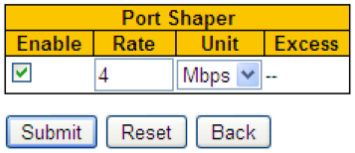


Рисунок 72 Настройка формирователей выходного порта

- **Enable**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включение или отключение формирователей выходного порта. Формирование трафика порта осуществляется ограничением скорости порта.
- **Rate, Unit**
  Диапазон: 100~3281943 кбит/с/ 1~3281 Мбит/с
  По умолчанию: 500 кбит/с
  Функция: ограничение скорости пакетов, передаваемых портом. Пакеты со скоростью, превышающей значение, отбрасываются.
  Нажмите <Назад>, чтобы закрыть текущую страницу конфигурации и вернуться на предыдущую страницу конфигурации.
  Выбрать порт для настройки шейпинга трафика можно в правом верхнем углу страницы.

Настройте формирователи очередей, как показано на рисунке 73.

Queue Shaper					Queue Scheduler	
Queue	Enable	Rate	Unit	Excess	Weight	Percent
Q7	☐	500	kbps	☐	--	--
Q6	☑	4	Mbps	☐	--	--
Q5	☑	8	Mbps	☑	20	13%
Q4	☐	500	kbps	☐	20	13%
Q3	☐	500	kbps	☐	20	13%
Q2	☐	500	kbps	☐	40	25%
Q1	☐	500	kbps	☐	40	25%
Q0	☐	500	kbps	☐	20	13%

Рисунок 73 Настройка формирователи очередей

- **Enable**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включить или отключить формирователи очередей.
- **Rate, Unit**
  Диапазон: 100~3281943 кбит/с/ 1~3281 Мбит/с
  По умолчанию: 500 кбит/с
  Функция: ограничение скорости пакетов, передаваемых очередью порта. Пакеты со скоростью, превышающей значение, отбрасываются.
  Нажмите <Back>, чтобы закрыть текущую страницу конфигурации и вернуться на предыдущую страницу конфигурации.
  Выбрать порт для настройки шейпинга трафика можно в правом верхнем углу страницы.

Настройте Port Storm Control как показано на рисунке 74.

Global Storm Policer Configuration

Frame Type	Enable	Rate	Unit
Unicast	☑	1	kfps
Multicast	☐	1	fps
Broadcast	☐	1	fps

Submit Reset

Рисунок 74 Настройка Port Storm Control

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

- **Enable**

Опции: Enable / Disable
По умолчанию: Disable
Функция: включение или отключение управления штормом портов.

- **Rate, Unit**
  Диапазон: 1~1024000fps/ 1~1024kfps
  По умолчанию: 1 кадр/с
  Функция: Настройте пороговое значение для ограничения скорости порта, и пакеты, превышающие пороговое значение, будут отброшены.

Просмотрите счетчики очереди, как показано на рисунок 75.

Queuing Counters

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	1328270	897	0	0	0	0	0	0	0	0	0	0	0	0	0	6852
2	236399	1092247	0	0	0	0	0	0	0	0	0	0	0	0	0	693
3	284	222112	0	0	0	0	0	0	0	0	0	0	0	0	0	13096
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Рисунок 75 Просмотр счетчиков очереди.

Отображение количества пакетов, которые каждая очередь отправляет/получает. Нажмите <port>, чтобы перейти на страницу «подробной статистики порта», как показано на рисунке 48.

9. Безопасность

9.1. 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 2.

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.

Таблица 2 Уровни пользователей

9.1.1. Веб конфигурирование

Конфигурирование пользователей.

Создать пользователя можно как показано на рисунке 76:

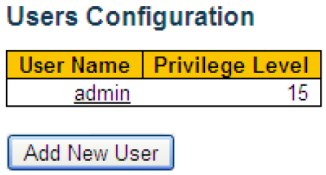


Рисунок 76 Создание нового пользователя.

Нажмите <Add New User>, чтобы настроить пользователя другого уровня, коммутатор поддерживает до 20 пользователей.

Настройте пользователя другого уровня, как показано на рисунке 77:

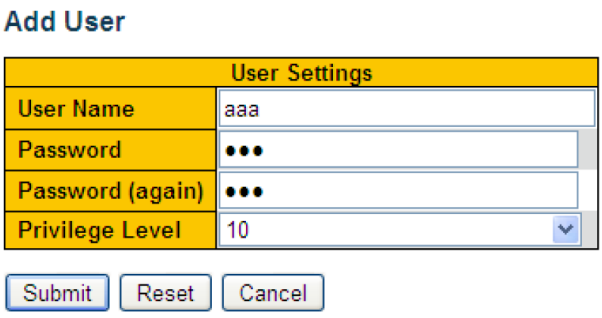


Рисунок 77 Конфигурирование пользователя.

- **Name**
  Диапазон: 1~16 символов
- **Password**
  Диапазон: 1~32 символа
  Функция: настройка пароля, который будет использоваться при доступе текущего пользователя к коммутатору.
- **Password (again)**

Диапазон: 1~32 символа
Функция: подтверждение пароля.

- **Privilege Level**
  Диапазон: 0~15
  Функция: настроить уровень пользователя, пользователи разных уровней имеют разные права на работу.

Просмотрите список пользователей, как показано на рисунке 78:

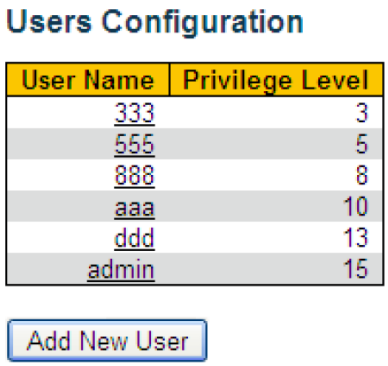


Рисунок 78 Список пользователя.

- **Key name**
  Функция: выберите имя ключа, которое будет использоваться при доступе текущего пользователя к коммутатору в режиме ssh.

Измените конфигурацию пользователя, как показано на рисунке 79:

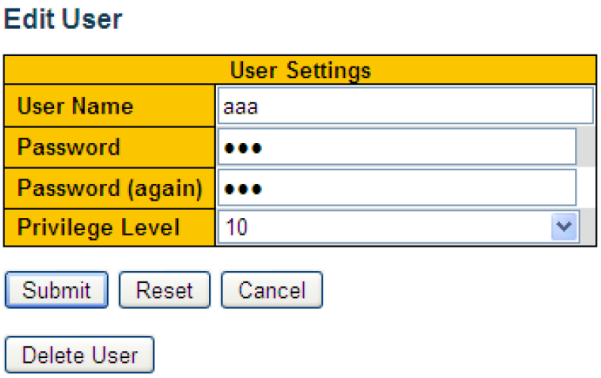
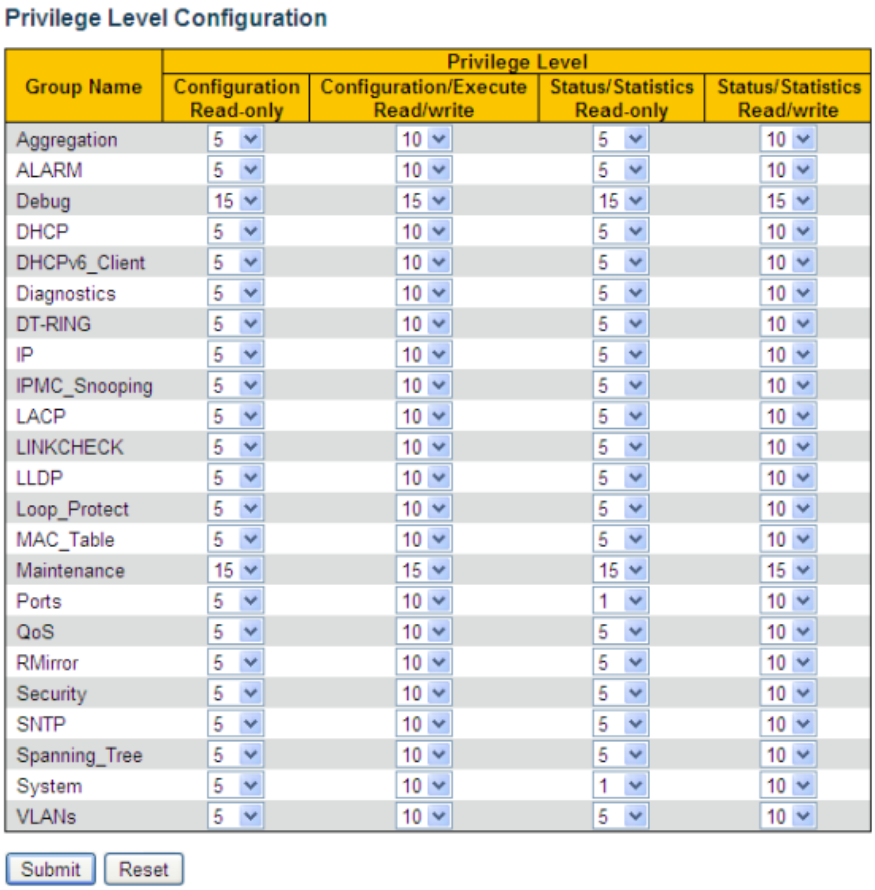


Рисунок 79 Модификация пользователя.

Вы можете изменить пароль пользователя и уровень привилегий.
Нажмите <Delete User>, чтобы удалить текущего пользователя.

Настройте уровень привилегий групп, как показано на рисунке 80:



Privilege Level Configuration

Group Name	Privilege Level			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
ALARM	5	10	5	10
Debug	15	15	15	15
DHCP	5	10	5	10
DHCPv6_Client	5	10	5	10
Diagnostics	5	10	5	10
DT-RING	5	10	5	10
IP	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LINKCHECK	5	10	5	10
LLDP	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
Maintenance	15	15	15	15
Ports	5	10	1	10
QoS	5	10	5	10
RMirror	5	10	5	10
Security	5	10	5	10
SNTP	5	10	5	10
Spanning_Tree	5	10	5	10
System	5	10	1	10
VLANs	5	10	5	10

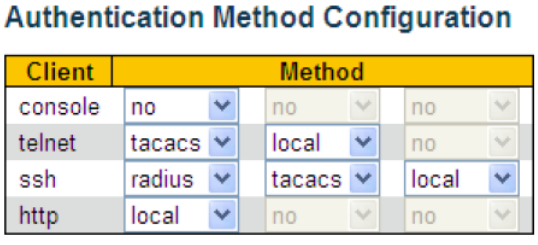
Submit Reset

Рисунок 80 Настроика уровеня привилегий групп.

Когда уровень привилегий пользователя такой же или выше, чем уровень привилегий группы, пользователь может получить доступ к группе или настроить ее. Право доступа или настройки основано на привилегии пользователя.

9.2. Конфигурация входа в систему для аутентификации

Настройте режим доступа для коммутатора, режим аутентификации и порядок аутентификации, как показано на рисунке 81.



Authentication Method Configuration

Client	Method		
console	no	no	no
telnet	tacacs	local	no
ssh	radius	tacacs	local
http	local	no	no

Рисунок 81 Настроика режим доступа для коммутатора.

- **Client**
  Опции: консоль/telnet/ssh/http
  Функция: выберите режим доступа для переключения.
- **Method 1/Method 2/Method 3**

Варианты: нет/локальные/tacacs/радиус
По умолчанию: локальный
Функция: Методы слева направо: метод 1, метод 2 и метод 3. Выберите порядок проверки подлинности. 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: нет означает, что аутентификация отключена и вход в систему невозможен. local означает использование имени пользователя и пароля, установленных в local, для выполнения аутентификации. tacacs означает использование имени пользователя и пароля, установленных на сервере TACACS+ для аутентификации. радиус означает использование имени пользователя и пароля, установленных на сервере RADIUS для аутентификации.

9.3. SSH конфигурация

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 удаленно входят в коммутатор через SSH.

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.

9.3.1. Веб конфигурирование

Включить SSH протокол можно как показано на рисунке 82.

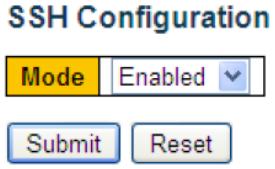


Рисунок 82 Включение SSH протокола.

- **Режим**
  Параметры: Включено/Выключено
  По умолчанию: включено

Функция: включить/отключить протокол SSH. Если он включен, коммутатор работает как SSH-сервер.

9.4. SSL конфигурация

SSL (Secure Socket Layer) — это протокол безопасности, обеспечивающий безопасный канал для Протокол прикладного уровня на основе TCP, например, 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.

9.4.1. Веб конфигурирование

Включить HTTPS протокол можно как на рисунке 83:

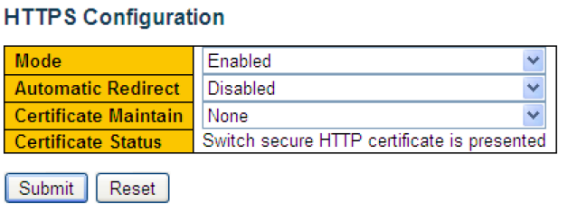


Рисунок 83 Включение HTTPS протокола.

- **Режим**
  Параметры: Включено/Выключено
  По умолчанию: отключено
  Функция: включить или отключить протокол HTTPS. После включения HTTPS пользователи могут использовать http://ip-адрес и безопасную ссылку https://ip-адрес для доступа к коммутатору.
- **Automatic Redirect**
  Опции: Включено/Выключено
  По умолчанию: отключено
  Функция: Включено означает, что пользователи должны использовать безопасную ссылку https://ip-адрес для доступа к коммутатору. Отключено означает, что пользователи могут использовать http://ip-адрес и безопасную ссылку https://ip-адрес для доступа к коммутатору. Параметр «Автоматическое перенаправление» можно настроить, только если включен «Режим».
- **Certificate Maintain**
  Варианты: Нет/Удалить/Загрузить/Создать
  По умолчанию: Нет

Функция: поддержка сертификата HTTPS. Параметр «Сохранение сертификата» можно настроить, только если «Режим» отключен. Удалить используется для удаления существующего сертификата HTTPS с коммутатора. Загрузка используется для загрузки правильного сертификата HTTPS в
переключаться с помощью веб-браузера или URL-адреса. Generate указывает, что коммутатор автоматически создает правильный сертификат HTTPS.

- **Certificate Status**
  Параметры: Переключатель защищенного HTTP-сертификата представлен/Переключатель защищенного HTTP-сертификата не представлен/Переключатель защищенного HTTP-сертификата создается
  Функция: Отображает состояние сертификата HTTPS в коммутаторе. Наличие защищенного HTTP-сертификата коммутатора указывает на то, что сертификат доступен в коммутаторе. В этом случае вы можете войти на веб-страницу коммутатора через HTTPS. Безопасный HTTP-сертификат коммутатора не представлен означает, что в коммутаторе нет доступного сертификата. В этом случае вы не сможете войти на веб-страницу через HTTPS. Генерируется защищенный HTTP-сертификат переключателя указывает, что сертификаты HTTPS создаются.

Создать сертификат HTTPS, можно как показано на рисунке 84.

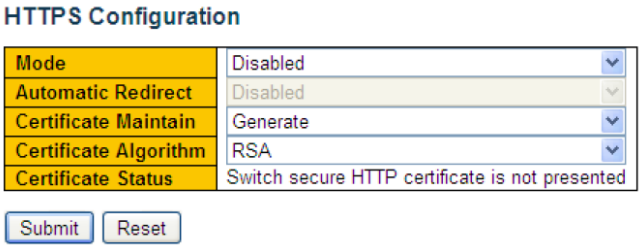


Рисунок 84 Конфигурирование HTTPS протокола.

- **Certificate Algorithm**
  Опции: RSA/DSA
  По умолчанию: RSA
  Функция: выберите алгоритм генерации сертификата HTTPS.

Загрузите сертификат HTTPS, как показано на рисунке 85 и 86.

Рисунок 85 Загрузка серитификата.

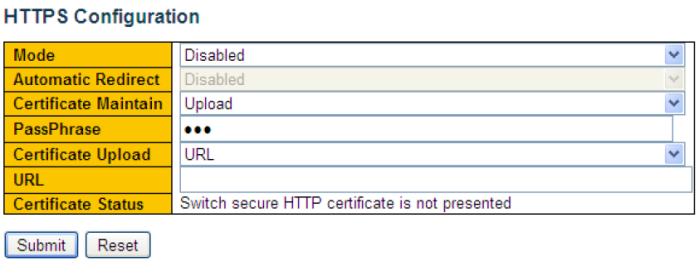


Рисунок 86 Загрузка серитификата.

- **PassPhrase**
  Функция: используется для шифрования сертификата.
- **Загрузка сертификата**
  Опции: Веб-браузер/URL
  По умолчанию: Веб-браузер
  Функция: выберите метод загрузки сертификата.
- **File Upload**
  Функция: выберите файл сертификата HTTPS, хранящийся в локальной папке.
- **URL-адрес**
  Функция: настроить путь хранения файла сертификата HTTPS. Поддерживаемые протоколы: HTTP, HTTPS, TFTP и FTP, формат конфигурации следующий: http://10.10.10.10:80/new_image_path/new_image.dat или FTP://имя_пользователя:пароль@10.10.10.10/путь_нового_изображения/new_image.dat.

  Когда сертификат HTTPS представлен в коммутаторе, введите имя пользователя и пароль для успешного входа в коммутатор через HTTPS.

9.5. Управление доступом

Записи доступа могут быть настроены для управления доступом к коммутатору, чтобы ограничить хосты. который может получить доступ к коммутатору, а также к режиму доступа. Можно настроить максимум 16 записей доступа. Хост, который соответствует любой из записей доступа, может успешно получить доступ к коммутатору.

Настройте запись управления доступом, как показано на рисунке 87.

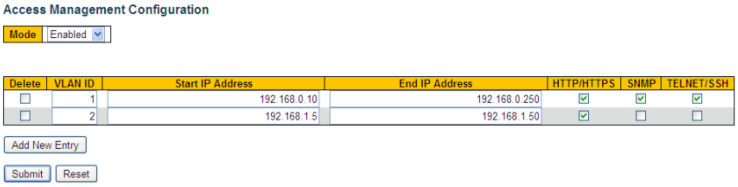


Рисунок 87 Настройка записи управления доступом.

- **Режим**
  Параметры: Включено/Выключено
  По умолчанию: отключено

Функция: включение или отключение управления доступом к коммутатору. Disable: доступ к коммутатору не ограничен.

- **VLAN ID**
  Диапазон: 1~4094
  Функция: Настройка идентификатора VLAN для записи управления доступом.
- **Start IP Address/End IP Address**
  Функция: Настройка диапазона IP-адресов для записи управления доступом.
- **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.
- **ТЕЛНЕТ/SSH**
  Функция: при выборе TELNET/SSH хост, который соответствует идентификатору VLAN и IP-адресу в записи доступа, может получить доступ к коммутатору через TELNET/SSH.
  Нажмите <Add New Entry>, чтобы настроить запись управления доступом. Коммутатор поддерживает до 16 записей управления доступом.

Просмотрите статистику управления доступом, как показано на рисунке 88.

Access Management Statistics Auto-refresh ☐ Refresh Clear

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	513	513	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	46	46	0
SSH	0	0	0

Рисунок 88 Просмотр статистики управления доступом.

Настройте тайм-ауты для режимов доступа к коммутатору, как показано на рисунке 89.

Login Timeout

Service Type	Timeout			
Command Line	10	min	0	sec
WEB	5	min	0	sec

Submit Reset

Рисунок 88 Настройка тайм-ауты для режимов доступа к коммутатору

- **Timeout**
  504 / 5 000
  Результаты перевода
  Перевод
  Диапазон: (0~1440) мин (0~3600) с
  По умолчанию: 10 минут для командной строки, 5 минут для Интернета.

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.

9.6. SNMP v1 / SNMP v2c

Простой протокол управления сетью (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 упреждающе сообщает об этом в NMS с помощью пакета-ловушки.

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

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

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

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

9.6.1. MIB

Любой управляемый ресурс называется управляемым объектом. База управляющей информации (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 собственный МИБ. NMS может читать/записывать MIB на основе разрешений. На рисунке 89 показаны взаимосвязи между NMS, агентом и MIB.

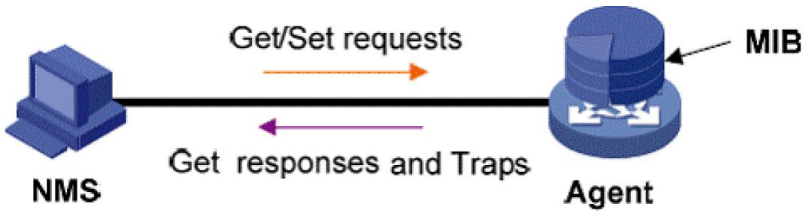


Рисунок 89 Связь между NMS, агентом и MIB

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 90, OID объекта A равен 1.2.1.1.

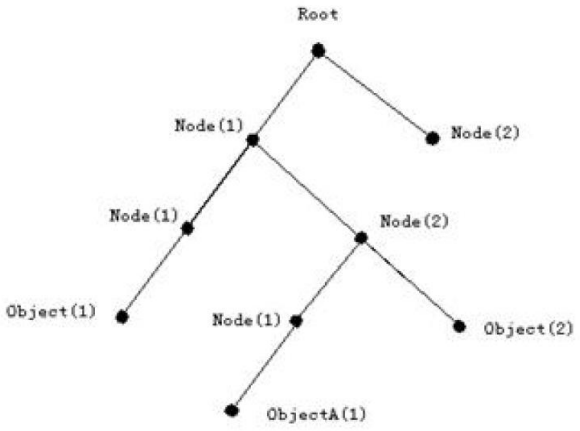


Рисунок 90 Структура MIB

9.6.2. Веб конфигурация

Включите протокол SNMP и выберите версию SNMP, как показано на рисунке 91:

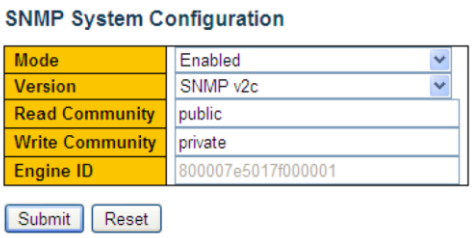


Рисунок 91 Включение протокола SNMP и выбор версии SNMP

- **Mode**
  Опции: Enable / Disable
  По умолчанию: Enable
  Функция: включить / отключить SNMP.
- **Version**
  Опции: SNMP v1 / SNMP v2c / SNMP v3
  По умолчанию: SNMP v2c
  Функция: выберите версию SNMP. SNMP v2c совместим с SNMP v1; SNMP v3 совместим с SNMP v1 и SNMP v2c.
- **Read Community**
  Диапазон: 0~255 символов
  По умолчанию: общедоступный
  Функция: Настройка имени сообщества только для чтения.
  Описание: Информация MIB коммутатора может быть прочитана только в том случае, если имя сообщества, переносимое пакетом SNMP, совпадает с именем, настроенным на коммутаторе.
- **Read Community**
  Диапазон: 0~255 символов
  По умолчанию: частный
  Функция: Настройка имени сообщества чтения-записи.
  Описание: Информация MIB коммутатора может быть прочитана и записана только в том случае, если имя сообщества, переносимое пакетом SNMP, совпадает с именем, настроенным на коммутаторе.

  Настройте режим global trap, как показано на рисунке 92.

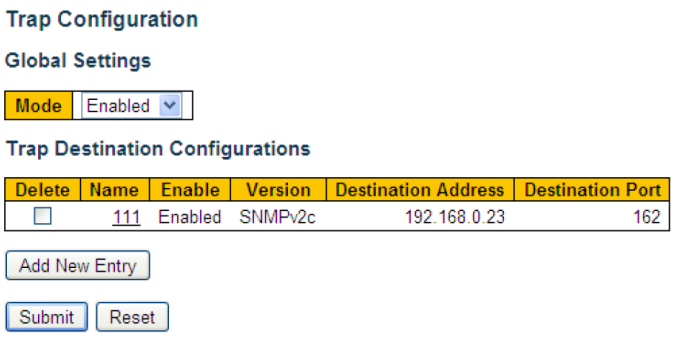


Рисунок 92 Конфигурирование режима Global Trap

- **Mode**
  Опции: Enable / Disable
  По умолчанию: Enable
  Функция: включить/отключить режим глобальной ловушки.
  Нажмите <Add New Entry>, чтобы настроить запись ловушки, коммутатор поддерживает максимум 4 записи ловушки. Нажмите <Name>, чтобы изменить запись прерывания.

  Настройте запись trap, как показано на рисунке 93.

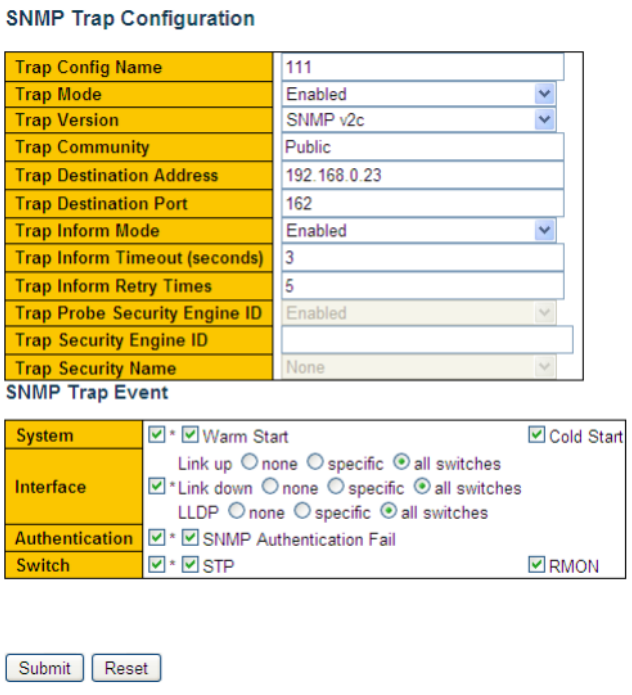


Рисунок 93 Конфигурирование Trap записи

- **Trap Config Name**
  Диапазон: 1~255 символов
  Функция: настроить имя записи ловушки.
- **Trap Mode**
  Параметры: Включено/Выключено
  По умолчанию: отключено
  Функция: включить/отключить запись ловушки. После включения режима trap коммутатор может отправить сообщение trap в NMS.
- **Trap Version**
  Опции: SNMP v1/SNMP v2c/SNMP v3
  По умолчанию: SNMP v2c
  Функция: Установите версию пакетов-ловушек, отправляемых с коммутатора на сервер.
- **Trap Community**
  Диапазон: 0~255 символов
  По умолчанию: общедоступный
  Функция: Настройка сообщества, переносимого сообщением-ловушкой.
- **Trap Destination Address**
  Формат: A.B.C.D.
  Функция: Настройка адреса сервера для получения сообщений-ловушек.
- **Trap Destination Port**
  Диапазон: 1~65535
  По умолчанию: 162
  Функция: Настройка номера порта для отправки сообщений-ловушек.
- **Trap Inform Mode**
  Параметры: Включено/Выключено
  По умолчанию: отключено

Функция: следует ли отправлять ответ коммутатору после получения сервером пакета-ловушки.

- **Trap Inform Timeout**
  Диапазон: 0~2147 с
  По умолчанию: 3 с
  Функция: Установите время ожидания для отправки пакетов-ловушек. После отправки trap-пакета на сервер коммутатор повторно передает trap-пакет, если в течение этого времени не получает ответа от сервера.
- **Trap Inform Retry Times**
  Диапазон: 0~255
  По умолчанию: 5
  Функция: Установите количество повторных передач пакетов с прерыванием по тайм-ауту. Если накопленное количество раз передачи превышает значение этого параметра, а сервер еще не отвечает, считается, что передача trap-пакета не удалась.
- **Warm Start/ Cold Start**
  Параметры: Включено/Выключено
  По умолчанию: отключено
  Функция: отправлять ли сообщение-ловушку или нет при переключении теплого/холодного пуска.
- **Link up/ Link down**
  Варианты: нет/конкретные/все переключатели
  По умолчанию: нет
  Функция: Отправлять ли пакет прерывания порта вверх/вниз при изменении состояния порта.
- **LLDP**
  Варианты: нет/конкретные/все переключатели
  По умолчанию: нет
  Функция: следует ли отправлять пакет-ловушку протокола обнаружения канального уровня (LLDP) при изменении статуса соседа.
- **SNMP Authentication Fail**
  Параметры: Включено/Выключено
  По умолчанию: отключено
  Функция: отправлять сообщение-ловушку или нет при сбое аутентификации SNMP.
- **STP**
  Параметры: Включено/Выключено
  По умолчанию: отключено
  Функция: отправлять или нет сообщение-ловушку при изменении статуса STP.

9.7. SNMPv3

SNMP v3 обеспечивает механизм аутентификации модели безопасности на основе пользователей (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. Чтобы обеспечить связь между NMS и агентом, их версии SNMP

должны совпадать. Для агента можно настроить разные версии SNMP, чтобы он мог использовать разные версии для связи с разными NMS.

SNMP v3 предоставляет четыре таблицы 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 представления относится к информации представления MIB, которая указывает информацию MIB, к которой могут получить доступ пользователи. Представление MIB может содержать все узлы определенного поддерева MIB (то есть пользователям разрешен доступ ко всем узлам поддерева MIB) или не содержать ни одного из узлов определенного поддерева MIB (то есть пользователям не разрешен доступ ни к одному из узлов). узел поддерева MIB). Вы можете определить права доступа MIB в таблице доступа по имени группы, модели безопасности и уровню безопасности.

9.7.1. Веб конфигурирование

Включите протокол SNMP и выберите версию SNMP, как показано на рисунке 94.

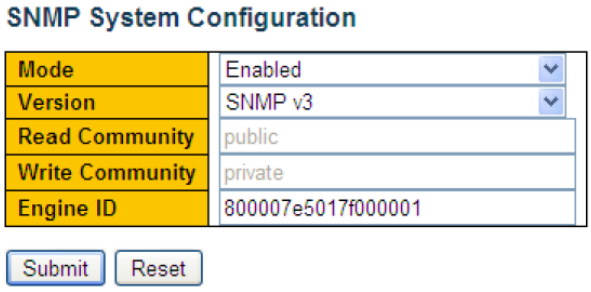


Рисунок 94 Включение протокола SNMP и выбор версии SNMP

- **Mode**
  Опции: Enabled/Disabled
  По умолчанию: Enabled
  Функция: включить/отключить SNMP.
- **Version**
  Опции: SNMP v1/SNMP v2c/SNMP v3
  По умолчанию: SNMP v2c
  Функция: выберите версию SNMP. SNMP v2c совместим с SNMP v1; SNMP v3 совместим с SNMP v1 и SNMP v2c.
- **Engine ID**
  Диапазон: Идентификатор двигателя представляет собой четное количество цифр в шестнадцатеричном представлении, которое не может состоять только из нулей или всех букв F. Диапазон четного числа цифр от 10 до 64.
  Функция: Установите идентификатор механизма для системы SNMP v3. При изменении идентификатора механизма пользователи, соответствующие идентификаторам устройств в таблице пользователей, удаляются.

Настройте режим Global trap, как показано на рис. 95.

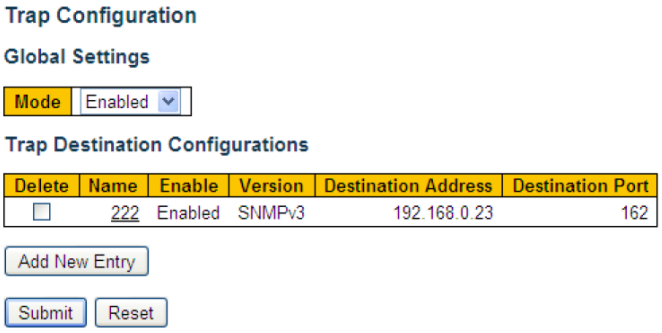


Рисунок 95 Конфигурирование режима Global Trap

- **Mode**
  Опции: Enable / Disable
  По умолчанию: Disable
  Функция: включить/отключить режим глобальной ловушки.
  Нажмите <Add New Entry>, чтобы настроить запись ловушки, коммутатор поддерживает максимум 4 записи ловушки. Нажмите <Имя>, чтобы изменить запись прерывания.

Настройте Trap entry, как показано на рисунке 96.

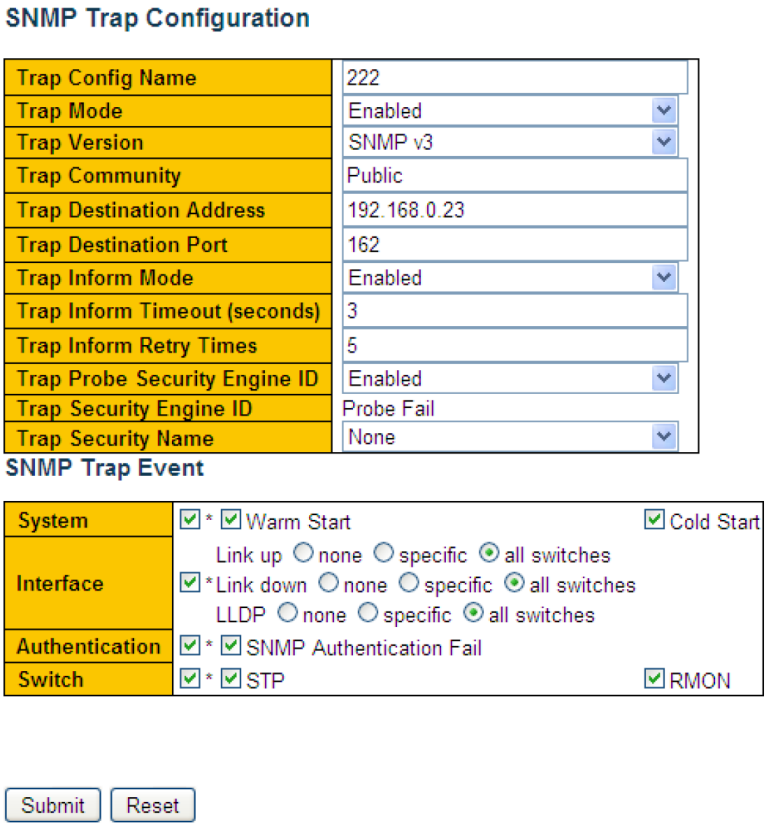


Рисунок 96 Конфигурирование Trap entry

- **Trap Config Name**
  Диапазон: 1~255 символов
  Функция: настроить имя записи ловушки.
- **Trap Mode**
  Параметры: Включено/Выключено
  По умолчанию: отключено
  Функция: включить/отключить запись ловушки. После включения режима trap коммутатор может отправить сообщение trap в NMS.
- **Trap Version**
  Опции: SNMP v1/SNMP v2c/SNMP v3
  По умолчанию: SNMP v2c
  Функция: Установите версию пакетов-ловушек, отправляемых с коммутатора на сервер.
- **Trap Community**
  Диапазон: 0~255 символов
  По умолчанию: общедоступный
  Функция: Настройка сообщества, переносимого сообщением-ловушкой.
- **Trap Destination Address**
  Формат: A.B.C.D.
  Функция: Настройка адреса сервера для получения сообщений-ловушек.
- **Trap Destination Port**
  Диапазон: 1~65535
  По умолчанию: 162
  Функция: Настройка номера порта для отправки сообщений-ловушек.
- **Trap Inform Mode**
  Параметры: Включено/Выключено
  По умолчанию: отключено
  Функция: Укажите, следует ли отправлять ответ на коммутатор после того, как сервер получит пакет-ловушку.
- **Trap Inform Timeout**
  Диапазон: 0~2147 с
  По умолчанию: 3 с
  Функция: Установите время ожидания для отправки пакетов-ловушек. После отправки trap-пакета на сервер коммутатор повторно передает trap-пакет, если в течение этого времени не получает ответа от сервера.
- **Trap Inform Retry Times**
  Диапазон: 0~255
  По умолчанию: 5
  Функция: Установите количество повторных передач пакетов с прерыванием по тайм-ауту. Если накопленное количество раз передачи превышает значение этого параметра, а сервер еще не отвечает, считается, что передача trap-пакета не удалась.
- **Trap Probe Security Engine ID**
  Параметры: Включено/Выключено
  По умолчанию: включено
  Функция: установка идентификатора механизма безопасности, передаваемого в пакетах ловушек SNMP v3. Если для него установлено значение Enabled, коммутатор автоматически проверяет и получает идентификатор модуля

безопасности. Если для него установлено значение Disabled, идентификатор механизма безопасности получается из значения Trap Security Engine ID.

- **Trap Security Engine ID**
  Диапазон: Идентификатор двигателя представляет собой четное количество цифр в шестнадцатеричном представлении, которое не может состоять только из нулей или всех букв F. Диапазон четного числа цифр от 10 до 64.
  Функция: Настройка идентификатора Trap Security Engine ID, переносимого сообщением-ловушкой.
- **Warm Start/ Cold Start**
  Параметры: Включено/Выключено
  По умолчанию: отключено
  Функция: отправлять ли сообщение-ловушку или нет при переключении теплого/холодного пуска.
- **Link up/ Link down**
  Варианты: нет/конкретные/все переключатели
  По умолчанию: нет
  Функция: Отправлять ли пакет прерывания порта вверх/вниз при изменении состояния порта.
- **LLDP**
  Варианты: нет/конкретные/все переключатели
  По умолчанию: нет
  Функция: отправлять ли пакет-ловушку LLDP при изменении статуса соседа.
- **SNMP Authentication Fail**
  Параметры: Включено/Выключено
  По умолчанию: отключено
  Функция: отправлять сообщение-ловушку или нет при сбое аутентификации SNMP.
- **STP**
  Параметры: Включено/Выключено
  По умолчанию: отключено
  Функция: отправлять или нет сообщение-ловушку при изменении статуса STP.

Настройте community, как показано на рис. 97.

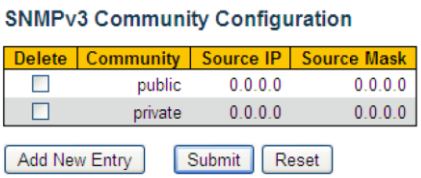


Рисунок 97 Конфигурирование community

- **Community**
  Диапазон: 1~32 символа
  Функция: Настройка имени сообщества.
  Если выбран SNMP v3, можно задать имя сообщества, чтобы разрешить системе управления сетью (NMS) доступ к коммутатору через SNMPv1 и SNMPv2. В этом случае имя сообщества в NMS должно совпадать с именем на коммутаторе. Права доступа для имени сообщества зависят от конфигурации таблицы групп и таблицы доступа.

- **Source IP**
  Формат: A.B.C.D.
  Функция: Настройка IP-адреса NMS.
- **Source Mask**
  Функция: Сеть указывает, что вы можете настроить диапазон пула IP-адресов, а диапазон адресов определяется маской подсети. Маска подсети представляет собой число длиной 32 бита, состоящее из строки 1 и строки 0. «1» соответствует полям номера сети и полям номера подсети, а «0» соответствует полям номера хоста. IP-адрес NMS определяется IP-адресом источника и маской источника.
  Нажмите <Add New Entry>, чтобы настроить community, коммутатор поддерживает до 16 community.

  Настройте таблицу пользователей, как показано на рисунке 98.

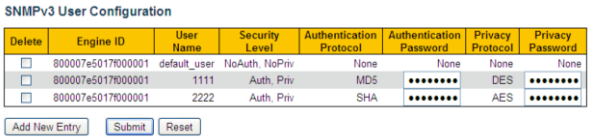


Рисунок 98 Конфигурирование таблицы пользователей

- **Engine ID**
  Диапазон: Идентификатор двигателя представляет собой четное количество цифр в шестнадцатеричном представлении, которое не может состоять только из нулей или всех букв F. Диапазон четного числа цифр от 10 до 64.
  Функция: Установите идентификатор пользовательского движка. Если идентификатор ядра пользователя отличается от идентификатора ядра системы SNMPv3, пользователь в настоящее время неэффективен.
- **User Name**
  Диапазон: 1~32 символа
  Функция: Создать имя пользователя.
- **Security Level**
  Варианты: NoAuth,NoPriv/Auth,NoPriv/Auth,Priv
  Функция: Настройка уровня безопасности текущего пользователя.
  Описание: NoAuth,NoPriv указывает, что ни аутентификация, ни шифрование не требуются. Auth,NoPriv указывает, что требуется аутентификация, но не шифрование. Auth,Priv указывает, что требуется как аутентификация, так и шифрование.
- **Authentication Protocol**
  Опции: MD5/SHA
  Функция: выбор алгоритма аутентификации. Протокол аутентификации и пароль аутентификации должны быть установлены, когда уровень безопасности установлен на Auth, NoPriv или NoAuth, Priv.
- **Authentication Password**
  Диапазон: 8~32 символа (MD5) 8~40 символов (SHA)
  Функция: Создать пароль аутентификации.
- **Privacy Protocol**
  Опции: DES/AES

Функция: выберите протокол шифрования. Протокол конфиденциальности и пароль конфиденциальности должны быть установлены, когда уровень безопасности установлен на Auth, Priv.

- **Privacy Password**
  Диапазон: 8~32 символа
  Функция: Создать пароль шифрования.
  Нажмите <Добавить новую запись>, чтобы настроить запись пользователя. Поддерживается не более 16 пользователей.

Настройте групповую таблицу, как показано на рисунке 99.

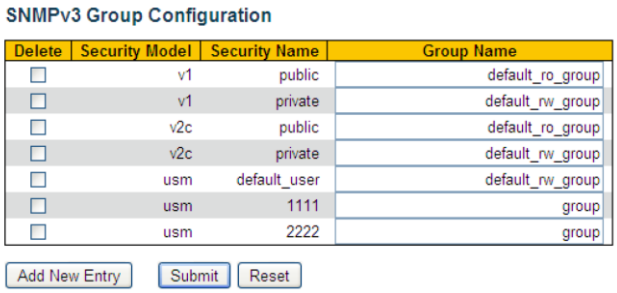


Рисунок 99 Конфигурирование групповой таблицы

- **Security Model**
  По умолчанию: v1/v2/usm
  Описание: Выберите модель безопасности текущей группы (версия SNMP). SNMP v3 использует модель безопасности на основе пользователей (USM).
- **Security Name**
  Диапазон: все существующие сообщества/имена пользователей, 1~32 символа
  Функция: Настройка имени безопасности. Если используется модель безопасности v1/v2, имя безопасности должно совпадать с именем сообщества. Если используется модель безопасности usm, имя безопасности должно совпадать с именем пользователя в пользовательской таблице.
- **Group Name**
  Диапазон: 1~32 символа
  Функция: Настройте имя групповой таблицы, пользователи с одинаковым именем группы принадлежат к одной группе.
  Нажмите <Добавить новую запись>, чтобы настроить групповую таблицу. Поддерживается не более 16 групп.

Настройте таблицу просмотра, как показано на рисунке 100.

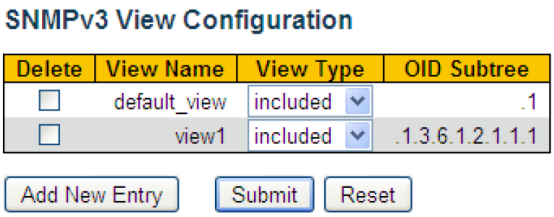


Рисунок 100 Конфигурирование таблицы просмотра

- **View Name**
  Диапазон: 1~32 символа
  Функция: Настройка имени представления.
- **View Type**
  Опции: включены/исключены
  По умолчанию: включено
  Функция: включено указывает, что текущее представление включает все узлы дерева MIB. Excluded указывает, что текущее представление не включает узлы дерева MIB.
- **OID Subtree**
  Функция: MIB-дерево, обозначенное OID корневого узла дерева.
  Нажмите <Добавить новую запись>, чтобы настроить таблицу просмотра. Поддерживается не более 16 записей просмотра.

  Настройте таблицу доступа, как показано на рисунке 101.

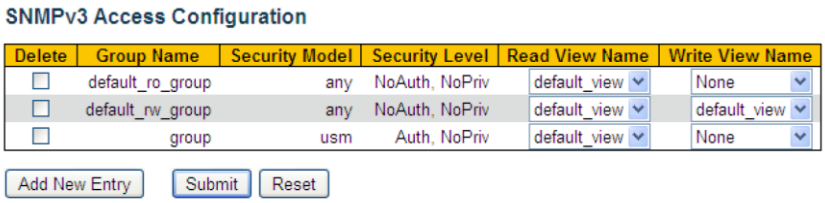


Рисунок 101 Конфигурирование таблицу доступа SNMPv3

- **Group Name**
  Диапазон: все существующие имена групп, 1~32 символа
  Функция: Пользователи в группе имеют одинаковые права доступа.
- **Security Model**
  По умолчанию: любой/v1/v2/usm
  Функция: Установите модель безопасности (т. е. номер версии SNMP), используемую при доступе текущей группы к коммутатору. SNMPv3 принимает модель безопасности на основе пользователя (USM), и значение any указывает, что может быть принята любая модель безопасности. Имя группы и модель безопасности в таблице доступа должны совпадать с таковыми в таблице группы.
- **Security Level**
  Варианты: NoAuth,NoPriv/Auth,NoPriv/Auth,Priv
  Функция: Выберите уровень безопасности текущей группы.
  Описание: NoAuth,NoPriv указывает, что ни аутентификация, ни шифрование не требуются. Auth,NoPriv указывает, что требуется аутентификация, но не шифрование. Auth,Priv указывает, что требуется как аутентификация, так и шифрование. Когда требуется аутентификация/шифрование, пользователь может получить доступ к указанной информации MIB только в том случае, если протокол аутентификации/шифрования и пароль аутентификации/шифрования идентичны настроенным в пользовательской таблице.
  Уровни безопасности: NoAuth,NoPriv, Auth,NoPriv и Auth,Priv в порядке возрастания. Доступ к содержимому с более низким уровнем безопасности разрешен с более высоким уровнем безопасности. Например, если и протокол аутентификации/шифрования, и пароль аутентификации/шифрования верны,

уровень безопасности настроен как Auth, к NoPriv можно успешно получить доступ с уровнями безопасности Auth, NoPriv и Auth, Priv, но нельзя получить доступ с уровнем безопасности NoAuth, NoPriv. уровень.

- **Read View Name**
  Параметры: default_view/Нет/все существующие имена представлений.
  Функция: Выберите имя представления только для чтения.
- **Write View Name**
  Параметры: default_view/Нет/все существующие имена представлений.
  Функция: Выберите имя представления записи.
  Нажмите <Добавить новую запись>, чтобы настроить таблицу доступа. Поддерживается не более 16 записей доступа.

9.8. RMON

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

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

9.8.1. Группы RMON

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

- Группа статистики

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

- Группа истории

Группа 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.

- Группа событий

Группа событий используется для определения индексов событий и методов обработки событий. События, определенные в группе событий, используются в элементе конфигурации группы тревог. Событие запускается, когда контролируемое устройство соответствует условию тревоги. События рассматриваются в следующем способы:

Журнал: 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.

Нет: указывает на отсутствие действий.

- Группа сигналов тревоги

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.

9.8.2. Веб конфигурирование

Настройте таблицу статистики, как показано на рисунке 102.

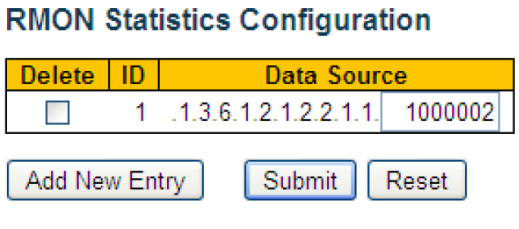


Рисунок 102 Конфигурирование RMON таблицы статистики

- **ID**
  Диапазон: 1~65535
  Функция: Настройка номера записи статистики. Группа статистики поддерживает до 128 записей.
- **Data Source**
  Диапазон: 100000portid
  Функция: Выберите порт, статистика которого должна быть собрана.

Просмотрите статус группы статистики, как показано на рис. 103.

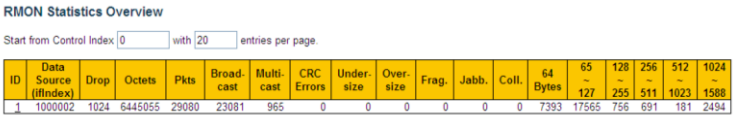


Рисунок 103 Обзор статуса группы статистики

Drop: количество пакетов, отброшенных портом.
Octets: количество байтов, полученных портом.
Pkts: количество пакетов, полученных портом.
Broadcast: количество широковещательных пакетов, полученных портом.
Multicast: количество многоадресных пакетов, полученных портом.
Ошибки CRC: количество пакетов с ошибками CRC длиной от 64 до 9600 байт, полученных портом.
Undersize: количество пакетов размером менее 64 байт, полученных портом.
Oversize: количество пакетов размером более 9600 байт, полученных портом.
Frag.: количество пакетов с ошибками CRC размером менее 64 байт, полученных портом.
Jabb.: количество пакетов ошибок CRC размером более 9600 байт, полученных портом. Coll.: количество коллизий, полученных портом в полудуплексном режиме.
64 байта: количество пакетов длиной 64 байта, полученных портом.
65~127: количество пакетов длиной от 65 до 127 байт, полученных портом.
128~255: количество пакетов длиной от 128 до 255 байт, полученных портом.
256~511: количество пакетов длиной от 256 до 511 байт, полученных портом.
512~1023: количество пакетов длиной от 512 до 1023 байт, полученных портом.
1024~1588: количество пакетов

Настройте таблицу истории, как показано на рисунке 104.

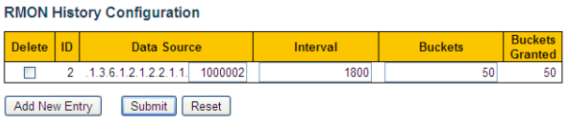
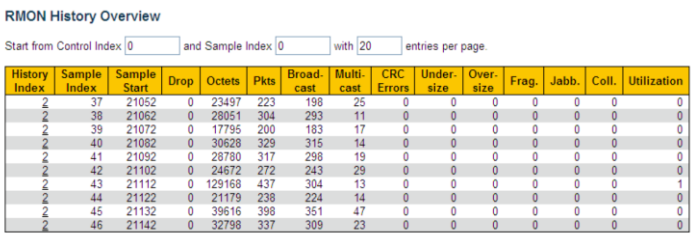


Рисунок 104 Конфигурирование талицы истории

- **ID**
  Диапазон: 1~65535
  Функция: Настройка номера записи истории. Группа истории поддерживает до 256 записей.
- **Data Source**
  Параметры: 100000portid
  Функция: Выберите порт, информация которого должна быть запрошена.
- **Interval**
  Диапазон: 1~3600 с
  По умолчанию: 1800 сек.
  Функция: Настройка периода выборки порта.
- **Buckets**
  Диапазон: 1~65535
  По умолчанию: 50
  Функция: Настраивает количество последних значений выборки информации о порте, хранящейся в RMON.

Просмотрите статус группы истории, как показано на рисунке 105.

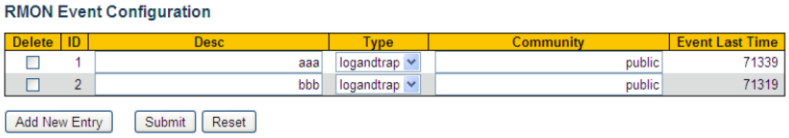

RMON History Overview

Start from Control Index 0 and Sample Index 0 with 20 entries per page.

History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
2	37	21052	0	23497	223	198	25	0	0	0	0	0	0	0
2	38	21062	0	28051	304	293	11	0	0	0	0	0	0	0
2	39	21072	0	17795	200	183	17	0	0	0	0	0	0	0
2	40	21082	0	30628	329	315	14	0	0	0	0	0	0	0
2	41	21092	0	28780	317	298	19	0	0	0	0	0	0	0
2	42	21102	0	24672	272	243	29	0	0	0	0	0	0	0
2	43	21112	0	129168	437	304	13	0	0	0	0	0	0	1
2	44	21122	0	21179	238	224	14	0	0	0	0	0	0	0
2	45	21132	0	39616	398	351	47	0	0	0	0	0	0	0
2	46	21142	0	32798	337	309	23	0	0	0	0	0	0	0

Рисунок 105 Обзор состояние группы истории

Настройте таблицу событий, как показано на рисунке 106.


RMON Event Configuration

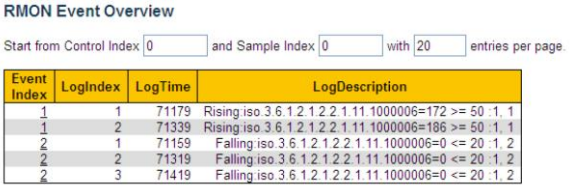
Delete	ID	Desc	Type	Community	Event Last Time
☐	1	aaa	logandtrap	public	71339
☐	2	bbb	logandtrap	public	71319

Add New Entry | Submit | Reset

Рисунок 106 Конфигурирование Event Table

- **ID**
  Диапазон: 1~65535
  Функция: Настройка порядкового номера записи события. Группа событий поддерживает до 128 записей.
- **Desc**
  Диапазон: 0~127 символов
  Функция: Опишите событие.
- **Type**
  Опции: none/log/snmptrap/logandtrap
  По умолчанию: нет
  Функция: Настроить тип события для аварийных сигналов, то есть режим обработки аварийных сигналов.
- **Community**
  Диапазон: 0~127 символов
  По умолчанию: общедоступный
  Функция: настроить имя сообщества для отправки события ловушки. Значение должно быть таким же, как в SNMP.
- **Event Last Time**
  Функция: Отображает значение sysUpTime, когда событие использовалось в последний раз. 6.

Просмотрите статус группы событий, как показано на рис. 107.


RMON Event Overview

Start from Control Index 0 and Sample Index 0 with 20 entries per page.

Event Index	LogIndex	LogTime	LogDescription
1	1	71179	Rising:iso.3.6.1.2.1.2.2.1.11.1000006=172 >= 50 :1, 1
1	2	71339	Rising:iso.3.6.1.2.1.2.2.1.11.1000006=186 >= 50 :1, 1
2	1	71159	Falling:iso.3.6.1.2.1.2.2.1.11.1000006=0 <= 20 :1, 2
2	2	71319	Falling:iso.3.6.1.2.1.2.2.1.11.1000006=0 <= 20 :1, 2
2	3	71419	Falling:iso.3.6.1.2.1.2.2.1.11.1000006=0 <= 20 :1, 2

Рисунок 107 Обзор статуса группы событий

Настройте таблицу аварийных сигналов, как показано на рисунке 108.

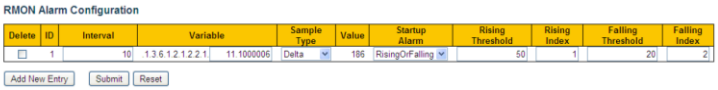
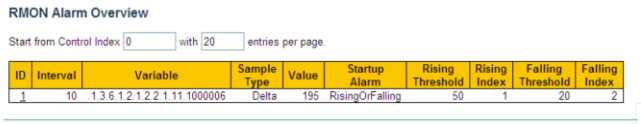


Рисунок 107 Настройка таблицы сигналов тревоги

- **ID**
  Диапазон: 1~65535
  Функция: Настройка номера записи тревоги. Группа тревог поддерживает до 256 записей.
- **Interval**
  Диапазон: 1~2147483647 с
  По умолчанию: 30 с
  Функция: Настройка периода выборки.
- **Variable**
  Формат: A.100000portid
  Диапазон: A： 10~21
  Функция: Выберите информацию MIB порта для мониторинга.
  InOctets: A=10, количество байтов, полученных портом.
  InUcastPkts: A=11, количество одноадресных пакетов, полученных портом.
  InNUcastPkts: A=12, количество широковещательных и многоадресных пакетов, полученных портом.
  InDiscards: A=13, количество пакетов, отброшенных портом.
  InErrors: A=14, количество пакетов с ошибками, полученных портом.
  InUnknownProtos: A=15, количество неизвестных пакетов, полученных портом.
  OutOctets: A=16, количество байтов, отправленных портом.
  OutUcastPkts: A=17, количество одноадресных пакетов, отправленных портом.
  OutNUcastPkts: A=18, количество широковещательных и многоадресных пакетов, отправленных портом. OutDiscards: A=19, количество отброшенных пакетов, отправленных портом.
  OutErrors: A=20, количество пакетов ошибок, отправленных портом.
  OutQLen: A=21, длина пакетов в очереди выхода порта.
- **Sample Type**
  Опции: Абсолют/Дельта
  По умолчанию: Дельта
  Функция: выберите метод сравнения значения выборки и порога.
  Описание: Абсолют: прямое сравнение каждого значения выборки с порогом; Дельта: значение выборки минус предыдущее значение выборки, затем используйте разницу для сравнения с порогом.
- **Startup Alarm**
  Варианты: Rising/Falling/RisingOrFalling
  По умолчанию: RisingOrFalling
  Функция: выберите тип аварийного сигнала.
- **Rising Threshold**
  Диапазон: 1~2147483647
  Функция: установить порог повышения. Когда значение выборки превышает нарастающий порог и типом тревоги является RisingAlarm или RisOrFallAlarm, срабатывает тревога и активируется индекс нарастающих событий.

- **Rising Index**
  Диапазон: 1~65535
  Функция: Установите индекс нарастающего события. Это способ подачи сигнала тревоги.
- **Falling Threshold**
  Диапазон: 1~2147483647
  Функция: установить порог падения. Когда значение выборки ниже порога падения и тип тревоги FallingAlarm или RisOrFallAlarm, срабатывает тревога и активируется индекс событий падения.
- **Falling Index**
  Диапазон: 1~65535
  Функция: Установить индекс падающего события. Это метод обработки падающего сигнала тревоги.

Просмотрите статус группы сигналов тревоги, как показано на рисунке 108.


RMON Alarm Overview

Start from Control Index 0 with 20 entries per page.

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
1	10	.1.3.6.1.2.1.2.2.1.11.1000006	Delta	195	RisingOrFalling	50	1	20	2

Рисунок 108 Настройка таблицы сигналов тревоги

9.9. Конфигурирование TACACS+

Система управления доступом к контроллеру доступа к терминалу (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. На рисунке 109 показана структура.

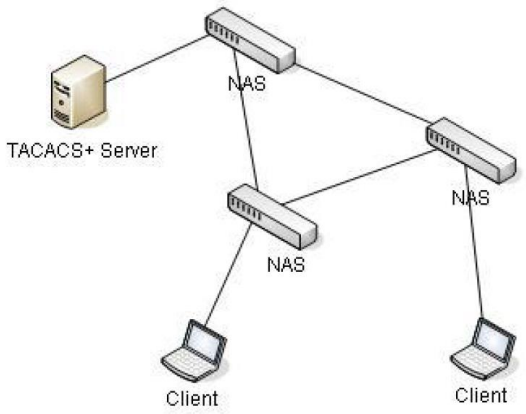


Рисунок 109 Структура TACACS+

Протокол аутентифицирует, авторизует и взимает плату с 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.

9.9.1. Веб конфигурирование

Настройте глобальные параметры TACACS+, как показано на рисунке 110.

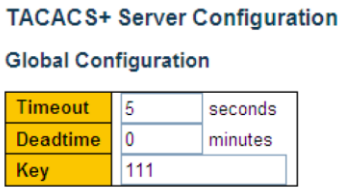


Рисунок 110 Конфигурирование глобальных параметров TACACS+

- **Timeout**
  Диапазон: 1~1000 с
  По умолчанию: 5 с
  Функция: Установите дополнительное время для ответа от сервера TACACS+. Если после отправки пакета запроса TACACS+ устройство по-прежнему не получает ответа от сервера TACACS+ по истечении указанного времени, аутентификация завершается неудачно, и устройство считает сервер TACACS+ недействительным.
- **Deadtime**
  Диапазон: 0~1440мин
  По умолчанию: 0 мин.
  Функция: Настраивает период, когда сервер недействителен. В течение этого периода устройство не отправляет сообщения запроса TACACS+ на сервер. Значение 0 означает отключение функции. Вы можете включить эту функцию, только если настроено более одного сервера TACACS+.
- **Key**
  Диапазон: 0~63 символа
  Функция: 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+.

Настройте сервер TACACS+, как показано на рисунке 111.

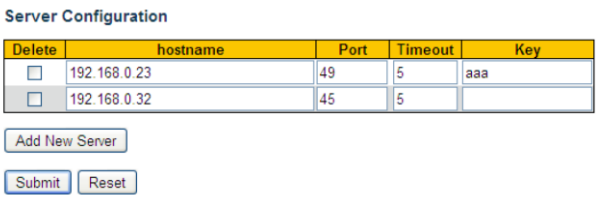


Рисунок 111 Конфигурирование сервеа TACACS+

- **Hostname**
  Функция: Настройка IP-адреса или имени хоста сервера TACACS+. Можно настроить максимум 5 серверов TACACS+.
- **Port**
  Диапазон: 0~65535
  По умолчанию: 49
  Функция: Установите TCP-порт сервера TACACS+ для аутентификации.
- **Timeout**
  Диапазон: 1~1000 с
  Функция: Установите дополнительное время для ответа от сервера TACACS+. Если после отправки пакета запроса TACACS+ устройство по-прежнему не получает ответа от сервера TACACS+ по истечении указанного времени, аутентификация завершается неудачно, и устройство считает сервер TACACS+ недействительным.
- **Key**
  Диапазон: 0~63 символа
  Функция: 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+.

9.10. Конфигурирование RADIUS

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 112 показывает структуру.

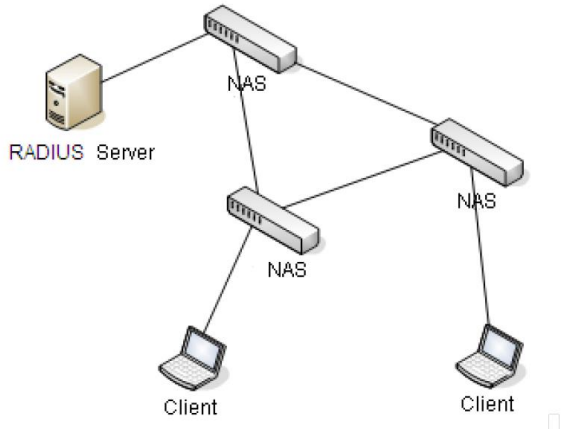


Рисунок 112 Radius структура

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 проверки подлинности.

9.10.1. Веб конфигурирование

Настройте глобальные параметры RADIUS, как показано на рисунке 113.

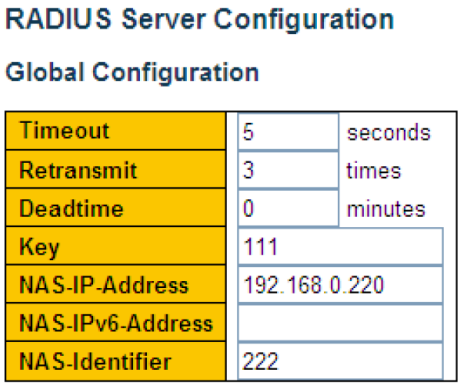


Рисунок 113 Конфигурирование глобальных параметров RADIUS

- **Timeout**
  Диапазон: 1~1000 с
  По умолчанию: 5 с
  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.
- **Retransmit**
  Диапазон: 1~1000
  По умолчанию: 3
  Функция: Установите максимальное количество попыток повторной передачи для пакетов запроса RADIUS. Если устройство по-прежнему не получает ответные пакеты от сервера RADIUS после максимальных попыток повторной передачи, аутентификация завершается ошибкой, и устройство считает, что сервер RADIUS недействителен.
- **Deadtime**
  Диапазон: 0~1440мин
  По умолчанию: 0 мин.
  Функция: Настраивает период, когда сервер недействителен. В течение этого периода устройство не отправляет сообщения запроса RADIUS на сервер. Значение 0 означает отключение функции. Вы можете включить эту функцию, только если настроено более одного сервера RADIUS.
- **Key**
  Диапазон: 0~63 символа
  Функция: установите ключ для повышения безопасности связи между клиентом и сервером RADIUS. Две стороны совместно используют ключ для проверки легитимности пакетов. Обе стороны могут получать пакеты друг от друга только

тогда, когда ключи совпадают. Поэтому убедитесь, что настроенный ключ совпадает с ключом на сервере RADIUS.

- **NAS-IP-Address**
  Функция: Конфигурирует исходный адрес, используемый для отправки сообщений запроса RADIUS оборудованием. Если адрес источника не указан, то в качестве адреса источника будет рассматриваться адрес интерфейса для отправки сообщений.
- **NAS-Identifier**
  Диапазон: 0~253 символа
  Функция: настраивает идентификатор, используемый для отправки оборудованием запросов RADIUS.

Настройте сервер RADIUS, как показано на рисунке 114.

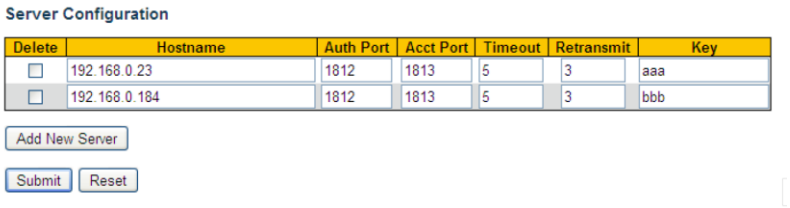
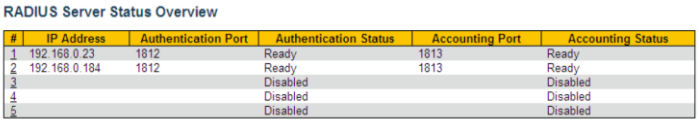


Рисунок 114 Конфигурирование RADIUS сервера

- **Hostname**
  Функция: Настройка IP-адреса или имени хоста сервера RADIUS. Можно настроить не более 5 серверов RADIUS.
- **Auth Port**
  Диапазон: 0~65535
  По умолчанию: 1812
  Функция: Установить UDP-порт сервера RADIUS для аутентификации.
- **Acct Port**
  Диапазон: 0~65535
  По умолчанию: 1813
  Функция: Установить UDP-порт RADIUS-сервера для учета. Поскольку RADIUS использует разные порты UDP для получения и отправки сообщений проверки подлинности и учета, необходимо настроить разные номера портов для проверки подлинности и учета.
- **Timeout**
  Диапазон: 1~1000 с
  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.
- **Retransmit**
  Диапазон: 1~1000
  Функция: Установите максимальное количество попыток повторной передачи для пакетов запроса RADIUS. Если устройство по-прежнему не получает ответные пакеты от сервера RADIUS после максимальных попыток повторной передачи, аутентификация завершается ошибкой, и устройство считает, что сервер RADIUS недействителен.

- **Key**
  Диапазон: 0~63 символа
  Функция: установите ключ для повышения безопасности связи между клиентом и сервером RADIUS. Две стороны совместно используют ключ для проверки легитимности пакетов. Обе стороны могут получать пакеты друг от друга только тогда, когда ключи совпадают. Поэтому убедитесь, что настроенный ключ совпадает с ключом на сервере RADIUS.

Просмотрите состояние сервера RADIUS, как показано на рисунке 115.

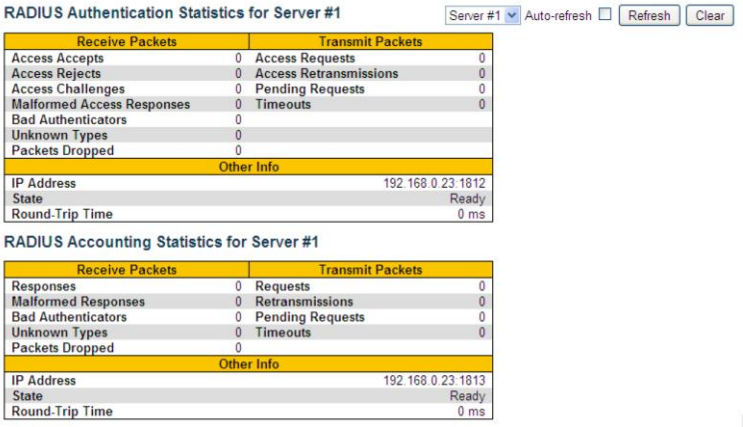

RADIUS Server Status Overview

#	IP Address	Authentication Port	Authentication Status	Accounting Port	Accounting Status
1	192.168.0.23	1812	Ready	1813	Ready
2	192.168.0.184	1812	Ready	1813	Ready
3			Disabled		Disabled
4			Disabled		Disabled
5			Disabled		Disabled

Рисунок 115 Просмотр состояния RADIUS сервера

Щелкните на запись, чтобы перейти на страницу «подробной статистики сервера RADIUS».

Просмотрите подробную статистику сервера RADIUS, как показано на рисунке 116.


RADIUS Authentication Statistics for Server #1

Server #1 Auto-refresh Refresh Clear

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
IP Address		192.168.0.23:1812	
State		Ready	
Round-Trip Time		0 ms	

RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address		192.168.0.23:1813	
State		Ready	
Round-Trip Time		0 ms	

Рисунок 116 Просмотр детальной статистики RADIUS сервера

Выберите сервер и просмотрите подробную статистику назначенного сервера.

10. Сеть

10.1. Port Security

Безопасность портов ограничивает максимальное количество пользователей на порт, которые однозначно идентифицируются по MAC-адресам и идентификатору vlan. Если ограничение MAC-адресов для порта включено, максимальное количество пользователей на порту равно MAC-адресу. Если количество MAC-адресов на порту превышает максимальный предел, запускается соответствующее действие.

10.1.1. Веб конфигурация

Настройте параметры ограничения безопасности портов mac, как показано на рисунке 116.

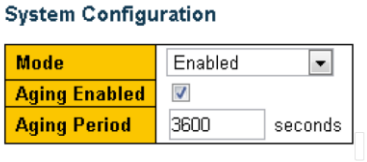


Рисунок 116 Конфигурация системы

- **Mode:**
  Опции: включить/отключить
  По умолчанию: Отключить
  Функция: включение/выключение функции глобального ограничения Mac.
- **Aging Enable:**
  Опции: включить/отключить
  По умолчанию: Отключить
  Функция: включить/отключить глобальную функцию старения Mac.
- **Aging Period:**
  Диапазон： 10~10000000c
  По умолчанию: 3600 c
  Функция: mac-адрес может устареть к этому периоду

Конфигурация ограничения портов Mac, как показано на рисунке 117.

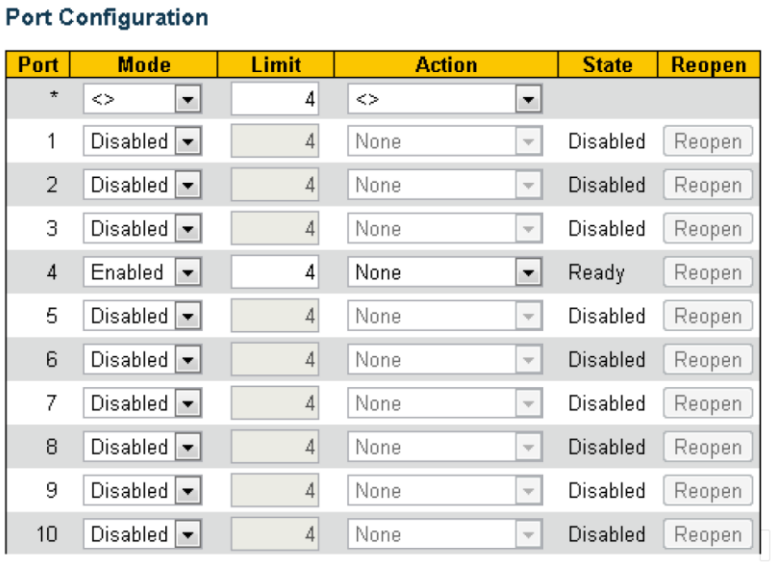


Рисунок 117 Конфигурация ограничения портов Mac

- **Mode:**
  Опции: включить/отключить
  По умолчанию: Отключить
  Функция: включить/отключить функцию ограничения портов Mac.
- **Limit:**

Диапазон: 1~1024
По умолчанию: 4
Функция: настроить максимальное количество Mac.

- **Action:**
  Вариант: нет/ловушка/отключение/ловушка и отключение
  По умолчанию: нет
  Функция:
  Если предел достигнут, коммутатор может выполнить одно из следующих действий:
  None: Не разрешайте больше, чем Limit MAC-адресов на порту, но не предпринимайте никаких дальнейших действий. Ловушка: если на порту видно MAC-адреса Limit + 1, отправьте ловушку SNMP. Если старение отключено, будет отправлена только одна ловушка SNMP, но если старение включено, новые ловушки SNMP будут отправляться каждый раз, когда будет превышено ограничение.
  Завершение работы: если на порту видны MAC-адреса Limit + 1, выключите порт. Это означает, что все защищенные MAC-адреса будут удалены из порта, и новый адрес не будет получен. Даже если соединение будет физически отключено и снова подключено к порту (путем отсоединения кабеля), порт останется отключенным. Есть три способа повторно открыть порт:
  1) Загрузите стек или выберите новый главный коммутатор,
  2) Отключите и снова включите Limit Control на порту или стековом коммутаторе,
  3) Нажмите кнопку «Повторно открыть».
  Trap & Shutdown: если на порту обнаружены MAC-адреса Limit + 1, будут предприняты действия «Trap» и «Shutdown», описанные выше.
- **State:**
  Опция: Отключено/Готово/Достигнут предел/Выключение
- **Reopen:**
  Если порт отключен этим модулем, вы можете снова открыть его, нажав эту кнопку.

Состояние Port Security Switch можно посомтреть, как показано на рисунке 118.

Port Security Switch Status

User Module Legend

User Module Name	Abbr
Limit Control	L
802.1X	8
Voice VLAN	V

Port Status

Port	Users	State	MAC Count	
			Current	Limit
1	---	Disabled	-	-
2	---	Disabled	-	-
3	---	Disabled	-	-
4	L--	Ready	0	4
5	---	Disabled	-	-
6	---	Disabled	-	-
7	---	Disabled	-	-
8	---	Disabled	-	-
9	---	Disabled	-	-
10	---	Disabled	-	-

Рисунок 118 Состояние Port Security Switch

Состояние порта безопасности порта показано на рисунке 119.

Port Security Status Port 5

MAC Address	VLAN ID	State	Time of Addition	Ageing Time(s)
54-e6-fc-6a-fe-a0	1	Forwarding	1970-01-01T07:19:41+00:00	3597

Рисунок 119 Состояние порта

10.2. Конфигурация IEEE802.1X

Для обеспечения безопасности WLAN комитет IEEE802 LAN/WAN предложил протокол 802.1X. Как общий механизм управления доступом для портов 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 контроля портов Устройства 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, как показано на рисунке 120. Аутентификация пользователя и авторизация управления доступом на основе порта требуют следующих элементов:

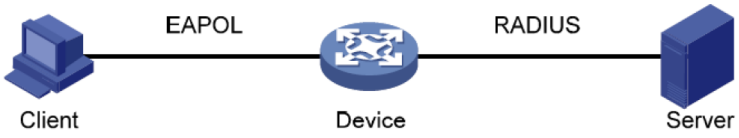


Рисунок 120 структура IEEE802.1X

Клиент: обычно указывает пользовательский терминал. Когда пользователь хочет выйти в Интернет, он запускает клиентскую программу и вводит необходимое имя пользователя и пароль. Клиентская программа отправит запрос на соединение. Клиент должен поддерживать EAPOL (Extensible Authentication Protocol). по локальной сети).

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.

10.2.1. Веб конфигурация

Настройте глобальные параметры IEEE802.1X, как показано на рисунке 121.

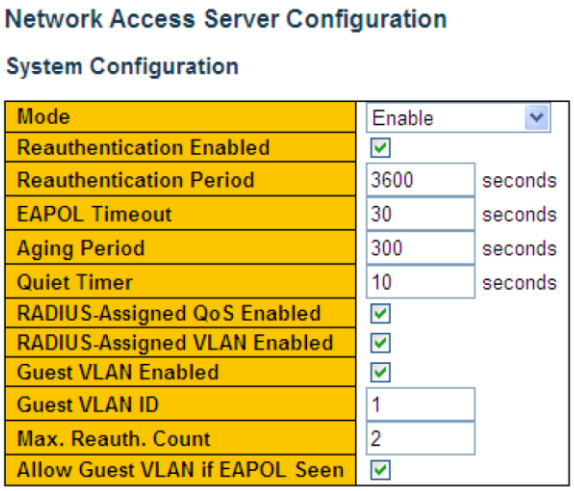


Рисунок 121 глобальня конфигурация параметров IEEE802.1X

- **Mode**
  Опции: включить/отключить
  По умолчанию: Отключить
  Функция: включение/отключение глобальной функции безопасности IEEE802.1x.
- **Reauthentication Enabled**
  Опции: включить/отключить
  По умолчанию: Отключить
  Функция: Настройка необходимости регулярной повторной аутентификации при успешном выполнении аутентификации.
- **Reauthentication Period**
  Диапазон: 1~3600 с
  По умолчанию: 3600 с
  Функция: при успешной аутентификации установите временной интервал для повторной аутентификации. «Период повторной аутентификации» можно настроить только при включении «Повторная аутентификация включена».

- **EAPOL Timeout**
  Диапазон: 1~65535 с
  По умолчанию: 30 с
  Функция: Установите сверхурочное время для ответа от клиента. После отправки пакета запроса Identity EAPOL устройство повторно отправит пакет запроса Identity EAPOL, если оно по-прежнему не получит ответа от клиента по истечении указанного времени.
- **Aging Period**
  Диапазон: 10~1000000 с
  По умолчанию: 300 с
  Функция: Настройка периода старения. Когда «Повторная аутентификация включена» отключена, временной интервал для повторной аутентификации равен 2*период устаревания.
- **Quiet Timer**
  Диапазон: 10~1000000 с
  По умолчанию: 10 с
  Функция: если аутентификация не удалась, устройство переходит в режим ожидания. В период молчания устройство не отвечает на запросы аутентификации от клиента.
- **RADIUS-Assigned QoS Enabled**
  Опции: включить/отключить
  По умолчанию: Отключить
  Функция: если эта функция включена, после прохождения клиентом аутентификации сервер передает на устройство информацию об авторизации. Если на сервере установлен флажок **RADIUS-Assigned QoS Enabled**, информация авторизации включает информацию CoS, назначенную для авторизации. Оборудование изменит значение CoS порта аутентификации клиента на основе присвоенного значения.
- **RADIUS-Assigned VLAN Enabled**
  Опции: включить/отключить
  По умолчанию: Отключить
  Функция: если эта функция включена, после прохождения клиентом аутентификации сервер передает на устройство информацию об авторизации. Если на сервере установлен флажок **RADIUS-Assigned VLAN Enabled**, информация авторизации включает информацию VLAN, назначенную для авторизации. Оборудование добавит порт аутентификации клиента в назначенную VLAN.
- **Guest VLAN Enabled**
  Опции: включить/отключить
  По умолчанию: Отключить
  Функция: если этот параметр включен, если пользователь не аутентифицирован или не может быть аутентифицирован, устройство добавляет порт аутентификации клиента в гостевую VLAN. Все пользователи, имеющие доступ к этому порту, имеют право доступа к ресурсам в гостевой VLAN.
- **Guest VLAN ID**
  Диапазон: 1~4095
  По умолчанию: 1
  Функция: настройка идентификатора гостевой VLAN。
- **Max. Reauth. Count**
  Диапазон: 1~255

По умолчанию: 2

Функция: Установить максимальное количество попыток повторной передачи для пакетов запроса Identity EAPOL. Если устройство по-прежнему не получает ответных пакетов от клиента после максимальных попыток повторной передачи, устройство будет считать аутентификацию неудачной.

- **Allow Guest VLAN if EAPOL Seen**

  Опции: включить/отключить

  По умолчанию: Отключить

  Функция: если этот параметр включен, если пользователь не аутентифицирован или не может быть аутентифицирован, устройство добавляет порт аутентификации клиента в гостевую VLAN. Если этот параметр отключен, устройство добавляет порт в гостевую VLAN только в том случае, если этот порт не имеет записи кадра EAPOL.

Настройте порт IEEE802.1X, как показано на рисунке 122.

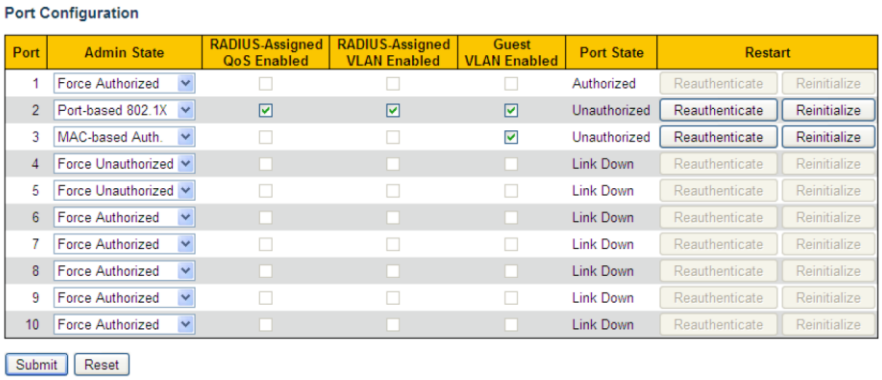


Рисунок 122 конфигурирование IEEE802.1X порта

- **Port**

  Опции: все порты коммутатора.

- **Admin State**

  Опции: Force Authorized/Force Unauthorized/Port-based 802.1X/MAC-based Auth.

  По умолчанию: Force Authorized

  Функция: выберите режим аутентификации порта.

  Описание: **Force Authorized** означает, что порт всегда находится в авторизованном состоянии и позволяет пользователям получать доступ к сетевым ресурсам без аутентификации.

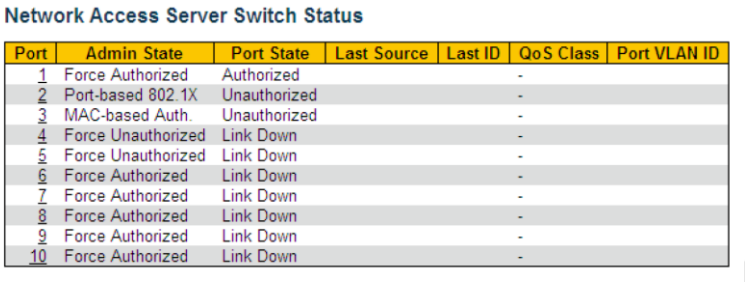
  Force Unauthorized означает, что порт всегда находится в неавторизованном состоянии и не позволяет пользователям проводить аутентификацию, а коммутатор не предоставляет услуги аутентификации клиентам, которые получают доступ к коммутатору с этого порта. **MAC-based Auth** указывает, что пользователи, использующие порт, должны пройти аутентификацию соответственно. Когда пользователь находится в автономном режиме, только пользователь не может использовать сеть. **Port-based 802.1X** 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.

- **RADIUS-Assigned QoS Enabled**

Опции: Включить/Выключить
По умолчанию: Отключить
Функция: включение или отключение RADIUS-Assigned QoS на порту.

- **RADIUS-Assigned VLAN Enabled**
  Опции: Включить/Выключить
  По умолчанию: Отключить
  Функция: Включить или отключить RADIUS-Assigned VLAN на порту.
- **Guest VLAN Enabled**
  Опции: Включить/Выключить
  По умолчанию: Отключить
  Функция: включить или отключить гостевую VLAN на порту.
- **Port State**
  Варианты: Globally Disabled, Authorized, Unauthorized, Link Down, x Auth/y Unauth
  Функция: отображение состояния аутентификации порта. **Globally Disabled** указывает, что IEEE802.1X отключен глобально; **Authorized** указывает, что пользователь, подключенный к порту, проходит аутентификацию; **Unauthorized** указывает, что пользователь, подключенный к порту, не может пройти аутентификацию; **Link Down** указывает, что порт не работает; x Auth/y Unauth указывает, что x пользователей авторизованы, а y пользователей не авторизованы, когда режим аутентификации порта — аутентификация на основе MAC.
  Если режим аутентификации порта — аутентификация на основе MAC-адреса или 802.1X на основе порта, вы можете нажать кнопку <Reauthenticate>/<Reinitialize> для повторной аутентификации. Во время повторной аутентификации состояние порта изменяется на **Unauthorized**.

Просмотрите конфигурацию IEEE802.1X, как показано на рисунке 123.



Network Access Server Switch Status

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Authorized			-	
2	Port-based 802.1X	Unauthorized			-	
3	MAC-based Auth.	Unauthorized			-	
4	Force Unauthorized	Link Down			-	
5	Force Unauthorized	Link Down			-	
6	Force Authorized	Link Down			-	
7	Force Authorized	Link Down			-	
8	Force Authorized	Link Down			-	
9	Force Authorized	Link Down			-	
10	Force Authorized	Link Down			-	

Рисунок 123 просмотр конфигурации IEEE802.1X

Нажмите <порт>, чтобы открыть страницу «Статистика IEEE802.1X».

Просмотрите статистику IEEE802.1X, как показано на рисунке 124.

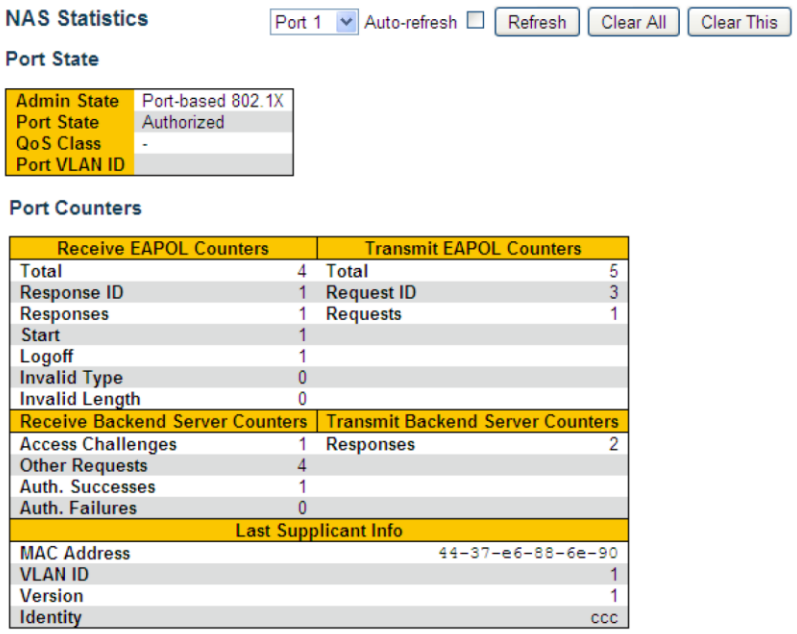


Рисунок 124 Просмотр статистики IEEE802.1X

10.3. ACL

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

Коммутаторы серии фильтруют пакеты в соответствии с согласованным ACL. Каждая запись состоит из нескольких условий в логической связи. Записи ACL не зависят друг от друга.

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

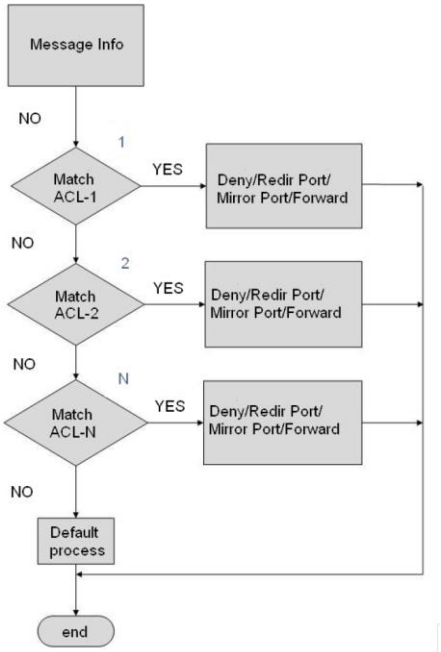


Рисунок 125 Блок-схема обработки ACL

10.3.1. Веб конфигурация

Настройте порты ACL, как показано на рисунке 126.

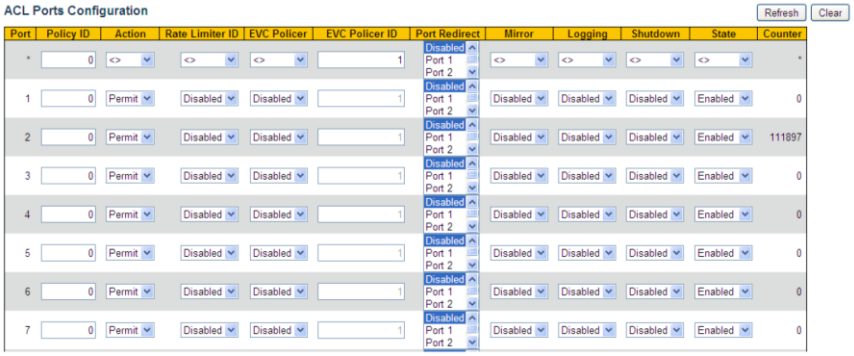


Рисунок 126 Конфигурирование ACL на портах

- **Policy ID**
  Диапазон: 0~255
  По умолчанию: 0
  Функция: Настройка идентификатора политики порта.
- **Action**
  Варианты: Запретить/Разрешить
  По умолчанию: Разрешить
  Функция: Настройте действие по отношению к пакету, который не соответствует какой-либо записи ACL. Запретить: пакеты, не соответствующие какой-либо записи, будут отклонены. Разрешить: пакеты, не соответствующие какой-либо записи, будут пересылаться.
- **Rate Limiter ID**

Диапазон: Отключено/1~16
По умолчанию: отключено
Функция: включить ли функцию ограничения скорости порта и выбрать ID ограничителя скорости.

- **EVC Policer**
  Параметры: Включено/Выключено
  По умолчанию: отключено
  Функция: включение/отключение ограничителя портов EVC.
- **EVC Policer ID**
  Диапазон: 1~256
  По умолчанию: 1
- **Port Redirect**
  Опции: Отключено/любой порт
  По умолчанию: отключено
  Функция: включить/отключить функцию перенаправления портов. После включения функции перенаправления портов пакеты, не соответствующие какой-либо записи ACL, будут перенаправлены на указанный порт.
- **Mirror**
  Параметры: Включено/Выключено
  По умолчанию: отключено
  Функция: включить/отключить функцию зеркалирования портов. После включения функции зеркалирования портов пакеты, не соответствующие какой-либо записи ACL, будут пересылаться как на порт назначения, так и на порт назначения зеркала.
- **Logging**
  Параметры: Включено/Выключено
  По умолчанию: отключено
  Функция: включение/отключение функции ведения журнала портов. Включено: если порт получает пакет, который не соответствует ни одной записи ACL, пакет записывается в системный журнал. Отключено: если порт получает пакет, не соответствующий записи ACL, пакет не записывается в системный журнал.
- **Shutdown**
  Параметры: Включено/Выключено
  По умолчанию: отключено
  Функция: отключать порт или нет. Включено: если порт получает пакет, который не соответствует ни одной записи ACL, порт отключается. Отключено: если порт получает пакет, не соответствующий записи ACL, порт не отключается.
- **Counter**
  Функция: отображение количества пакетов, не соответствующих какой-либо записи ACL, полученных каждым портом.

Настройте ограничитель скорости ACL, как показано на рисуноке 127.

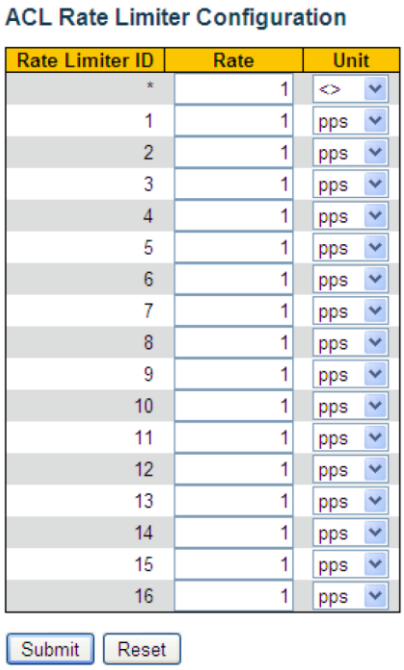


Рисунок 127 Конфигурирование ограничителя скорости ACL

- **Rate Unit**
  Диапазон: 0~3276700 pps/ 0~1000000 кбит/с (шаг 100)
  По умолчанию: 1 pps
  Функция: Установите ограниченную скорость идентификатора ограничителя скорости.

  Настройте запись ACL, как показано на рисунке 128.

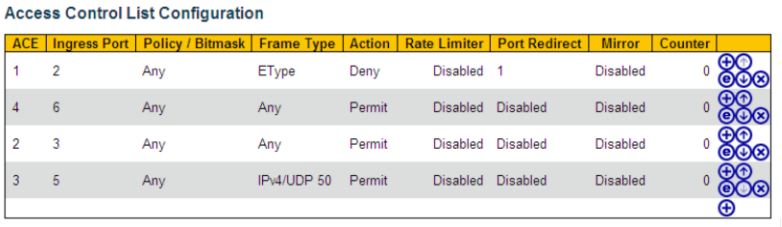


Рисунок 128 Конфигурирование записей ACL

При наличии нескольких записей ACL устройство сравнивает пакет с записями ACL одну за другой (сверху вниз). Как только совпадение найдено, действие предпринимается, и дальше ничего не происходит проводится сравнение.
Нажмите <+>, чтобы добавить новую запись ACL; нажмите <e> чтобы изменить запись ACL; нажмите <x>, чтобы удалить запись ACL, нажмите <↑>, чтобы переместить текущую запись вверх; нажмите <↓>, чтобы переместиться вниз по текущему вход.
ACE — это идентификатор записи ACL, который нумеруется на основе временной последовательности создания записи. 4.

Настройте параметры записи ACL
Настройте параметры записи ACL, как показано на рисунке 129.

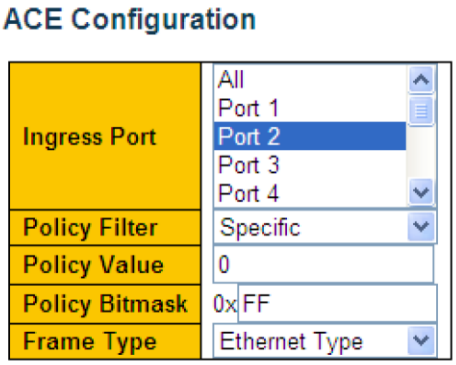


Рисунок 129 Конфигурирование записей парметров ACL

- **Ingress Port**
  Опция: Все/любой порт
  По умолчанию: Все
  Функция: выберите порт, на котором действует запись управления доступом (ACE).
- **Policy Filter**
  Опиции: любые/конкретные
  По умолчанию: любой
  Функция: Установить условие ACE — идентификатор политики. Если для него установлено значение «Специфический», необходимо установить значение политики и битовую маску политики. Когда значение политики пакета, полученного входным портом, соответствует настройкам этого параметра, условие успешно соблюдено.
- **Policy Value**
  Диапазон: 0~255
  Функция: Настройка значения политики.
- **Policy Bitmask**
  Диапазон: 0x0~0xFF
  Функция: Установите битовую маску политики. Значение политики и битовая маска политики используются для сопоставления при фильтрации политики. Битовая маска политики преобразуется в двоичные числа, а затем выравнивается по правому краю со значением политики (в двоичном режиме). Значение 1 указывает на то же самое, а значение 0 указывает на то, что разрешено любое значение.
- **Frame Type**
  Варианты: Любой/Тип Ethernet/IPv4
  По умолчанию: любой
  Функция: Установить условие - тип пакета. Когда тип пакета, полученного входным портом, соответствует настройкам этого параметра, условие выполняется успешно.

Настройте параметры VLAN, как показано на рисунке 130.

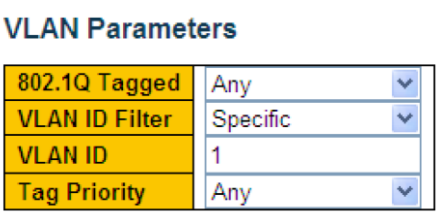


Рисунок 130 Конфигурирование параметров VLAN

- **802.1Q Tagged**
  Варианты: Любой/ Отключено/ Включено
  По умолчанию: любой
  Функция: Установите условие — тег 802.1Q. Значение Disabled указывает на немаркированные пакеты, а значение Enabled указывает на тегированные пакеты. Когда пакет, полученный входным портом, соответствует настройкам этого параметра, условие выполняется успешно.
- **VLAN ID Filter**
  Варианты: любой/конкретный (1~4095)
  По умолчанию: любой
  Функция: Установить условие--VID. Если установлено значение «Специфический», необходимо ввести значение VID. Когда VID в пакете, полученном входным портом, соответствует настройкам этого параметра, условие успешно соблюдено. Когда для 802.1Q Tagged установлено значение Disabled, для этого параметра необходимо установить значение Any.
- **Tag Priority**
  Вариант: Любой/0/1/2/3/4/5/6/7/0-1/2-3/4-5/6-7/0-3/4-7
  По умолчанию: любой
  Функция: Установить условие-приоритет тега. Когда приоритет в пакете, полученном входным портом, соответствует настройкам этого параметра, условие выполняется успешно. Когда для 802.1Q Tagged установлено значение Disabled, для этого параметра необходимо установить значение Any.

Настройте параметры фрейма EtherType, как показано на рисунке 131.

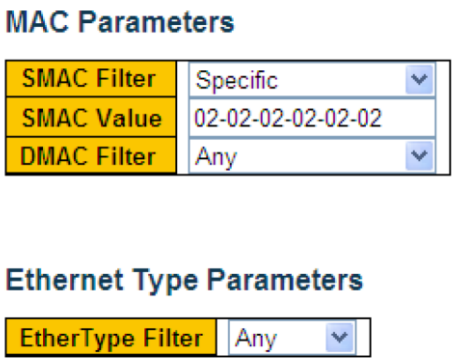


Рисунок 131 Конфигурирование параметров EtherType

- **SMAC Filter**
  Варианты: любой/конкретный
  По умолчанию: любой
  Функция: Установите условие — MAC-адрес источника. Если для него установлено значение «Специфический», необходимо установить исходный MAC-адрес. Когда исходный MAC-адрес в пакете, полученном входным портом, соответствует настройкам этого параметра, условие выполняется успешно.
- **DMAC Filter**
  Варианты: Любой/ UC/ MC/ BC/ Особый
  По умолчанию: любой

Функция: Установите условие — MAC-адрес назначения. Если для него установлено значение «Специфический», необходимо установить MAC-адрес назначения. Когда MAC-адрес получателя в пакете, полученном входным портом, соответствует настройкам этого параметра, условие выполняется успешно.

- **EtherType Filter**
  Параметры: любой/конкретный (0x600~0xFFFF, исключая 0x800(IPv4), 0x806(ARP), 0x86DD(IPv6)) По умолчанию: любой
  Функция: Установите условие — тип Ethernet. Если для него установлено значение «Специфический», необходимо указать тип Ethernet.
  устанавливать. Когда пакет Ethernet, полученный входным портом, соответствует настройкам этого параметра, условие успешно выполнено.

Настройте параметры кадра IPv4, как показано на рисунке 132.

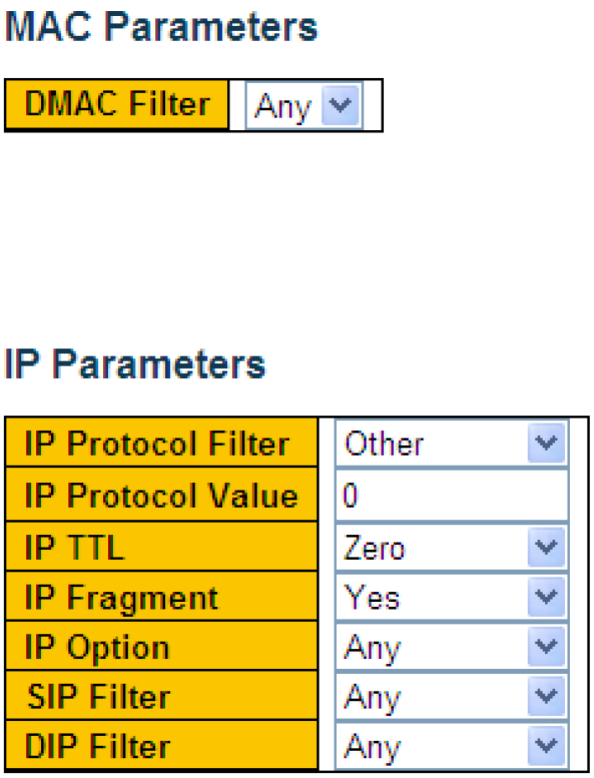


Рисунок 132 Конфигурирование параметров кадра IPv4

- **DMAC Filter**
  Варианты: Any/ UC/ MC / BC
  По умолчанию: ANY
  Функция: Установите условие — MAC-адрес назначения. Когда MAC-адрес получателя в пакете, полученном входным портом, соответствует настройкам этого параметра, условие выполняется успешно.
- **IP Protocol Filter**
  Варианты: любой/ICMP/UDP/TCP/другой (0~255)
  По умолчанию: любой
  Функция: Установите условие — тип протокола пакета IPv4. Если для него установлено значение ICMP, UDP или TCP, необходимо установить соответствующие параметры. Если для него установлено значение «Другой», необходимо установить идентификатор протокола. Когда тип протокола в пакете

IPv4, полученном входным портом, соответствует настройкам этого параметра, условие выполняется успешно.

- **IP TTL**
  Варианты: любой/ненулевой/нулевой
  По умолчанию: любой
  Функция: Установите условие — поле TTL в IP-пакетах. Ненулевое значение указывает, что условие выполняется, когда IP TTL в пакете IPv4 больше 0, а значение Zero указывает, что условие не выполняется, когда IP TTL в пакете IPv4 больше 0.
- **IP Fragment**
  Варианты: Любой/Да/Нет
  По умолчанию: любой
  Функция: Задать условие -- IP-фрагмент. Когда IP-фрагмент в пакете IPv4, полученном входным портом, соответствует настройкам этого параметра, условие выполняется успешно.
- **IP Option**
  Варианты: Любой/Да/Нет
  По умолчанию: любой
  Функция: Установите условие -- вариант IP. Когда параметр IP в пакете IPv4, полученном входным портом, соответствует настройкам этого параметра, условие выполняется успешно.
- **SIP Filter**
  Варианты: Любой/Хост/Сеть
  По умолчанию: любой
  Функция: Установите условие — исходный IP-адрес. Если установлено значение Host, необходимо задать IP-адрес. Если установлено значение Сеть, необходимо задать IP-адрес и маску подсети. Когда исходный IP-адрес в пакете IPv4, полученном входным портом, соответствует настройкам этого параметра, условие выполняется успешно.
- **DIP Filter**
  Варианты: Любой/Хост/Сеть
  По умолчанию: любой
  Функция: Установите условие — IP-адрес назначения. Если установлено значение Host, необходимо задать IP-адрес. Если установлено значение Сеть, необходимо задать IP-адрес и маску подсети. Когда IP-адрес назначения в пакете IPv4, полученном входным портом, соответствует настройкам этого параметра, условие успешно выполняется.

Настройте параметры ICMP, как показано на рисунке 133.

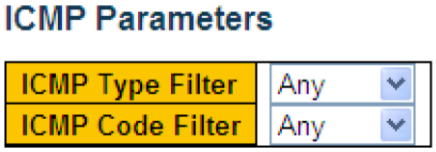


Рисунок 133 Конфигурирование параметров ICMP

- **ICMP Type FFFilter**
  Варианты: любой/конкретный（0~255）
  По умолчанию: любой

Функция: Установите условие — тип ICMP. Если установлено значение «Специфический», необходимо установить тип ICMP. Когда тип ICMP в пакете IPv4, полученном входным портом, соответствует настройкам этого параметра, условие выполняется успешно.

- **ICMP Code Filter**
  Варианты: любой/конкретный（0~255）
  По умолчанию: любой
  Функция: Установите условие — код ICMP. Если установлено значение «Специфический», необходимо установить код ICMP. Когда код ICMP в пакете IPv4, полученном входным портом, соответствует настройкам этого параметра, условие выполняется успешно.

Настройте параметры UDP, как показано на рисунке 134.

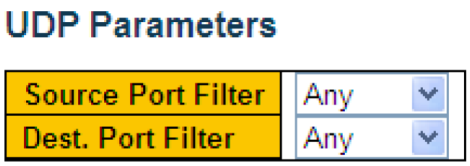


Рисунок 134 Конфигурирование параметров UDP

- **Source Port Filter/ Dest. Port Filter**
  Варианты: любой/конкретный (0~65535)/диапазон (0~65535)
  По умолчанию: любой
  Функция: Установите условие — идентификатор исходного порта UDP и идентификатор порта назначения. Если для них установлено значение «Специфический», необходимо установить идентификатор порта. Когда для них установлено значение Range, необходимо установить диапазон идентификаторов портов. Когда идентификаторы портов UDP в пакете IPv4, полученном входным портом, соответствуют настройкам параметров, условие успешно выполняется.

Настройте параметры TCP, как показано на рисунке 135.

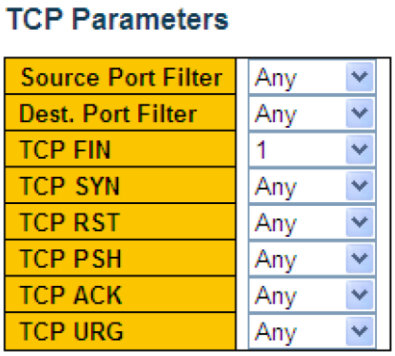


Рисунок 135 Конфигурирование параметров TCP

- **Source Port Filter/ Dest. Port Filter**
  Варианты: любой/конкретный (0~65535)/диапазон (0~65535)
  По умолчанию: любой

Функция: Установите условие — идентификатор исходного порта TCP и идентификатор порта назначения. Если для них установлено значение «Специфический», необходимо установить идентификатор порта. Когда для них установлено значение Range, необходимо установить диапазон идентификаторов портов. Когда идентификаторы портов TCP в пакете IPv4, полученном входным портом, соответствуют настройкам параметров, условие успешно выполняется.

- **TCP FIN/SYN/RST/PSH/ACK/URG**
  Варианты: Любой/1/0
  По умолчанию: любой
  Функция: Установите условие — поля управления TCP. Когда контрольные поля TCP в пакете IPv4, полученном входным портом, соответствуют настройкам параметров, условие успешно соблюдено.

Настройте действие записи ACL, как показано на рисунке 136.

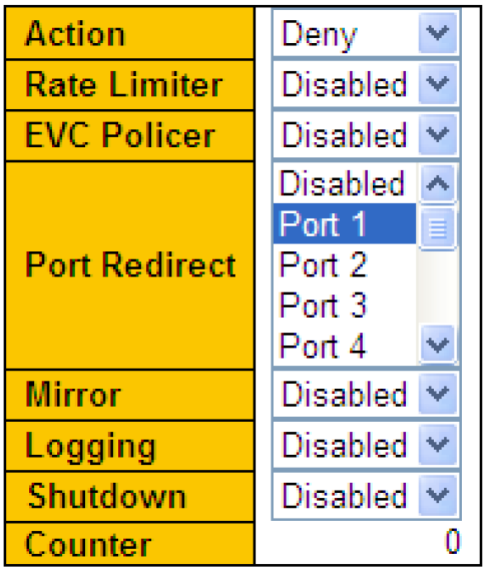


Рисунок 136 Конфигурирование действие записи ACL

- **Action**
  Опции: Запретить/Разрешить/Фильтровать
  По умолчанию: Разрешить
  Функция: укажите режим обработки входным портом пакета, соответствующего ACE. Значение Deny указывает на отбрасывание пакета, значение Permit указывает на пересылку пакета, а значение Filter указывает на фильтрацию пакета и необходимость выбора порта фильтрации.
- **Rate Limiter**
  Опции: Отключено/1~16
  По умолчанию: отключено
  Функция: включить ли функцию ограничения скорости порта и выбрать ID ограничителя скорости.
- **EVC Policer**
  Параметры: Включено/Выключено
  По умолчанию: отключено
  Функция: включение/отключение ограничителя портов EVC.
- **EVC Policer ID**

Диапазон: 1~256
По умолчанию: 1
Функция: после включения ограничителя EVC настройте идентификатор ограничителя EVC для порта.

- **Port Redirect**
  Опции: Отключено/любой порт
  По умолчанию: отключено
  Функция: включить/отключить функцию перенаправления портов. После включения функции перенаправления портов пакеты, соответствующие любой записи, будут пересылаться на указанный порт.
- **Mirror**
  Параметры: Включено/Выключено
  По умолчанию: отключено
  Функция: включить/отключить функцию зеркалирования портов. После включения функции зеркалирования портов пакеты, соответствующие любой записи, будут пересылаться как на порт назначения, так и на порт назначения зеркала.
- **Logging**
  Параметры: Включено/Выключено
  По умолчанию: отключено
  Функция: включение/отключение функции ведения журнала портов.
  Функция: включение/отключение функции ведения журнала портов. Включено: если порт получает пакет, соответствующий любой записи ACL, пакет записывается в системный журнал. Отключено: если порт получает пакет, соответствующий записи ACL, пакет не записывается в системный журнал.
- **Shutdown**
  Параметры: Включено/Выключено
  По умолчанию: отключено
  Функция: отключать порт или нет. Включено: если порт получает пакет, соответствующий любой записи ACL, порт отключается. Отключено: если порт получает пакет, соответствующий записи ACL, порт не отключается.
- **Counter**
  Функция: отображение количества пакетов, соответствующих ACE, которые получает каждый порт.

Просмотрите записи ACL, как показано на рисунке 137.

ACL Status

User	ACE	Frame Type	Action	Rate Limiter	Mirror	CPU	Counter	Conflict
rp_mirror_cpu	1	EType	Filter	Disabled	Enabled	Yes	0	No
devSmacDrop	1	EType	Deny	Disabled	Disabled	No	0	No
bootp	1	IPv4/UDP 67-68	Filter	Disabled	Enabled	Yes	298	No
arp	1	ARP	Filter	Disabled	Enabled	Yes	199870	No
static	1	EType	Deny	Disabled	Disabled	No	0	No
static	4	Any	Permit	Disabled	Disabled	No	0	No
static	2	Any	Permit	Disabled	Disabled	No	0	No
static	3	IPv4/UDP 50	Permit	Disabled	Disabled	No	0	No
static	5	EType	Permit	Disabled	Disabled	No	0	No
static	6	IPv4/Other 0	Permit	Disabled	Disabled	No	0	No

Рисунок 137 Посмотр записей ACL

- **Conflict**
  Варианты: Нет/Да
  Функция: Отображает состояние конфликта записи ACL. Если ресурсов для создания записи ACL недостаточно, для параметра Конфликт для этой записи

задано значение Да. В противном случае для параметра «Конфликт» для этой записи установлено значение «Нет».

11. Port Aggregation

11.1. Static Aggregation

Port channel 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, которые присоединиться к группе портов может участвовать в агрегации ссылок и стать членом канала порта. 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 138, три порта на коммутаторах A и B объединяются, образуя канал портов. Пропускная способность канала порта — это общая пропускная способность этих трех портов.

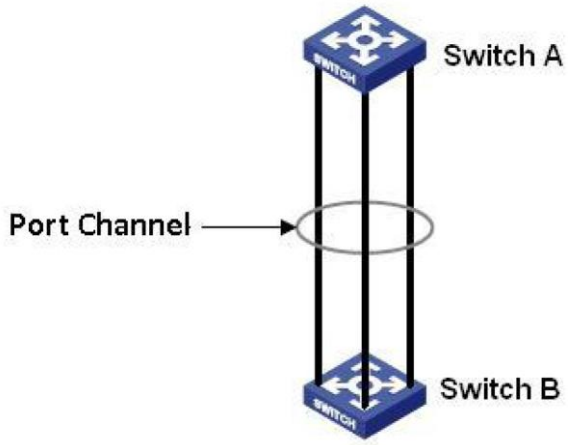


Рисунок 138 Посмотр записей ACL

Если коммутатор A отправляет пакеты на коммутатор B по каналу порта, коммутатор A определяет порт-участник для передачи трафика на основе результата 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.

11.1.1. Веб конфигурация

Настройте режим распределения нагрузки канала порта, как показано на рисунке 137.

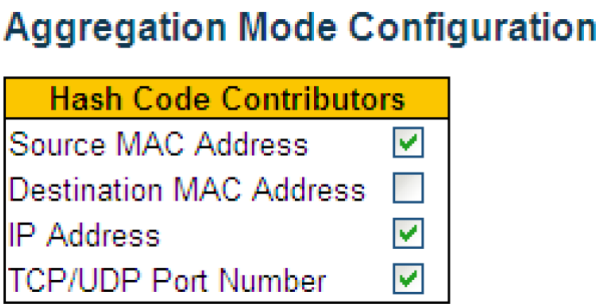


Рисунок 138 Настройка режим распределения нагрузки канала порта

- **Hash Code Contributors**
  Опции: MAC-адрес источника/MAC-адрес назначения/IP-адрес/Номер порта TCP/UDP
  По умолчанию: исходный MAC-адрес/IP-адрес/номер порта TCP/UDP
  Функция: Установите режим распределения нагрузки канала порта.
  Описание: MAC-адрес источника указывает на распределение нагрузки на основе MAC-адреса источника. MAC-адрес назначения указывает на распределение нагрузки на основе MAC-адреса назначения. IP-адрес указывает распределение нагрузки на основе IP-адреса. Номер порта TCP/UDP указывает на распределение нагрузки на основе номера порта TCP/UDP.

  Настройте участников порта группы агрегации, как показано на рис. 139.

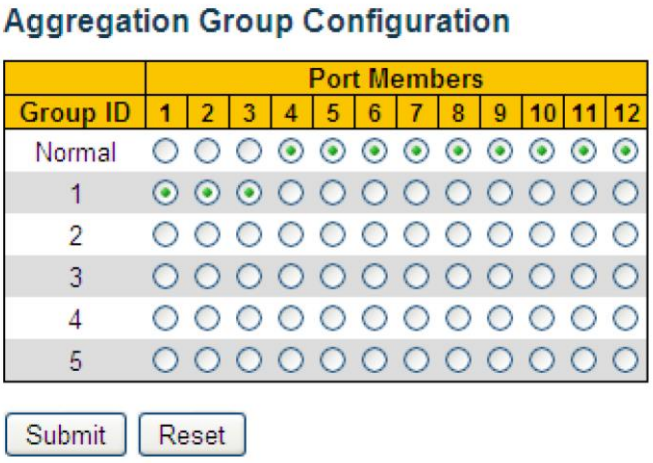


Рисунок 139 Настройка участников порта группы агрегации

- **Port Member**
  Функция: выбор членов порта группы агрегации.
  Описание: Все порты-члены в одной группе агрегации имеют одинаковую конфигурацию. Количество транковых групп зависит от количества портов коммутатора. Каждая группа может содержать максимум 8 портов.

11.2. LACP

Протокол управления агрегацией каналов (LACP) основан на стандарте IEEE802.3ad. Он используется для обмена информацией с одноранговым портом через блок данных протокола управления агрегацией каналов (LACPDU), чтобы выбрать порт-участник в группе динамического агрегирования.

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

1. Сравните идентификаторы оборудования на обоих концах (идентификатор оборудования = приоритет оборудования LACP + MAC-адрес оборудования). Сначала сравните приоритеты LACP. Если приоритеты LACP совпадают, сравните их MAC-адреса. Выберите оборудование с меньшим идентификатором в качестве основного оборудования.

2. Сравните идентификаторы портов ведущего оборудования (идентификатор порта = приоритет порта LACP + номер порта). Сначала сравните приоритеты LACP портов. Если приоритеты портов LACP совпадают, сравните номера портов. Выберите порт с меньшим идентификатором в качестве эталонного порта.

3. Если этот порт и эталонный порт имеют одинаковые значения ключей и одинаковые конфигурации атрибутов порта в состоянии Up, а одноранговые порты этого порта и эталонного порта имеют одинаковые значения ключей и конфигурации атрибутов порта, этот порт может стать порт участника динамической группы агрегации.

11.2.1. Веб конфигурация

Настройте порт LACP, как показано на рисунке 140.

LACP Port Configuration

Ports	LACP Enabled	Key		Role	Timeout	Prio
*	☑	<>		<>	<>	32768
1	☑	Auto		Active	Fast	32768
2	☑	Auto		Active	Fast	32768
3	☑	Auto		Active	Fast	32768
4	☑	Auto		Active	Fast	32768
5	☑	Auto		Active	Fast	32768
6	☑	Auto		Active	Fast	32768
7	☑	Auto		Active	Fast	32768
8	☑	Auto		Active	Fast	32768
9	☑	Auto		Active	Fast	32768
10	☑	Auto		Active	Fast	32768

Submit Reset

Рисунок 140 Настройка порта LACP

- **LACP Enabled**
  Опции: включить/отключить
  По умолчанию: Отключить
  Функция: включить или отключить LACP на порту.
- **Key**

Опции: Авто/Особый (1~65535)
По умолчанию: Авто
Функция: Настройка значения ключа порта. Авто означает, что значение ключа зависит от скорости порта, ключ=1 (10Мб), ключ=2 (100Мб), ключ=3 (1000Мб). Порты с разными значениями ключей не могут быть добавлены в группу агрегации.

- **Role**
  Варианты: активный/пассивный
  По умолчанию: Активно
  Функция: выбирает состояние роли LACP. Активный порт будет активно отправлять сообщения LACPDU на одноранговый порт. Пассивный порт будет отправлять сообщения LACPDU на одноранговый порт после получения сообщений LACPDU от одноранговой порта.
- **Timeout**
  Варианты: быстро/медленно
  По умолчанию: быстро
  Функция: Настраивает интервал для активного порта для отправки сообщений LACPDU. Fast указывает, что интервал равен 1 с. Slow означает, что интервал составляет 30 секунд.
- **Prio**
  По умолчанию: 1~65535
  По умолчанию: 32768
  Функция: Настраивает приоритет LACP порта, который используется для выбора эталонного порта. В качестве эталонного порта выбирается порт с более низким приоритетом в ведущем оборудовании.

Просмотрите состояние системы LACP, как показано на рис. 141.

LACP System Status

Aggr ID	Partner System ID	Partner Key	Partner Prio	Last Changed	Local Ports
LLAG1	00-01-c1-01-00-02	2	32768	0d 00:00:28	1,2

Рисунок 141 Просмотр сосояние LACP

Просмотрите состояние порта LACP, как показано на рис. 142.

LACP Status

Ports	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	Yes	2	LLAG1	00-01-c1-01-00-02	1	32768
2	Yes	2	LLAG1	00-01-c1-01-00-02	2	32768
3	Yes	2	-	-	-	-
4	Yes	2	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-
7	No	-	-	-	-	-
8	No	-	-	-	-	-
9	No	-	-	-	-	-
10	No	-	-	-	-	-

Рисунок 142 Просмотр сосояние порта LACP

- **LCAP**
  Варианты: Да/Нет
  Функция: просмотр состояния порта LACP. Да означает, что LACP включен и порт подключен. Нет означает, что LACP не включен или порт не подключен.

Просмотрите статистику порта LACP, как показано на рисунке 143.

LACP Statistics

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	333	326	0	0
2	222	221	0	0
3	0	7	0	0
4	0	7	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0

Рисунок 143 Просмотр сосояние порта LACP

12. Конфигурация loop detection

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. Цикл отправки ЦП периодически обнаруживает пакеты на порт. Если какой-либо порт коммутатора получает пакеты обнаружения петель, определяется, что в сети существуют петли. Отключите порт, который отправляет пакеты обнаружения петли, и через некоторое время порт автоматически подключится и продолжит обнаружение. Интервал времени для отправки пакетов обнаружения петель и время восстановления порта можно настроить в программном обеспечении.

12.1. Веб конфигурация

Настройте функцию обнаружения петель на порту, как показано на рис. 144.

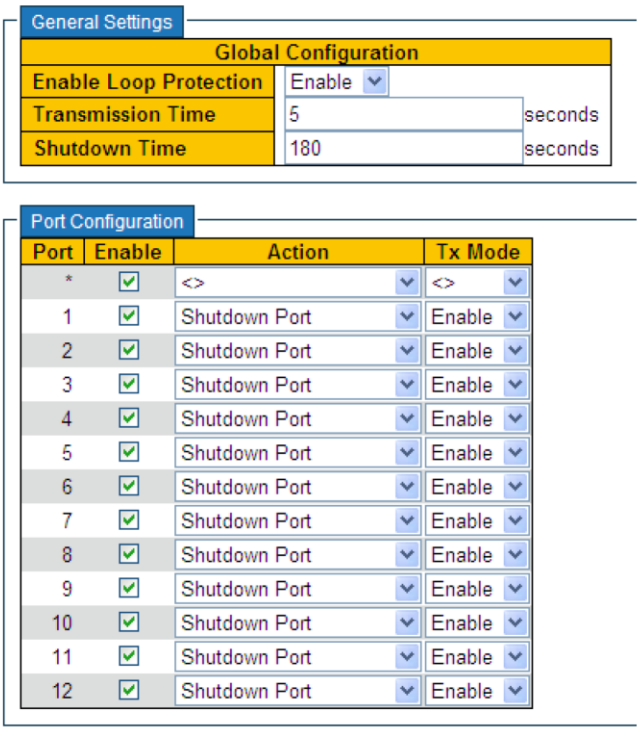


Рисунок 144 Настройка функции обнаружения петель на порту

- **Enable Loop Protection**
  Опции: включить/отключить
  По умолчанию: Отключить
  Функция: включение или отключение функции глобального обнаружения петель порта.
- **Transmission Time**
  Диапазон: 1~10 с
  По умолчанию: 5 с
  Функция: Настройка временного интервала для отправки пакетов обнаружения петель.
- **Shutdown Time**
  Диапазон: 0~604800с
  По умолчанию: 180 с
  Функция: Настройте время восстановления порта, 0 указывает, что порт не может быть подключен автоматически до перезапуска устройства.
- **Enable**
  Опции: включить/отключить
  По умолчанию: Включить
  Функция: Включить или отключить функцию обнаружения петли порта.
- **Action**
  Опция: порт выключения/порт выключения и журнал/только журнал
  По умолчанию: порт выключения
  Функция: укажите действие, которое будет выполняться, когда порт обнаружит наличие петли.
- **Tx Mode**
  Опции: включить/отключить
  По умолчанию: Включить
  Функция: отправлять ли пакеты обнаружения петель или нет.

Просмотрите состояние защиты от петель, как показано на рисунке 145.

Loop Protection Status

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	0	Up	-	-
2	Shutdown	Enabled	14	Down	-	2015-11-14T13:29:24+08:00
3	Shutdown	Enabled	8	Disabled	Loop	2015-11-14T13:30:55+08:00
4	Shutdown	Enabled	1	Down	-	2015-11-14T13:26:33+08:00
5	Shutdown	Enabled	0	Down	-	-
6	Shutdown	Enabled	0	Down	-	-
7	Shutdown	Enabled	0	Down	-	-
8	Shutdown	Enabled	0	Down	-	-
9	Shutdown	Enabled	0	Down	-	-
10	Shutdown	Enabled	0	Down	-	-
11	Shutdown	Enabled	0	Down	-	-
12	Shutdown	Enabled	0	Down	-	-

Рисунок 145 Просмотр состояния защиты от петель

- **Loop Protection Status**
  Опции: --/Цикл
  Функция: Статус обнаружения петель показывает наличие петель в сети, в которой включена функция обнаружения петель порта. Цикл указывает на наличие циклов, а -- указывает на отсутствие цикла.

13. Промышленные протоколы

13.1. EtherNet/IP

EtherNet/IP — это протокол уровня промышленных приложений для приложений промышленной автоматизации. Он основан на стандартных протоколах TCP/IP и UDP/IP и использует фиксированное аппаратное и программное обеспечение Ethernet для определения протокола прикладного уровня для настройки, доступа и управления устройствами промышленной автоматизации.

Эта серия коммутаторов позволяет пользователям устанавливать состояние порта (включить/выключить) с помощью протокола EtherNet/IP для получения информации об устройстве, информации о порте, информации о сигналах тревоги, информации о кольце ST, информации DRP и информации RSTP.

13.1.1. Веб конфигурация

Настройте протокол EtherNet/IP, как показано на рисунке 146.

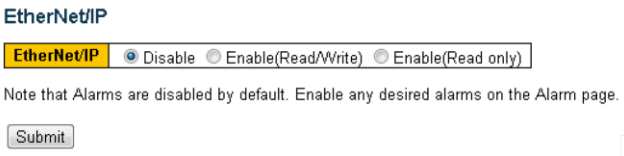


Рисунок 146 Настройка протокола EtherNet/IP

Опция: Отключить/Включить (Чтение/Запись)/Включить (Только чтение)
По умолчанию: Отключить

Функция: Включите EtherNet/IP и используйте протокол EtherNet/IP для настройки состояния устройства.

13.2. Modbus TCP

Протокол ModbusTCP — это протокол Modbus, основанный на Ethernet TCP/IP. Modbus — это протокол передачи сообщений прикладного уровня, который использует для связи Master/Slave (Master/Slave). Modbus — это простой прикладной протокол клиент/сервер. Сервер анализирует, обрабатывает запросы и отправляет ответы клиенту.

Эта серия коммутаторов позволяет пользователям устанавливать статус порта (включение/отключение) с использованием протокола ModbusTCP для получения информации об устройстве, информации о порте, информации о тревоге, информации о кольце ST, информации DRP и информации RSTP.

13.2.1. Веб конфигурация

Настройте протокол Modbus/TCP, как показано на рисунке 147.

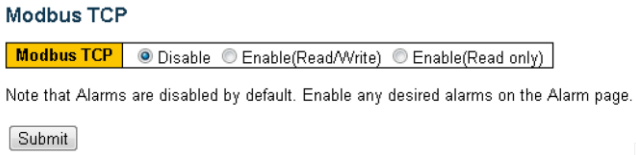


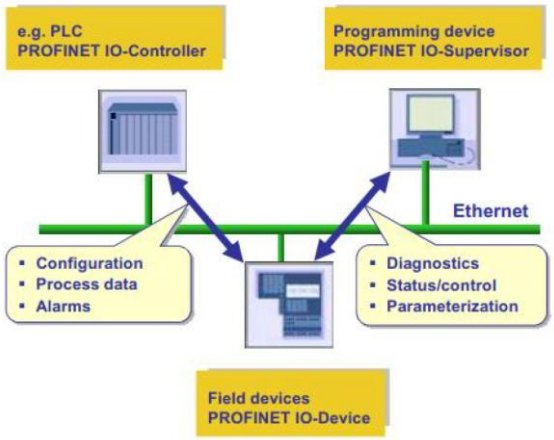
Рисунок 147 Настройка протокола Modbus/TCP

Опция: Отключить/Включить (Чтение/Запись)/Включить (Только чтение)
По умолчанию: Отключить
Функция: Включите Modbus TCP и используйте протокол Modbus TCP для настройки состояния устройства.

13.3. PROFINET

PROFINET — это промышленная коммуникационная сеть на основе Ethernet для всех представлений приложений от PROFIBUS International (PI). Он охватывает ключевые рынки и ключевые технологии автоматизации как сегодня, так и в будущем. Благодаря реализации PROFINET I/O можно легко автоматизировать производство и процессы. Кроме того, обмен данными по PROFINET I/O осуществляется между контроллером ввода/вывода (ПЛК и т. д.) и устройствами ввода/вывода (полевыми устройствами).

В сетевой структуре ввода/вывода PROFINET есть три основные роли. Это контроллер ввода-вывода, супервизор ввода-вывода и устройства ввода-вывода. Он следует модели поставщика и потребителя для обмена данными. Подробные описания приведены ниже.



I/O Controller

I/O Controller — это роль для управления устройством ввода-вывода. В сети ввода-вывода PROFINET может существовать ровно один контроллер. Однако это позволяет нескольким контроллерам реализовать резервирование системы. Типичным контроллером является программируемый логический контроллер (ПЛК), на котором выполняется программа автоматизации.

I/O Supervisor

I/O Supervisor может быть устройством программирования, которое управляет I/O Controller, персональным компьютер или устройство HMI для ввода в эксплуатацию или диагностики.

I/O Device

I/O Device — это распределенное полевое устройство, которое подключено к одному или нескольким I/O controller через PROFINET ввод/вывод. Он периодически отправляет данные о переключении на контроллер в соответствии с поддерживаемым временем цикла. Коммутатор PROFINET действует как устройство ввода/вывода PROFINET. Он поддерживает множество полезных атрибутов для I/O controller для настройки или мониторинга. Подробные атрибуты описаны в файле GSD и в следующей теме.

GSD

Технические характеристики устройств ввода-вывода описаны в файле GSD. GSD представляет собой XML.

основанный на. Возможна генерация с помощью любого стандартного редактора XML.

- Список всех доступных модулей и подмодулей
- Допустимые слоты (слоты/подслоты) для модулей и субмодулей
- Шинные интерфейсы (DAP = Device Access Point) • Параметры модулей

13.3.1. Веб конфигурация

Настройте протокол PROFINET, как показано на рисунке 148.

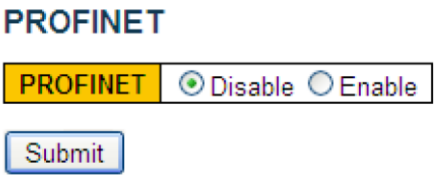


Рисунок 147 Настройка протокола PROFINET

Опция: Отключить/Включить
По умолчанию: Отключить
Функция: включение/выключение протокола PROFINET.

14. Multicast

14.1. IGMP Snooping

Отслеживание протокола управления группами Интернета (IGMP Snooping) — это протокол многоадресной рассылки на уровне канала передачи данных. 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.

Существует три версии протокола групповых сообщений Интернета (IGMP): IGMPv1, IGMPv2 и IGMPv3. IGMPv1 определен в RFC1112, IGMPv2 определен в RFC2236, а IGMPv3 определен в RFC3376.

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

IGMPv2 на основе IGMPv1 предоставляет пакет выхода механизма быстрого выхода для членов группы. При использовании этого механизма, когда последний участник покидает группу многоадресной рассылки, маршрутизатор получает команду провести быструю конвергенцию. По сравнению с IGMPv1, IGMPv2 поддерживает два типа пакетов запросов: пакет общего запроса и пакет запроса для конкретной группы. Коммутатор периодически отправляет пакет общего запроса для запроса членства. Когда хост покидает группу многоадресной рассылки, после того как коммутатор получает сообщение о выходе, коммутатор отправляет пакет запроса для конкретной группы, чтобы определить, все ли члены покинули группу многоадресной рассылки.

В IGMPv3 добавлена функция фильтрации источника хоста. Эта функция позволяет хосту указать, следует ли получать или отклонять пакеты от некоторых конкретных источников группы многоадресной рассылки.

Querier: периодически отправляет пакеты общего запроса IGMP для запроса статуса членов группы многоадресной рассылки, сохраняя информацию о группе многоадресной рассылки. Когда в сети существует несколько запросчиков, они автоматически выбирают в качестве запрашивающего тот, у кого наименьший IP-адрес. Только выбранный запросчик периодически отправляет пакеты общего запроса IGMP. Остальные запросы только получают и пересылают пакеты запросов IGMP.

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

Прокси-сервер отслеживания IGMP. Функция прокси-сервера отслеживания IGMP настраивается на граничном устройстве для уменьшения количества пакетов отчетов IGMP и оставления пакетов, полученных вышестоящим устройством, тем самым улучшая общую производительность вышестоящего устройства. Устройство, на котором настроена функция прокси-сервера отслеживания IGMP, функционирует как хост своего восходящего устройства и функционирует как запросчик своего нижестоящего хоста.

IGMP Snooping управляет и обслуживает членов группы многоадресной рассылки путем обмена соответствующими пакетами между устройствами с поддержкой IGMP. Соответствующие пакеты следующие:

Пакет общего запроса: запросчик 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 отправляющее запрос, пересылает пакет на все подключенные к нему порты.

Пакет конкретного запроса. Если устройство хочет покинуть группу многоадресной рассылки, оно отправляет пакет выхода IGMP. После получения пакета отпуска запрашивающий отправляет специальный пакет запроса (IP-адрес назначения: IP-адрес группы многоадресной рассылки), чтобы подтвердить, содержит ли группа другие порты-члены.

Пакет отчета о членстве: если устройство хочет получить данные группы многоадресной рассылки, оно немедленно отправляет пакет отчета IGMP (IP-адрес назначения: IP-адрес группы многоадресной рассылки) для ответа 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).

14.1.1. Веб конфигурирование

Включите IGMP Snooping, как показано на рисунке 148.

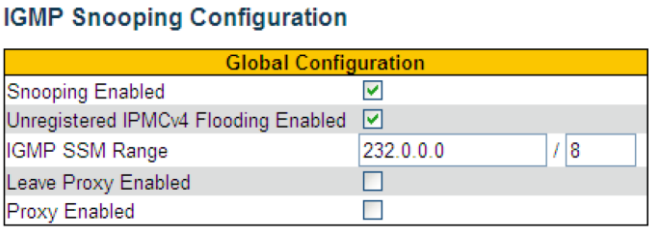


Рисунок 148 Включение IGMP Snooping

- **Snooping Enabled**
  Опции: Включить/Отключить.
  По умолчанию: Отключить

Функция: включение или отключение глобального протокола отслеживания IGMP.

- **Unregistered IPMCv4 Flooding Enabled**
  Опции: Включить/Отключить.
  По умолчанию: Включить
  Функция: настройка незарегистрированного действия многоадресной рассылки. Включить: при получении незарегистрированного многоадресного пакета коммутатор транслирует пакет внутри VLAN (все порты, кроме входного). Disable: при получении незарегистрированного многоадресного пакета коммутатор отбрасывает его. Незарегистрированные многоадресные пакеты относятся к многоадресным пакетам без соответствующих записей пересылки на коммутаторе.
- **IGMP SSM Range**
  Формат: A.B.C.D/4~32
  По умолчанию: 232.0.0.0/8
  Функция: только хосты и маршрутизаторы с адресом в пределах значения этого параметра могут запускать сервисную модель многоадресной рассылки с учетом источника IGMP (SSM) при условии, что хосты и маршрутизаторы поддерживают сервисную модель IGMP SSM. Модель службы SSM предоставляет пользователям услугу передачи с указанием источников многоадресной рассылки для клиента.
- **Leave Proxy Enabled**
  Опции: включено/выключено.
  По умолчанию: отключено
  Функция: Укажите, следует ли пересылать пакеты отпуска запрашивающему устройству. Когда он включен, пакеты отпуска не пересылаются.
- **Proxy Enabled**
  Опции: включено/выключено.
  По умолчанию: отключено
  Функция: Укажите, пересылать ли запрашивающему отправителю пакеты отпуска и пакеты отчетов участников. Когда эта функция включена, пакеты отпуска и пакеты отчетов участников не пересылаются.

Настройте порт IGMP, как показано на рисунке 149.

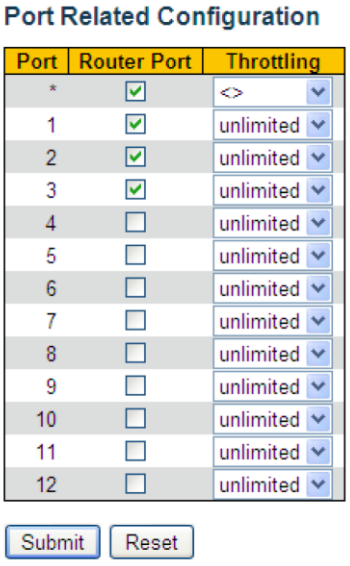


Рисунок 149 Настройка порта IGMP

- **Router Port**
  Опции: включено/выключено.
  По умолчанию: отключено
  Функция: настройка порта маршрутизатора.
- **Throttling**
  Опции: неограниченно/1~10
  По умолчанию: неограниченно
  Функция: ограничить ли количество записей многоадресной рассылки, полученных портом.

Настройте IGMP Snooping VLAN, как показано на рисунке 150.

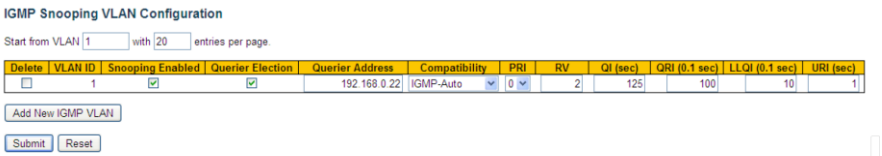


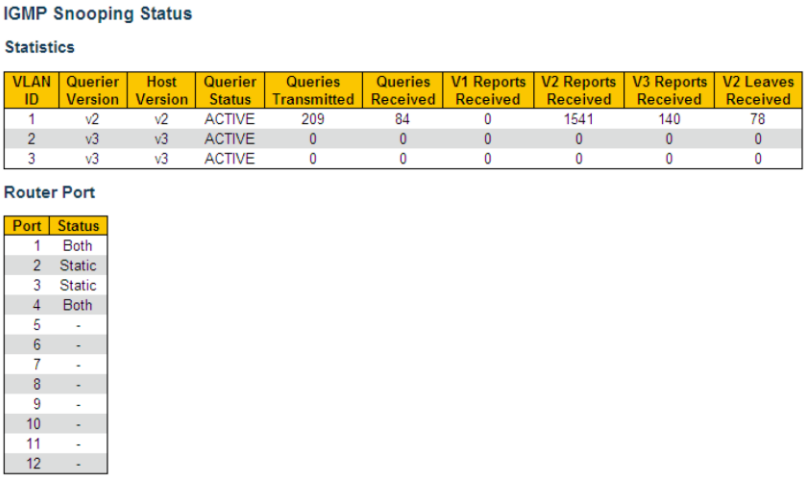
Рисунок 150 Настройка IGMP Snooping VLAN

- **VLAN ID**
  Опции: все созданные идентификаторы VLAN.
- **Snooping Enabled**
  Опции: Включить/Отключить.
  По умолчанию: Отключить
  Функция: включение или отключение функции отслеживания VLAN IGMP. Предварительным условием использования этой функции является включение глобальной функции IGMP Snooping.
- **Querier Election**
  Опции: Включить/Отключить.
  По умолчанию: Включить
  Функция: включение или отключение функции запроса IGMP для выбранной VLAN. Предварительным условием использования этой функции является включение глобальной функции IGMP Snooping и функции VLAN IGMP Snooping.
  Описание: Если в сети несколько запросчиков, они автоматически выберут в качестве запрашивающего тот, у которого наименьший IP-адрес. Если есть только одно устройство, которое включает функцию запроса IGMP, оно будет запросчиком.
- **Querier Address**
  Формат: A.B.C.D.
  Функция: Настройте исходный IP-адрес для отправки пакета запроса. Если адрес запроса не установлен, в качестве адреса запроса используется IP-адрес порта VLAN.
- **Compatibility**
  Варианты: IGMP-Auto/Forced IGMPv1/Forced IGMPv2/Forced IGMPv3
  По умолчанию: IGMP-авто.
  Функция: настройка версии IGMP.
- **PRI (приоритет интерфейса)**
  Диапазон: 0~7

По умолчанию: 0
Функция: настройка приоритета пакета управления IGMP.

- **RV (переменная устойчивости)**
  Диапазон: 1~255
  По умолчанию: 2
  Функция: укажите параметр устойчивости функции запроса IGMP.
  Описание: Чем больше параметр, тем хуже сетевое окружение. Пользователь может установить подходящий параметр надежности в соответствии с реальной сетью.
- **QI (интервал запроса)**
  Диапазон: 1~31744 с.
  По умолчанию: 125 с.
  Функция: Настройка интервала отправки пакета общего запроса.
- **QRI (интервал ответа на запрос)**
  Диапазон: 0~31744 (единица измерения: 0,1 с)
  По умолчанию: 100
  Функция: настройка максимального времени ответа на ответный пакет общего запроса.
- **LLQI (интервал запроса последнего участника)**
  Диапазон: 0~31744 (единица измерения: 0,1 с)
  По умолчанию: 10
  Функция: настройка максимального времени ответа на конкретный пакет запроса.
- **URI (интервал нежелательных отчетов)**
  Диапазон: 0~31744 с.
  По умолчанию: 1 с
  Функция: установите интервал повторной отправки хостом пакета отчета для присоединения к группе многоадресной рассылки. Нажмите <Добавить новую IGMP VLAN>, чтобы настроить запись IGMP Snooping VLAN. Поддерживается максимум 32 записи IGMP Snooping VLAN.

Просмотрите статус IGMP Snooping, как показано на рисунке 151.



IGMP Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
1	v2	v2	ACTIVE	209	84	0	1541	140	78
2	v3	v3	ACTIVE	0	0	0	0	0	0
3	v3	v3	ACTIVE	0	0	0	0	0	0

Router Port

Port	Status
1	Both
2	Static
3	Static
4	Both
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-

Рисунок 151 Просмотр статуса IGMP Snooping

- **Router Port Status**
  Варианты: Both/Static/Dynamic
  Функция: отображение состояния порта маршрутизатора. Статический указывает, что порт статически настроен как порт маршрутизатора, Динамический указывает,

что порт динамически запоминается как порт маршрутизатора, а Оба указывают, что порт статически настроен как порт маршрутизатора или динамически изучается как порт маршрутизатора.

Просмотрите список участников многоадресной рассылки, как показано на рисунке 152.

		Port Members											
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12
1	224.0.1.1	✓		✓									
1	225.10.24.3	✓		✓									
1	226.81.9.8	✓		✓									
1	239.2.11.71	✓		✓									
1	239.5.5.5	✓		✓									
1	239.77.124.213	✓		✓									
1	239.255.255.250	✓		✓									
1	239.255.255.254	✓		✓									

Рисунок 151 IGMP Snooping список рассылки

14.2. GRMP

Протокол регистрации общих атрибутов (GARP) используется для распространения, регистрации и отмены определенной информации (VLAN, многоадресного адреса) между коммутаторами в одной сети.

При использовании GARP информация о конфигурации члена GARP будет распространяться на всю коммутационную сеть. Член GARP инструктирует других членов GARP зарегистрировать или отменить свою собственную конфигурационную информацию посредством сообщения о присоединении или выходе соответственно. Участник также регистрирует или отменяет информацию о конфигурации других участников на основе сообщений 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 Join.

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 на других коммутаторах, Объект отправляет сообщение Leave. Сообщения о выходе делятся на два типа: LeaveEmpty и Leave. Сообщение LeaveIn отправляется для отмены зарегистрированного атрибута, а сообщение LeaveIn отправляется для отмены зарегистрированного атрибута LeaveEmpty отправляется сообщение об отмене атрибута, который еще не зарегистрирован.

После запуска объекта GARP он запускает таймер LeaveAll. По истечении времени таймера сущность отправляет сообщение LeaveAll.

Таймеры GARP включают таймер удержания, таймер присоединения, таймер выхода и таймер выхода из всех.

Таймер удержания: при получении регистрационного сообщения объект GARP не отправляет сообщение о присоединении немедленно, а запускает таймер удержания. По истечении времени таймера сущность отправляет все сообщения о регистрации, полученные в течение предыдущего периода, в одном сообщении «Присоединиться», что снижает отправка пакетов для лучшей стабильности сети.

Таймер присоединения: Чтобы гарантировать получение сообщений о присоединении другими объектами приложения, объект приложения GARP запускает таймер присоединения после отправки сообщения о присоединении. Если нет сообщение до истечения таймера присоединения, объект снова отправляет сообщение о присоединении. Если получить сообщение о присоединении до истечения таймера, объект не отправляет второе сообщение о присоединении.

Таймер выхода: когда объект приложения GARP хочет отменить информацию о атрибут, сущность отправляет сообщение Выход. Объект, получивший сообщение, начинает Leave Timer. Если сообщение о присоединении не получено до истечения таймера, объект, получающий сообщение, отменяет информацию об атрибуте.

Таймер LeaveAll: при запуске объекта приложения GARP запускается таймер LeaveAll. Когда таймера истекает, объект отправляет сообщение LeaveAll, чтобы другие объекты приложения GARP повторно зарегистрировали все атрибуты. Затем объект снова запускает таймер LeaveAll для нового цикла.

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.

14.2.1. Веб конфигурирование

Глобальная конфигурация GMRP, показано на рисунке 152.

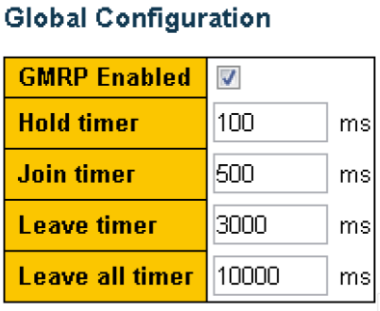


Рисунок 152 Глобальная конфигурация GMRP

- **GMRP Enabled:**
  Опция: Включить/Выключить
  По умолчанию: отключено
  Функция: включить глобальную функцию gmrp.
- **Timer:**

Опция: таймер удержания/таймер присоединения/таймер выхода/таймер выхода из всех
По умолчанию: 100/500/3000/10000 мс
Функция: настройка значения глобального таймера gmrp.

Конфигурация порта GMRP, как показано на рисунке 153.

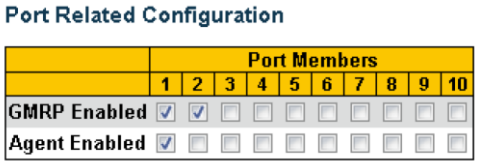


Рисунок 153 Конфигурация порта GMRP

- **GMRP Enabled:**
  Опция: Включено/Выключено
  По умолчанию: отключено
  Функция: включить порт gmrp.
- **Agent Enabled:**
  Опция: Включено/Выключено
  По умолчанию: отключено
  Функция: включить агент gmrp порта.

Конфигурация таблицы MAC-адресов агента, как показано на рисунке 154.

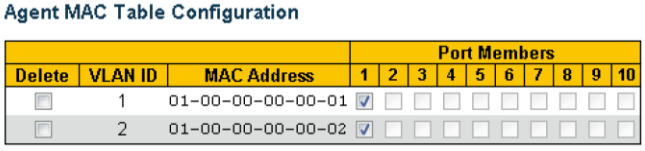


Рисунок 154 Конфигурация таблицы MAC-адресов агента

Функция: настройка статического многоадресного MAC-адреса агента, привязанного к порту и виртуальной локальной сети.

Статус таблицы MAC-адресов GMRP, как показано на рисунке 155.

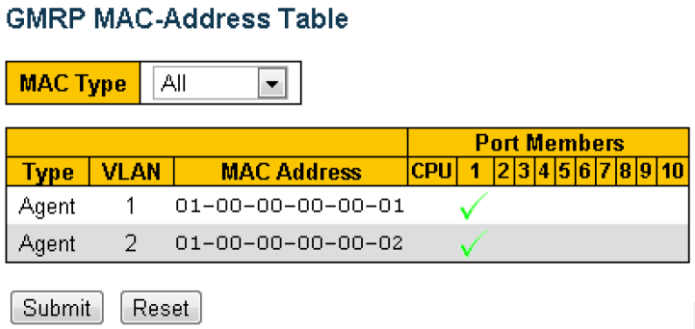


Рисунок 155 Статус таблицы MAC-адресов GMRP

- **MAC Type**
  Опция: Все/Агент/Динамический
  По умолчанию: Все

15. LLDP

Протокол обнаружения канального уровня (LLDP) обеспечивает стандартный механизм обнаружения канального уровня. Он инкапсулирует информацию об устройстве, такую как возможности, адрес управления, идентификатор устройства и идентификатор интерфейса, в блоке данных протокола обнаружения канального уровня (LLDPDU) и объявляет LLDPDU своим напрямую подключенным соседям. После получения LLDPDU соседи сохраняют эту информацию в MIB для запроса и проверки состояния канала NMS.

15.1. Веб конфигурирование

Настройте LLDP, как показано на рисунке 156.

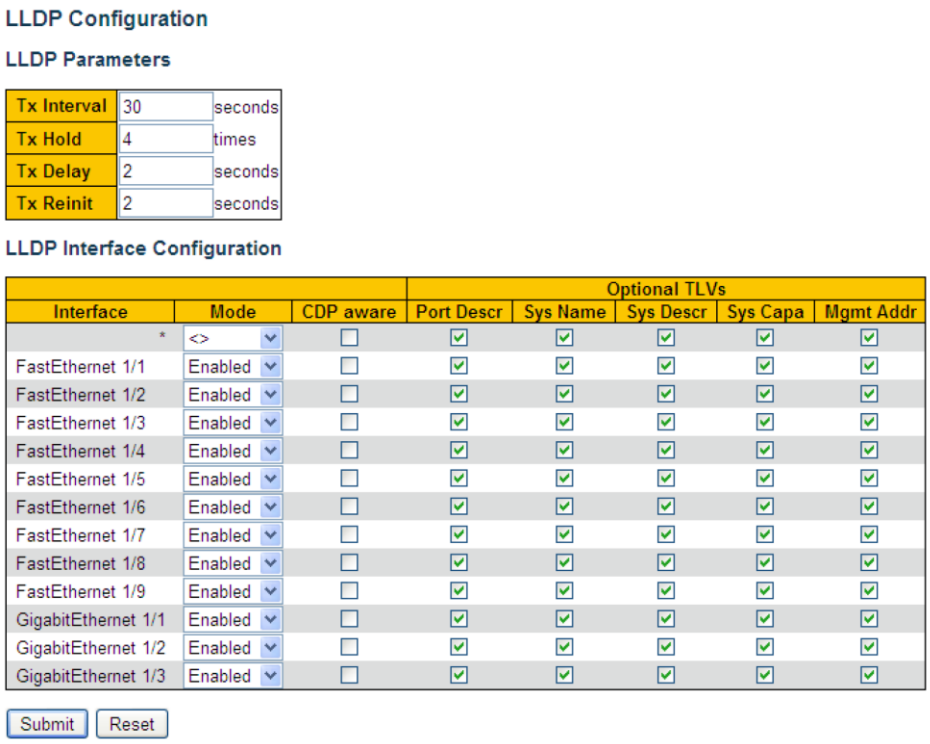


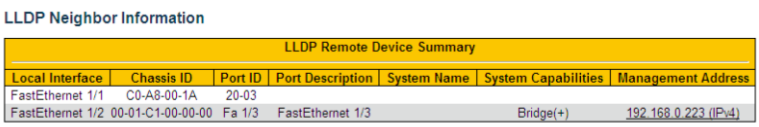
Рисунок 156 Настройка LLDP

- **Tx Interval**
  Диапазон: 5~32768 с.
  По умолчанию: 30 с.
  Функция: Настройте временной интервал для отправки пакетов LLDP.
- **Tx Hold**
  Диапазон: 2~10 раз
  По умолчанию: 4 раза
  Функция: установка количества времен удержания передачи. Эффективная продолжительность пакета LLDP = интервал передачи x удержание передачи.
- **Tx Delay**
  Диапазон: 1~8192 с.
  По умолчанию: 2 с.

Функция: установка интервала передачи между новым пакетом LLDP и предыдущим пакетом LLDP после изменения информации о конфигурации. Значение Tx Delay не может превышать 1/4 значения Tx Interval.

- **Tx Reinit**
  Диапазон: 1~10 с
  По умолчанию: 2 с.
  Функция: после отключения LLDP на порту или перезапуска коммутатора коммутатор отправляет кадр отключения LLDP соседнему узлу, чтобы объявить, что предыдущий пакет LLDP недействителен. Tx Reinit относится к интервалу между передачей кадра выключения LLDP и
  повторная инициализация пакета LLDP.
- **Mode**
  Опции: Включено/Отключено/Только прием/Только передача.
  По умолчанию: включено
  Функция: установка пакетного режима LLDP. Включенный режим указывает, что коммутатор может отправлять пакеты LLDP, а также получать и идентифицировать пакеты LLDP; отключенный режим указывает, что коммутатор не отправляет пакеты LLDP и не получает пакеты LLDP; единственный режим Rx указывает, что коммутатор принимает и идентифицирует только пакеты LLDP; единственный режим Tx указывает, что коммутатор отправляет только пакеты LLDP.
- **Port Descr**
  Опиции: включено/выключено.
  По умолчанию: включено
  Функция: Включение указывает, что пакеты LLDP будут содержать описание порта.
- **Sys Name**
  Опции: включено/выключено.
  По умолчанию: включено
  Функция: Включение указывает, что пакеты LLDP будут содержать системное имя.
- **Sys Descr**
  Опции: включено/выключено.
  По умолчанию: включено
  Функция: Включение указывает, что пакеты LLDP будут содержать описание системы.
- **Sys Capa**
  Опции: включено/выключено.
  По умолчанию: включено
  Функция: Включение указывает, что пакеты LLDP будут нести возможности системы.
- **Mgmt Addr**
  Опции: включено/выключено.
  По умолчанию: включено
  Функция: Включение указывает, что пакеты LLDP будут содержать адрес управления.

Просмотрите информацию о соединении LLDP, как показано на рисунке 157.


LLDP Neighbor Information

LLDP Remote Device Summary

Local Interface	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
FastEthernet 1/1	C0-A8-00-1A	20-03				
FastEthernet 1/2	00-01-C1-00-00-00	Fa 1/3	FastEthernet 1/3		Bridge(+)	192.168.0.223 (IPv4)

Рисунок 157 Просмотр информации LLDP

16. MAC Address Configuration

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

MAC-адрес может быть статическим или динамическим.

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

Динамические MAC-адреса изучаются 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 MAC-адрес источника кадра, устанавливает сопоставление с принимающим портом и запрашивает порт пересылки в таблице MAC-адресов на основе MAC-адреса назначения кадра. Если совпадение обнаружено, коммутатор пересылает кадр данных из соответствующего порта. Если совпадение не найдено, коммутатор передает кадр в своем широковещательном домене.

Срок устаревания начинается с момента добавления динамического MAC-адреса в таблицу MAC-адресов. Если ни один порт не получает кадр с MAC-адресом в течение одного-двухкратного времени устаревания, коммутатор удаляет запись MAC-адреса из таблицы динамических адресов пересылки. Статические MAC-адреса не учитывают концепцию времени устаревания.

Настройте время устаревания MAC-адреса, как показано на рисунке 158.

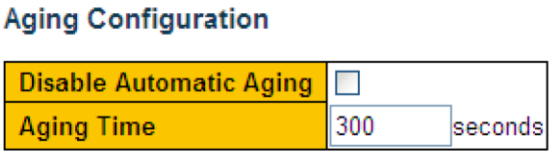


Рисунок 158 Настройка время устаревания MAC-адреса

- **Disable Automatic Aging**
  Опции: Включить/Отключить.
  По умолчанию: По умолчанию
  Функция: Включение/выключение устаревания MAC-адреса. Включение означает, что вам необходимо настроить время устаревания. Отключить означает, что динамически полученный адрес не устаревает со временем.
- **Aging Time**
  Диапазон: 10~1000000 с
  По умолчанию: 300 с.
  Функция: Установите время устаревания записи динамического MAC-адреса.

Настройте динамический MAC-адрес, как показано на рисунке 159.

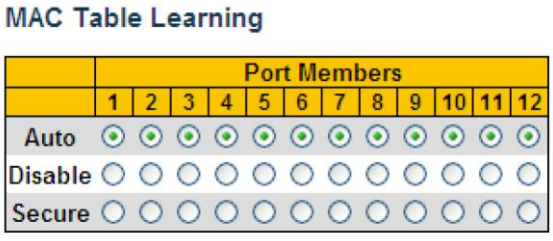


Рисунок 159 Настройка динамического MAC-адреса

Port Members
Опции: Авто/Отключить.
По умолчанию: Авто
Функция: определяет, будет ли порт динамически изучать таблицу MAC-адресов. Auto указывает, что порт может динамически изучать таблицу MAC-адресов. Отключить означает, что порту запрещено динамически изучать таблицу MAC-адресов. Безопасность: включить безопасное обучение Mac для порта. Изучаются только статические записи MAC, все остальные кадры отбрасываются.

Настройте статический MAC-адрес, как показано на рисунке 160.

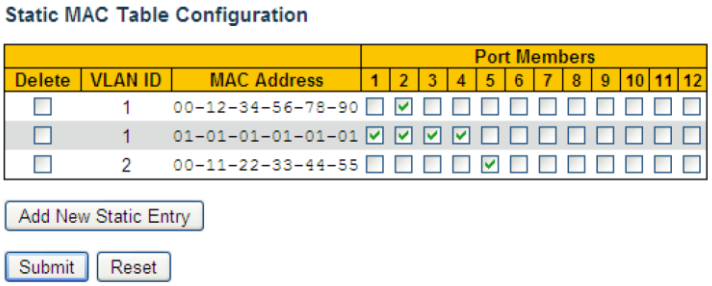


Рисунок 160 Настройка статического MAC-адреса

- **VLAN ID**
  Опции: все созданные идентификаторы VLAN.
  По умолчанию: VLAN 1.
  Функция: настройка идентификатора VLAN статического MAC-адреса.
- **MAC address**
  Формат: ЧЧ-ЧЧ-ЧЧ-ЧЧ-ЧЧ-ЧЧ (Н — шестнадцатеричное число).
  Функция: настройка MAC-адреса. Для одноадресного MAC-адреса — младший бит первого байта.
  равно 0. Для многоадресного MAC-адреса младший бит в первом байте равен 1.
- **Port Members**
  Функция: выберите порты для пересылки пакетов с этим MAC-адресом назначения.
  Нажмите <Add New Static Entry>, чтобы настроить запись статического MAC-адреса.
  Поддерживается максимум 64 записи статического MAC-адреса.

Просмотрите таблицу MAC-адресов, как показано на рисунке 161.

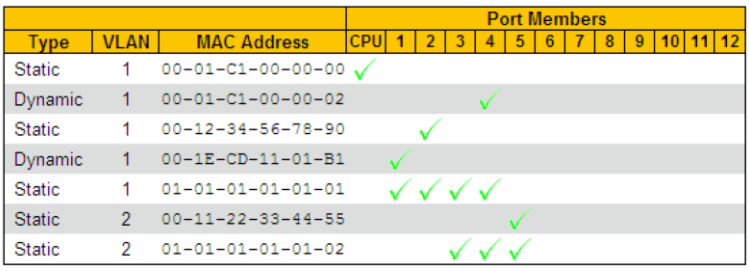


Рисунок 161 Просмотрит таблицы MAC-адресов

17. VLAN

17.1. Конфигурация VLAN

Одну локальную сеть можно разделить на несколько логических виртуальных локальных сетей (VLAN). Устройство может взаимодействовать только с устройствами в одной VLAN. В результате широковещательные пакеты ограничиваются VLAN, что оптимизирует безопасность локальной сети.

Раздел VLAN не ограничен физическим местоположением. Каждая VLAN рассматривается как логическая сеть. Если хосту в одной VLAN необходимо отправить пакеты данных хосту в другой VLAN, необходимо задействовать маршрутизатор или устройство уровня 3.

Чтобы сетевые устройства могли различать пакеты из разных VLAN, в пакеты необходимо добавить поля для идентификации VLAN. В настоящее время наиболее часто используемым протоколом идентификации VLAN является IEEE802.1Q. В таблице 3 показана структура кадра 802.1Q.

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

Таблица 3 Структура фрейма 802.1Q.

4-байтовый заголовок 802.1Q в качестве тега VLAN добавляется к традиционному кадру данных Ethernet. ТПИД: 16 бит. Он используется для идентификации кадра данных, содержащего тег VLAN. Значение 0x8100. Значение TPID, указанное в протоколе 802.1Q, равно 0x8100.

PRI: три бита, определяющие приоритет пакета 802.1p.

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

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

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

17.1.1. Port-based VLAN

Раздел VLAN может быть основан на портах или MAC-адресах. 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 этой VLAN.

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

Доступ: В режиме доступа порт можно добавить только к одной VLAN. По умолчанию все порты коммутатора являются портами доступа и принадлежат VLAN1. Пакеты,

пересылаемые портом доступа, не имеют тегов VLAN. Порты доступа обычно используются для подключения к терминалам, не поддерживающим 802.1Q.

Trunk: В режиме магистрали порт можно добавить ко многим VLAN. Магистральный порт принимает только помеченные пакеты. При отправке пакетов PVID на магистральном порте можно указать, будет ли передаваться тег. Он несет этот тег при отправке других пакетов. Магистральные порты обычно используются для подключения сетевых передающих устройств.

Гибридный: в гибридном режиме порт можно добавить во многие VLAN. Вы можете установить тип пакетов, которые будут приниматься гибридным портом, а также указать, будет ли передаваться тег, когда гибридный порт отправляет пакеты. Гибридный порт можно использовать для подключения сетевых устройств и пользовательских устройств. Разница между гибридным портом и магистральным портом заключается в следующем: гибридный порт не несет тег при отправке пакетов из нескольких VLAN, а магистральный порт не несет тег только при отправке пакетов PVID.

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

17.1.2. Веб конфигурирование

Настройте разрешенные VLAN для порта доступа, как показано на рисунке 162.

Global VLAN Configuration

Allowed Access VLANs	1,2,100,200
Ethertype for C-Tag	88A8

Рисунок 162 Конфигурирование разрешенных VLAN для порта доступа

- **Allowed Access VLANs**
  Опции: 1~4093.
  По умолчанию: 1
  Функция: настройка разрешенных VLAN для порта доступа. При наличии нескольких VLAN их можно разделить запятой (,) и тире (-), где тире используется для разделения двух последовательных идентификаторов VLAN, а запятая используется для разделения двух непоследовательных идентификаторов VLAN.

  Настройте порт VLAN, как показано на рисунке 163.

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	2	<>	☑	<>	<>	2	1
1	Access	2	C-Port	☑	Tagged and Untagged	Untag All	2	1
2	Access	2	C-Port	☑	Tagged and Untagged	Untag All	2	
3	Access	100	C-Port	☑	Tagged and Untagged	Untag All	100	
4	Access	100	C-Port	☑	Tagged and Untagged	Untag All	100	
5	Access	200	C-Port	☑	Tagged and Untagged	Untag All	200	
6	Access	200	C-Port	☑	Tagged and Untagged	Untag All	200	
7	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1,2,100,200	
8	Hybrid	1	C-Port	☐	Tagged and Untagged	Untag Port VLAN	1-3	2
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

Submit Reset

Рисунок 163 Конфигурирование портов VLAN

- **Mode**
  Опции: Access/Trunk/Hybrid
  По умолчанию: Access

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

- **Port VLAN（PVID）**
  Диапазон: 1~4094
  По умолчанию: 1
  Функция: Каждый порт имеет PVID. При получении нетегированного пакета порт добавляет к пакету тег в соответствии с PVID.
- **Ingress Filtering**
  Опции: Включить/Отключить.
  По умолчанию: Отключить
  Функция: включение/отключение функции фильтрации входящего трафика гибридного порта. Входная фильтрация включена принудительно для порта доступа и транкового порта, настроить параметр нельзя. Включить: если идентификатор VLAN в пакете отсутствует в списке разрешенных VLAN, пакет отбрасывается.
  Отключить: если идентификатор VLAN в пакете отсутствует в списке разрешенных VLAN, примите пакет и перенаправьте его в механизм MAC.
- **Ingress Acceptance**
  Опции: Tagged and Untagged/ Tagged Only/ Untagged Only
  По умолчанию: Tagged and Untagged.
  Функция: установите тип пакетов, которые будут приниматься гибридным портом. Для порта доступа и магистрального порта принудительно установлены значения с тегами и без тегов, и их нельзя изменить. Значения Tagged и Untagged указывают, что гибридный порт может принимать тегированные и нетегированные пакеты; значение «Только тегированные» указывает, что гибридный порт принимает только тегированные пакеты и отбрасывает нетегированные пакеты; значение «Только без тегов» указывает, что гибридный порт принимает только нетегированные пакеты и отбрасывает тегированные пакеты.
- **Egress Tagging**
  Опции: Untag Port VLAN/ Unatg All/ Tag All
  По умолчанию: Untag Port VLAN.
  Функционал: установите обработку передачи пакетов для магистрального порта или гибридного порта. Для выходной маркировки настроено принудительное Unatg All для порта доступа, настроить этот параметр невозможно. Untag Port VLAN: Если идентификатор VLAN в пакете совпадает с PVID и в списке разрешенных VLAN, пересылайте пакет после удаления тега. Если идентификатор VLAN в пакете отличается от PVID и в списке разрешенных VLAN, сохраните тег и переправьте пакет. Пометить все: если идентификатор VLAN в пакете находится в списке разрешенных VLAN, сохраните тег и переправьте пакет. Отменить тегирование всех: если идентификатор VLAN в пакете находится в списке разрешенных VLAN, пересылайте пакет после удаления тега.
- **Allowed VLANs**
  Диапазон: 1-4094
  Диапазон: 1-4094
  Функция: настройка разрешенных VLAN для магистрального/гибридного порта. Если порт доступа допускает только одну VLAN, значение этого параметра соответствует значению порта VLAN и его нельзя изменить. Если для этого параметра установлено несколько VLAN, вы можете разделить VLAN запятой (,) и тире (-), где тире используется для разделения двух последовательных

идентификаторов VLAN, а запятая используется для разделения двух непоследовательных VLAN. идентификаторы.

- **Forbidden VLANs**
  Диапазон: 1-4094
  Функция: настройка запрещенных VLAN для порта. После установки этого параметра для порта порт никогда не станет портом-членом VLAN, включая динамически зарегистрированную VLAN через GVRP. Если для этого параметра установлено несколько VLAN, вы можете разделить VLAN запятой (,) и тире (-), где тире используется для разделения двух последовательных идентификаторов VLAN, а запятая используется для разделения двух непоследовательных VLAN. идентификаторы.

Просмотрите все созданные VLAN и участников портов, как показано на рисунке 163.

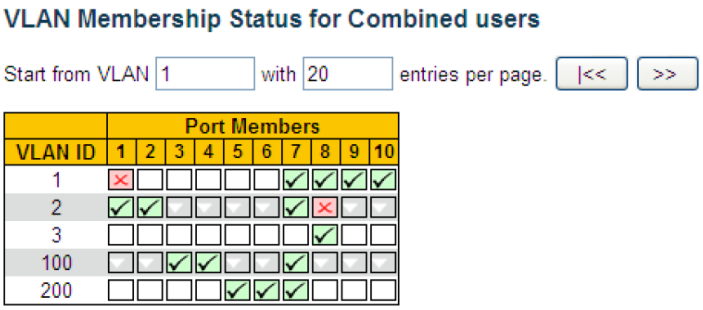
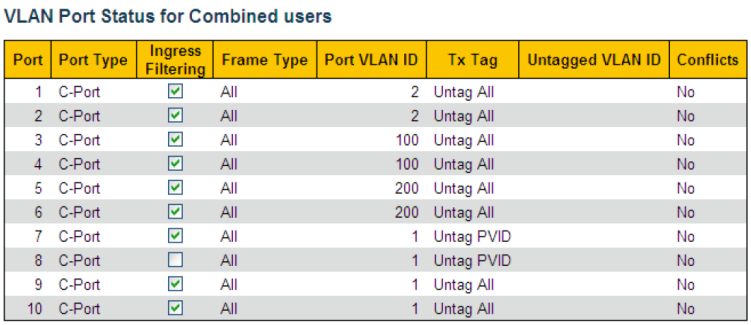


Рисунок 163 Просмотр всех созданных VLAN

✓ указывает, что порт является портом-членом текущей VLAN; X указывает, что текущая VLAN принадлежит к запрещенным VLAN порта. На каждой странице может отображаться от 1 до 99 записей VLAN, а по умолчанию отображается 20 записей VLAN.

Вы можете указать идентификатор первой записи VLAN на первой странице.

Просмотрите конфигурацию порта VLAN, как показано на рисунке 164.



Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	☑	All	2	Untag All		No
2	C-Port	☑	All	2	Untag All		No
3	C-Port	☑	All	100	Untag All		No
4	C-Port	☑	All	100	Untag All		No
5	C-Port	☑	All	200	Untag All		No
6	C-Port	☑	All	200	Untag All		No
7	C-Port	☑	All	1	Untag PVID		No
8	C-Port	☐	All	1	Untag PVID		No
9	C-Port	☑	All	1	Untag All		No
10	C-Port	☑	All	1	Untag All		No

Рисунок 164 Просмотр конфигурацию порта VLAN

17.2. Конфигурирование PVLAN

PVLAN (частная VLAN) использует двухуровневые технологии изоляции для реализации сложной функции изоляции трафика порта, обеспечивая сетевую безопасность и изоляцию широковещательного домена.

Верхняя VLAN — это VLAN общего домена, в которой порты являются портами восходящей линии связи. Нижние сети VLAN представляют собой изолированные домены, 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. Домены изоляции не могут взаимодействовать друг с другом.

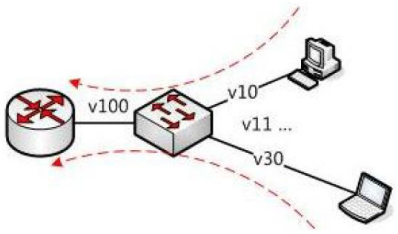


Рисунок 165 PVLAN

Как показано на рисунке 165, общий домен — это VLAN100, изолированные домены — VLAN 10 и VLAN 30; устройство в изолированных доменах может взаимодействовать с устройством в общем домене, например, VLAN 10 может взаимодействовать с VLAN 100; VLAN 30 также может взаимодействовать с VLAN 100, но устройство в разных доменах не может работать. Получение данных друг с другом, например, VLAN 10 не может получить данные с VLAN 30.

Функцию PVLAN можно реализовать посредством специальной настройки портов.

- ✓ PVID портов восходящей линии связи совпадает с идентификатором VLAN общего домена; PVID нисходящей линии связи порты совпадают с идентификатором VLAN их собственного домена изоляции.
- ✓ Порты восходящей линии связи настроены на гибридный режим и назначены общим VLAN домена и всем изолированные домены; порты нисходящей линии связи настроены на гибридный режим и назначены виртуальной локальной сети общего домена и собственному домену изоляции.
- ✓ Пакеты, отправленные портами-членами PVLAN, не имеют тегов.

17.3. GVRP

Протокол регистрации общих атрибутов (GARP) используется для распространения, регистрации и отмены определенной информации (VLAN, адрес многоадресной рассылки) между коммутаторами в одной сети.

При использовании GARP информация о конфигурации члена GARP будет распространяться на всю коммутационную сеть. Член GARP инструктирует других членов GARP зарегистрировать или отменить свою собственную конфигурационную информацию посредством сообщения о присоединении/выходе соответственно. Участник также регистрирует или отменяет информацию о конфигурации других участников на основе сообщений 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 отменить свою собственную информацию о других коммутаторах, объект отправляет сообщение Leave.

После запуска объекта GARP он запускает таймер LeaveAll. По истечении времени таймера сущность отправляет сообщение LeaveAll.

Таймеры GARP включают таймер удержания, таймер присоединения, таймер выхода, таймер выхода из всех.

Таймер удержания: когда коммутатор с поддержкой GARP получает сообщение о регистрации, он запускает таймер удержания, а не немедленно отправляет сообщение о присоединении. Когда таймер удержания истечет, он поместит всю регистрационную информацию, полученную за это время, в одно сообщение о присоединении и отправит его, уменьшив количество сообщений для стабильности сети.

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

Таймер выхода: когда коммутатор с поддержкой GARP желает, чтобы другие коммутаторы аннулировали информацию его атрибута, он отправляет сообщение Leave. Другие коммутаторы с поддержкой GARP, получившие это сообщение, активируют таймер выхода. Если они не получат сообщение о присоединении до истечения времени таймера, они аннулируют эту информацию атрибута.

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

GVRP (Протокол регистрации VLAN GARP) — это приложение GARP, основанное на рабочем механизме GARP для поддержания информации о динамической регистрации VLAN устройства и распространения этой информации на другие устройства.

Устройство с поддержкой GVRP может получать информацию о регистрации VLAN от других устройств и динамически обновлять информацию о регистрации локальной VLAN, а устройство может распространять информацию о регистрации локальной VLAN на другие устройства, обеспечивая согласованность информации VLAN на всех устройствах в одной и той же локальной сети. Информация о регистрации VLAN, распространяемая GVRP, содержит не только информацию о локальной статической регистрации, настроенную вручную, но также информацию о динамической регистрации от других устройств.

17.3.1. Веб конфигрирование

Включите протокол GVRP и установите соответствующие таймеры, как показано на рисунке 166.

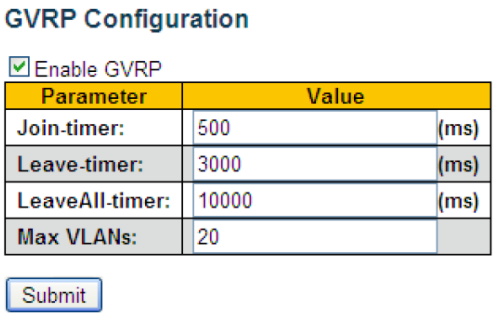


Рисунок 166 Конфигурирование протокола GVRP

- **Enable GVRP**
  Опции: Включить/Отключить.
  По умолчанию: Отключить
  Функция: включить/отключить протокол GVRP.
- **Join-timer**
  Диапазон: 100 мс~327600 мс
  По умолчанию: 500 мс
  Функция: Настройте значение таймера соединения. Значение должно быть кратно 100.
- **Leave-timer**
  Диапазон: 100 мс~327600 мс
  По умолчанию: 3000 мс
  Функция: Настройка значения таймера уровня. Значение должно быть кратно 100.
- **LeaveAll-timer**
  Диапазон: 100 мс~327600 мс
  По умолчанию: 10000 мс
  Функция: настройка значения таймера отпуска. Значение должно быть кратно 100.
  Объяснение: Если время ожидания таймеров LeaveAll на разных устройствах истекает одновременно, устройства одновременно отправят сообщение LeaveAll, что увеличит количество сообщений. Чтобы избежать этого, фактическое время работы таймера LeaveAll является случайным значением и превышает время одного таймера LeaveAll и менее чем в 1,5 раза больше времени таймера LeaveAll.
- **Max VLANs**
  Диапазон: 1~4094
  По умолчанию: 20
  Функция: установите максимальное количество сетей VLAN, динамически регистрируемых на порте GVRP. Для настройки этого параметра необходимо отключить функцию GVRP.

Настройте порт GVRP, как показано на рисунке 167.

Рисунок 167 Конфигурирование порта GVRP

- **Mode**
  Опции: включено/выключено.
  По умолчанию: отключено
  Функция: Включение/выключение функции GVRP порта.

  Отобразите статически настроенную и динамически зарегистрированную информацию о VLAN, как показано на рисунке 168.

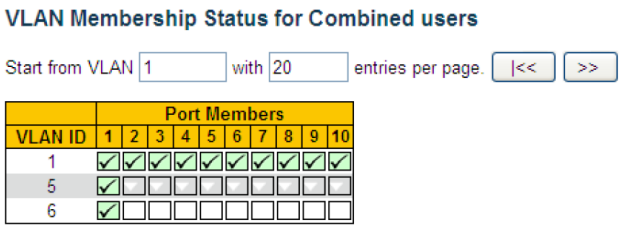


Рисунок 168 Информация о VLAN

18. Резервирование

18.1. ST-RING

ST-Ring и ST-Ring+ — это собственные протоколы резервирования ООО «СТЭ». Они позволяют сети восстанавливаться в течение 50 мс в случае сбоя соединения, 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 нельзя использовать вместе.

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

Ведомое устройство: кольцо может включать в себя несколько подчиненных устройств. Ведомые 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.

Главный резервный порт: если кольцо имеет несколько резервных портов, резервный порт с большим MAC-адресом является главным резервным портом. Он находится в состоянии пересылки.

Подчиненный резервный порт: если в кольце имеется несколько резервных портов, все резервные порты, кроме главного резервного порта, являются подчиненными резервными портами. Они находятся в состоянии блокировки.

Состояние пересылки. Если порт находится в состоянии пересылки, он может как получать, так и отправлять данные.

Состояние блокировки: если порт находится в состоянии блокировки, он может принимать и пересылать только пакеты протокола ST-Ring, но не другие пакеты.

18.1.1. ST-Ring-Port

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

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

1. Настройте коммутатор A в качестве ведущего, а остальные коммутаторы в качестве ведомых.

2. Кольцевой порт 1 на ведущем устройстве находится в состоянии пересылки, а кольцевой порт 2 — в состоянии блокировки. Оба порта ведомого устройства находятся в состоянии пересылки.

3. Если линк-CD неисправен, как показано на рисунке 169.

а) Когда канал CD неисправен, порты 6 и 7 на ведомом устройстве находятся в состоянии блокировки. Порт 2 ведущего устройства переходит в состояние пересылки, обеспечивая нормальную связь.

б) Когда неисправность устранена, порт 6 и порт 7 ведомого устройства находятся в состоянии пересылки. Порт 2 ведущего устройства переходит в состояние блокировки. Происходит переключение каналов, и каналы восстанавливаются до состояния, существовавшего до неисправности компакт-диска.

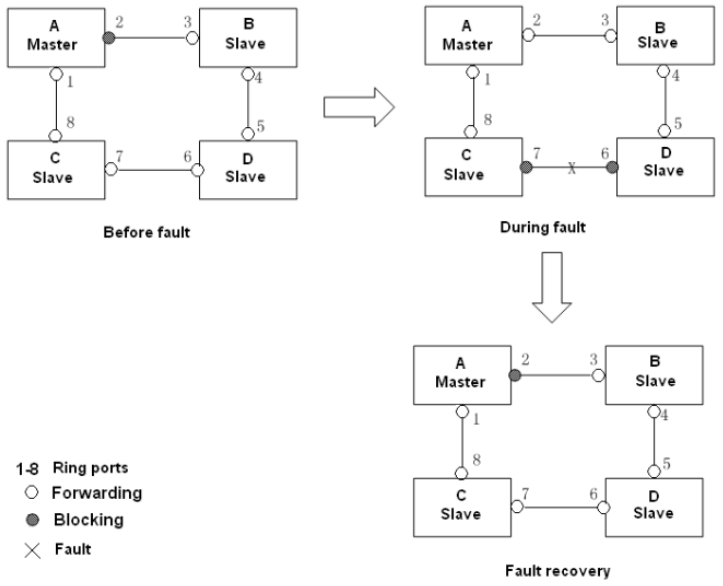


Рисунок 169 неисправность канала CD

4. Если линия AC неисправна, как показано на рисунке 170.

а) Когда канал AC неисправен, порт 1 находится в состоянии блокировки, а порт 2 переходит в состояние пересылки, обеспечивая нормальную связь по каналу.

б) После устранения неисправности порт 1 все еще находится в состоянии блокировки, а порт 8 — в состоянии пересылки. Никакого переключения не происходит.

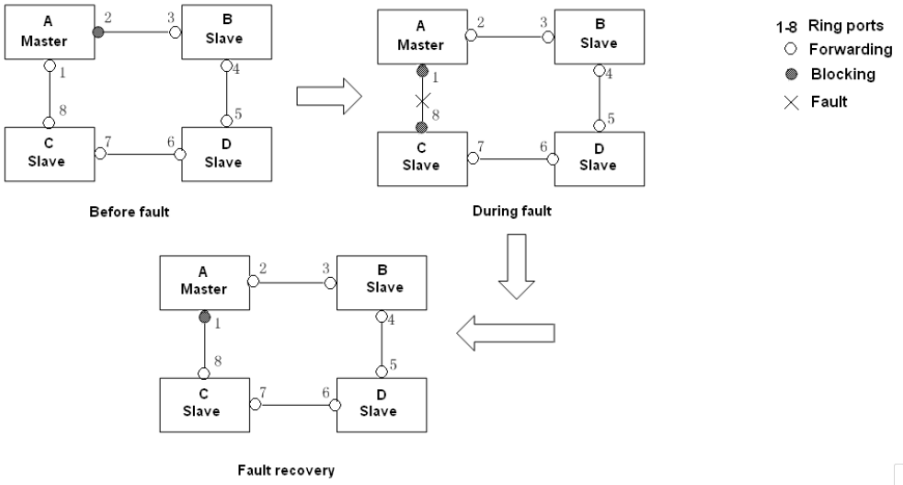


Рисунок 170 ST-RING неисправнось канала

18.1.2. ST-Ring –VLAN

ST-Ring-VLAN позволяет пересылать пакеты из разных VLAN по разным путям. Каждый путь пересылки для VLAN образует ST-Ring-VLAN.

Разные кольца ST-VLAN могут иметь разных мастеров. Как показано на рисунке 171, настроены две сети ST-Ring-VLAN.

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

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

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

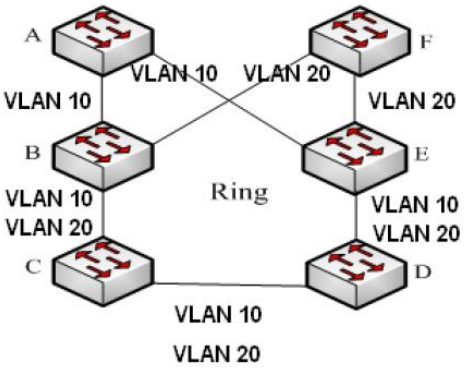


Рисунок 171 ST-RING-VLAN

18.1.3. ST-Ring+

ST-Ring+ может обеспечить резервное копирование для двух колец ST, как показано на рисунке 172. Один резервный порт настроен соответственно на коммутаторе C и коммутаторе D. Какой порт является главным резервным портом, зависит от MAC-адресов двух портов. В случае сбоя главного резервного порта или его канала подчиненный резервный порт будет пересылать пакеты, предотвращая образование петель и обеспечивая нормальную связь между резервными кольцами.

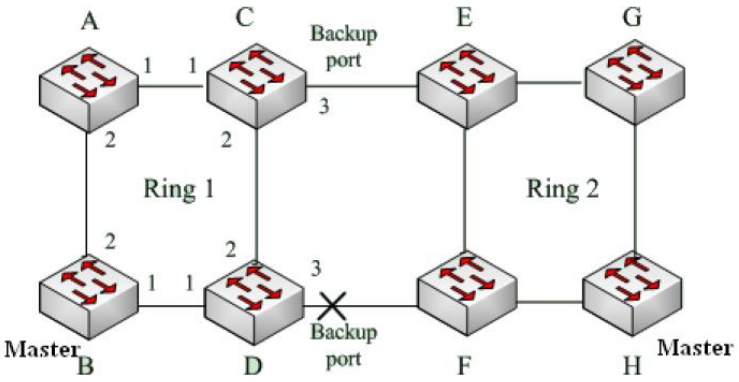


Рисунок 172 ST-RING+ топология

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 устройств.
- ✓ На каждом коммутаторе для кольца можно настроить только два порта.
- ✓ Для двух соединенных колец резервные порты можно настроить только в одном кольце.
- ✓ В одном кольце можно настроить максимум два резервных порта.
- ✓ На коммутаторе для одного кольца можно настроить только один резервный порт.
- ✓ ST-Ring-Port и ST-Ring-VLAN нельзя настроить на одном коммутаторе одновременно.

18.1.4. Веб конфигурирование

Настройте режим резервного кольца ST-Ring, как показано на рисунке 173.

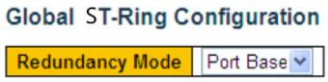


Рисунок 173 Конфигурация резервного кольцевого режима

- **Redundancy Mode**
  Варианты: на основе порта/на основе Vlan
  По умолчанию: на основе порта
  Функция: выберите режим резервного звонка ST-Ring.

Настройте ST-Ring-Port и ST-Ring-VLAN, как показано на рисунках 174 и 175.

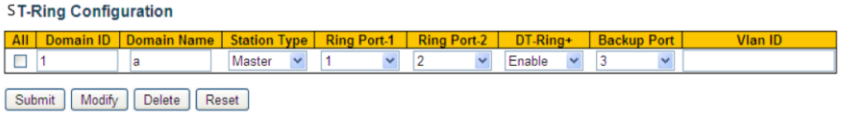


Рисунок 174 Конфигурация ST-Ring-Port

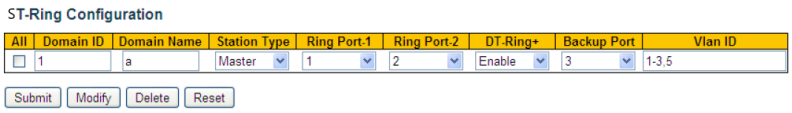


Рисунок 175 Конфигурация ST-Ring-VLAN

- **Domain ID**
  Диапазон: 1~32
  Функция: Идентификатор домена используется для различения разных колец. Один коммутатор поддерживает максимум 16 колец на базе VLAN, количество колец на основе портов зависит от количества портов коммутатора.
- **Domain Name**
  Диапазон: 1~31 символ
  Функция: Настройка доменного имени.
- **Station Type**
  Опции: Главный/Подчиненный
  По умолчанию: Мастер
  Функция: выберите роль коммутатора в кольце.
- **Ring Port-1/Ring Port-2**
  Опции: все порты коммутатора
  Функция: выберите два кольцевых порта.
- **ST-RING+**
  Опции: Включить/Отключить.
  По умолчанию: Отключить
  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.
- **VLAN ID**
  Опции: все созданные VLAN.
  Функция: выберите сети VLAN для кольцевого порта. При наличии нескольких VLAN их можно разделить запятой (,) и тире (-), где тире используется для разделения двух последовательных идентификаторов VLAN, а запятая используется для разделения двух непоследовательных идентификаторов VLAN.

Просмотрите и измените конфигурацию ST-Ring, как показано на рисунке 176.

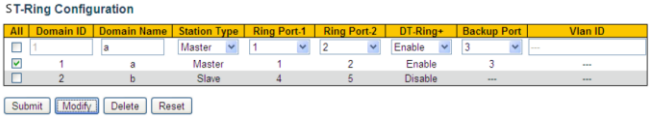


Рисунок 176 ST-Ring конфигурация

Выберите запись ST-Ring, нажмите <Modify>, чтобы отредактировать конфигурацию записи ST-Ring; нажмите <Delete> для удаления назначенной записи ST-Ring.

Щелкните запись ST-Ring на рисунке 176, чтобы отобразить состояние ST-Ring и порта, как показано на рисунке 177.

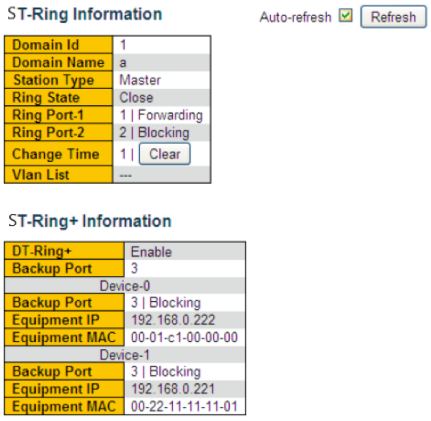


Рисунок 177 ST-Ring состояние

18.2. DRP

Протокол распределенного резервирования (DRP) разработан для передачи данных в сетях с кольцевой топологией. Это может предотвратить широковещательные штормы в кольцевых сетях. Если 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 ведущего устройства без фиксированного ведущего устройства. DRP предоставляет следующие возможности:

- Время восстановления, не зависящее от масштаба сети

DRP обеспечивает время восстановления, независимое от масштаба сети, за счет оптимизации механизма пересылки пакетов обнаружения кольца. DRP позволяет сетям восстанавливаться в течение 20 мс за счет прерывания отчетности в реальном времени, что повышает надежность передачи данных в реальном времени. Эта функция позволяет коммутаторам обеспечивать более высокую надежность приложений - в энергетике, железнодорожном транспорте и многих других отраслях, требующих контроля в режиме реального времени.

- Разнообразные функции обнаружения ссылок

Чтобы повысить стабильность сети, DRP предоставляет разнообразные функции обнаружения каналов для типичных сетевых сбоев, включая обнаружение быстрого отключения, обнаружение однонаправленного оптоволоконного канала, проверку качества канала и проверку работоспособности оборудования, обеспечивая правильную передачу данных.

- Применимо к нескольким сетевым топологиям

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

- Мощные функции диагностики и обслуживания

DRP предоставляет мощные механизмы запроса состояния и сигнализации для диагностики и обслуживания сети, а также механизм предотвращения непреднамеренных операций и неправильных конфигураций, которые могут привести к кольцевым сетевым штормам.

Режимы DRP

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

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

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

Статусы портов DRP

Состояние пересылки: если порт находится в состоянии пересылки, он может получать и пересылать пакеты данных.

Состояние блокировки: если порт находится в состоянии блокировки, он может получать и пересылать пакеты DRP, но не другие пакеты данных.

Первичный порт: указывает порт кольца (корневой), статус которого настроен пользователем как принудительная пересылка при замыкании кольца.

Роли DRP

DRP определяет роли коммутаторов путем пересылки пакетов Announce, предотвращая образование петель резервными кольцами.

INIT: указывает устройство, на котором включено DRP, а два кольцевых порта находятся в состоянии «Соединение отключено». Корневой: указывает устройство, на котором включено DRP и по крайней мере один кольцевой порт находится в состоянии соединения. В кольце корень выбирается в соответствии с векторами пакетов Announce. Это может измениться в зависимости от топологии сети. Root периодически отправляет свои собственные пакеты Announce другим устройствам. Статусы кольцевых портов: один кольцевой порт находится в состоянии пересылки, а другой — в состоянии блокировки. При получении пакета Announce от другого устройства корневой узел 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 включено DRP, отвечающее хотя бы одному из следующих условий: один кольцевой порт находится в состоянии Link up, а другой — в Link down, ухудшение CRC, приоритет не менее 200. B-Root сравнивает и пересылает пакеты Announce. Если вектор полученного пакета объявления меньше вектора его собственного пакета объявления, B-Root меняет свою роль на Root; в противном случае он пересылает полученный пакет и не меняет свою роль. Статусы кольцевых портов: Один кольцевой порт находится в состоянии пересылки.

Нормальный: указывает на устройство, на котором включено DRP, и оба кольцевых порта находятся в состоянии соединения без ухудшения CRC и приоритета больше 200. Нормальный режим только пересылает пакеты Announce, но не проверяет содержимое пакетов.

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

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

Вектор пакета Announce содержит следующую информацию для назначения ролей.

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

Таблица 4 Вектор пакета Announce

Статус канала: значение устанавливается равным 1, если один кольцевой порт находится в состоянии «Соединение отключено», и равно 0, если оба кольцевых порта находятся в состоянии «Соединение установлено».

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

Скорость ухудшения CRC: соотношение количества пакетов CRC и порога в 15 минут.

Приоритет роли: значение можно установить в веб-интерфейсе.

Параметры в Таблице 4 сравниваются в следующей процедуре:

1. Сначала проверяется значение статуса ссылки. Устройство с большим значением статуса связи

считается имеющим больший вектор.

2. Если два сравниваемых устройства имеют одинаковое значение статуса соединения, значения CRC

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

3. Если два сравниваемых устройства имеют одинаковое значение состояния канала и значение ухудшения CRC, значения приоритета роли, IP-адреса и MAC-адреса сравниваются последовательно. Считается, что устройство с большим значением имеет больший вектор.

4. Устройство с большим вектором выбирается корневым.

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

1. При запуске все переключатели находятся в состоянии INIT. Когда состояние одного порта меняется на Link up,

коммутатор становится корневым и отправляет пакеты Announce другим коммутаторам в кольце для выбора.

2. Коммутатор с наибольшим вектором пакета Announce выбирается корневым. Кольцевой порт, который первым подключается к корневому порту, находится в состоянии пересылки, а другой кольцевой порт находится в состоянии блокировки. Среди других коммутаторов в кольце коммутатор с одним кольцевым портом в состоянии «Link down» или «CRC ухудшен» является B-Root. Коммутатор, у которого оба кольцевых порта находятся в состоянии соединения и без ухудшения CRC, является нормальным.

Процедура устранения неисправности показана на следующем рисунке:

1. В исходной топологии A является корнем; порт 1 находится в состоянии пересылки, а порт 2 — в состоянии блокировки. B, C и D являются нормальными, а их кольцевые порты находятся в состоянии пересылки.

2. При неисправности link CD DRP меняет статус порта 6 и порта 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 у A, потому что порт 7 и порт 6 находятся в состоянии «Соединение отключено». В этом случае, если вектор D больше, чем вектор C, D выбирается как корень, а C становится B-корнем. При получении пакета Announce D,

A обнаруживает, что вектор D больше, чем его собственный вектор, и оба его кольцевых порта находятся в состоянии соединения. Таким образом, A становится нормальным и меняет статус порта 2 на пересылку.

3. Когда канал CD восстанавливается, D по-прежнему является корневым, поскольку его вектор больше, чем вектор C.

- Если основной порт не настроен на D, порт 7 все еще находится в состоянии блокировки, а порт 8 находится в состоянии блокировки состояние пересылки.
- Если порт 7 на D настроен как основной порт, порт 7 переходит в состояние пересылки, а порт 8находится в состоянии блокировки DRP меняет состояние порта 6 на пересылку. В результате C становится Нормальным. Поэтому, роли переключателей не меняются при восстановлении канала.

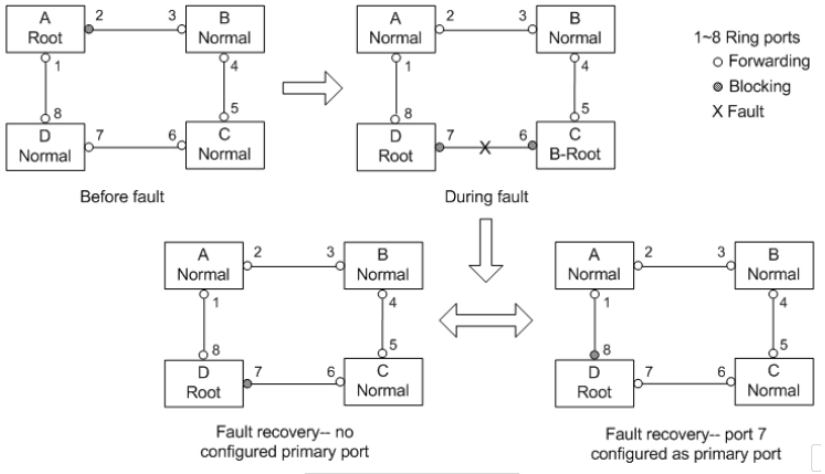


Рисунок 178 DRP разрыв канала

- Реализация режима DRP-VLAN-Based.

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

Кольцевые каналы DRP-VLAN10/20 на базе: AB-BC-CD-DE-EA.

Кольцевые каналы DRP-VLAN30 на базе: FB-BC-CD-DE-EF.

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

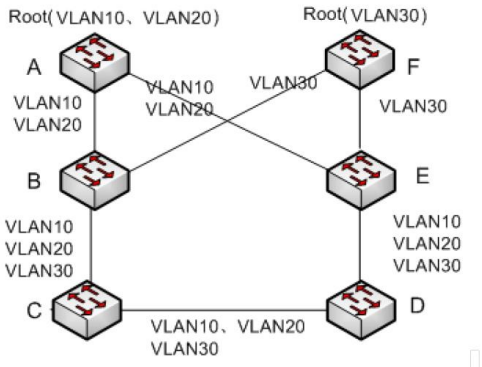


Рисунок 179 DRP-VLAN-Based

- Резервное копирование DRP

DRP также может обеспечить резервное копирование для двух колец DRP, предотвращая образование петель и обеспечивая нормальную связь между кольцами. Резервный порт: указывает порт связи между кольцами DRP. Можно настроить несколько резервных портов, но они должны находиться в одном кольце. Первый резервный порт,

который подключается, является главным резервным портом, который находится в состоянии пересылки. Все остальные резервные порты являются подчиненными. Они находятся в состоянии блокировки. Как показано на рис. 180, 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.

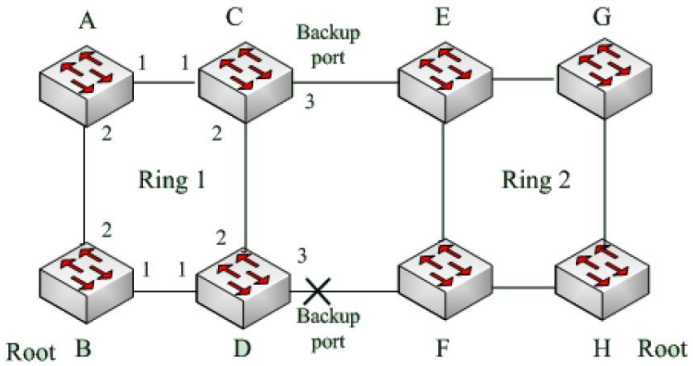


Рисунок 180 Резервное копирование DRP

18.3. DHP

Как показано на рисунке 181, A, B, C и D крепятся к кольцу. Протокол двойного подключения (DHP) выполняет следующие функции, если он включен на A, B, C и D:

- A, B, C и D могут взаимодействовать друг с другом, не влияя на правильную работу устройства в кольце.
- Если связь между A и B неисправна, A все равно может связываться с B, C и D посредством Устройство 1 и Устройство 2.

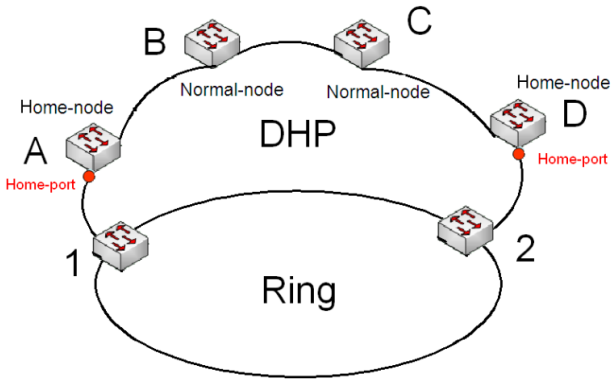


Рисунок 181 DHP

Реализация DHP основана на DRP. Механизм выбора и назначения ролей в DHP такой же, как и в DRP. DHP обеспечивает резервное копирование канала посредством настройки домашнего узла, обычного узла и домашнего порта.

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

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

- Отправка ответных пакетов корневому серверу при получении пакетов Announce от корневого узла. Корневой узел определяет состояние кольца как закрытое, если получает ответные пакеты. Если корневой узел не получает ответные пакеты, он определяет состояние кольца как открытое.
- Блокировка DRP-пакетов внешних сетей и изоляция канала DHP от внешней сети.
- Отправка пакетов очистки записи на подключенные устройства во внешних сетях при изменении топологии канала DHP.

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

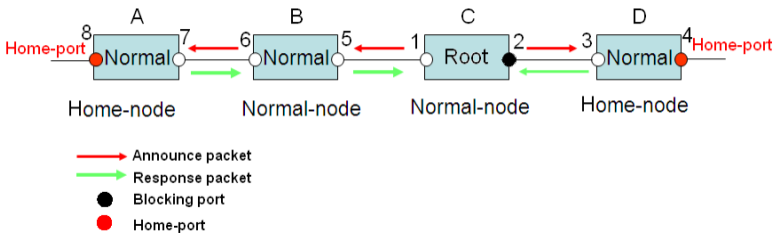


Рисунок 182 Конфигурация DHP

Как показано на рисунке 181, конфигурации A, B, C и D на рисунке 182 следующие:

- Конфигурация DRP: C — корень; порт 2 находится в состоянии блокировки; A, B и D — нормальные; все остальные кольцевые порты находятся в состоянии пересылки.
- Конфигурация DHCP: A и D — домашние узлы; порт 8 и порт 4 являются домашними портами; Б и C являются нормальными узлами.

Выполнение:

1. C, корень, отправляет пакеты Announce через два своих кольцевых порта. Домашний порт 8 и домашний порт 4 завершают полученные пакеты Announce и отправляют ответные пакеты в C. C идентифицирует состояние кольца как закрытое. Порт 2 находится в состоянии блокировки.

2. Когда канал между A и B заблокирован, топология включает два канала: A и B-C-D.

   - A избирается корневым. 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 посредством устройства 1 и устройства 2, как показано на рисунке 183.

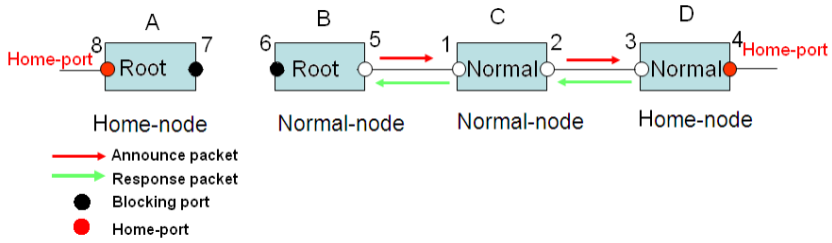


Рисунок 183 DHP разрыв канала

Конфигурации DRP отвечают следующим требованиям:

- Все коммутаторы в одном кольце должны иметь одинаковый номер домена.

- Одно кольцо содержит только один ROOT, но может содержать несколько B-ROOTs или Normals.
- На каждом коммутаторе для кольца можно настроить только два порта.
- Для двух соединенных 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.

18.3.1. Веб конфигурирование

Настройте режим резервирования DRP, как показано на рисунке 184.

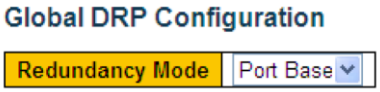


Рисунок 184 Конфигурирование DRP

- **Redundancy Mode**
  Варианты: на основе порта/на основе Vlan
  По умолчанию: на основе порта
  Функция: настройка режима резервирования DRP.

Настройте DRP-Port-Based и DRP-VLAN-Based, как показано на рисунках 185 и 186.

Рисунок 185 Конфигурирование DRP-Port-Based

Рисунок 186 Конфигурирование DRP-VLAN-Based

- **Domain ID**
  Диапазон: 1~32
  Функция: Каждое кольцо имеет уникальный идентификатор домена. Один коммутатор поддерживает максимум 8
  Кольца на основе VLAN, количество колец на основе портов зависит от количества портов коммутатора.
- **Domain Name**
  Диапазон: 1~31 символ
  Функция: Настройка доменного имени.
- **Ring Port-1/Ring Port-2**
  Опции: все порты коммутатора
  Функция: выберите два кольцевых порта.
- **Primary Port**
  Опции: --/Ring Port-1/Ring Port-2
  По умолчанию: --

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

- **DHP Mode**
  Опции: Disable/Normal-Node/Home-Node.
  По умолчанию: Отключить
  Функция: отключить DHCP или настроить режим DHCP.
- **DHP Home Port**
  Опции: Ring-Port-1/Ring-Port-2/Ring-Port-1-2
  Функция: настройка домашнего порта для домашнего узла DHP.
  Описание: Если в канале DHCP имеется только одно устройство, оба кольцевых порта домашнего узла должны быть настроены как домашние порты.
- **CRC Threshold**
  Диапазон: 25~65535
  По умолчанию: 100
  Функция: настройка порога CRC.
  Описание: Этот параметр используется при выборе корня. Система подсчитывает количество полученных CRC. Если количество CRC одного кольцевого порта превышает пороговое значение, система считает, что порт имеет ухудшение CRC. В результате значение ухудшения CRC устанавливается равным 1 в векторе пакета Announce порта.
- **Role Priority**
  Диапазон: 0~255
  По умолчанию: 128
  Функция: настройка приоритета переключателя.
- **Backup Port**
  Опции: все порты коммутатора
  Функция: Настройка резервного порта.
- **VLAN List**
  Опции: Все созданные VLAN.
  Функция: выберите сети VLAN, управляемые текущим кольцом на основе DRP-VLAN.
- **Protocol Vlan ID**
  Диапазон: 1~4093
  Описание: Идентификатор VLAN должен быть одним из служебных VLAN.
  Функция: пакеты DRP с идентификатором VLAN служат основой для диагностики и обслуживания кольца на основе DRP-VLAN.

Просмотрите и измените конфигурацию DRP, как показано на рисунке 187.

Рисунок 186 Просмотр и изменение конфигурациия DRP

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

Щелкните запись DRP на рисунке 186, чтобы отобразить состояние DRP и порта, как показано на рисунке 187.

DRP Information

Domain ID	1
Domain Name	a
Role State	ROOT
Ring State	Close
Ring Port-1	1 | FORWARD
Ring Port-2	2 | BLOCK
Primary Port	Ring Port-1
DHP Mode	Disable
DHP Home Port	---
CRC Threshold	100
Role Priority	128
Backup Port	3 | INIT

Рисунок 187 DRP статус

18.4. RSTP / STP

Протокол связующего дерева (STP), стандартизированный в IEEE802.1D, представляет собой протокол локальной сети, используемый для предотвращения широковещательных штормов, вызванных зацикливанием каналов, и обеспечения резервного копирования каналов. 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 порту приходится ждать в два раза дольше? задержка пересылки для перехода в состояние пересылки.

Чтобы преодолеть этот недостаток, IEEE создает стандарт 802.1w в дополнение к 802.1D. IEEE802.1w определяет протокол быстрого связующего дерева (RSTP). По сравнению с STP, RSTP обеспечивает гораздо более быструю конвергенцию за счет добавления альтернативного порта и резервного порта для корневого порта и назначенного порта соответственно. Если корневой порт недействителен, альтернативный порт может быстро перейти в состояние пересылки.

Root bridge: служит корнем дерева. В сети имеется только один Root bridge. Root bridge измененяется с топологией сети. Root bridge периодически отправляет BPDU другим устройствам, которые пересылают BPDU для обеспечения стабильности топологии.

Root port: указывает лучший порт для передачи от non-root bridges к Root bridge. Лучшим портом является порт с наименьшей стоимостью для Root bridge. Non-root bridges взаимодействует с Root bridge через Root port. Non-root bridges 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 Backup port корневого порта. В случае сбоя корневого порта альтернативный порт становится новым корневым портом.

Backup port: указывает Backup port назначенного порта. При выходе из строя назначенного порта Backup port становится новым назначенным портом и пересылает данные.

18.4.1. BPDU

Чтобы предотвратить образование петель, все мосты локальной сети рассчитывают связующее дерево. Процесс расчета включает передачу BPDU между устройствами для определения топологии сети. В таблице 5 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	…

Таблица 5 BPDU

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

Стоимость корневого пути: стоимость пути к корневому мосту.

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

Идентификатор назначенного порта: приоритет порта+номер порта.

Возраст сообщения: продолжительность, в течение которой BPDU может распространяться в сети.

Максимальный срок: максимальная продолжительность хранения BPDU на устройстве. Если возраст сообщения превышает максимальный возраст, BPDU отбрасывается. Время приветствия: интервал отправки BPDU. Задержка пересылки: задержка изменения статуса (отбрасывание-обучение-пересылка).

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

1. На начальном этапе

Каждый порт всех устройств генерирует BPDU, выступая в качестве корневого моста; Идентификатор корневого моста и идентификатор назначенного моста являются идентификатором локального устройства; стоимость корневого пути равна 0; назначенный порт является местным портом.

2. Выбор лучшего BPDU

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

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

Устройства сравнивают BPDU всех портов и определяют лучший BPDU. Принципы сравнение BPDU выглядит следующим образом:

- BPDU с меньшим идентификатором корневого моста имеет более высокий приоритет.
- Если идентификаторы корневого моста двух BPDU одинаковы, сравниваются стоимости их корневых путей. Чем меньше стоимость корневого пути в BPDU плюс стоимость пути локального порта, тем выше приоритет BPDU.
- Если стоимость корневого пути двух BPDU также одинакова, идентификаторы назначенного моста, идентификаторы назначенного порта и идентификаторы порта, получающего BPDU, дополнительно сравниваются

в заказ. BPDU с меньшим идентификатором имеет более высокий приоритет. BPDU с меньшим идентификатором корневого моста имеет более высокий приоритет.

3. Выбор корневого моста

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

4. Выбор корневого порта

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

5. Расчет BPDU назначенного порта

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

- Замените идентификатор корневого моста на идентификатор корневого моста BPDU корневого порта.
- Замените стоимость корневого пути на стоимость корневого пути BPDU корневого порта плюс стоимость пути.
- Замените назначенный идентификатор моста идентификатором локального устройства.
- Замените назначенный идентификатор порта идентификатором локального порта.

6. Выбор назначенного порта

Если рассчитанный BPDU лучше, то устройство выбирает порт в качестве назначенного, 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 принимать и пересылать только пакеты RSTP, но не другие пакеты.

18.4.2. Веб конфигурирование

Установите временные параметры сетевого моста, как показано на рисунке 188.

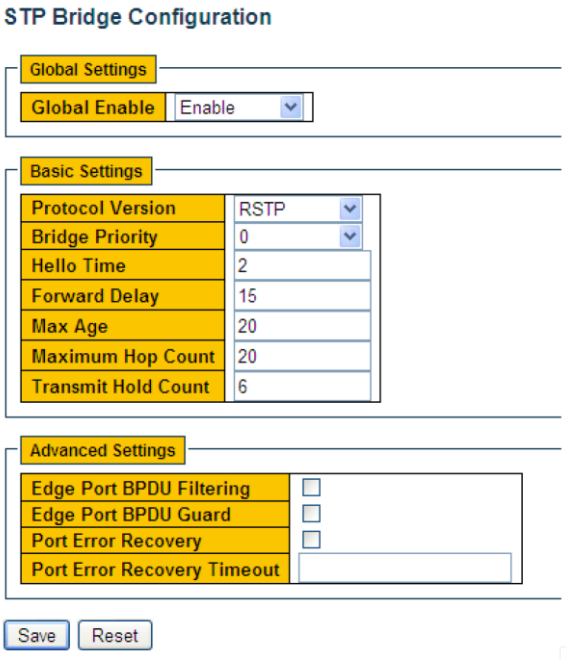


Рисунок 188 Конфигурирование временных параметров

- **Global Enable**
  Опции: Включить/Отключить.
  По умолчанию: Отключить
  Функция: отключить или включить связующее дерево.
- **Protocol Priority**
  Опции: MSTP/RSTP/STP.
  По умолчанию: MSTP
  Функция: выберите протокол связующего дерева.
- **Brigde Priority**
  Диапазон: 0~61440. 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.
- **Forward Delay**
  Диапазон: 4~30 с
  По умолчанию: 15 с.
  Функция: настройка времени изменения статуса с «Отбрасывания» на «Обучение» или с «Обучения» на «Пересылку».
- **Max Age**
  Диапазон: 6~40 с.
  По умолчанию: 20 с.
  Функция: максимальная продолжительность хранения BPDU на устройстве.
  Описание: Если значение возраста сообщения в BPDU больше указанного значения, то BPDU отбрасывается.
- **Transmit Hold Count**
  Диапазон: 1~10
  По умолчанию: 6
  Функция: Установите максимальное количество пакетов BPDU, которые может быть отправлен портом в течение каждого времени приветствия.
- **Edge Port BPDU Filtering**
  Опции: Включить/Отключить.
  По умолчанию: Отключить
  Функция: контролирует, принимает ли пограничный порт и пересылает ли пакеты BPDU.
- **Edge Port BPDU Guard**
  Опции: Включить/Отключить.
  По умолчанию: Отключить
  Функция: контролировать, переходит ли пограничный порт в состояние отключения из-за ошибки и отключается ли он.
  при получении пакетов BPDU.
- **Port Error Recovery**
  Опции: Включить/Отключить.
  По умолчанию: Отключить

Функция: контроль возможности автоматического восстановления порта из состояния ошибки в нормальное состояние.

- **Port Error Recovery Timeout**
  Диапазон: 30~86400 с
  Функция: установка времени восстановления порта из состояния ошибки в нормальное состояние.

Настройте порт RSTP, как показано на рисунке 189.

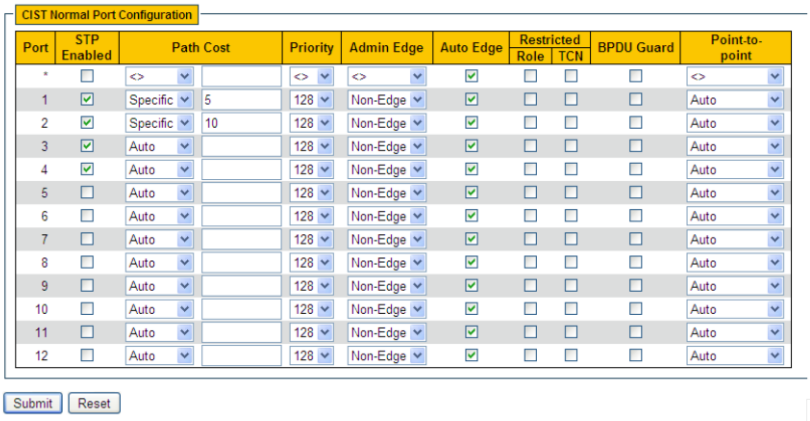


Рисунок 189 Конфигурирование порта RSTP

- **STP Enabled**
  Опции: Включить/Отключить.
  По умолчанию: Отключить
  Функция: включить или отключить STP/RSTP на портах.
- **Path Cost**
  Опции: Авто/Специальный (1~200000000)
  По умолчанию: Авто
  Описание: стоимость пути порта используется для расчета наилучшего пути. Значение параметра зависит от полосы пропускания. Чем больше значение, тем ниже стоимость. Вы можете изменить роль порта, изменив значение параметра стоимости пути. Чтобы настроить значение вручную, выберите «Нет» для параметра «Счетчик затрат».
- **Priority**
  Диапазон: 0~240. Шаг 16.
  По умолчанию: 128
  Функция: настройка приоритета порта, который определяет роли портов.
- **Admin Edge**
  Опции: без края/края
  По умолчанию: без края
  Функция: Установите, является ли текущий порт граничным портом.
  Описание: Когда порт напрямую подключен к терминалу и не подключен к другим устройствам или общему сегменту сети, порт считается пограничным портом. Граничный порт может быстро перейти из состояния блокировки в состояние пересылки без задержки ожидания. После того как пограничный порт получает пакеты BPDU, он становится неграничным портом.
- **Auto Edge**
  Опции: Включить/Отключить.
  По умолчанию: Включить

Функция: укажите, следует ли включать функцию автоматического обнаружения пограничного порта.

- **Restricted Role**
  Опции: Включить/Отключить.
  По умолчанию: Отключить
  Функция: Ограниченный порт никогда не будет выбран в качестве корневого узла, даже если ему предоставлен наивысший приоритет.
- **Restricted TCN**
  Опции: Включить/Отключить.
  По умолчанию: Отключить
  Функция: порт с ограниченным TCN не будет активно отправлять сообщения TCN.
- **BPDU Guard**
  Опции: Включить/Отключить.
  По умолчанию: Отключить
  Функция: контролирует, переходит ли пограничный порт в состояние отключения из-за ошибки и отключается ли он при получении пакетов BPDU.
- **Point-to-point**
  Варианты: Авто/Принудительно Истина/Принудительно Ложь.
  По умолчанию: Авто
  Функция: Установите тип соединения для порта. Если порт подключен к каналу «точка-точка», порт может быстро перейти в другое состояние.
  Описание: Auto указывает, что коммутатор автоматически определяет тип канала на основе состояния дуплекса порта. Когда порт работает в полнодуплексном режиме, коммутатор считает, что тип канала, подключенного к порту, — «точка-точка»; когда порт работает в полудуплексном режиме, коммутатор считает, что тип канала, подключенного к порту, является общим. Принудительное соединение «точка-точка» означает, что канал, подключенный к порту, является каналом «точка-точка», а принудительное совместное использование означает, что канал, подключенный к порту, является общим каналом.

18.5. MSTP

Хотя RSTP обеспечивает быструю конвергенцию, он, как и STP, имеет следующий недостаток: все мосты в локальной сети используют одно связующее дерево, и пакеты всех VLAN пересылаются по связующему дереву. Как показано на рисунке 190, некоторые конфигурации могут блокировать соединение между коммутатором A и коммутатором C. Поскольку коммутатор B и коммутатор D не входят в VLAN 1, они не могут пересылать пакеты VLAN 1. В результате порт VLAN 1 коммутатора A не может связаться с коммутатором C.

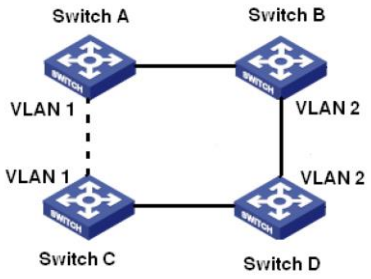


Рисунок 190 Недостаток RSTP

Чтобы решить эту проблему, был создан протокол Multiple Spanning Tree (MSTP). Это обеспечивает как быструю конвергенцию, так и отдельные пути пересылки для трафика различных VLAN, обеспечивая лучший механизм распределения нагрузки для резервных каналов.

MSTP сопоставляет одну или несколько VLAN с одним экземпляром. Коммутаторы с одинаковой конфигурацией образуют регион. Каждый регион содержит несколько взаимно независимых связующих деревьев. Регион служит узлом коммутации. Он участвует в расчетах с другими регионами на основе алгоритма связующего дерева, вычисляя общее связующее дерево. На основе этого алгоритма сеть на рисунке 230 формирует топологию, показанную на рисунке 191. И коммутатор A, и коммутатор C находятся в регионе 1. Ни одна ссылка не блокируется, поскольку в регионе нет петель. То же самое и с Регионом 2. Регион1 и Регион2 аналогичны узлам коммутатора. Эти два «переключателя» образуют петля. Поэтому ссылку следует заблокировать.

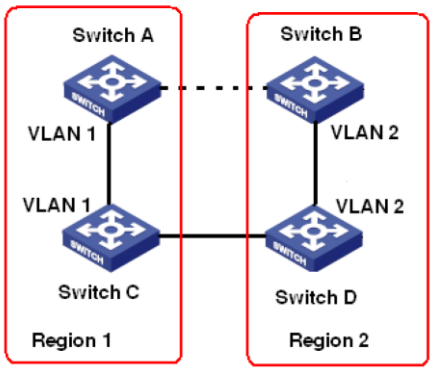


Рисунок 191 MSTP топология

Концепция MSTP представлена на рисунках 192 - 195.

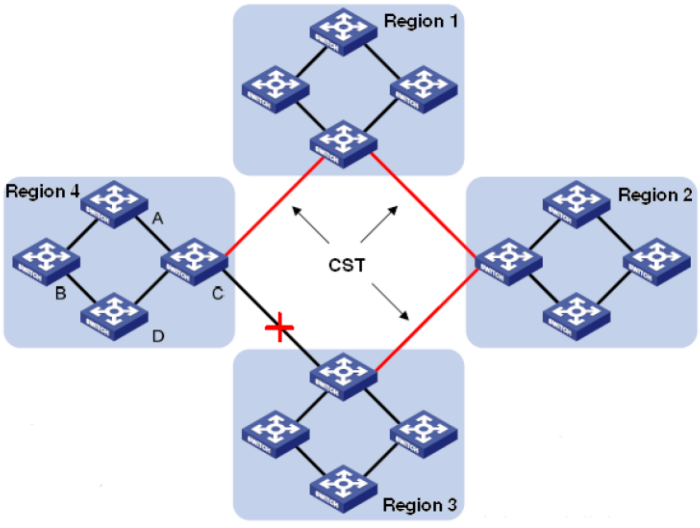


Рисунок 192 MSTP концепт

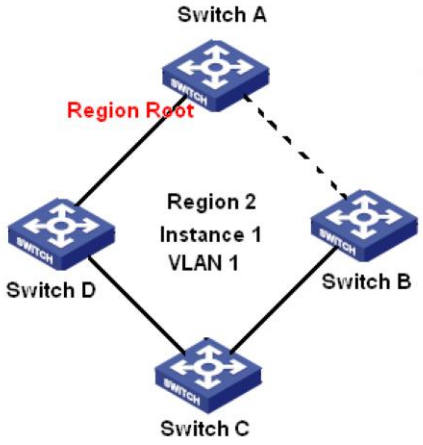


Рисунок 193 Mapping to Instance 1

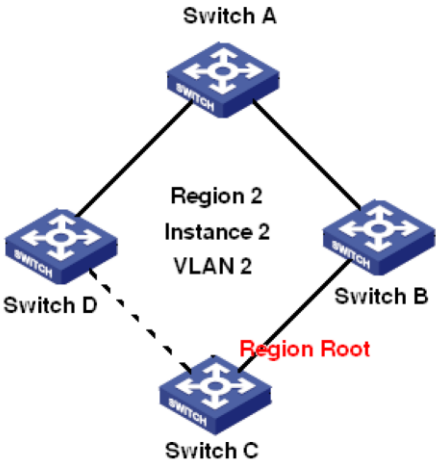


Рисунок 194 Mapping to Instance 2

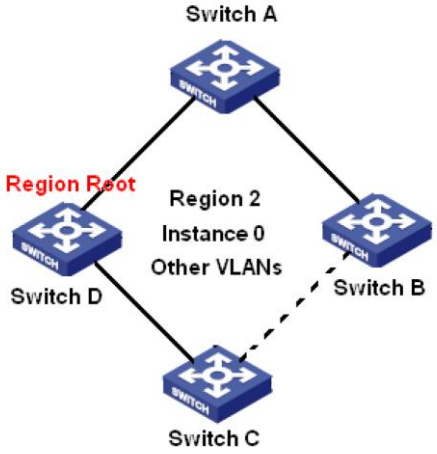


Рисунок 195 другие VLAN Mapping to Instance 0

Instance: совокупность нескольких VLAN. Одна VLAN (как показано на Рисунок 193 и Рисунок 194) или несколько сетей VLAN с одинаковой топологией (как показано на рисунке 195) могут быть сопоставлены одному экземпляру; то есть одна VLAN может формировать связующее дерево, а несколько VLAN могут совместно использовать одно связующее дерево. Разные экземпляры сопоставляются с разными связующими деревьями. Экземпляр 0 — это связующее дерево для устройств всех регионов, а остальные экземпляры — это связующее дерево для устройств определенного региона.

Множественный регион связующего дерева (region MST): Коммутаторы с одинаковым именем региона MSTP, уровнем версии и сопоставлением VLAN с экземпляром находятся в одном region MST. Как показано на рисунке 192, region1, region 2, region 3 и region 4 — это четыре разных region MST.

Таблица сопоставления VLAN: состоит из сопоставления между VLAN и связующими деревьями (Рисунок 192). Таблица сопоставления VLAN региона 2 представляет собой сопоставление между VLAN 1 и экземпляром 1, как показано на рисунке 193; VLAN 2 сопоставлена с экземпляром 2, как показано на рисунке 194. Остальные VLAN сопоставлены с экземпляром 0, как показано на рисунке 195.

Общее и внутреннее связующее дерево (CIST): указывает экземпляр 0, то есть связующее дерево, охватывающее все устройства в коммутационной сети. Как показано на рисунке 192, CIST включает IST и CST.

Внутреннее связующее дерево (IST): указывает сегмент CIST в регионе MST, то есть экземпляр 0 каждого региона, как показано на рисунке 195.

Общее связующее дерево (CST): указывает связующее дерево, соединяющее все регионы MST в коммутационной сети. Если каждый регион MST является узлом устройства, CST представляет собой связующее дерево, рассчитанное на основе STP/RSTP этими узлами устройств. Как показано на рисунке 192, красные линии обозначают связующее дерево.

MSTI (множественный экземпляр связующего дерева): один регион MST может формировать несколько связующих деревьев, и они независимы друг от друга. Каждое связующее дерево представляет собой MSTI, как показано на рисунках 193 и 194. 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 связующие деревья имеют разную топологию, и их региональные корни также могут быть разными. Как показано на рисунках 193, 194 и 195, эти три экземпляра имеют разные региональные корни. Корневой мост MSTI рассчитывается на основе STP/RSTP в текущем регионе MST. Корневой мост IST — это устройство, подключенное к другому региону MST и выбранное на основе полученной информации о приоритете.

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

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

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

Состояние обучения: указывает, что порт изучает MAC-адреса, но не пересылает трафик. Состояние отбрасывания: указывает, что порт не запоминает MAC-адреса и не пересылает трафик. Корневой порт: указывает лучший порт от некорневого моста к корневому мосту, то есть порт с наименьшей стоимостью для корневого моста. Некорневой мост взаимодействует с корневым мостом через корневой порт. Некорневой мост имеет только один корневой порт. Корневой мост не имеет корневого порта. Корневой порт может находиться в состоянии пересылки, обучения или отбрасывания.

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 отбрасывания.

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). Главный порт — это специальный граничный порт.

Это корневой порт для CIST и главный порт для других экземпляров. Главный порт может находиться в состоянии пересылки, обучения или отмены.

Альтернативный порт: указывает резервный порт корневого порта или главного порта. В случае сбоя корневого порта или главного порта альтернативный порт становится новым корневым портом или главным портом. Главный порт может находиться только в состоянии сброса.

Резервный порт: указывает резервный порт назначенного порта. В случае сбоя назначенного порта 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.

В регионе рассчитывается несколько связующих деревьев. Каждое связующее дерево представляет собой MSTI. Экземпляр 0 — это IST, а другие экземпляры — это MSTI.

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

2. Расчет MSTI

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

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

18.5.1. Веб конфигурирование

Установите временные параметры сетевого моста, как показано на рисунке 196.

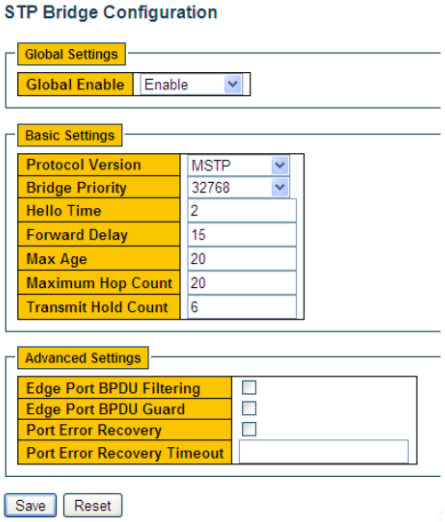


Рисунок 196 Конфигурирование временных параметров для сетевого моста

- **Global Enable**
  Опции: Включить/Отключить.
  По умолчанию: Отключить
  Функция: отключить или включить связующее дерево.
- **Protocol Priority**
  Опции: MSTP/RSTP/STP.
  По умолчанию: MSTP
  Функция: выберите протокол связующего дерева.
- **Brigde Priority**
  Диапазон: 0~61440. 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.
- **Forward Delay**
  Диапазон: 4~30 с
  По умолчанию: 15 с.
  Функция: настройка времени изменения статуса с «Отбрасывания» на «Обучение» или с «Обучения» на «Пересылку».
- **Max Age**
  Диапазон: 6~40 с.
  По умолчанию: 20 с.
  Функция: максимальная продолжительность хранения BPDU на устройстве.
  Описание: Если значение возраста сообщения в BPDU больше указанного значения, то BPDU отбрасывается.
- **Maximum Hop Count**
  Диапазон: 6~40
  По умолчанию: 20
  Функция: настройка максимального количества переходов в регионе MST. Максимальное количество переходов региона MST ограничивает масштаб региона MST; максимальное количество прыжков регионального корня равно максимальному количеству прыжков региона MST.
  Описание. Начиная с корневого моста связующего дерева в регионе MST, из номера перехода вычитается 1, когда BPDU проходит через устройство в регионе. Устройство удаляет BPDU с номером перехода 0.
- **Transmit Hold Count**
  Диапазон: 1~10
  По умолчанию: 6
  Функция: Установите максимальное количество пакетов BPDU, которые может быть отправлен портом в течение каждого времени приветствия.
- **Edge Port BPDU Filtering**
  Опции: Включить/Отключить.
  По умолчанию: Отключить
  Функция: контролирует, принимает ли пограничный порт и пересылает ли пакеты BPDU.

- **Edge Port BPDU Guard**
  Опции: Включить/Отключить.
  По умолчанию: Отключить
  Функция: контролирует, переходит ли пограничный порт в состояние отключения из-за ошибки и отключается ли он при получении пакетов BPDU.
- **Port Error Recovery**
  Опции: Включить/Отключить.
  По умолчанию: Отключить
  Функция: контроль возможности автоматического восстановления порта из состояния ошибки в нормальное состояние.
- **Port Error Recovery Timeout**
  Диапазон: 30~86400 с
  Функция: установка времени восстановления порта из состояния ошибки в нормальное состояние.

Настройте сопоставление MSTI, как показано на рисунке 197.

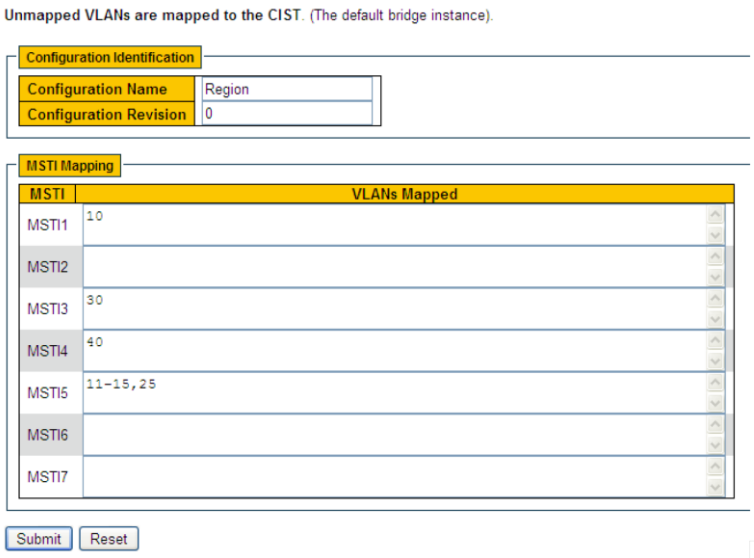


Рисунок 197 Конфигурирование сопоставление MSTI

- **Configuration Name**
  Диапазон: 1–32 символа
  По умолчанию: MAC-адрес устройства.
  Функция: Настройте имя региона MST.
- **Configuration Revision**
  Опции: 0~65535.
  По умолчанию: 0
  Функция: настройка параметра ревизии региона MSTP.
  Описание: параметр версии, имя региона MST и таблица сопоставления VLAN кодируют регион MST, к которому принадлежит устройство. Если все конфигурации одинаковы,
  устройства находятся в одном регионе MST.
- **VLANs Mapped**
  Диапазон: 1~4094
  Функция: настройка таблицы сопоставления VLAN в регионе MST. При наличии нескольких VLAN их можно разделить запятой (,) и тире (-), где используется тире.

для разделения двух последовательных идентификаторов VLAN, а для разделения двух непоследовательных идентификаторов VLAN используется запятая.
Описание. По умолчанию все сети VLAN сопоставляются с экземпляром 0. Одна VLAN сопоставляется только с одним экземпляром связующего дерева. Если VLAN с существующим сопоставлением сопоставлена с другим экземпляром,
предыдущее сопоставление отменяется. Если сопоставление между назначенной VLAN и экземпляром
удален, эта VLAN будет сопоставлена с экземпляром 0.

Настройте приоритет моста коммутатора в назначенном экземпляре, как показано на рисунке 198.

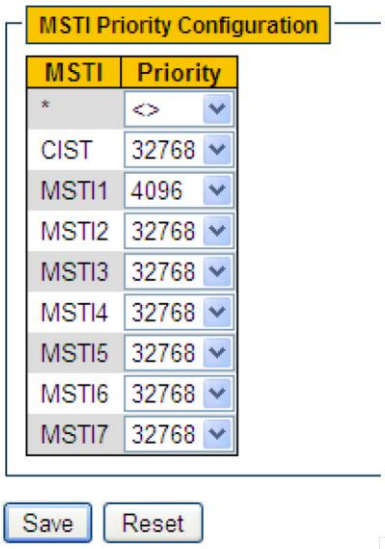


Рисунок 198 Конфигурирование приоритет моста коммутатора

- **Priority**
  Диапазон: 0~61440 с шагом 4096.
  По умолчанию: 32768
  Функция: настройка приоритета моста коммутатора в указанном экземпляре.
  Описание: Приоритет моста определяет, может ли коммутатор быть выбран региональным корнем экземпляра связующего дерева. Чем меньше значение, тем выше приоритет. Установив более низкий приоритет, определенное устройство можно назначить корневым мостом связующего дерева.
  Устройство с поддержкой MSTP можно настроить с разными приоритетами в разных экземплярах связующего дерева.
  Нажмите <Сохранить>, чтобы текущие настройки вступили в силу.

Настройте порты CIST, как показано на рисунке 199.

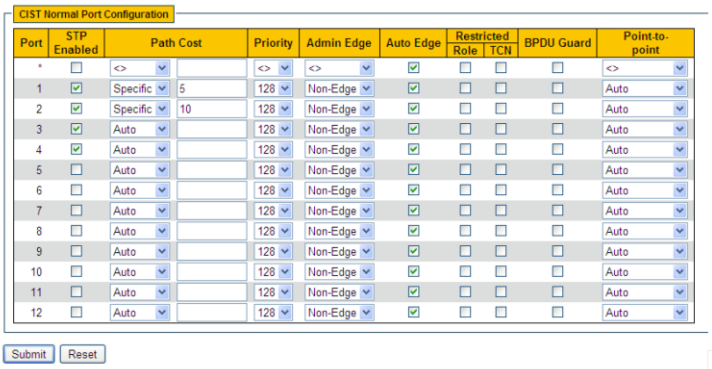


Рисунок 199 Конфигурирование CIST портов

- **STP Enabled**
  Опции: Включить/Отключить.
  По умолчанию: Отключить
  Функция: включить или отключить STP/RSTP на портах.
- **Path Cost**
  Опции: Авто/Специальный (1~200000000)
  По умолчанию: Авто
  Описание: стоимость пути порта используется для расчета наилучшего пути. Значение параметра зависит от полосы пропускания. Чем больше значение, тем ниже стоимость. Вы можете изменить роль порта, изменив значение параметра стоимости пути. Чтобы настроить значение вручную, выберите «Нет» для параметра «Счетчик затрат».
- **Priority**
  Диапазон: 0~240. Шаг 16.
  По умолчанию: 128
  Функция: настройка приоритета порта, который определяет роли портов.
- **Admin Edge**
  Опции: Non-Edge/Edge
  По умолчанию: Non-Edge
  Функция: Установите, является ли текущий порт граничным портом.
  Описание: Когда порт напрямую подключен к терминалу и не подключен к другим устройствам или общему сегменту сети, порт считается пограничным портом. Грань может быстро перейти из состояния блокировки в состояние пересылки без задержки ожидания. После того как пограничный порт получает пакеты BPDU, он становится неграничным портом.
- **Auto Edge**
  Опции: Включить/Отключить.
  По умолчанию: Включить
  Функция: включить ли функцию автоматического обнаружения пограничного порта.
- **Restricted Role**
  Опции: Включить/Отключить.
  По умолчанию: Отключить
  Функция: Ограниченный порт никогда не будет выбран в качестве корневого узла, даже если ему предоставлен наивысший приоритет.
- **Restricted TCN**
  Опции: Включить/Отключить.

По умолчанию: Отключить
Функция: порт с ограниченным TCN не будет активно отправлять сообщения TCN.

- **BPDU Guard**
  Опции: Включить/Отключить.
  По умолчанию: Отключить
  Функция: контролирует, переходит ли пограничный порт в состояние отключения из-за ошибки и отключается ли он при получении пакетов BPDU.
- **Point-to-point**
  Варианты: Авто/Принудительно Истина/Принудительно Ложь.
  По умолчанию: Авто
  Функция: Установите тип соединения для порта. Если порт подключен к каналу «точка-точка», порт может быстро перейти в другое состояние.
  Описание: Auto указывает, что коммутатор автоматически определяет тип канала на основе состояния дуплекса порта. Когда порт работает в полнодуплексном режиме, коммутатор считает, что тип канала, подключенного к порту, — «точка-точка»; когда порт работает в полудуплексном режиме, коммутатор считает, что тип канала, подключенного к порту, является общим. Принудительное соединение «точка-точка» означает, что канал, подключенный к порту, является каналом «точка-точка», а принудительное совместное использование означает, что канал, подключенный к порту, является общим каналом.

Настройте порты MSTI, как показано на рисунке 200.

Рисунок 200 Конфигурирование MSTI портов

- **Select MSTI**
  Диапазон: MST1~MST7
  По умолчанию: MST1
  Функция: выберите MSTI, нажмите <Get>, чтобы войти на страницу конфигурации портов MSTI, как показано на следующем рисунке.

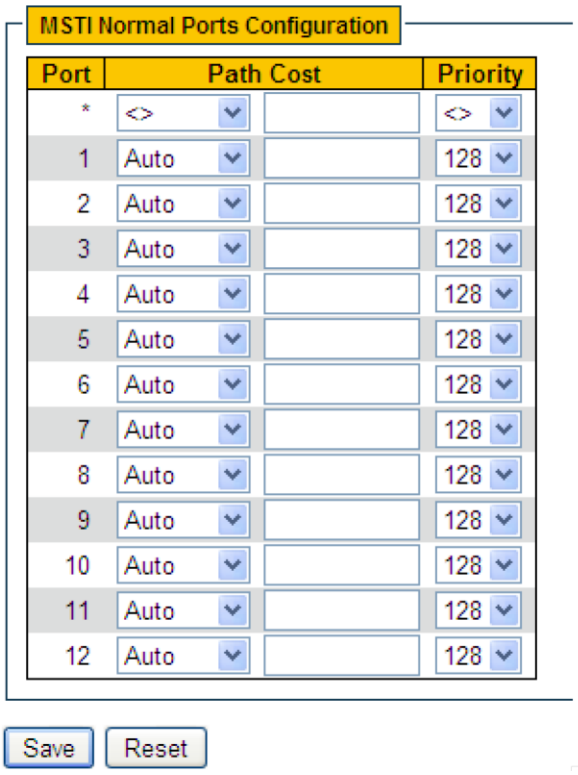


Рисунок 201 Конфигурирование MSTI портов

- **Path Cost**
  Опции: Auto/Specific (1~200000000)
  По умолчанию: Auto
  Функция: настройка стоимости пути порта в назначенном экземпляре.
  Описание: Стоимость пути к порту используется для расчета оптимального пути. Этот параметр зависит от пропускной способности. Чем больше пропускная способность, тем ниже стоимость. Изменение стоимости пути к порту может изменить путь передачи между устройством и корневым мостом, тем самым изменяя роль порта. Порт с поддержкой MSTP можно настроить с разной стоимостью пути в разных экземплярах связующего дерева.
- **Priority**
  Диапазон: 0~240. Шаг 16.
  По умолчанию: 128
  Функция: настройте приоритет порта в назначенном экземпляре.
  Описание: Приоритет порта определяет, будет ли он выбран корневым портом. В том же случае порт с более низким приоритетом будет выбран корневым портом. Порты с поддержкой MSTP могут быть настроены с разными приоритетами и играть разные роли портов в разных экземплярах связующего дерева.

Просмотрите состояние моста, как показано на рисунке 202.

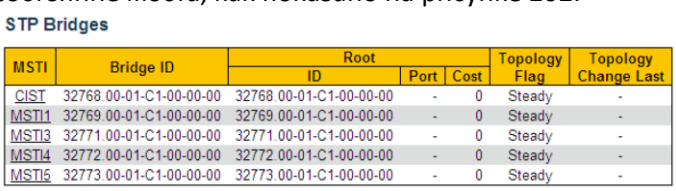
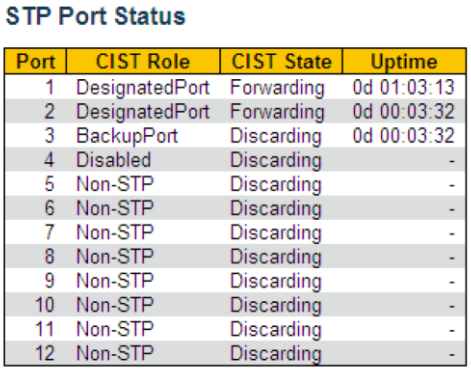


Рисунок 202 Просмотр состояние

Просмотрите состояние портов STP, как показано на рисунке 203.

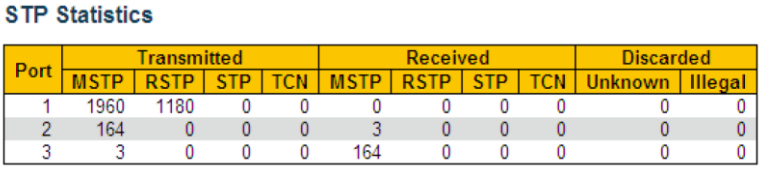


STP Port Status

Port	CIST Role	CIST State	Uptime
1	DesignatedPort	Forwarding	0d 01:03:13
2	DesignatedPort	Forwarding	0d 00:03:32
3	BackupPort	Discarding	0d 00:03:32
4	Disabled	Discarding	-
5	Non-STP	Discarding	-
6	Non-STP	Discarding	-
7	Non-STP	Discarding	-
8	Non-STP	Discarding	-
9	Non-STP	Discarding	-
10	Non-STP	Discarding	-
11	Non-STP	Discarding	-
12	Non-STP	Discarding	-

Рисунок 203 Просмотр состояние STP портов

Просмотрите статистику пакетов портов STP, как показано на рисунке 204.



STP Statistics

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1	1960	1180	0	0	0	0	0	0	0	0
2	164	0	0	0	3	0	0	0	0	0
3	3	0	0	0	164	0	0	0	0	0

Рисунок 204 Просмотр статистики STP портов

19. Alarm

Коммутаторы этой серии поддерживают следующие типы сигналов тревоги:

- Сигнализация мощности: если функция включена, сигнал тревоги будет генерироваться.
- Сигнал использования памяти/CPU: если эта функция включена, сигнал тревоги срабатывает, при превышении порога использовании CPU/памяти.
- Тревога конфликта IP/MAC: если функция включена, то для срабатывания происхоидт при конфшикте IP/MAC.
- Сигнал тревоги порта: если эта функция включена, сигнал тревоги срабатывает, когда порт находится в состоянии соединения.
- Сигнал тревоги ring: если эта функция включена, при размыкании кольца срабатывает сигнал тревоги.
- Сигнализация CRC и потери пакетов: если эта функция включена, сигнал тревоги генерируется, когда количество ошибок CRC/потеря пакетов порта превышает указанный порог.
- Сигнал скорости порта A: Если эта функция включена, сигнал тревоги генерируется, когда входящий / скорость исходящего трафика порта превышает указанный порог.
- Сигнализация питания SFP.

19.1. Веб конфигурирование

Настройте и отобразите сигнализацию питания, сигнализацию использования памяти/процессора, как показано на рисунке 205.

Alarm Configuration

Alarm Type	Enable	Threshold		Margin Value		Status
Power Alarm	☑	---		---		Power-1:Power Down | Power-2:Power On
Mem Usage Alarm	☑	85	(50~100)	5	(1~20)	Normal
CPU Usage Alarm	☑	85	(50~100)	5	(1~20)	Normal

Рисунок 205 Конфигурирование тревоги

- **Power Alarm**
  Опции: Включить/Отключить.
  По умолчанию: Отключить
  Функция: включить/отключить сигнализацию по питанию.
- **Status**
  Опции: Включение/Выключение питания.
  Описание: Включение питания означает, что питание находится в состоянии подключения и связь работает нормально. Power Down означает, что питание отключено или работает ненормально.
- **Mem/CPU Usage Alarm**
  Опции: Включить/Отключить.
  По умолчанию: Отключить
  Функция: включить/выключить сигнализацию об использовании памяти.
- **Threshold (%)**
  Диапазон: 50~100
  По умолчанию: 85
  Функция: Установите порог использования памяти/ЦП. Когда загрузка памяти/ЦП коммутатора превышает пороговое значение, генерируется сигнал тревоги.
  Размер маржи (%)
  Диапазон: 1~20
  По умолчанию: 5
  Функция: Установите значение предела использования памяти/ЦП.
  Описание: Если загрузка памяти/ЦП колеблется около порогового значения, сигналы тревоги 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 загрузка памяти/ЦП ниже порогового значения на значение поля или более. Например, порог использования памяти устанавливается
  до 60%, а значение маржи установлено на 5%. Если использование памяти коммутатора ниже или равно 60 %, сигнал тревоги не генерируется. Если использование памяти превышает 60%, будет сгенерирован сигнал тревоги. Тревога будет сброшена только в том случае, если использование памяти будет равно или ниже 55%.
- **Alarm Status**
  Опции: Нормальный/Тревога.
  Функция: просмотр состояния использования памяти/CPU коммутатора. Тревога означает, что загрузка памяти/CPU превышает пороговое значение и вызывает тревогу.

  Настройте и отобразите сигнал тревоги о конфликте IP/MAC, как показано на рисунке 206.

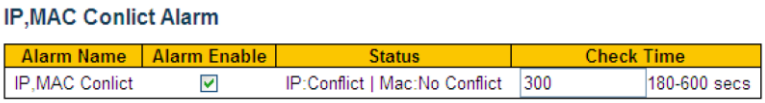


Рисунок 206 Конфигурирование сигнал тревоги о конфликте IP/MAC

- **IP, MAC Conflict**
  Опции: Включить/Отключить.
  По умолчанию: Включить
  Функция: включить/выключить сигнализацию конфликта IP/MAC.
- **Status**
  Варианты: Конфликт/Нет конфликта.
  Описание. При возникновении конфликта IP/MAC отображается сообщение «Конфликт»; в противном случае отображается сообщение «Нет конфликтов».
- **Check Time**
  Диапазон: 180~600 с
  По умолчанию: 300 с.
  Функция: настройка интервала обнаружения конфликтов IP/MAC.

Настройте и отобразите сигнал тревоги ST-Ring, как показано на рисунке 207.

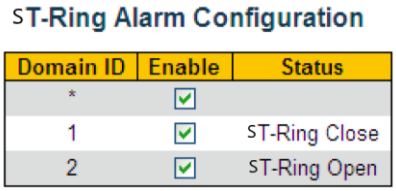


Рисунок 207 Конфигурирование сигнал тревоги ST-Ring

- **ST-Ring Alarm Configuration**
  Опции: Включить/Отключить.
  По умолчанию: Отключить
  Функция: Включение/выключение сигнала тревоги ST-Ring.
- **Status**
  Опции: ST-кольцо Close/ST-кольцо Open.
  Описание: ST-Ring Close означает, что ST-Ring закрыт. ST-Ring Open означает, что ST-Ring разомкнут или, находится в ненормальном состоянии.

Настройте и отобразите сигнал тревоги DRP, как показано на рисунке 208.

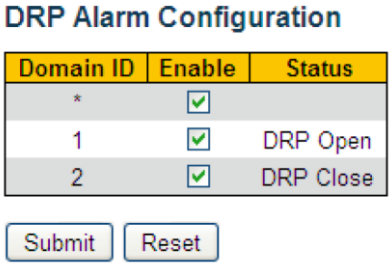


Рисунок 208 Конфигурирование сигнал тревоги DRP

DRP Alarm Configuration
Опции: отключить/включить.
По умолчанию: Отключить
Функция: Включение/выключение сигнализации DRP.

Положение дел
Опции: Закрытие DRP/Открытие DRP.
Описание: DRP Close означает, что DRP закрыт. DRP Open означает, что DRP открыт или находится в ненормальном состоянии.

Настройте и отобразите сигнал тревоги порта, как показано на рисунке 209.

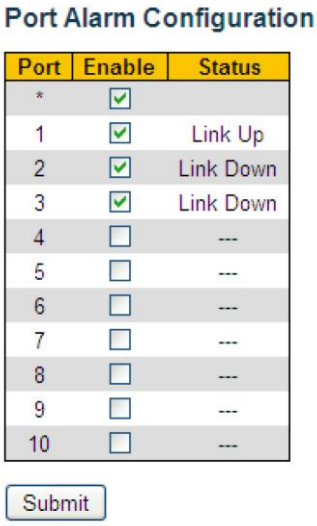


Рисунок 209 Конфигурирование сигнала тревоги порта

- **Port Alarm Configuration**
  Опции: отключить/включить.
  По умолчанию: Отключить
  Функция: Включить/отключить сигнализацию порта.
- **Status**
  Опции: соединение вверх/связь вниз.
  Описание: Link Up означает, что порт находится в состоянии подключения и поддерживает нормальную связь. Link Down означает, что порт отключен или находится в ненормальном соединении (сбой связи).

Настройте и отобразите сигнал CRC и потери пакетов, как показано на рисунке 210.

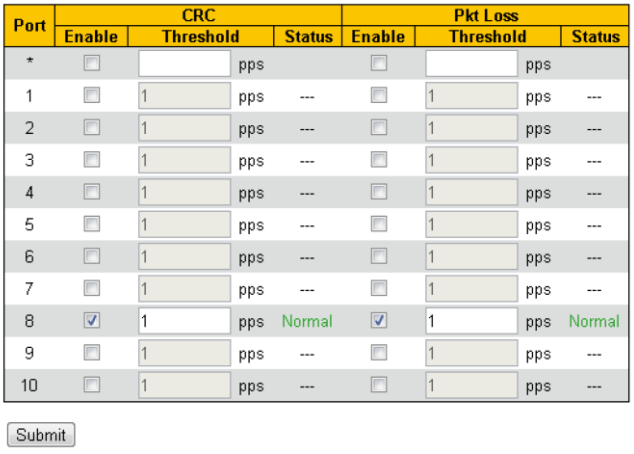


Рисунок 210 Конфигурирование сигнала тревоги CRC и потери пакетов

- **CRC/Pkt Loss Alarm**
  Опции: Включить/Отключить.
  По умолчанию: Отключить

Функция: Включение/выключение сигнала тревоги потери CRC/Pkt.

- **Threshold**
  Диапазон: от 1 до 1000000 имп./с.
  Функция: настройка порога тревоги потери CRC/Pkt порта.
- **Alarm Status**
  Опции: Тревога/Нормальный
  Функция: просмотр состояния потери CRC/Pkt порта. Сигнал тревоги означает, что потеря CRC/Pkt порта превышает пороговое значение и вызывает сигнал тревоги.

Настройте и отобразите сигнал тревоги скорости порта, как показано на рисунке 211.

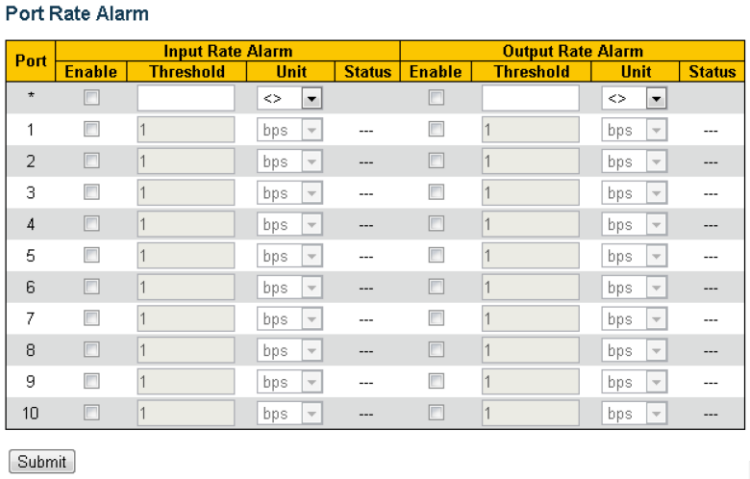


Рисунок 211 Конфигурирование сигнала тревоги скорости порта

- **input rate alarm/output rate alarm**
  Опции: Включить/Отключить.
  По умолчанию: Отключить
  Функция: включить/выключить сигнализацию о трафике порта.
- **Threshold**
  Диапазон: от 1 до 10000000000бит/с или от 1 до 1000000кбит/с.
  Функция: настройка порога трафика порта.
- **Alarm Status**
  Опции: Тревога/Нормальный
  Функция: просмотр состояния трафика порта. Тревога означает, что скорость входящего/исходящего трафика превышает пороговое значение и вызывает тревогу.

Настройте и отобразите сигнал тревоги RX Power порта SFP, как показано на рисунке 212.

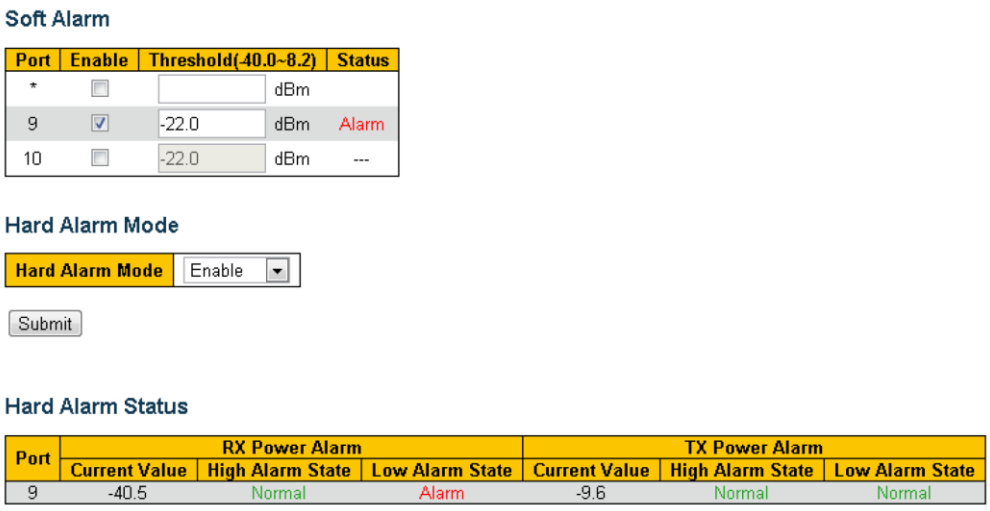


Рисунок 212 Конфигурирование сигнала тревоги SFP

- **Software Alarm**
  Опции: Включить/Отключить.
  По умолчанию: Отключить
  Функция: Включение/выключение сигнала тревоги по питанию SFP RX.
- **Threshold**
  Диапазон: -40~8,2 (единица измерения: дБм)
  По умолчанию: -22,0 дБм
  Функция: настройка порогового значения для сигнализации мощности RX порта SFP.
- **Alarm Status**
  Опции: NotSupportDDM/NotExist/Нормальный/Тревога.
  Описание: программный сигнал тревоги относится к порту, получающему сигнал тревоги оптической мощности, который требует, чтобы SFP поддерживал функцию DDM. Если SFP не вставлен в порт, состояние — NotExist. Если SFP вставлен, но DDM не поддерживается, состояние — NotSupportDDM. Если вставлен SFP с поддержкой ddm, принимаемая оптическая мощность ниже порогового значения, то будет сгенерирован сигнал тревоги, состояние — «Тревога». Если вставлен SFP с поддержкой ddm, принимаемая оптическая мощность не ниже порога, то состояние нормальное.
- **Hardware Alarm**
  Опции: Включить/Отключить.
  По умолчанию: Отключить
  Функция: включение/отключение аппаратного сигнала тревоги питания SFP.
- **Alarm Status**
  Опции: Тревога/Нормальный
  Функция: просмотр состояния аварийного сигнала оборудования питания SFP. Поддерживает сигнализацию мощности SFP Tx/Rx, но порог сигнализации мощности SFP Tx не настраивается.

20. Link check

Проверка канала предполагает периодическое взаимодействие пакетов протокола для оценки соединения канала и отображения состояния связи порта. В случае неисправности проблему можно вовремя обнаружить и устранить.

Порт, для которого включена проверка состояния канала, периодически (каждые 1 с) отправляет пакеты проверки канала для проверки состояния канала. Если порт не получает пакет проверки канала от одноранговой стороны в течение периода ожидания приема (5 с), это указывает на то, что канал ненормальный, и порт отображает состояние неисправности Rx. Если порт получает пакет проверки канала от одноранговой стороны и пакет показывает, что пакет проверки канала получен от локального устройства в течение периода ожидания приема (5 секунд), порт отображает нормальное состояние. Если порт получает пакет проверки канала от одноранговой стороны, но пакет показывает, что пакет проверки канала не получен от локального устройства в течение периода ожидания приема (5 секунд), порт отображает состояние ошибки Tx. Если соединение с портом не работает, порт отображает состояние соединения.

Порт, для которого отключена проверка состояния канала, работает в пассивном режиме. То есть он не отправляет пакет проверки канала в активном режиме. Однако после получения пакета проверки канала от одноранговой стороны этот порт немедленно возвращает пакет проверки канала, чтобы сообщить одноранговому концу, что он получил пакет проверки канала.

20.1. Веб конфигурирование

Настройте проверку канала, как показано на рисунке 213.

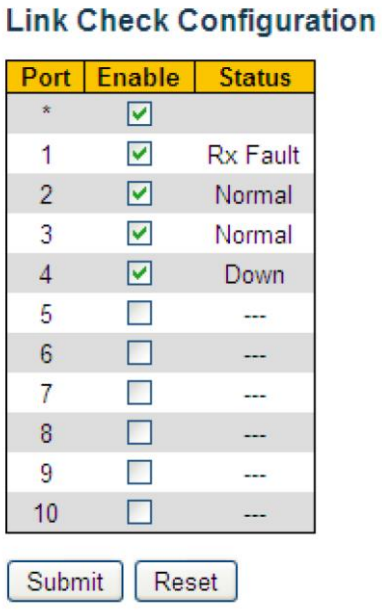


Рисунок 213 Конфигурирование проверки канала

- **Enable**
  Опции: отключить/включить.
  По умолчанию: Отключить

Функция: Включить/отключить проверку соединения на порту.
Status
Варианты: Up/Normal/--/Rx Fault/Tx Fault/Down
Описание: Если для порта включена проверка канала и порт отправляет и получает данные нормально, отображается значение «Нормальный». Если одноранговая сторона не получает пакеты обнаружения от устройства, отображается сообщение Tx Fault. Если устройство не получает пакеты обнаружения от одноранговой стороны, отображается сообщение Rx Fault. Если порт не работает, отображается сообщение «Вниз». Если проверка канала не включена для порта, отображается --. В момент включения проверки соединения на порту соединения отображается up.

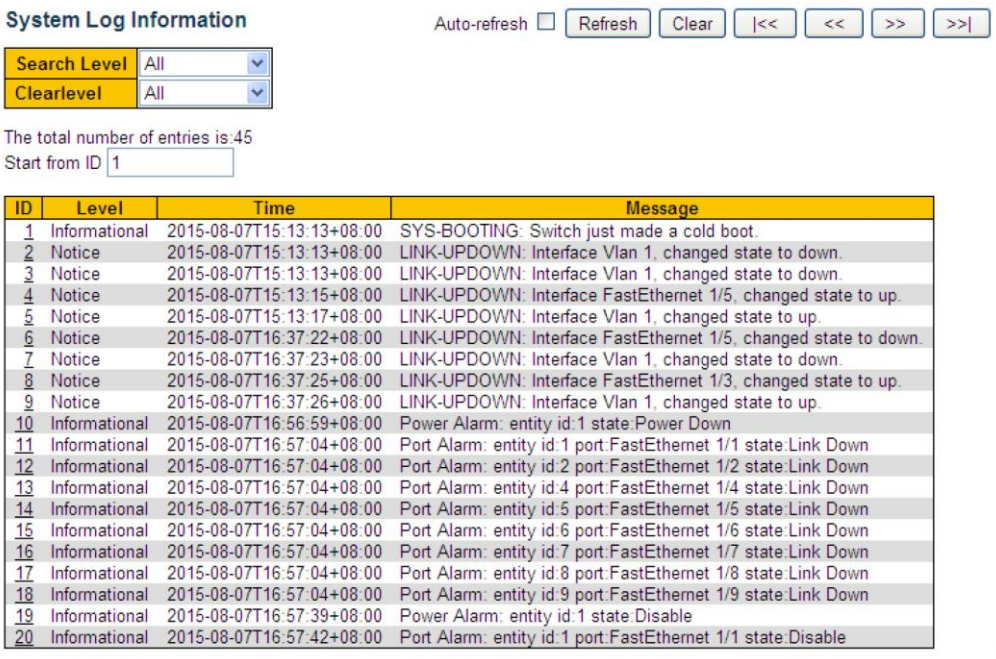
21. Журнал событий

Функция журнала в основном записывает состояние системы, неисправности, отладку, аномалии и другую информацию. При соответствующей настройке коммутатор может загружать журналы на сервер с поддержкой системного журнала в режиме реального времени.

Журнал содержит информацию о тревогах, широковещательном шторме, перезагрузке, памяти и информацию о действиях пользователей.

21.1. Веб конфигурирование

Настройте системный журнал, как показано на рисунке 214.



ID	Level	Time	Message
1	Informational	2015-08-07T15:13:13+08:00	SYS-BOOTING: Switch just made a cold boot.
2	Notice	2015-08-07T15:13:13+08:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
3	Notice	2015-08-07T15:13:13+08:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
4	Notice	2015-08-07T15:13:15+08:00	LINK-UPDOWN: Interface FastEthernet 1/5, changed state to up.
5	Notice	2015-08-07T15:13:17+08:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.
6	Notice	2015-08-07T16:37:22+08:00	LINK-UPDOWN: Interface FastEthernet 1/5, changed state to down.
7	Notice	2015-08-07T16:37:23+08:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
8	Notice	2015-08-07T16:37:25+08:00	LINK-UPDOWN: Interface FastEthernet 1/3, changed state to up.
9	Notice	2015-08-07T16:37:26+08:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.
10	Informational	2015-08-07T16:56:59+08:00	Power Alarm: entity id:1 state:Power Down
11	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:1 port:FastEthernet 1/1 state:Link Down
12	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:2 port:FastEthernet 1/2 state:Link Down
13	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:4 port:FastEthernet 1/4 state:Link Down
14	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:5 port:FastEthernet 1/5 state:Link Down
15	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:6 port:FastEthernet 1/6 state:Link Down
16	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:7 port:FastEthernet 1/7 state:Link Down
17	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:8 port:FastEthernet 1/8 state:Link Down
18	Informational	2015-08-07T16:57:04+08:00	Port Alarm: entity id:9 port:FastEthernet 1/9 state:Link Down
19	Informational	2015-08-07T16:57:39+08:00	Power Alarm: entity id:1 state:Disable
20	Informational	2015-08-07T16:57:42+08:00	Port Alarm: entity id:1 port:FastEthernet 1/1 state:Disable

Рисунок 214 Конфигурирование системного журнала

- **Search Level**
  Опции: Error/Warning/Notice/Information/All.
  По умолчанию: все
  Функция: выберите уровень отображаемой информации журнала.
  Очистить уровень
  Опции: Ошибка/Предупреждение/Уведомление/Информация/Все.
  По умолчанию: все
  Функция: выберите уровень информации журнала, которую необходимо удалить. Нажмите <Очистить>, чтобы удалить информацию журнала назначенного уровня.
- **The total number**
  Функция: отображает количество журналов, соответствующих условиям запроса.
- **Start from ID**
  Функция: установить начальный идентификатор записей журнала на текущей странице. Вы можете нажать «Обновить», чтобы обновить записи журнала на текущей странице. На каждой странице могут отображаться 20 записей журнала.
  Нажмите >>, чтобы просмотреть записи журнала на следующей странице. Начальный идентификатор следующей страницы — это идентификатор последней записи журнала на текущей странице.
  Нажмите <<, чтобы просмотреть записи журнала на предыдущей странице.
  Нажмите >>|, чтобы просмотреть записи журнала на последней странице. Конечный идентификатор — это идентификатор последней записи журнала.
  Нажмите |<<, чтобы просмотреть записи журнала на первой странице. Начальный идентификатор — это идентификатор первой записи журнала.

  Загрузите журнал на сервер в режиме реального времени, как показано на рисунке 215.

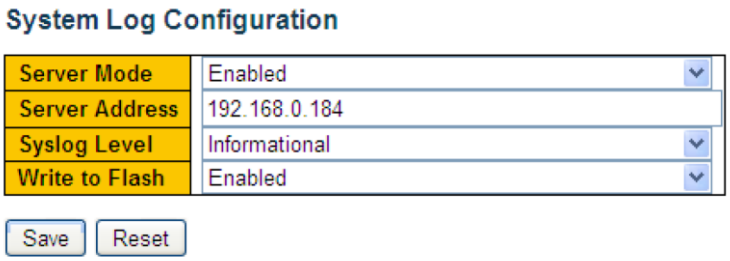


Рисунок 215 Загрузка жупнала на сервер в режиме реального времени

- **Server Mode**
  Опции: отключить/включить.
  По умолчанию: Отключить
  Функция: Включить/отключить загрузку журнала на сервер в режиме реального времени.
- **Server Address**
  Функция: настройте IP-адрес сервера, на который загружается информация журнала.
- **Syslog Level**
  Опция: Error/Warning/Notice/Information
  По умолчанию: Information
  Функция: выберите уровень информации журнала для загрузки на сервер.

- **Write to Flash**
  Опция: включено/отключено
  По умолчанию: отключено
  Функция: записывать лог во флеш или нет.

22. Зеркалирование

Благодаря функции зеркалирования портов коммутатор копирует все полученные или переданные кадры данных из порта (зеркалирование порта источника) в другой порт (зеркалирование порта назначения). Порт назначения зеркалирования подключен к анализатору протоколов или монитору RMON для мониторинга сети, управления и диагностики неисправностей.

Коммутатор поддерживает только один порт назначения зеркалирования, но несколько портов источника.

Несколько исходных портов могут находиться либо в одной VLAN, либо в разных VLAN. Порт источника зеркалирования и порт назначения могут находиться в одной VLAN или в разных VLAN.

Порт источника и порт назначения не могут быть одним и тем же портом.

22.1. Веб конфигурирование

Настройте функцию зеркалирования портов, как показано на рисунке 216.

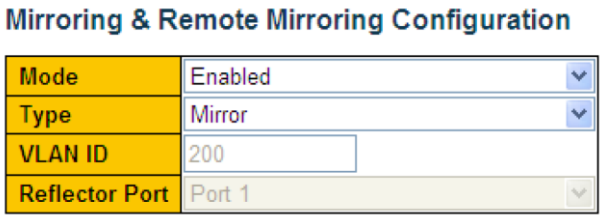


Рисунок 216 Конфигурирование функции зеркалирования портов

- **Mode**
  Опции: Включить/Отключить.
  По умолчанию: Отключить
  Функция: включить/отключить функцию зеркалирования портов.
- **Type**
  Опции: Mirror
  Функция: использовать функцию зеркалирования портов.

Выберите пункт назначения зеркалирования и исходный порт, как показано на рисунке 217.

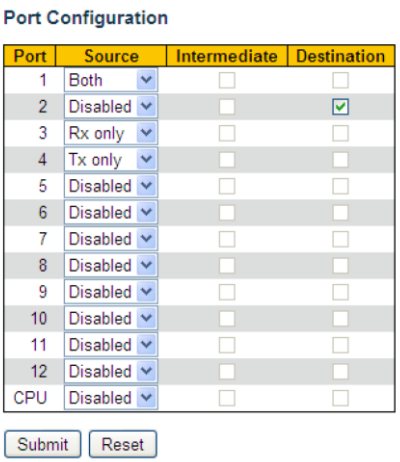


Рисунок 217 Конфигурирование пункт назначения зеркалирования и исходный порт

- **Source**
  Опции: только прием/только передача/оба
  Функция: выберите данные для зеркалирования в исходном порту зеркалирования.
  Только Rx: указывает, что в исходном порту зеркалируются только полученные пакеты.
  Только Tx: указывает, что в исходном порту зеркалируются только переданные пакеты.
  Оба: указывает, что как переданные, так и полученные пакеты зеркалируются в исходном порту.
- **Destination**
  Функция: выберите порт, который будет портом назначения зеркалирования. Существует один и только один зеркальный порт назначения.

  Диапазон: 1~16 символов
- **Password**

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.