Промышленный управляемый

Коммутатор STEZ49xx

Руководство пользователя

Оглавление

1. Описание устройства

1.1. Введение

Коммутаторы серии STEZ49xx применяются в энергетике, железнодорожном транспорте, добыче угля и многих других отраслях промышленности и могут корректно работать в суровых условиях. Данная серия поддерживает протоколы резервирования RSTP, ST-Ring и DRP, гарантируя надежную работу системы. Коммутаторы соответствуют стандартам IEC61850-3 и IEEE1613.

1.2. Модели серии

В портфолио серии STEZ49xx входят следующие коммутаторы (см ниже). Перечень артикулов и наименований не исчерпывающий. Данное руководство применяется ко всем коммутаторам серии STEZ49xx.

- **STEZ4924-4G** (артикул 70010001) – управляемый коммутатор L2, монтаж в стойку, 24 порта 10/100Base-TX, 4 порта 100/1000Base-X SFP, 100-240VAC/110-220VDC (85-264VAC/77-300VDC) резервированные источники питания;
- **STEZ4924SFP-4G** (артикул 70010002) - управляемый коммутатор L2, монтаж в стойку, 24 порта 100Base-X SFP, 4 порта 100/1000Base-X SFP, 100-240VAC/110-220VDC (85-264VAC/77-300VDC) резервированные источники питания;
- **STEZ4916SFP-8T-4G** (артикул 70010003) – управляемый коммутатор L2, монтаж в стойку, 16 портов 100Base-X SFP, 8 портов 10/100Base-TX, 4 порта 100/1000Base-X SFP, 100-240VAC/110-220VDC (85-264VAC/77-300VDC) резервированные источники питания;
- **STEZ4912SFP-12T-4G** (артикул 70010004) – управляемый коммутатор L2, монтаж в стойку, 12 портов 100Base-X SFP, 12 портов 10/100Base-TX, 4 порта 100/1000Base-X SFP, 100-240VAC/110-220VDC (85-264VAC/77-300VDC) резервированные источники питания;
- **STEZ4916-8MM-4G** (артикул 70010005) - управляемый коммутатор L2, монтаж в стойку, 16 портов 10/100Base-TX, 8 портов 100Base-FX MM, разъем SC, 1310nm, 5km, 4 порта 100/1000Base-X SFP, 100-240VAC /110-220VDC (85-264VAC/77-300VD) резервированные источники питания.

1.3. Функции программного обеспечения

Коммутаторы серии STEZ49xx предоставляют множество программных функций, удовлетворяющих различные требования клиентов.

- Протоколы резервирования: RSTP/STP, ST-Ring, DRP
- Поддержка мультикаст протоколов: IGMP Snooping, GMRP и static multicast
- VLAN, PVLAN, QoS и ARP
- Управление шириной канала: port trunk, port rate limiting
- Безопасность: ACL, port isolate
- Синхронизация времени: SNTP
- Обновление ПО через FTP, загрузка / выгрузка конфигурационного файла

- Port mirroring, LLDP, контроль линии
- Функции уведомления: port alarm, power alarm, ring alarm, конфликт IP/MAC адресов, temperature alarm и port traffic alarm
- Управление устройством: CLI, Telnet (SSH), Web.

2. Управление коммутатором

Управление коммутатором возможно посредством:

- Консольного порта
- Telnet/SSH
- Web браузера

2.1. Тип просмотра

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

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

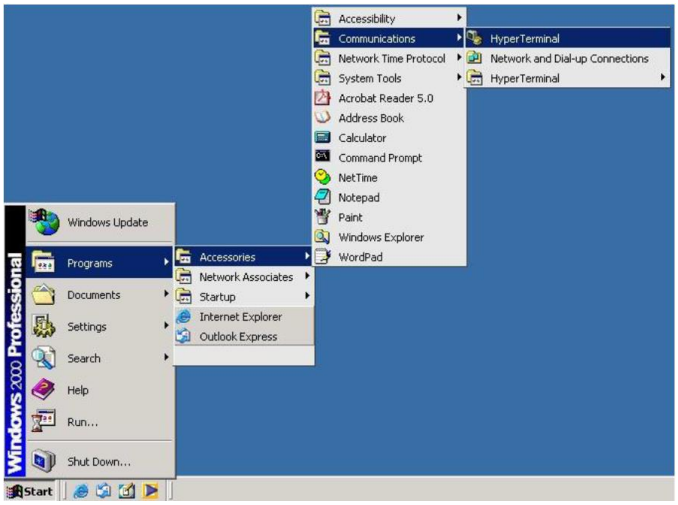
Когда коммутатор конфигурируется через интерфейс командной строки, то можно использовать для получения справки по команде "?". В справочной информации есть разные форматы описания параметров. Например, <1, 255> означает диапазон чисел; <H.H.H.H> означает IP-адрес; <H:H:H:H:H:H> означает MAC-адрес; слово<1,31> означает

диапазон строк. Кроме того, с помощью ↑ и ↓ можно делать прокрутку недавно использовавшихся команд.

2.2. Управление коммутатором через консольный порт

Для управления коммутатором можно использовать консоль или Telnet (SSH). Управление с помощью командной строки через последовательный консольный RS-232 порт (115200, 8, none, 1, none). Для настройки с помощью последовательного консольного RS-232 порта используйте кабель RJ45 к DB9-F (DB-9 «мама»), чтобы подключить консольный RS-232 порт коммутатора с COM портом вашего компьютера.
Для того, чтобы получить доступ к консоли через последовательный RS-232 кабель:

- На рабочем столе Windows выберите Пуск > Программы > Стандартные > Связь > Hyper Terminal

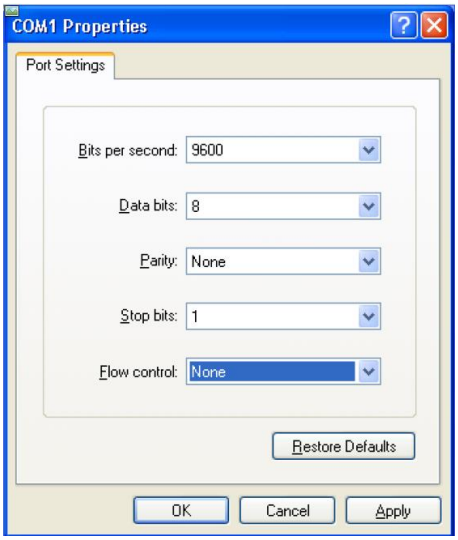


Можно использовать любой другой эмулятор терминала, такой как Putty.

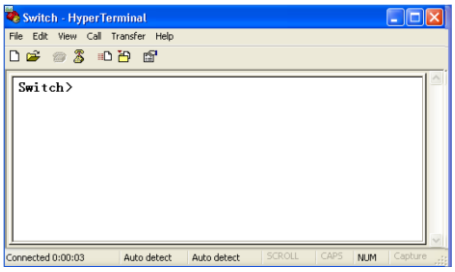
- Введите имя для нового соединения

- Выберите номер COM порта для его использования

- Настройка свойств COM порта. 9600 для бит в секунду, 8 для бит данных, None для четности, 1 для стоповых битов и none для управления потоком.



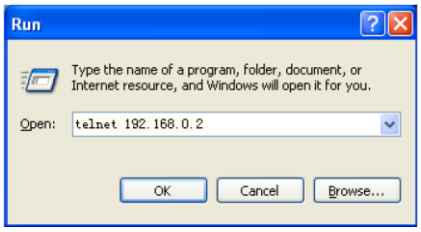
- Появится окно входа в систему. Введите имя пользователя и пароль (пароль такой же, как и для Web браузера), затем нажмите enter.



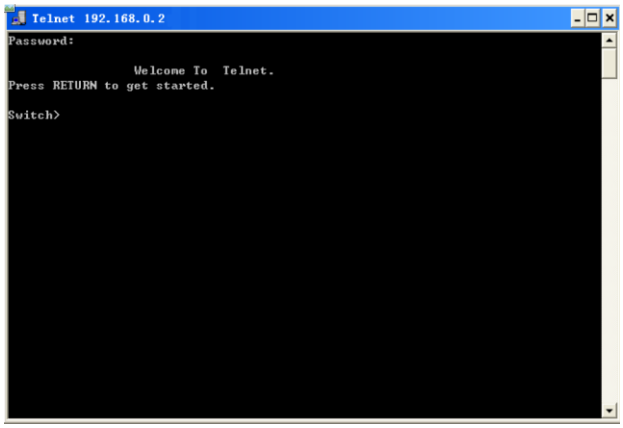
2.3. Управление коммутатором через Telnet

Пользователи могут использовать Telnet для настройки коммутаторов.

- Набрать telnet *IP адрес коммутатора* из командной строки windows (или любой аналог)



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



2.4. Управление коммутатором через Web

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

3. Статус коммутатора

3.1. Базовая информация

Основная информация о коммутаторе включает MAC-адрес, серийный номер, IP-адрес, маску подсети, шлюз, имя системы, модель устройства и информацию о версии, как показано на следующем рисунке.

Item	Information
MAC Address	00-00-00-00-19-39
SN	S3MOT12030189
IP Address	192.168.0.22
Subnet Mask	255.255.255.0
GateWay	192.168.0.1
System Name	SWITCH
Device Model	
Software Version	ID:1 R1004 (2014-12-24 14:53)
FW Version	V4.0.2 (2014-7-11 23:33)
Hardware Version	V4.0

3.2. Состояние порта

На странице состояния порта отображается номер порта, состояние администрирования, состояние соединения, скорость, дуплекс и управление потоком, как показано на следующем рисунке.

Port ID	Administration Status	Operation Status	Link	Speed	Duplex	Flow Control	RX	TX
S1/FE1	Enable	Enable	Down	---	---	---	---	---
S1/FE2	Enable	Enable	Down	---	---	---	---	---
S1/FE3	Enable	Enable	Down	---	---	---	---	---
S1/FE4	Enable	Enable	Up	100M	Full-duplex	Off	Enable	Enable
S1/FE5	Enable	Enable	Down	---	---	---	---	---
S1/FE6	Enable	Enable	Down	---	---	---	---	---
S1/FE7	Enable	Enable	Down	---	---	---	---	---
S1/FE8	Enable	Enable	Down	---	---	---	---	---
S4/GE1	Enable	Enable	Down	---	---	---	---	---
S4/GE2	Enable	Enable	Down	---	---	---	---	---
S4/GE3	Enable	Enable	Down	---	---	---	---	---
S4/GE4	Enable	Enable	Down	---	---	---	---	---

- **Port ID**
  Отображение типа и идентификатора портов. Идентификатор порта имеет формат Sα/β. α указывает номер слота, в котором находится плата, β указывает тип порта и идентификатор платы/панели, на которой находится порт.
  FE/FX/GE/GX указывает на тип порта:
  FE: 10/100Base-TX RJ45 порт
  FX: 100Base-FX порт
  GE: 10/100/1000Base-TX RJ45 порт
  GX: Gigabit SFP слот
- **Administration Status**
  Отображение статуса администрирования портов.
  Enable: Порт доступен и разрешает передачу данных.
  Disable: Порт заблокирован без передачи данных.
- **Operation status**
  Отображение рабочего состояния портов.
- **Link**
  Отображение состояния соединения портов.

Up: Порт находится в состоянии Linkup и может нормально обмениваться данными.
Down: порт находится в состоянии Linkdown и не может обмениваться данными.

- **Speed**
  Отображение скорости связи портов Linkup.
- **Duplex**
  Отображение дуплексного режима портов Linkup.
  Full-duplex: порт может одновременно принимать и передавать данные.
  Half-duplex: порт одновременно принимает или передает данные.
- **Flow Control**
  Отображение состояния управления потоком портов Linkup.
- **RX**
  Опции: Enable/Disable.
  Enable: порт может получать данные.
  Disable: Порт не может принимать данные.
- **TX**
  Опции: Enable/Disable.
  Enable: порт может передавать данные.
  Disable: Порт не может передавать данные.

3.3. Статистика на порту

Статистика порта охватывает количество байтов/пакетов, которые каждый порт отправляет/получает, ошибки CRC и количество пакетов размером менее 64 байт, как показано на следующем рисунке.

Port ID	State	Link	Bytes Sent	Packets Sent	Bytes Received	Packets Received	CRC Error	Packets 64 bytes
S1/FE1	Enable	Down	0	0	0	0	0	0
S1/FE2	Enable	Down	0	0	0	0	0	0
S1/FE3	Enable	Down	0	0	0	0	0	0
S1/FE4	Enable	Up	1670419	7399	14367882	171176	0	0
S1/FE5	Enable	Down	0	0	0	0	0	0
S1/FE6	Enable	Down	0	0	0	0	0	0
S1/FE7	Enable	Down	0	0	0	0	0	0
S1/FE8	Enable	Down	0	0	0	0	0	0
S4/GE1	Enable	Down	0	0	0	0	0	0
S4/GX2	Enable	Down	0	0	0	0	0	0
S4/GE3	Enable	Down	0	0	0	0	0	0
S4/GE4	Enable	Down	0	0	0	0	0	0

Reset

Вы можете нажать <Reset>, чтобы перезапустить сбор статистики.

3.4. Информация о системе

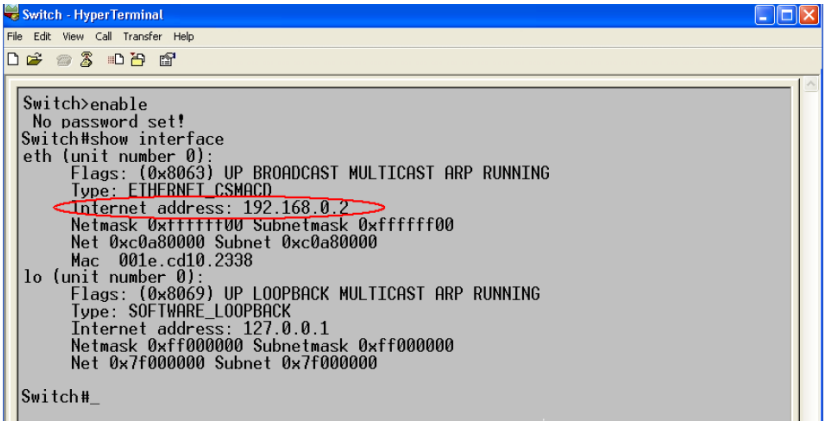
Операционная информация о системы включает время работы устройства, использование ЦП, использование памяти, температуру устройства и время устройства (местное время), как показано на следующих рисунках.

Device Operating	
Device Operating Time:	1Days,0H:35M:50S
CPU Usage:	2%(30 seconds), 1%(5 minutes)
Memory Usage:	68%
Device Temperature:	+33C
Device Time:	2015.01.20 20:20:21 Tuesday

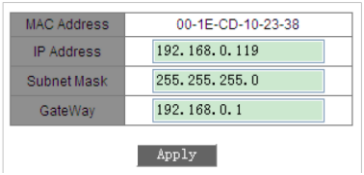
4. Базовая конфигурация

4.1. IP Address

Узнать IP-адрес коммутатора с помощью консольного порта. Войдите в интерфейс командной строки коммутатора через консольный порт. Запустите команду «show interface» в привилегированном режиме, чтобы просмотреть IP-адрес коммутатора. Как показано на следующем рисунке, IP-адрес обведен красным.

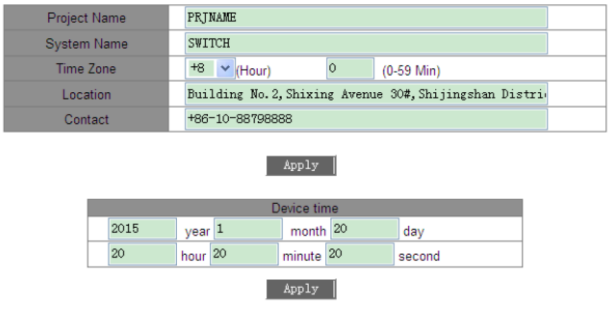


Назначить новый IP-адрес коммутатора и шлюз можно вручную, как показано на следующем рисунке.



4.2. Базовая информация

Основная информация включает имя проекта, имя системы, часовой пояс, местоположение, контакт и системное время, как показано на следующих рисунках.



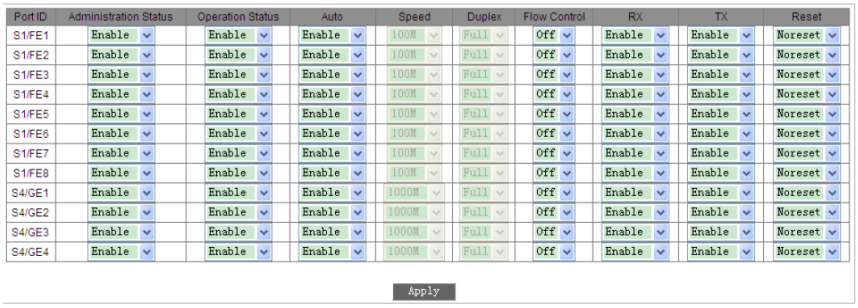
- **Project name**
  Диапазон: 1~64 символа
- **System name**
  Диапазон: 1~32 символа
- **Time zone**

Часовой пояс Опции: 0,+1,+2,+3,+4,+5,+6,+7,+8,+9,+10,+11,+12,+13,-1,-2,- 3, -4, -5, -6, -7, -8, -9, -10, -11, -12 час
0~59 мин.
По умолчанию: 0 часов 0 минут
Функция: выбор местного часового пояса.

- **Location**
  Значение: английские символы.
  Диапазон: 1~255 символов.
- **Device time**
  Портфолио: {ГГГГ, ММ, ДД, ЧЧ, ММ, СС}
  Диапазон: ГГГГ (год) от 2000 до 2099, ММ (месяц) от 1 до 12, ДД (день) от 1 до 31, ЧЧ (час) от 0 до 23, ММ (минуты) и СС (секунды) от от 0 до 59.
  Функция: установка системной даты и времени. Коммутатор может продолжать хронометраж после подачи питания.

4.3. Конфигурация порта

В конфигурации порта вы можете настроить состояние порта, скорость порта, управление потоком и другую информацию, как показано на следующем рисунке.



- **Administration Status**
  Опции: Enable/Disable
  По умолчанию: Enable
  Функция: Разрешить передачу данных на порт или нет.
  Описание: Enable означает, что порт включен и разрешает передачу данных; Disable указывает, что порт отключен и запрещает передачу данных. Эта опция напрямую влияет на аппаратное состояние порта и запускает аварийные сигналы порта.
- **Operation Status**
  Описание: Когда административный статус «Enable», рабочее состояние устанавливается на принудительное включение; когда административный статус «Disable», рабочий статус устанавливается на принудительное отключение.
- **Auto**
  Опции: Enable/Disable
  По умолчанию: Enable
  Функция: настроить статус автоматического согласования портов.
  Описание. Если для параметра «Авто» установлено значение «Enable», скорость порта и режим дуплекса будут автоматически согласовываться в соответствии со статусом подключения к порту; когда для параметра Auto установлено значение «Disable», можно настроить скорость порта и режим дуплекса.
- **Speed**
  Варианты: 10 / 100 / 1000 мбит/с

Функция: принудительно настроить скорость портов.

Описание: если для параметра Auto установлено значение Disable, можно настроить скорость порта.

- **Duplex**

  Варианты: Half/Full

  Функция: Настройка дуплексного режима портов.

  Описание: Если для параметра Авто установлено значение «Disable», можно настроить дуплексный режим 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.

- **Flow Control**

  Опции: off/on.

  По умолчанию: off

  Функция: включение/отключение функции управления потоком на назначенном порту.

  Описание: После включения функции управления потоком 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 (half/full), управление потоком у них реализуется по-разному. Если устройства работают в полнодуплексном режиме, принимающая сторона отправит специальный кадр, 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.

- **RX**

  Опции: Enable/Disable

  По умолчанию: Enable

  Функция: Разрешить порту получать данные или нет.

  Описание: Enable указывает, что порт может получать данные; Disable указывает, что порт не может получать данные.

- **TX**

  Опции: Enable/Disable

  По умолчанию: Enable

  Функция: Разрешить порту получать данные или нет.

  Описание: Enable указывает, что порт может передавать данные; Disable указывает, что порт не может передавать данные.

- **Reset**

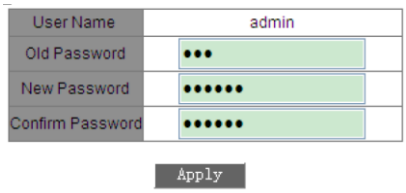
  Опции: Reset/Noreset

  По умолчанию: Noreset

  Функция: сбросить порт или нет.

4.4. Изменения пароля

Можно изменить пароль для имени пользователя «admin», как показано на следующем рисунке.

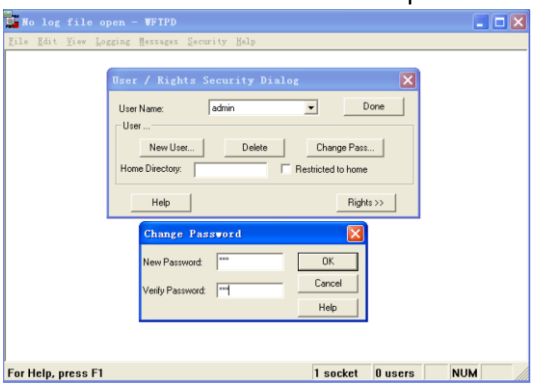


4.5. Обновление ПО

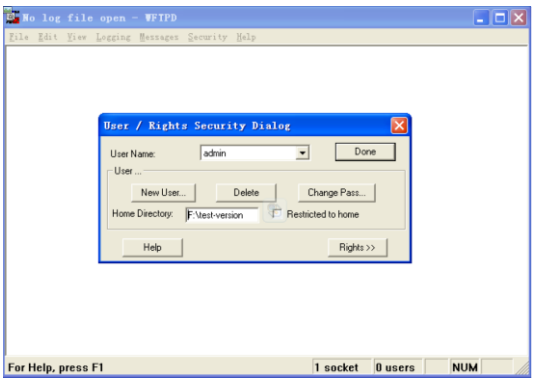
Обновления программного обеспечения могут помочь коммутатору повысить его производительность. Для коммутаторов этой серии обновления программного обеспечения включают обновление версии программного обеспечения BootROM и обновление версии системного программного обеспечения. Версия программного обеспечения BootROM должна быть обновлена до версии системного программного обеспечения. Если версия BootROM не меняется, можно обновить только версию системного ПО. Для обновления версии программного обеспечения требуется FTP-сервер.

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

- Нажмите [Security] → [Users/Rights]. Отображается диалоговое окно «Диалоговое окно «Users/Rights Security Dialog». Нажмите <New User>, чтобы создать нового пользователя FTP, как показано на следующем рисунке. Создайте имя пользователя и пароль, например, имя пользователя «admin» и пароль «123». Нажмите <OK>.



- Укажите путь расположения файла обновления ПО в «Home Directory», как показано на следующем рисунке. Нажмите <Done>.

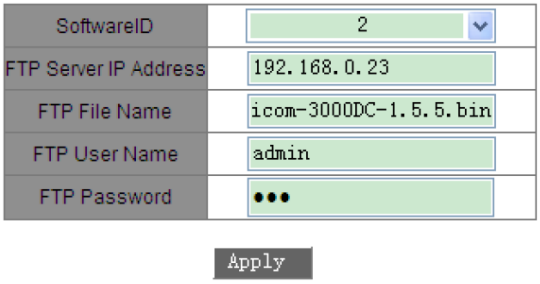


- Чтобы обновить программное обеспечение BootROM, введите следующую команду в привилегированном режиме:

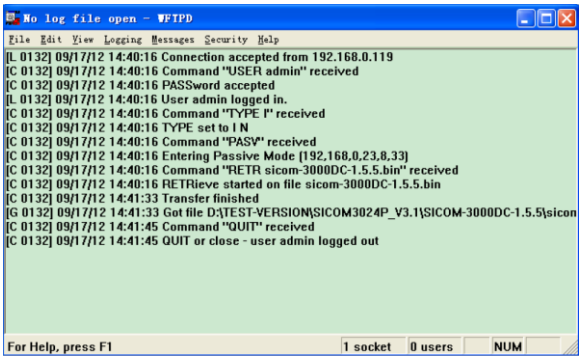
  Switch#**update bootrom** *<File_name> <Ftp_server_ip_address> <User_name> <Password>*

Параметр	**Описание**
File_name	Имя BootROM файла
Ftp_server_ip_address	IP адрес FTP сервера
User_name	Имя пользователя FTP
Password	Пароль FTP

- На следующем рисунке показана страница обновления программного обеспечения. Введите IP-адрес FTP-сервера, имя файла (на сервере), имя пользователя FTP и пароль. Нажмите <Apply>.



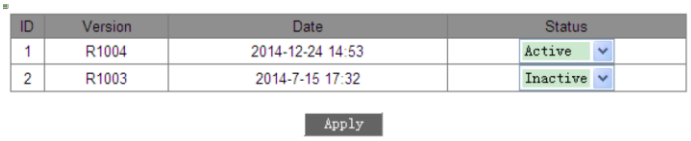
- Обеспечьте нормальную связь между FTP-сервером и коммутатором, как показано на следующем рисунке.



- Когда обновление будет завершено, как показано на следующем рисунке, перезагрузите устройство и откройте страницу основной информации о коммутаторе, чтобы проверить, успешно ли выполнено обновление и активна ли новая версия.

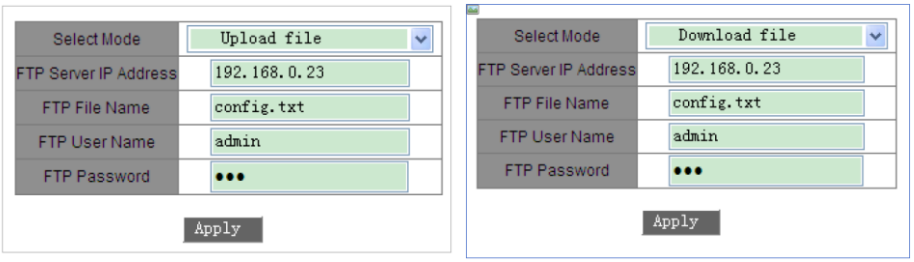
4.6. Запрос версии программного обеспечения

На коммутатор можно загрузить две версии программного обеспечения, но одновременно в активном состоянии может находиться только одна. Запрашивая версии программного обеспечения, вы можете узнать идентификаторы, даты выпуска и статусы двух версий, как показано на следующем рисунке.



4.7. Загрузка / выгрузка конфигурационного файла

Функция резервного копирования конфигурации может сохранять текущие файлы конфигурации коммутатора на сервере. При изменении конфигурации коммутатора вы можете загрузить исходные файлы конфигурации с сервера для переключения через FTP. Загрузка файлов заключается в загрузке файлов конфигурации коммутатора на сервер и их сохранении в файлы *.doc и *.txt. Загрузка файлов — это загрузка сохраненных файлов конфигурации с сервера на коммутатор, как показано на следующих рисунках.



После загрузки файла конфигурации на коммутатор необходимо перезапустить коммутатор, чтобы конфигурация вступила в силу.

5. Расширенная конфигурация

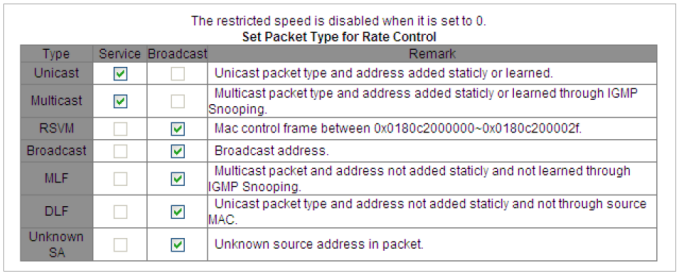
5.1. Ограничение скорости порта (Port Rate Limiting)

Ограничение скорости порта — это ограничение скорости пакетов, получаемых или передаваемых портом, и отбрасывание пакетов, скорость которых превышает пороговое значение. Функция действует на все пакеты на выходе, но только на определенные типы пакетов на входе. Следующие пакеты контролируются на входе.

- Unicast packets: указывают на одноадресные пакеты, добавленные статически или исходные MAC-адреса, которых изучены.
- Multicast packets: указывают пакеты, добавленные статически или полученные с помощью IGMP Snooping или GMRP.
- Reserved multicast packets: указывают пакеты с MAC-адресами в диапазоне от 0x0180c2000000 до 0x0180c200002f.
- Broadcast packets: указывают на пакеты с MAC-адресом назначения FF:FF:FF:FF:FF:FF.
- Unknown multicast packets: указывают на пакеты, которые не добавлялись статически и не были изучены с помощью IGMP Snooping или GMRP.
- Unknown unicast packets: указывают на пакеты, которые не добавляются статически и исходные MAC-адреса которых не изучены.
- Unknown source packets: указывают на пакеты с неизвестными исходными MAC-адресами.

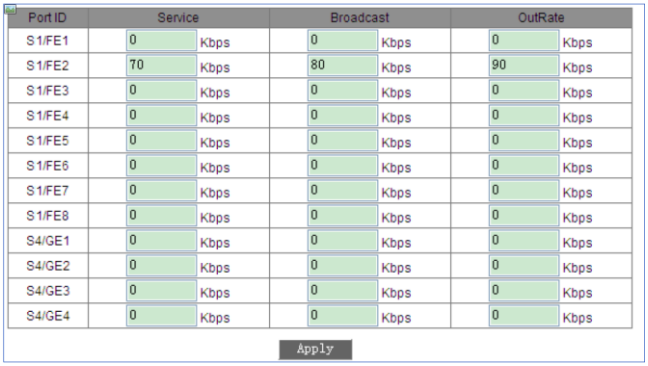
Для конфигурирования через Web интерфейс:

- Выберите типы пакетов для управления скоростью, как показано на следующем рисунке.



Приемник разделяет управление скоростью на два типа: управление скоростью обслуживания и управление скоростью вещания. Каждый пакет может быть добавлен только к одному типу управления скоростью.

- Настройте управление скоростью порта, как показано на следующем рисунке.



Port ID	Service	Broadcast	OutRate
S1/FE1	0 Kbps	0 Kbps	0 Kbps
S1/FE2	70 Kbps	80 Kbps	90 Kbps
S1/FE3	0 Kbps	0 Kbps	0 Kbps
S1/FE4	0 Kbps	0 Kbps	0 Kbps
S1/FE5	0 Kbps	0 Kbps	0 Kbps
S1/FE6	0 Kbps	0 Kbps	0 Kbps
S1/FE7	0 Kbps	0 Kbps	0 Kbps
S1/FE8	0 Kbps	0 Kbps	0 Kbps
S4/GE1	0 Kbps	0 Kbps	0 Kbps
S4/GE2	0 Kbps	0 Kbps	0 Kbps
S4/GE3	0 Kbps	0 Kbps	0 Kbps
S4/GE4	0 Kbps	0 Kbps	0 Kbps

Apply

- **Service/Broadcast**
  Диапазон: 64~1000000Кбит/с
  Функция: Настройка управления скоростью для пакетов на порту. Пакеты, скорость которых выше указанного значения, отбрасываются.
  Описание: Скорость входящего трафика для порта 100M варьируется от 64 до 100000 Кбит/с.
  Скорость входящего трафика для порта 1000M варьируется от 64 до 1000000 Кбит/с.
- **OutRate**
  Диапазон: 64~1000000Кбит/с
  Функция: ограничение скорости пакетов, пересылаемых портом.
  Описание. Скорость исходящего трафика для порта 100M варьируется от 64 до 100000 Кбит/с. Скорость входящего трафика для порта 1000M варьируется от 64 до 1000000 Кбит/с.

Если значение скорости установлено на 0, управление скоростью на порту отключено.

5.2. VLAN

Одна локальная сеть может быть разделена на несколько логических виртуальных локальных сетей (VLAN). Устройство может обмениваться данными только с устройствами в той же VLAN. В результате широковещательные пакеты ограничиваются VLAN, что оптимизирует безопасность LAN.
Раздел VLAN не ограничен физическим расположением. Каждая VLAN рассматривается как логическая сеть. Если хосту в одной VLAN необходимо отправить пакеты данных на хост в другой VLAN, должен быть задействован маршрутизатор или устройство уровня 3.

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

VLAN 1 является VLAN по умолчанию и не может быть создана и/или удалена вручную.

5.3. Port-based VLAN

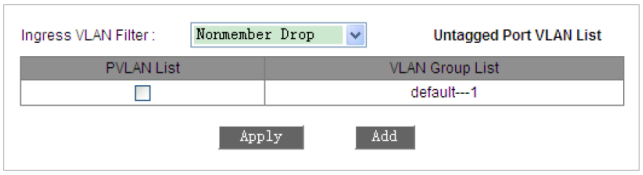
Раздел VLAN может быть либо на основе порта, либо на основе MAC-адреса. Коммутаторы этой серии поддерживают разделение VLAN на основе портов. Члены VLAN могут быть определены на основе портов коммутатора. После добавления порта в указанную VLAN порт может пересылать пакеты с тегом для VLAN.

- *Port Type*
  Порты делятся на два типа в зависимости от того, как они обрабатывают теги VLAN при пересылке пакетов.
  - Untag port: пакеты, пересылаемые портом без тегов, не имеют тегов VLAN. Порты Untag обычно используются для подключения к терминалам, которые не поддерживают 802.1Q. По умолчанию все порты коммутатора являются портами без тегов и принадлежат VLAN1.
  - Tag port: все пакеты, пересылаемые портом тега, содержат тег VLAN. Порты тегов обычно используются для подключения сетевых передающих устройств.
- *PVID*
  Каждый порт имеет PVID. При получении нетегированного пакета порт добавляет к пакету тег в соответствии с PVID. PVID порта — это идентификатор VLAN для порта Untag. По умолчанию PVID всех портов — это VLAN 1.

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

Обработка полученных пакетов		**Обработка отправляемых пакетов**	
Untagged packets	**Tagged packets**	**Port Type**	**Packet Processing**
Добавляйте теги PVID к непомеченным пакетам	➢ Если идентификатор VLAN в пакете есть в списке разрешенных VLAN, примите пакет. ➢ Если идентификатор VLAN в пакете отсутствует в списке разрешенных VLAN, пакет отбрасывается.	Untag	Переслать пакет после удаления тега.
		Tag	Хранить тег и пересылать пакет.

Настройте VLAN transparent transmission mode, как показано на следующем рисунке.

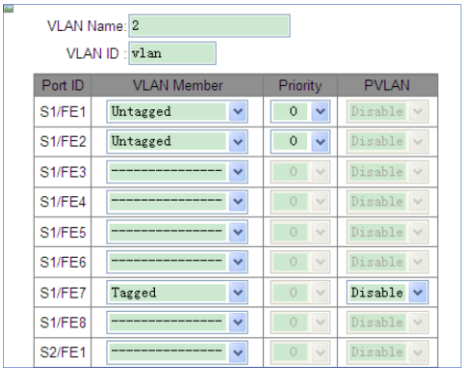


- **Ingress VLAN Filter**
  Варианты: Nonmember Drop/Nonmember Forward
  По умолчанию: Nonmember Drop
  Функция: настроить режим прозрачной передачи VLAN.
  Описание. Режим прозрачной передачи указывает, проверяет ли коммутатор входящие пакеты на порт. Если выбран вариант Nonmember Drop, пакет отбрасывается, если тег VLAN пакета отличается от VLAN порта. Если выбрано переадресация без участия, пакет принимается, когда тег VLAN пакета идентичен

тегу любого другого подключенного порта на коммутаторе; в противном случае пакет отбрасывается.

Создание VLAN

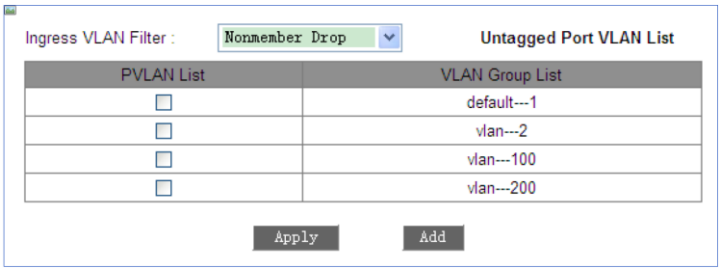
Нажмите <Add>, чтобы создать VLAN, далее как показано на следующем рисунке, выберите порты для добавления в VLAN и задайте параметры порта.



- **VLAN name**
  Диапазон: 1~31 символ
  Функция: Установите имя VLAN.
- **VLAN ID**
  Диапазон: 2~4093
  Функция: Настройка идентификатора VLAN.
  Описание: Идентификатор VLAN используется для различения VLAN между собой. Коммутаторы этой серии поддерживают до 256 VLAN.
- **VLAN Member**
  Варианты: tagged/untagged
  Функция: выберите тип порта в VLAN.
- **Priority**
  приоритет Диапазон: 0~7
  По умолчанию: 0
  Функция: Установите приоритет порта по умолчанию. При добавлении тега 802.1Q к нетегированному пакету значение поля PRI является приоритетным.
- **PVLAN**
  Опции: Enable/Disable
  По умолчанию: Disable
  Функция: чтобы добавить порт тега в сеть VLAN, необходимо включить или отключить PVLAN. Подробнее о PVLAN см. в следующей главе.

Порт Untag можно добавить только в одну VLAN. Идентификатор VLAN — это PVID порта. Значение по умолчанию — 1. Порт тега можно добавить в несколько VLAN.

Просмотрите список VLAN, как показано на следующем рисунке.

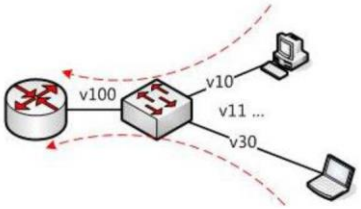


- **PVLAN List**
  Опции: выбрать/отменить выбор
  Функция: Включить или отключить функцию PVLAN. Подробнее см. в следующей главе

5.4. PVLAN

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

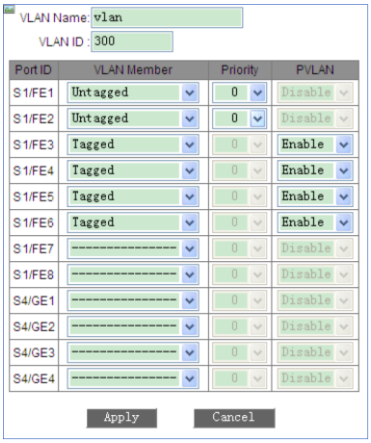
Верхняя VLAN — это VLAN с общим доменом, в которой порты являются восходящими портами. Нижние VLAN являются изолированными доменами, в которых порты являются портами нисходящей линии связи. Порты нисходящей линии связи могут быть назначены разным доменам изоляции, и они могут одновременно взаимодействовать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



Как показано на предыдущем рисунке, общий домен — это VLAN 100, а изолированные домены — это VLAN 10 и VLAN 30; устройства в изолированных доменах могут взаимодействовать с устройством в общем домене, например, VLAN 10 может взаимодействовать с VLAN 100; VLAN 30 также может взаимодействовать с VLAN100, но устройства в разных изолированных доменах не могут взаимодействовать друг с другом, например, VLAN 10 не может взаимодействовать с VLAN 30.

Когда порт тега с поддержкой PVLAN пересылает кадр, содержащий тег VLAN, тег VLAN будет удален.

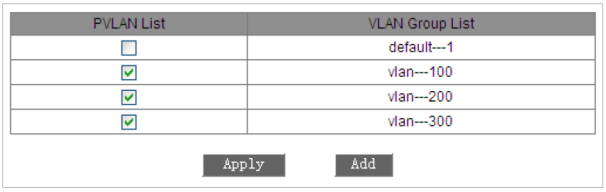
Включить PVLAN на порту, можно, как показано на следующем рисунке.



Вы можете включить PVLAN на Tag prot в VLAN.

Если VLAN является общим доменом, порт восходящей линии связи является Untag port, а порт нисходящей линии связи должен быть добавлен к VLAN в качестве Tag prot. Если VLAN является изолированным доменом, порт нисходящей линии связи является Untag port, а порт восходящей линии связи должен быть добавлен в VLAN в качестве Tag port.

Выбор VLAN-членов PVLAN, как показано на следующем рисунке.



- **PVLAN List**
  Опции: выбрать/отменить выбор
  По умолчанию: отменить выбор
  Функция: Выберите членов PVLAN.

5.5. Зеркалирование портов (Port Mirroring)

С функцией зеркального отображения портов коммутатор копирует все полученные или переданные кадры данных с одного порта (зеркальное отображение исходного порта) на другой порт (зеркальное отображение порта назначения). Порт назначения зеркалирования подключен к анализатору протокола или монитору RMON для мониторинга сети, управления и диагностики неисправностей.

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

Порт источника или назначения зеркалирования не может быть добавлен в Trunk group, в то время как порт, добавленный в Trunk group, не может быть установлен в качестве порта назначения или источника зеркалирования.

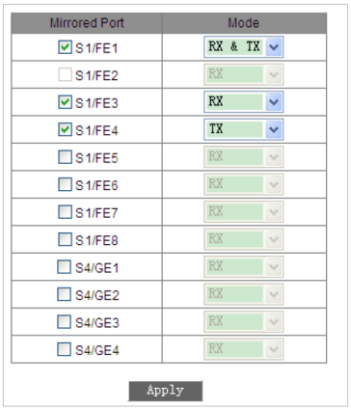
Порт-источник или порт назначения зеркального отображения не может быть установлен в качестве резервного порта (redundant port), в то же время redundant port не может быть установлен в качестве порта-источника или порта назначения зеркального отображения.

Для конфигурации через Web интерфейс необходимо выполнить:

Выберите порт назначения зеркалирования, как показано на следующем рисунке.

- **Mirroring Port**
  Параметры: Disable/переключить порт
  По умолчанию: Disable
  Функция: выберите порт, который будет портом назначения зеркалирования. Должен быть только один порт назначения зеркалирования.

Выберите исходные порты зеркалирования и режим зеркалирования, как показано на следующем рисунке.



- **Mode**
  Опции: RX/TX/RX & TX
  Функция: выберите данные для зеркального отображения
  TX указывает, что в исходном порту зеркалируются только передаваемые пакеты. RX указывает, что в исходном порту зеркалируются только полученные пакеты. TX&RX указывает, что как переданные, так и полученные пакеты зеркально отражены в исходном порту.

5.6. Port Trunk

Port trunk предназначен для привязки группы физических портов с одинаковой конфигурацией к логическому порту. Порты-члены в группе магистральных каналов могут не только распределять нагрузку, но и стать динамическим резервом друг для друга для повышения надежности соединения.

Port trunk и следующие конфигурации портов не могут использоваться вместе:

- Port redundancy: порт, добавленный в trunk group, не может быть настроен как резервный порт, в то время как резервный порт не может быть добавлен в группу соединительных линий.

- Port mirronring: Порт, добавленный в trunk group, не может быть настроен как порт назначения или исходный порт зеркального отображения, в то время как порт назначения или исходный порт зеркального отображения не может быть добавлен в trunk group.
- DHCP Snoping: Порт, добавленный в trunk group, не может быть настроен как DHCP Snooping Trust-Port, в то время как DHCP Snooping Trust-Port не может быть добавлен в trunk group.

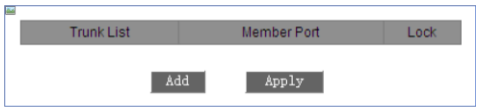
Кроме того, не рекомендуется выполнять следующие операции.

- Включать GMRP на trunk port.
- Добавлять GMRP-enabled port в trunk group.
- Добавлять trunk port в статическую запись unicast/multicast рассылки.
- Добавлять порт в статическую запись unicast/multicast рассылки в trunk group.

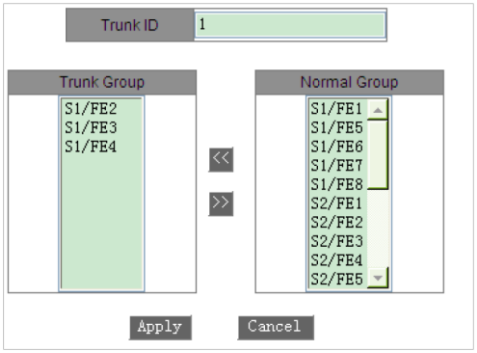
Гигабитные порты коммутаторов этой серии не поддерживают port trunk.
Порт можно добавить только в одну trunk group.

Для конфигурирования Port trunk:

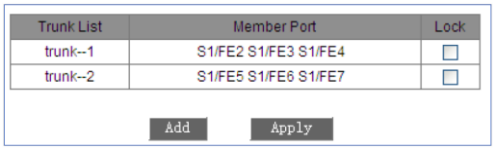
- Добавить Port Trunk
  Щелкните <Add>, чтобы добавить группу соединительных линий, как показано на следующем рисунке.



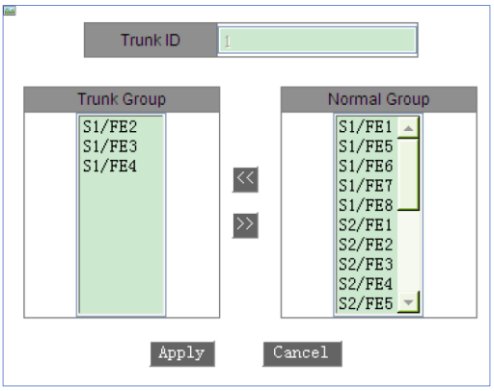
- Сконфигурируйте trunk group, как показано на следующем рисунке.



- **Trunk ID**
  Диапазон: 1~14
  Функция: установка идентификатора группы соединительных линий.
  Описание. Коммутаторы серии поддерживают до 14 групп соединительных линий. Каждая группа может содержать максимум 4 порта.
- Просмотрите список trunk group, как показано на следующем рисунке.



- **Lock**
  Заблокируйте порты-участники группы trunk group. После удаления заблокированных портов-участников из группы trunk group включить порты вручную, чтобы разблокировать порты.
  Вы можете изменить или удалить trunk group, как показано на следующем рисунке.



После изменения настроек члена группы (добавления нового порта в группу или удаления члена порта из группы) нажмите <Apply>, чтобы изменения вступили в силу. Если вы нажмете <Delete>, вы сможете удалить группу.

5.7. Проверка канала (Link Check)

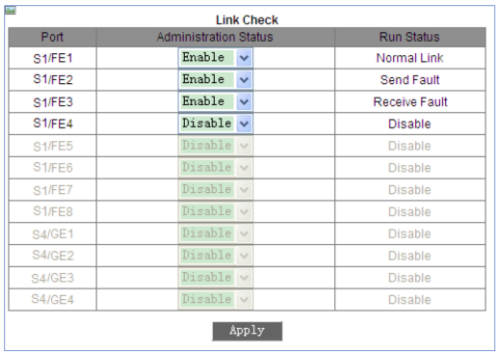
Проверка канала использует периодическое взаимодействие протокольных пакетов для оценки подключения канала и отображения состояния связи портов с включенным протоколом резервирования. В случае неисправности, проблема может быть обнаружена и устранена вовремя.

Порт, для которого включена проверка состояния соединения, периодически (каждую 1 с) отправляет пакеты для проверки состояния соединения. Если порт не получает пакет проверки канала от партнера в течение времени ожидания приема (5 с), это означает, что канал неисправен, и порт отображает состояние ошибки приема. Если порт получает пакет проверки канала от партнера, и пакет показывает, что пакет проверки канала получен от локального в течение периода ожидания приема (5 с), порт отображает нормальное состояние канала. Если порт получает пакет проверки канала от партнера, но пакет показывает, что пакет проверки канала не получен от локального в течение периода ожидания приема (5 с), порт отображает состояние ошибки отправки.

Порт, для которого отключена проверка состояния линии, работает в пассивном режиме. То есть он не отправляет пакет проверки связи в активном режиме. Однако после получения пакета проверки канала от удаленного узла этот порт немедленно возвращает пакет проверки канала, чтобы проинформировать удаленный узел о том, что он получил пакет проверки канала.

Функция действительна только для резервного порта с включенным протоколом. Когда кольцевой/резервный порт ISRP, кольцевой/резервный порт IS-Ring, порт RSTP, для которого включена проверка канала, неисправен (например, неправильный прием, ненормальная отправка), резервный протокол заблокирует этот порт.

Для конфигурирования Link Check, следуйте указаниям как на картинке ниже.



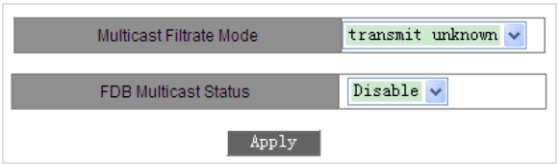
- **Administration Status**
  Опции: Enable/Disable
  По умолчанию: Enable
  Описание: Включить/выключить проверку связи на порту.
- **Run Status**
  Опции: Normal Link/Receive Fault/Disable/Send Fault
  Описание: если на кольцевом порту включена проверка канала и порт нормально отправляет и принимает данные, отображается Normal Link. Если партнер не получает пакеты обнаружения от устройства, отображается Send Fault. Если устройство не получает пакеты обнаружения от партнера, отображается Receive Fault. Если Link Check не включен для порта, отображается Disable.

Если партнер не поддерживает функцию Link Check, функция должна быть отключена на подключенном порту локального устройства.

5.8. Static Multicast

Вы можете настроить статическую таблицу многоадресных адресов. Вы можете добавить запись в таблицу в формате <multicast MAC address, VLAN ID, multicast member port>. При получении многоадресных пакетов коммутатор ищет в таблице соответствующий порт-член для пересылки пакетов.
Устройство поддерживает до 256 многоадресных записей.

Включите статическую многоадресную рассылку, как показано на следующем рисунке.

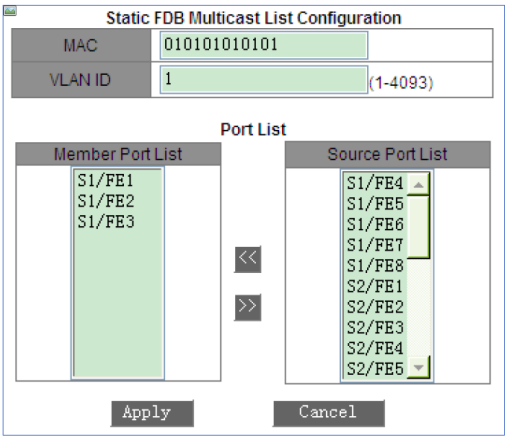


- **Multicast Filtrate Mode**
  Варианты: transmit unknown/drop unknown
  По умолчанию: transmit unknown
  Функция: настройка режима обработки неизвестных многоадресных пакетов.
  Описание: Неизвестные многоадресные пакеты — это пакеты, которые не

добавляются вручную и не изучаются с помощью IGMP Snooping или GMRP. Неизвестная передача указывает на то, что неизвестные многоадресные пакеты широковещательно передаются в соответствующих сетях VLAN; drop unknown указывает, что неизвестные многоадресные пакеты отбрасываются.

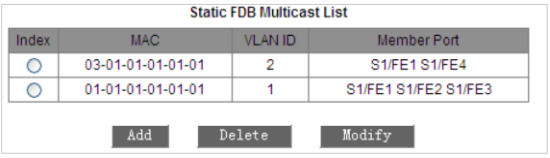
- **FDB Multicast Status**
  Опции: Enable/Disable
  По умолчанию: Disable
  Функция: включить или отключить статическую многоадресную рассылку. Статическая многоадресная рассылка и отслеживание IGMP не могут быть включены одновременно.

Добавить статическую многоадресную запись можно, как показано на следующем рисунке.



- **MAC**
  Портфолио: HHHHHHHHHHHH (H — шестнадцатеричное число.)
  Функция: Настройка группового адреса многоадресной рассылки. Младший бит старшего байта равен 1.
- **VLAN ID**
  Опции: все существующие VLAN
  Функция: Устанавливает идентификатор VLAN для записи. Только порты-участники VLAN могут пересылать многоадресные пакеты.
- **Member Port List**
  Выберите порты-члены для многоадресного адреса. Если хосты, подключенные к порту, должны получать пакеты с многоадресного адреса, вы можете настроить порт как порт-участник многоадресного адреса.

Просмотр, изменение или удаление статической многоадресной записи, как показано на следующем рисунке.



Список статических многоадресных адресов содержит MAC-адрес, идентификатор VLAN и порт участника. Чтобы удалить запись, выберите запись и нажмите <DELETE>. Чтобы изменить запись, выберите запись и нажмите <Modify>.

5.9. IGMP Snooping

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

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

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

IGMP Snooping управляет и поддерживает членов группы многоадресной рассылки путем обмена связанными пакетами между устройствами с поддержкой IGMP.
Связанные пакеты следующие:

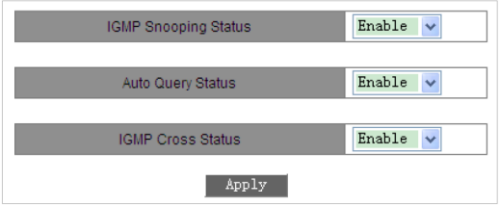
Пакет общего запроса: запрашивающий периодически отправляет пакеты общего запроса (IP-адрес назначения: 224.0.0.1), чтобы подтвердить, есть ли в группе многоадресной рассылки порты-члены. После получения пакета запроса устройство, не являющееся запросчиком, пересылает пакет на все подключенные к нему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

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

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), чтобы ответить на пакет запроса IGMP группы.

Пакет выхода: если устройство хочет покинуть группу многоадресной рассылки, оно отправит пакет выхода IGMP (IP-адрес назначения: 224.0.0.2).

Включить IGMP Snooping можно, как показано на следующем рисунке.



- **IGMP Snooping Status**
  Опции: Enable/Disable
  По умолчанию: Disable
  Функция: включить или отключить IGMP Snooping. IGMP Snooping и статическая многоадресная рассылка/GMRP не могут быть включены одновременно.
- **Auto Query Status**
  Опции: Enable/Disable
  По умолчанию: Disable
  Функция: включить или выключить автоматический запрос для выбора запрашивающего.
  Описание: Функцию автоматического запроса можно включить, только если включено IGMP Snooping.
- **IGMP Cross Status**
  Опции: Enable/Disable
  По умолчанию: Disable
  Функция: если эта функция включена, пакеты отчетов и отпусков могут пересылаться через кольцевые порты IS.

Просмотр списка участников многоадресной рассылки, можно как показано на следующем рисунке.

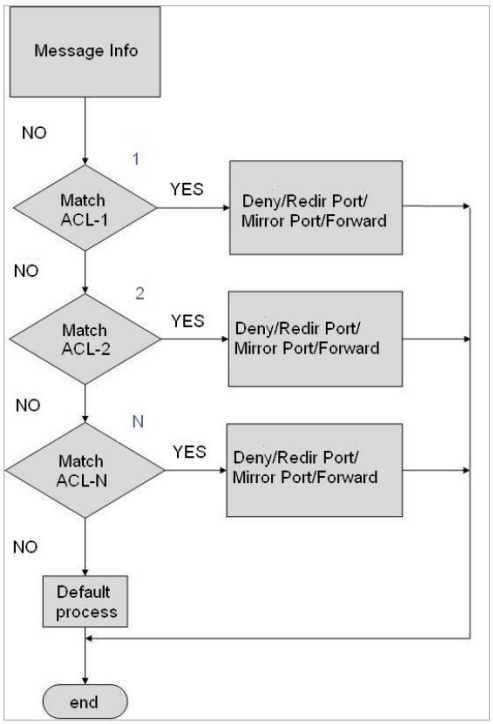
IGMP Member List

MAC	VLAN ID	Member
01-00-5E-7F-FF-FA	1	S1/FE1
01-00-5E-0A-18-03	1	S1/FE1
01-00-5E-51-09-08	1	S1/FE1

- **IGMP Member List**
  Комбинация: { MAC, VLAN ID, Member }
  В таблице многоадресной рассылки FDB, динамически полученной с помощью GMP Snooping, идентификатор VLAN является идентификатором VLAN портов-членов.

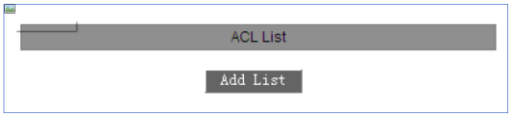
5.10. ACL (листы доступа)

Коммутаторы текущей серии фильтруют пакеты в соответствии с согласованным ACL. Каждая запись состоит из нескольких условий в логической связи И. Записи ACL не зависят друг от друга. Коммутатор сравнивает пакет с записями ACL в порядке возрастания идентификаторов записей. Как только совпадение найдено, выполняется действие, и дальнейшее сравнение не проводится, как показано на следующем рисунке.

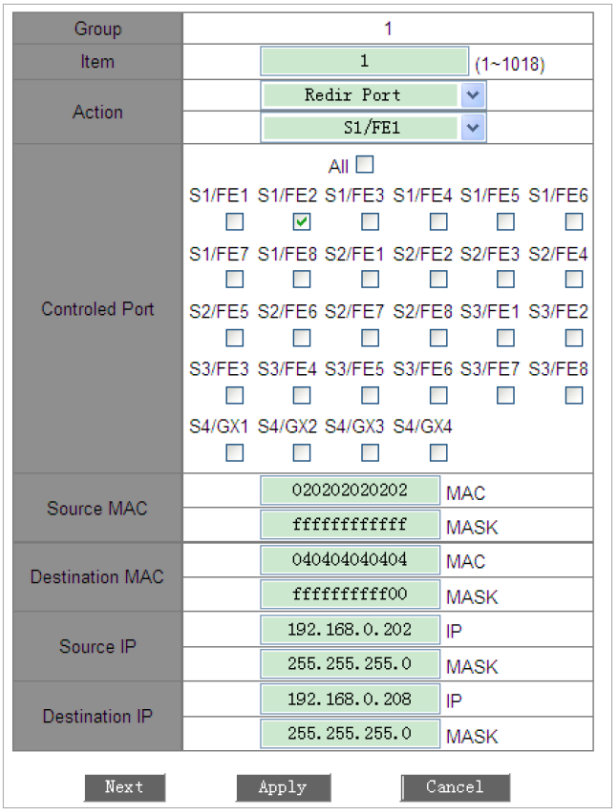


Конфигурирование ACL представлено ниже:

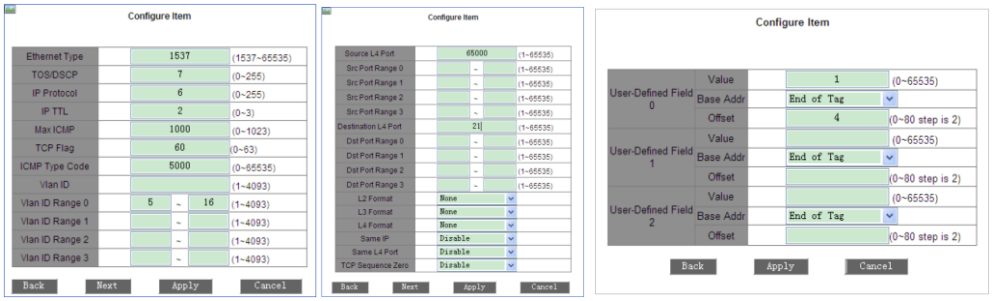
- Добавить запись ACL как показано ниже



- Установите параметры для записи ACL, как показано на следующем рисунке.



- Коммутатор предоставляет ряд параметров записи ACL. Вам нужно нажать <Next>, чтобы завершить настройку всех параметров, как показано на следующих рисунках.



- **Group**
  Принудительная конфигурация: 1
- **Item**
  Диапазон: 1~1018
  Функция: Установите идентификатор записи ACL. Вы можете настроить до 1023 записей ACL. Когда настроено несколько записей ACL, они сравниваются с пакетами в порядке возрастания идентификаторов.
- **Action**
  Варианты: Deny/Redir Port/Mirror Port/Forward
  По умолчанию: Deny
  Функция: настроить действие по отношению к пакету, соответствующему записи ACL.
  Deny: пакеты, соответствующие записи, будут отклонены.
  Redir Port: пакеты, соответствующие записи, будут перенаправлены на указанный порт. Вам необходимо указать порт в выпадающем списке.
  Mirror Port: пакеты, соответствующие записи, будут пересылаться как на порт назначения, так и на порт, указанный в раскрывающемся списке.
  Forward: пакеты, соответствующие записи, будут пересылаться на порт назначения.
- **Control Port**
  Варианты: все/один или несколько портов
  Функция: выберите порт, на который действует ACL.
- **Source MAC**
  Портфолио: {MAC, MASK}
  Формат: {HHHHHHHHHHHH, HHHHHHHHHHHH} (H — шестнадцатеричное число.)
  Функция: Настройка исходного MAC-адреса и маски подсети. Если исходный MAC-адрес и маска подсети пакета совпадают со значением этого параметра, то условие выполнено.
- **Destination MAC**
  Портфолио: {MAC, MASK}
  Формат: {HHHHHHHHHHHH, HHHHHHHHHHHH} (H — шестнадцатеричное число.)
  Функция: Настройка MAC-адреса назначения и маски подсети. Если MAC-адрес получателя и маска подсети пакета совпадают со значением этого параметра, то условие выполнено.
- **Source IP**
  Портфолио: {IP, MASK}
  Формат: {A.B.C.D, A.B.C.D}
  Функция: Настройка исходного IP-адреса и маски подсети. Если исходный IP-адрес и маска подсети пакета совпадают со значением этого параметра, то условие выполнено.
- **Destination IP**

Портфолио: {IP, MASK}
Формат: {A.B.C.D, A.B.C.D}
Функция: Настройка IP-адреса назначения и маски подсети. Если IP-адрес получателя и маска подсети пакета совпадают со значением этого параметра, то условие выполнено.

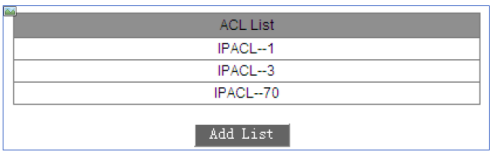
- **Ethernet Type**
  Диапазон: 1537~65535
  Функция: Настройка типа Ethernet. Если поле типа Ethernet пакета совпадает со значением этого параметра, то условие выполнено.
- **TOS/DSCP**
  Диапазон: 0~255
  Функция: Настройка типа службы. Если соответствующее поле пакета совпадает со значением этого параметра, то условие выполнено.
- **IP Protocol**
  Диапазон: 0~255
  Функция: Настройка значения протокола IP. Если соответствующее поле пакета совпадает со значением этого параметра, то условие выполнено.
- **IP TTL**
  Диапазон: 0~3
  Функция: Настройка поля TTL. Если установлено значение 0, TTL соответствующего пакета должен быть равен 0; если установлено значение 1, TTL соответствующего пакета должен быть равен 1; если установлено значение 2, TTL соответствующего пакета находится в диапазоне от 2 до 254; если установлено значение 3, значение TTL соответствующего пакета должно быть равно 255. Если соответствующее поле пакета соответствует этим правилам, то условие выполнено.
- **Max ICMP**
  Диапазон: 0~1023
  Функция: Настройка максимального значения ICMP. Значение указывает длину данных пакетов ICMP. Если длина данных пакета ICMP больше значения, то условие выполнено.
- **TCP Flag**
  Диапазон: 0~63
  Функция: Настройка флага TCP. Если соответствующее поле пакета совпадает со значением этого параметра, то условие выполнено.
- **ICMP Type Code**
  Диапазон: 0~65535
  Функция: Настройка кода типа ICMP. Если соответствующее поле пакета совпадает со значением этого параметра, то условие выполнено.
- **Vlan ID**
  Диапазон: 1~4093
  Функция: Настройка идентификатора VLAN. Если соответствующее поле пакета совпадает со значением этого параметра, то условие выполнено.
- **Vlan ID Range (0~3)**
  Портфолио: {X~Y} (X и Y (X≤Y) находятся в диапазоне от 1 до 4093. X и Y обозначают нижний и верхний пределы идентификаторов Vlan соответственно.)
  Функция: Настройка диапазона идентификаторов VLAN для пакетов. Условие выполняется, когда VLAN ID пакета находится в указанном диапазоне.
- **Source L4 Port**
  Диапазон: 1~65535

Функция: Настройка номера порта источника для пакетов протокола уровня 4. Если соответствующее поле пакета совпадает со значением, то условие выполнено.

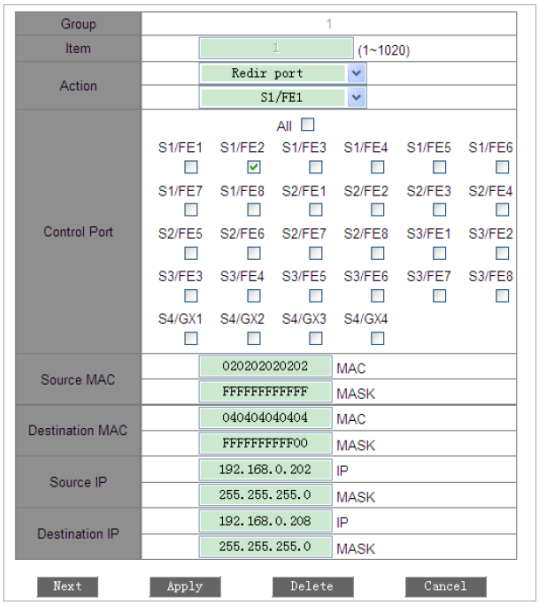
- **Src Port Range (0~3)**
  Портфолио: {X~Y} (X и Y (X≤Y) находятся в диапазоне от 1 до 65535. X и Y обозначают нижний и верхний пределы номеров исходных портов уровня 4 соответственно.)
  Функция: настройка диапазона номеров портов назначения для пакетов протокола уровня 4. Если соответствующее поле пакета находится в пределах указанного диапазона, то условие выполнено.
- **L2 Format**
  Варианты: None/L2_Others/Ethernet_II/IEEE_802_2_SNAP
  По умолчанию: None
  Функция: настройка формата кадра Ethernet уровня 2. None указывает, что это правило не используется; L2_Others указывает на все остальные форматы кадров Ethernet, кроме Ethernet_II и IEEE_802_2_SNAP. Когда формат кадра Ethernet пакета согласуется с указанным значением, условие выполняется.
- **L3 Format**
  Варианты: None/L3_Others/IPV4_without_frag/IPV6_without_exten
  По умолчанию: None
  Функция: настройка интернет-протокола уровня 3. None указывает, что это правило не используется; L3_Others указывает все интернет-протоколы уровня 3, кроме IPV4_without_frag и IPV6_without_exten. Когда интернет-протокол уровня 3 пакета соответствует указанному значению, условие выполняется.
- **L4 Format**
  Опции: None/L4_Others/TCP/UDP/ (ICMP/IGMP)
  По умолчанию: None
  Функция: Настройка типа протокола уровня 4. None указывает, что это правило не используется; L4_Others указывает все протоколы, кроме TCP, UDP, ICMP и IGMP. Когда тип протокола уровня 4 пакета соответствует указанному значению, условие выполняется.
- **Same IP**
  Опции: Disable/False/True
  По умолчанию: Disable
  Функция: Проверить, совпадает ли исходный IP-адрес пакета с IP-адресом получателя.
  Disable указывает, что правило не используется.
  False указывает, что условие выполнено, если IP-адрес источника пакета отличается от IP-адреса получателя.
  True указывает, что условие выполнено, если IP-адрес источника пакета идентичен IP-адресу получателя.
- **Same L4 Port**
  Опции: Disable/False/True
  По умолчанию: Disable
  Функция: Проверить, совпадает ли исходный номер порта 4-го уровня пакета с номером целевого порта 4-го уровня пакета.
  Disable указывает, что правило не используется.
  False указывает на то, что условие выполнено, если исходный номер порта 4-го уровня пакета отличается от его целевого номера порта 4-го уровня.
  True указывает на то, что условие выполнено, если исходный номер порта 4-го уровня пакета идентичен номеру целевого порта 4-го уровня.
- **TCP Sequence Zero**

Опции: Disable/False/True
По умолчанию: Disable
Функция: Проверить, равно ли поле TCP Sequence пакета 0.
Disable указывает, что правило не используется.
False указывает, что условие выполнено, если поле TCP Sequence пакета не равно 0.
True указывает, что условие выполнено, если поле TCP Sequence пакета равно 0.

- **User-Defined Field (0~2)**
  Портфолио: { Value, Base Addr, Offset }
  Диапазон или параметры:
  Значение: 1~65535
  Базовый адрес: End of Tag (Default)/End of EthType/End of IP Header
  Смещение: 0~80, шаг 2
  Функция: определить поле как условие ACL. Значение указывает значение, которое необходимо сопоставить; Base Addr указывает контрольную точку пакета; End of Tag указывает, что конец поля тега является контрольной точкой; End of EthType указывает, что конец поля EthType является контрольной точкой; End of IP Header указывает, что конец поля заголовка IP является контрольной точкой; Смещение указывает смещение значения по сравнению с контрольной точкой. Если смещение пакета по сравнению с базовым адресом равно Value, то условие выполнено.
- Просмотр ACL можно как показано ниже



Щелкните запись ACL на предыдущем рисунке. Затем измените или удалите запись ACL, как показано на следующем рисунке.



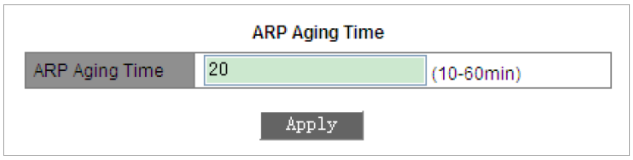
Нажмите <Apply>, чтобы изменения вступили в силу после внесения изменений. Нажмите <Delete>, чтобы удалить запись ACL.

5.11. ARP

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

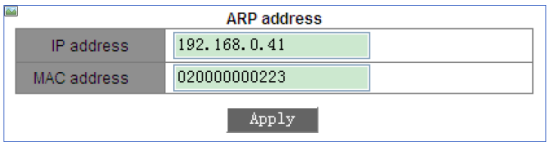
Записи ARP делятся на динамические и статические. Динамические записи генерируются и поддерживаются на основе обмена пакетами ARP. Срок действия динамических записей может истечь, они могут быть обновлены новым пакетом ARP или перезаписаны статической записью ARP. Статические записи настраиваются и поддерживаются вручную. Они не имеют срока действия и не перезаписываются динамическими записями ARP. Коммутатор поддерживает до 512 записей ARP (максимум 256 статических). Когда количество записей ARP превышает 512, новые записи автоматически перезаписывают старые динамические записи.

Настройка ARP aging time показана на следующем рисунке.



- **ARP Aging Time**
  Диапазон: 10~60 минут
  По умолчанию: 20 минут
  Функция: Настройка времени устаревания ARP.
  Описание. Время устаревания ARP — это время с момента добавления динамической записи ARP в таблицу до момента удаления записи из таблицы.

  Добавить статическую запись ARP можно как показано на следующем рисунке.

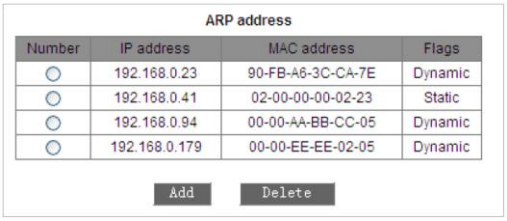


- **ARP address**
  Портфолио: {IP-адрес, MAC-адрес}
  Формат: {A.B.C.D, HHHHHHHHHHHH} (H — шестнадцатеричное число).
  Функция: настройка статической записи ARP.

IP-адрес статической записи ARP должен находиться в том же сегменте сети, что и IP-адрес коммутатора.

Если IP-адрес статической записи является IP-адресом коммутатора, система автоматически сопоставляет IP-адрес с MAC-адресом коммутатора.

Просмотреть или удалить ARP запись можно как показано на рисунке.



- **ARP address**
  Портфолио: {IP address, MAC address, Flags}
  Функция: отображение записей ARP, включая статические и динамические записи.
  Операция: выберите статическую запись в столбце «Номер». Нажмите <Delete>, чтобы удалить запись.

5.12. SNMP

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

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

- Станция управления сетью (NMS) — это станция, на которой работает программный клиент управления сетью с поддержкой SNMP. Это ядро для сетевого управления сетью SNMP.
- Агент — это процесс в управляемых сетевых устройствах. Он получает и обрабатывает пакеты запросов от NMS. Когда возникает тревога, агент заблаговременно сообщает об этом в NMS.

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

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

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

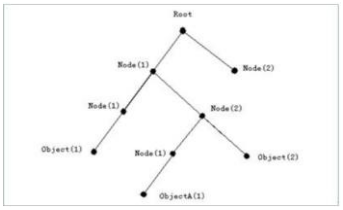
Коммутаторы этой серии поддерживают SNMPv2. SNMPv2 совместим с SNMPv1. SNMPv1 использует community для аутентификации. Имя community действует как пароль,

ограничивая доступ NMS к агентам. Если коммутатор не подтверждает имя сообщества, переносимое в пакете SNMP, пакет отбрасывается.

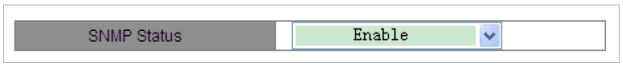
SNMPv2 также использует имя сообщества для аутентификации. Он совместим с SNMPv1 и расширяет функции SNMPv1. Чтобы обеспечить связь между NMS и агентом, их версии SNMP должны совпадать. На агенте можно настроить разные версии SNMP, чтобы он мог использовать разные версии для связи с разными NMS.

Любой управляемый ресурс называется управляемым объектом. Management Information Base (MIB) хранит управляемые объекты. Он определяет иерархические отношения управляемых объектов и атрибутов объектов, таких как имена, разрешения на доступ и типы данных. У каждого агента есть своя MIB. NMS может читать/записывать MIB на основе разрешений. На следующем рисунке показаны отношения 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 следующем рисунке, OID объекта A равен 1.2.1.1.

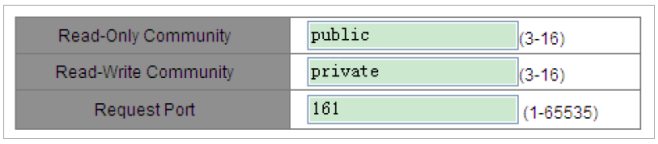


Включить SNMP можно, как показано на рисунке.



- **SNMP Status**
  Опции: Enable/Disable
  По умолчанию: Enable
  Функции: Включение или выключение SNMP

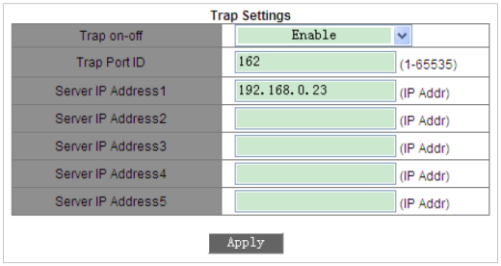
Настройка права доступа показана на следующем рисунке.



- **Read-Only Community**
  Диапазон: 3~16 символов
  По умолчанию: private
  Функция: Настройка имени сообщества только для чтения / записи.
  Описание: Информация MIB коммутатора может быть прочитана только в том случае, если community, переносимое пакетом SNMP, совпадает с именем, настроенным на коммутаторе.

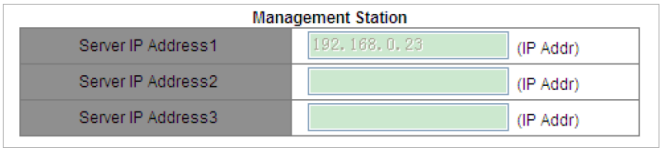
- **Request Port**
  Диапазон: 1~65535
  По умолчанию: 161
  Функция: Настройка номера порта для приема SNMP-запросов.

Установка параметров trap показана на следующем рисунке.



- **Trap on-off**
  Опции: Enable/Disable
  По умолчанию: Enable
  Функция: включить или выключить отправку ловушек.
- **Trap Port ID**
  Опции: 1~65535
  По умолчанию: 162
  Функция: Настройка номера порта для отправки сообщений-ловушек.
- **Server IP Address**
  Формат: A.B.C.D.
  Функция: Настройка адреса сервера для получения сообщений-ловушек. Вы можете настроить максимум пять серверов.

Просмотр IP-адреса сервера управления показано на следующем рисунке.



IP-адрес сервера управления не нужно настраивать вручную. Коммутатор автоматически отображает его, только если NMS работает на сервере и считывает и записывает информацию об узле MIB устройства.

5.13. ST-Ring

ST-Ring и ST-Ring+ — это проприетарные протоколы резервирования ООО "СТЭЗ". Время восстановления сети в течение 20 - 50 мс при сбое канала, обеспечивая стабильную и надежную связь. Кольца ST делятся на два типа: на основе портов (ST-Ring-Port) и на основе VLAN (ST-Ring-VLAN).

- ST-Ring-Port: указывает порт для пересылки или блокировки пакетов.
- ST-Ring-VLAN: указывает порт для пересылки или блокировки пакетов определенной VLAN. Это позволяет использовать несколько VLAN на касательном

порту, то есть один порт является частью разных резервных колец, основанных на разных VLAN.

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

5.13.1. Концепт

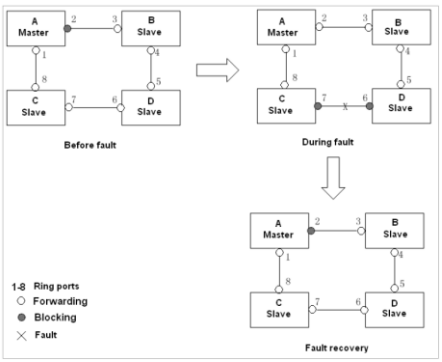
- Мастер: У одного кольца есть только один мастер. Мастер отправляет пакеты протокола ST-Ring и определяет состояние кольца. Когда кольцо закрыто, два кольцевых порта на ведущем устройстве находятся в состоянии пересылки и блокировки соответственно.
- Первичный порт: указывает кольцевой порт (на ведущем устройстве), состояние которого настроено как принудительная переадресация пользователем, когда кольцо закрыто.
- Ведомый: Кольцо может включать в себя несколько ведомых устройств. Подчиненные устройства прослушивают и пересылают пакеты протокола ST-Ring и сообщают информацию об ошибках ведущему устройству.
- Резервный порт: Порт для связи между кольцами IS называется резервным портом.
- Основной резервный порт: если кольцо имеет несколько резервных портов, резервный порт с большим MAC-адресом является основным резервным портом. Он находится в состоянии пересылки.
- Подчиненный резервный порт: если в кольце имеется несколько резервных портов, все резервные порты, кроме основного резервного порта, являются подчиненными резервными портами. Они находятся в состоянии блокировки.
- Состояние пересылки: если порт находится в состоянии пересылки, порт может как получать, так и отправлять данные.
- Состояние блокировки: если порт находится в состоянии блокировки, порт может получать и пересылать только пакеты протокола ST-Ring, но не другие пакеты.

5.13.2. Реализация ST-Ring-Port

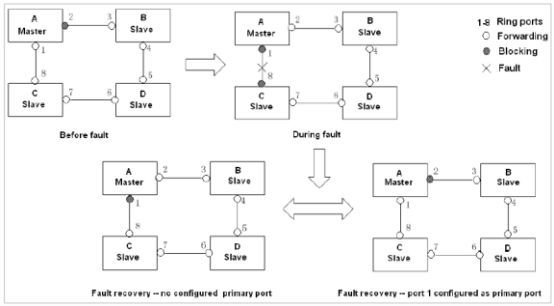
Порт пересылки на ведущем устройстве периодически отправляет пакеты протокола ST-Ring для определения состояния кольца. Если блокирующий порт мастера получает пакеты, кольцо замыкается; в противном случае кольцо разомкнуто.

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

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



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



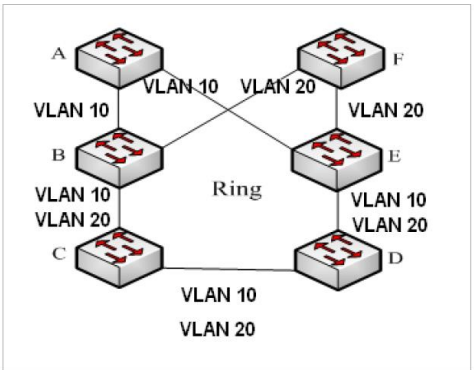
5.13.3. ST-RING-VLAN реализация

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

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

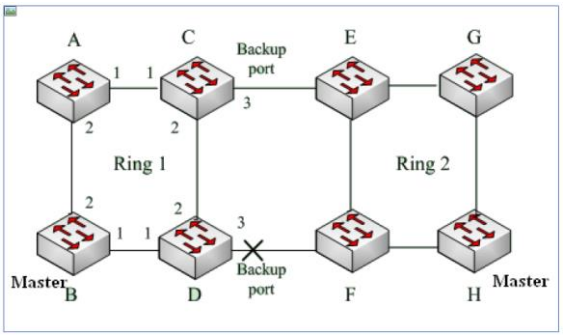
Кольцевые звенья ST-Ring-VLAN 20: FB-BC-CD-DE-EF.

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



5.13.4. ST-Ring+ Реализация

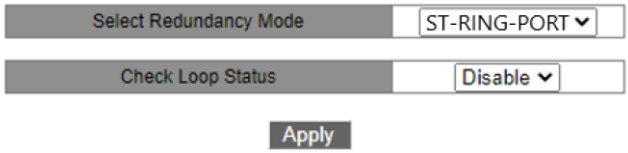
ST-Ring+ может обеспечить резервирование двух колец ST, как показано на следующем рисунке. Один резервный порт настроен соответственно на коммутаторе C и коммутаторе D. Какой порт является основным резервным портом, зависит от MAC-адресов двух портов. Если главный резервный порт или его канал выходят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



Конфигурации ST-Ring должны соответствовать следующим условиям:

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

Конфигурирование представлено на рисунке.



- **Select Redundancy Mode**
  Опции: ST-RING-PORT/ST-RING-VLAN
  По умолчанию: ST-RING-PORT
  Функция: Выбор режима резервирования.

Кольцевые протоколы на основе Port-based включают RSTP, ST-Ring-Port и DRP-Port, а кольцевые протоколы на основе VLAN-based включают ST-Ring-VLAN и DRP-VLAN.

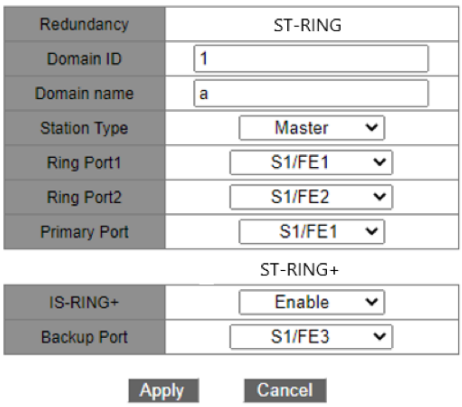
Кольцевые протоколы на основе VLAN-based являются взаимоисключающими, и для одного устройства можно настроить только тип кольцевого протокола на основе VLAN-based.

Кольцевой протокол на основе портов и кольцевой протокол на основе VLAN являются взаимоисключающими, и для одного устройства можно выбрать только один режим кольцевого протокола.

- **Check Loop Status**
  Опции: Disable/Enable
  По умолчанию: Disable
  Функция: включение или отключение определения статуса кольца.
  Описание: после включения определения состояния кольца коммутатор автоматически определяет состояние кольца. Когда некольцевой порт получает пакеты ST-Ring, порт блокируется. Поэтому используйте эту функцию с осторожностью.

Создание ST кольца представлено на рисунке.

Конфигурирование ST-Ring и ST-VLAN-Ring показано на рисунке



- **Redundancy**
  Принудительная конфигурация: ST-RING

- **Domain ID**
  Диапазон конфигурации: 1~32
  Функция: различать кольца.
  На одном коммутаторе можно настроить максимум **16 колец** на основе портов или **8 колец** на основе VLAN.
- **Domain Name**
  Диапазон: 1~31 символ
  Функция: настроить доменное имя.
- **Station Type**
  Опции: Master/Slave
  По умолчанию: Master
  Функция: выберите роль коммутатора в текущем кольце.
- **Ring Port1/Ring Port2**
  Опции: все порты коммутатора
  Функция: выберите два кольцевых порта.

Кольцевой порт ST-Ring или резервный порт нельзя добавить в trunk group. Порт, добавленный в trunk group, нельзя настроить в качестве кольцевого порта ST-Ring или резервного порта.

Кольцевой порт ST-Ring или резервный порт можно настроить как порт-источник или порт-получатель зеркалирования. Порт источника или назначения зеркалирования нельзя настроить в качестве кольцевого порта ST-Ring или резервного порта.

Кольцевые порты между кольцевыми протоколами на основе port-based RSTP, ST-Ring-Port и DRP-Port являются взаимоисключающими, то есть кольцевой порт и резервный порт ST-Ring-Port не должны быть настроены как порт RSTP, DRP-Port. кольцевой порт или резервный порт DRP-Port; Порт RSTP, кольцевой порт DRP-Port и резервный порт DRP-Port не должны быть настроены как кольцевой порт ST -Ring-Port или резервный порт.

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

- **Primary Port**
  Опции: Disable/All switch ports
  По умолчанию: Disable
  Функция: Настройка основного порта.
  Описание: Когда кольцо замкнуто, основной порт находится в состоянии пересылки.

Первичный порт (Primary Port) действует только тогда, когда кольцо закрыто.

Первичный порт (Primary Port) должен быть одним из двух кольцевых портов на ведущем устройстве.

- **ST-RING+**
  Опции: Enable/Disable
  По умолчанию: Disable
  Функция: включение или отключение функции ST-Ring+.
- **Backup Port**

Опции: все порты коммутатора

Функция: выберите один порт в качестве резервного порта.

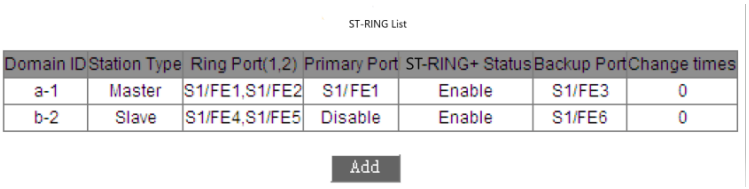
Объяснение: Резервный порт можно настроить только после включения функции ST-Ring+.

- **Add VLAN List**

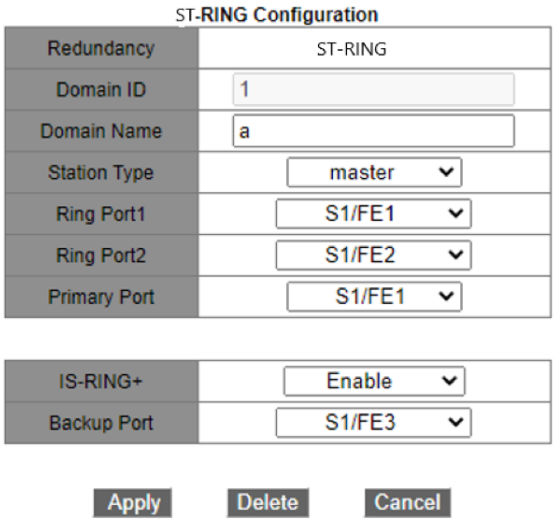
  Опции: Все созданные VLAN

  Функция: выберите VLAN, управляемые текущим кольцом ST-Ring-VLAN.

После завершения настройки созданные кольца отображаются в списке ST-RING, как показано на следующем рисунке.

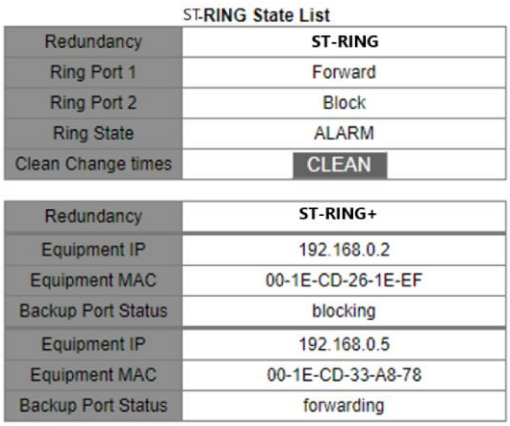


Просмотр и измените конфигурации ST-Ring.



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

Просмотр состояние ST-Ring и порта показано на следующем рисунке.



5.14. RSTP/STP

Стандартизированный в IEEE802.1D Spanning Tree Protocol (STP) представляет собой протокол локальной сети, используемый для предотвращения широковещательных штормов, вызванных петлями канала, и обеспечения резервирования канала. Устройства с поддержкой STP обмениваются пакетами и блокируют определенные порты, чтобы сократить «петли» на «деревья», предотвращая распространение и бесконечные петли. Недостаток STP заключается в том, что порт должен ждать в два раза больше задержки пересылки, чтобы перейти в состояние пересылки. Чтобы преодолеть этот недостаток, IEEE создает стандарт 802.1w в дополнение к 802.1D. IEEE802.1w определяет протокол Rapid Spanning Tree Protocol (RSTP). По сравнению с STP, RSTP достигает гораздо более быстрой конвергенции, добавляя альтернативный порт и резервный порт для корневого порта и назначенного порта соответственно. Если корневой порт недействителен, альтернативный порт может быстро войти в состояние пересылки.

5.14.1. Концепт.

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

5.14.2. BPDU

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

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

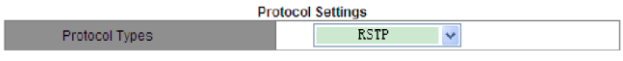
1. На начальном этапе каждый порт всех устройств генерирует BPDU с самим собой в качестве корневого моста; и идентификатор корневого моста, и идентификатор

назначенного моста являются идентификатором локального устройства; стоимость корневого пути равна 0; назначенный порт является локальным портом.

2. Выбор лучшего BPDU: все устройства отправляют свои собственные BPDU и получают BPDU от других устройств. При получении BPDU каждый порт сравнивает полученный BPDU со своим.
   - Если приоритет собственного BPDU выше, то порт не выполняет никаких операций.
   - Если приоритет полученного BPDU выше, то порт заменяет локальный BPDU на полученный.

   Устройства сравнивают BPDU всех портов и определяют лучший BPDU. Принципы сравнения BPDU следующие:
   - BPDU с меньшим идентификатором корневого моста имеет более высокий приоритет.
   - Если идентификаторы корневого моста двух BPDU совпадают, сравнивается их стоимость корневого пути. Если чем меньше стоимость корневого пути в BPDU плюс стоимость пути локального порта, тем выше приоритет BPDU.
   - Если стоимость корневого пути двух BPDU также одинакова, назначенные идентификаторы моста, назначенные идентификаторы портов и идентификаторы порта, получающего BPDU, далее сравниваются по порядку. BPDU с меньшим идентификатором имеет более высокий приоритет. BPDU с меньшим идентификатором корневого моста имеет более высокий приоритет. 3.
3. Выбор корневого моста: Корневой мост связующего дерева — это мост с наименьшим идентификатором моста.
4. Выбор корневого порта. Устройство без корневого моста выбирает порт, получающий лучший BPDU, в качестве корневого порта.
5. Расчет BPDU назначенного порта. На основе BPDU корневого порта и стоимости пути корневого порта устройство вычисляет BPDU назначенного порта для каждого порта следующим образом:
   - Замените идентификатор корневого моста идентификатором корневого моста BPDU корневого порта.
   - Замените стоимость корневого пути на стоимость корневого пути BPDU корневого порта плюс стоимость пути. корневого порта.
   - Замените назначенный идентификатор моста идентификатором локального устройства.
   - Замените назначенный идентификатор порта идентификатором локального порта.
6. Выбор назначенного порта: если рассчитанный BPDU лучше, то устройство выбирает порт в качестве назначенного порта, заменяет BPDU порта рассчитанным BPDU и отправляет рассчитанный BPDU. Если BPDU порта лучше, то устройство не обновляет BPDU порта и блокирует порт. Заблокированные порты могут получать и пересылать только пакеты RSTP, но не другие пакеты.

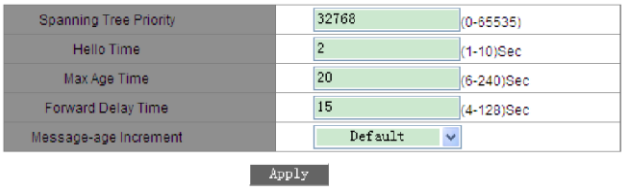
Включите STP/RSTP можно, как показано на следующем рисунке.



- **Protocol Types**
  Опции: Disable /RSTP/STP

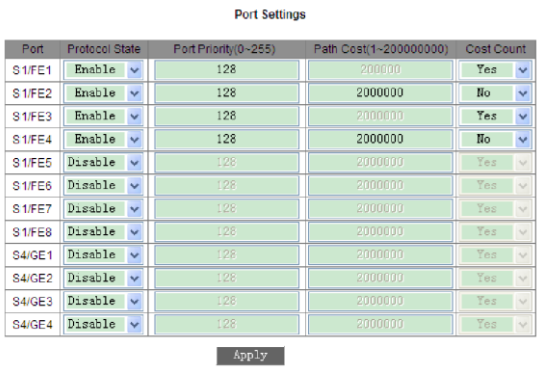
По умолчанию: Disable
Функция: отключить или включить RSTP или STP.

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



- **Spanning Tree Priority**
  Диапазон: 0~65535. Шаг 4096.
  По умолчанию: 32768
  Функция: настройка приоритета сетевого моста.
  Описание: Приоритет используется для выбора корневого моста. Чем меньше значение, тем выше приоритет.
- **Hello Time**
  Диапазон: 1~10 с
  По умолчанию: 2 с
  Функция: Настройка интервала отправки BPDU.
- **Max Age Time**
  Диапазон: 6~240 с
  По умолчанию: 20 с
  Описание: Если значение возраста сообщения в BPDU превышает указанное значение, то BPDU отбрасывается.
- **Forward Delay Time**
  Диапазон: 4~128 с
  По умолчанию: 15 с
  Функция: настройка времени изменения статуса с «Отбраковка» на «Обучение» или с «Обучение» на «Пересылка».
- **Message-age Increment**
  Варианты: Compulsion/Default
  По умолчанию: Default
  Функция: Настройте значение, которое будет добавляться к возрасту сообщения, когда BPDU проходит через сетевой мост.
  Описание: В принудительном режиме значение равно 1. В режиме по умолчанию значение равно max (max age time/16, 1).
  Forward Delay Time, Max Age Time, и Hello Time должны соответствовать следующим требованиям: 2 x (Forward Delay Time — 1,0 секунды) ≥ Max Age Time;
  Max Age Time ≥ 2 x (Hello Time + 1,0 секунды).

Включите RSTP на портах, как показано на следующем рисунке.



- **Protocol State**
  Опции: Enable/Disable
  По умолчанию: Disable
  Функция: включить или отключить STP на портах.

Порт RSTP нельзя настроить в качестве порта источника или порта назначения зеркалирования. Зеркальный исходный или целевой порт не может быть настроен как порт RSTP.

Порт RSTP нельзя добавить в группу trunk group. Порт, добавленный в группу trunk group, нельзя настроить как порт RSTP.

Кольцевые порты между кольцевыми протоколами на основе портов RSTP, ST-Ring-Port и DRP-Port являются взаимоисключающими, то есть порт RSTP не должен быть настроен как кольцевой порт ST-Ring-Port/DRP-Port или ST-Port. Резервный порт Ring-Port/ DRP-Port; Кольцевой порт ST-Ring-Port/DRP-Port и резервный порт ST-Ring-Port/DRP-Port не должны быть настроены как порт RSTP.

Не рекомендуется одновременно настраивать порты в группе изоляции как порты RSTP, а порты RSTP нельзя одновременно добавлять в группу изоляции.

- **Port Priority**
  Диапазон: 0~255. Шаг 16.
  По умолчанию: 128
  Функция: Настройка приоритета порта, который определяет роли портов.
- **Path Cost**
  Диапазон: 1~200000000
  По умолчанию: 2000000 (порт 10M), 200000 (порт 100M), 20000 (порт 1000M)
  Описание: Стоимость пути порта используется для расчета наилучшего пути. Значение параметра зависит от пропускной способности. Чем больше значение, тем ниже стоимость. Вы можете изменить роль порта, изменив значение параметра стоимости пути. Чтобы настроить значение вручную, выберите Нет для счетчика затрат.
- **Cost Count**
  Диапазон: Yes/No
  По умолчанию: Yes
  Описание: “Yes“ указывает, что стоимость пути порта принимает значение по умолчанию. “No” означает, что вы можете настроить стоимость пути.

Просмотреть состояние RSTP можно, как показано на следующем рисунке.

Root Info

Root MAC	00:1e:cd:11:01:b1
Root Priority	0x1000
Root Path Cost	200000
Root Port	S1/FE2
Max Age(s)	20
Hello Time(s)	2
Forward Delay(s)	15

Bridge Info

Bridge MAC	00:00:00:00:19:39
Bridge Priority	0x8000
Bridge Version	2
Max Age(s)	20
Hello Time(s)	2
Forward Delay(s)	15

Port Info

Port	Priority	Path Cost	Role	State	Link State
S1/FE1	0x80	2000000	Disabled	Discarding	Down
S1/FE2	0x80	200000	Root	Forwarding	Up
S1/FE3	0x80	2000000	Disabled	Discarding	Down
S1/FE4	0x80	200000	Alternate	Discarding	Up

5.15. DRP

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

В соответствии со стандартом IEC 62439-6 DRP использует механизм выбора мастера без фиксированного мастера. ISRP предоставляет следующие возможности:

- Время восстановления, не зависящее от масштаба сети DRP обеспечивает время восстановления, не зависящее от масштаба сети, за счет оптимизации механизма пересылки пакетов обнаружения кольца.
  DRP позволяет сетям восстанавливаться в течение 20 мс благодаря введению прерывания отчетов в реальном времени, что повышает надежность передачи данных в реальном времени. Эта функция позволяет коммутаторам обеспечивать более высокую надежность для приложений в энергетике, железнодорожном транспорте и многих других отраслях, требующих управления в режиме реального времени.
- Разнообразные функции обнаружения канала.
  Для повышения стабильности сети DRP предоставляет разнообразные функции обнаружения каналов для типичных сетевых сбоев, включая обнаружение быстрого отключения, обнаружение однонаправленных каналов оптоволокна, проверку качества каналов и проверку работоспособности оборудования, обеспечивая правильную передачу данных.
- Применимо к нескольким сетевым топологиям
  Помимо быстрого восстановления для простых кольцевых сетей, DRP также поддерживает сложные кольцевые топологии, такие как пересекающиеся кольца и касательные кольца. Кроме того, DRP поддерживает несколько экземпляров на основе VLAN, что подходит для различных сетевых приложений с гибкой сетью.
- Мощные функции диагностики и обслуживания
  ISRP предоставляет мощные механизмы запросов о состоянии и сигналов тревоги для диагностики и обслуживания сети, а также механизм предотвращения

непреднамеренных операций и неправильных конфигураций, которые могут привести к кольцевым сетевым штормам.

5.15.1. Концепт

- Режимы DRP
  DRP включает два режима: DRP-Port-Based и DRP-VLAN-Based.
  DRP-Port-Based: перенаправляет или блокирует пакеты на основе определенных портов.
  DRP-VLAN-Based: перенаправляет или блокирует пакеты на основе VLAN. Если порт находится в состоянии блокировки, блокируются только пакеты данных указанной сети VLAN. Таким образом, на портах касательного кольца можно настроить несколько VLAN. Порт может принадлежать разным кольцам ISRP 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.
- Роли DRP. DRP определяет роли коммутаторов, пересылая пакеты Announce, предотвращая образование петель в кольцах избыточности.
  INIT: указывает устройство, на котором включен DRP, а два кольцевых порта находятся в состоянии Link down.
  Root: указывает устройство, на котором включен DRP, и по крайней мере один кольцевой порт находится в состоянии соединения. В кольце корень выбирается в соответствии с векторами пакетов Announce. Это может измениться в зависимости от топологии сети. Root периодически отправляет свои собственные пакеты Announce на другие устройства. Статусы портов кольца: Один порт кольца находится в состоянии пересылки, а другой — в состоянии блокировки. Получив пакет Announce от другого устройства, Root сравнивает вектор пакета с вектором своего собственного пакета Announce. Если вектор полученного пакета больше, Root меняет свою роль на Normal или B-Root в зависимости от состояния канала и ухудшения CRC портов.
  B-Root: указывает устройство, на котором включен ISRP, отвечающее хотя бы одному из следующих условий: один кольцевой порт находится в состоянии соединения, а другой — в состоянии соединения, деградация CRC, приоритет не менее 200. B-Root сравнивает и пересылает пакеты Announce. Если вектор полученного пакета оповещения меньше вектора его собственного пакета оповещения, B-Root меняет свою роль на Root; в противном случае он пересылает полученный пакет и не меняет свою роль. Статусы портов кольца: Один порт кольца находится в состоянии пересылки. Нормальный: указывает устройство, на котором включен ISRP, и оба кольцевых порта находятся в состоянии соединения без ухудшения CRC, а приоритет выше 200. Нормальный только пересылает пакеты Announce, но не проверяет содержимое пакетов. Статусы кольцевых портов: Оба кольцевых порта находятся в состоянии пересылки.

5.15.2. Реализация

Каждый коммутатор поддерживает свой собственный вектор пакета Announce. Коммутатор с большим вектором будет выбран корневым. Вектор пакета Announce содержит следующую информацию для назначения роли.

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

Link status: Значение устанавливается равным 1, если один кольцевой порт находится в состоянии Link down, и устанавливается в 0, если оба кольцевых порта находятся в состоянии Link up.
CRC degradation status: если деградация CRC происходит на одном порту, значение устанавливается равным 1. Если деградация CRC не происходит на двух кольцевых портах, значение устанавливается равным 0.
CRC degradation rate: отношение количества пакетов CRC к порогу за 15 минут.
Role priority: значение можно установить в веб-интерфейсе.

Параметры в таблице сравниваются по следующей процедуре:

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

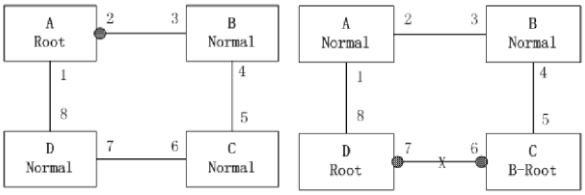
5.15.3. Реализация режима DRP-Port-Based

Роли коммутаторов следующие:

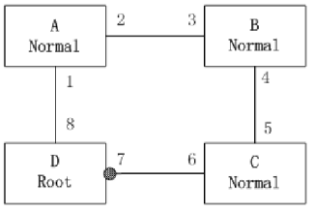
1. При запуске все коммутаторы находятся в состоянии INIT. Когда состояние одного порта изменяется на Link up, коммутатор становится корневым и отправляет пакеты Announce другим коммутаторам в кольце для выбора.
2. Коммутатор с наибольшим вектором пакета Announce выбирается корневым. Кольцевой порт, который подключается к корневому каналу первым, 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 в состоянии ухудшения CRC является B-Root. Коммутатор с обоими кольцевыми портами в состоянии Link up и отсутствием ухудшения CRC является нормальным.

Процедура устранения неисправности следующая:

1. В исходной топологии A — Root; порт 1 находится в состоянии пересылки, а порт 2 в состоянии блокировки. B, C и D являются нормальными, и их кольцевые порты находятся в состоянии пересылки, как показано на следующем рисунке.



2. Когда линк CD неисправен, ISRP изменяет статусы портов 6 и 7 на блокировку. В результате C и D становятся корнями. Поскольку A, C и D в данный момент являются корневыми, все они отправляют пакеты Announce. Векторы C и D больше, чем векторы A, потому что порты 7 и 6 находятся в состоянии Link Down. В этом случае, если вектор D больше, чем вектор C, D выбирается в качестве корня, а C становится корнем B. При получении пакета Announce от D, A обнаруживает, что вектор D больше, чем его собственный вектор, и оба его кольцевых порта находятся в состоянии Link up. Таким образом, A становится нормальным и меняет статус порта 2 на пересылку, как показано на предыдущем рисунке.

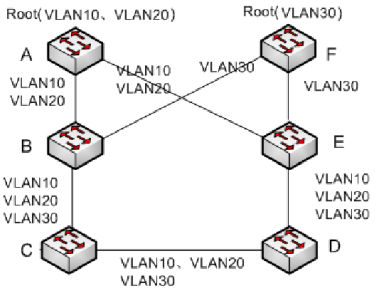


3. Когда канал CD восстанавливается, D по-прежнему является корневым, поскольку его вектор больше, чем вектор C. Поскольку D является корневым, порт 7 находится в состоянии блокировки. В этом случае порт 6 находится в состоянии Link up, поэтому DRP изменяет состояние порта 6 на переадресацию. В результате C становится Normal. Поэтому роли коммутаторов не меняются при восстановлении канала.

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

5.15.4. Реализация режима DRP-VLAN-Based

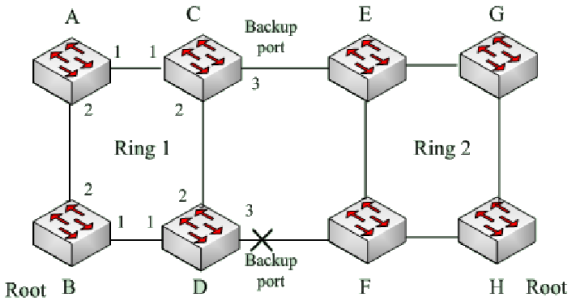
Кольцо на основе DRP-VLAN позволяет пересылать пакеты из разных VLAN по разным путям. Каждый путь пересылки для VLAN образует DRP-VLAN-Based. Различные кольца на основе DRP-VLAN могут иметь разные корни. Как показано на следующем рисунке, настроены два кольца на основе DRP-VLAN. Кольцевые каналы DRP-VLAN10/20-Based: AB-BC-CD-DE-EA. Кольцевые каналы DRP-VLAN30-Based: FB-BC-CD-DE-EF. Два кольца касаются звеньев BC, CD и DE. Коммутатор C и коммутатор D используют одни и те же порты в двух кольцах, но используют разные логические каналы на основе VLAN.



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

5.15.5. Резервирование ISRP

DRP также может обеспечивать резервирование 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 основным резервным портом, который находится в состоянии пересылки. Все остальные резервные порты являются подчиненными. Они находятся в состоянии блокировки. Как показано на следующем рисунке, на каждом коммутаторе можно настроить один резервный порт. Главный резервный порт находится в состоянии пересылки, а другие резервные порты — в состоянии блокировки. Если главный резервный порт или его канал неисправен, для пересылки данных будет выбран подчиненный резервный порт.



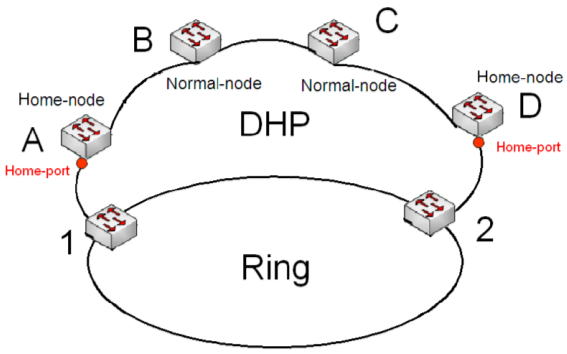
Изменение статуса канала влияет на статус резервных портов.

5.16. DHP

Как показано на следующем рисунке, A, B, C и D смонтированы на кольце. Протокол двойного подключения ISHP выполняет следующие функции, если он включен на A, B, C и D:

- A, B, C и D могут общаться друг с другом, не влияя на правильную работу устройства в кольце.

- Если связь между A и B неисправна, A все еще может связываться с B, C и D посредством Устройство 1 и Устройство 2.



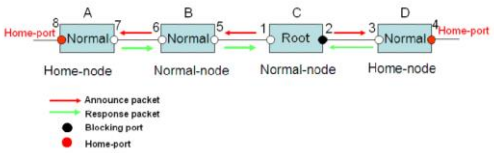
5.16.1. Концепт

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

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

- Отправка ответных пакетов в корневую зону при получении пакетов Announce из корневой зоны. Корень идентифицирует состояние кольца как закрытое, если он получает ответные пакеты. Если корень не получает ответные пакеты, он идентифицирует состояние кольца как открытое.
- Блокирование пакетов ISRP внешних сетей, и изоляция канала ISHP от внешних сетей.
- Отправка пакетов очистки входа на подключенные устройства во внешних сетях при изменении топологии канала ISHP. Обычный узел: указывает устройства в канале DHP, исключая устройства на обоих концах. Нормальные узлы передают ответные пакеты Home-node.

5.16.2. Реализация



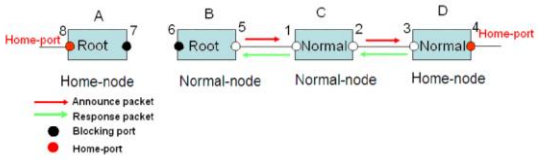
Как показано на рисунке, конфигурации A, B, C и D на рисунке 6 следующие:

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

Реализация:

a. C, Root, посылает пакеты Announce через свои два кольцевых порта. Домашний порт 8 и домашний порт 4 завершают полученные пакеты Announce и отправляют ответные пакеты на C. C идентифицирует состояние кольца как закрытое. Порт 2 находится в состоянии блокировки.

b. Когда канал между A и B заблокирован, топология включает два канала: A и B-C-D.
   - A избирается корнем. Порт 7 находится в состоянии блокировки.
   - B ссылке B-C-D B выбран в качестве корня. Порт 6 находится в состоянии блокировки. C становится нормальным. Порт 2 находится в состоянии пересылки. A может связываться с B, C и D через устройство 1 и устройство 2, как показано на следующем рисунке.



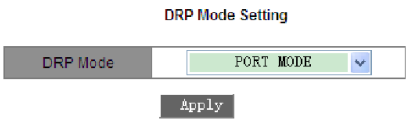
5.16.3. Описание

Конфигурации DRP отвечают следующим требованиям:

- Все коммутаторы в одном кольце должны иметь одинаковый номер домена.
- Одно кольцо содержит только один корень, но может содержать несколько корней B или нормалей.
- На каждом коммутаторе можно настроить только два порта для кольца.
- 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.

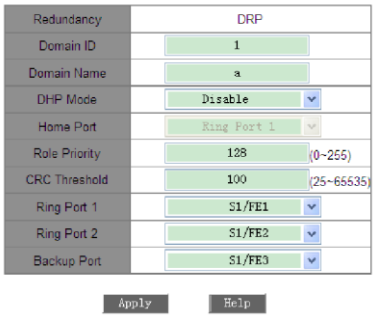
5.16.4. Конфигурация

Настройте режим DRP, как показано на следующем рисунке.



- **ISRP Mode**
  Опции: PORT MODE/VLAN MODE
  По умолчанию: PORT MODE
  Функция: Настройка режима DRP

Настройте кольцо DRP-Port-Based, как показано на следующем рисунке.



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

Не настраивайте кольцевой порт в качестве резервного порта.

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

DRP List

Domain ID	Role Status	Ring Port(1,2)	Backup Port	Ring Status
1-a	ROOT	S1/FE1,S1/FE2	S1/FE3	Ring-Close

Кольцевой порт DRP или резервный порт нельзя добавить в группу trunk group. Порт добавлен в trunk group не может быть настроена как кольцевой порт DRP или резервный порт.

Кольцевой порт DRP или резервный порт можно настроить как порт-источник или порт-получатель зеркального отображения. Порт источника или назначения зеркального отображения нельзя настроить в качестве кольцевого порта DRP или резервного порта.

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

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

Просмотр настройки параметров DRP-Port-Based.

Щелкните запись DRP на рисунке выше, вы можете просмотреть и изменить настройки параметров записи, как показано на следующем рисунке.

DRP Setting

Redundancy	DRP
Domain ID	1
Domain Name	a
DHP Mode	Disable
Home Port	Ring Port 1
Role Priority	128 (0~255)
CRC Threshold	100 (25~65535)
Ring Port 1	S1/FE1
Ring Port 2	S1/FE2
Backup Port	S1/FE3

Apply Delete Cancel Help

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

Просмотр роли и состояние портов кольца DRP, как показано на следующем рисунке.

DRP Status

Role Status	ROOT
Ring Port 1	FORWARD
Ring Port 2	BLOCK
Backup Port	BLOCK
Ring Status	Ring-Close
IP Address	192.168.0.222
MAC Address	08-00-3E-32-53-22

5.17. QoS

Quality of Service (QoS) позволяет предоставлять дифференцированные услуги на основе различных требований при ограниченной пропускной способности посредством управления трафиком и распределения ресурсов в IP-сетях. QoS пытается удовлетворить передачу различных услуг, чтобы уменьшить перегрузку сети и свести к минимуму влияние перегрузки на услуги с высоким приоритетом. QoS в основном включает в себя идентификацию услуг, управление перегрузками и предотвращение перегрузок.
Идентификация службы: объекты идентифицируются на основе определенных правил соответствия. Например, объекты могут быть тегами приоритета, переносимыми пакетами, приоритетом, отображаемым портами и виртуальными локальными сетями, или информацией о приоритете, отображаемой пятерками. Идентификация услуги является предварительным условием для QoS. Управление перегрузками: это обязательно для решения проблемы конкуренции за ресурсы. Управление перегрузками кэширует пакеты в очередях и определяет последовательность пересылки пакетов на основе определенного алгоритма планирования, обеспечивая приоритетную пересылку для ключевых служб. Предотвращение перегрузки: Чрезмерная перегрузка может привести к повреждению сетевых ресурсов. Предотвращение перегрузки отслеживает использование сетевых ресурсов. При обнаружении увеличения перегрузки функция использует упреждающее отбрасывание пакетов и настраивает объем трафика для решения проблемы перегрузки.

Каждый порт коммутатора имеет четыре очереди кэширования, от 0 до 3 в порядке возрастания приоритета. Вы можете настроить сопоставление между приоритетом и очередями. Когда кадр достигает порта, коммутатор определяет очередь для кадра в соответствии с информацией в заголовке кадра. Коммутатор поддерживает пять режимов сопоставления очередей для определения приоритета: наивысший приоритет, на основе портов, DIFF, TOS/DIFF и 802.1p.

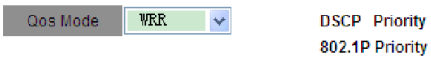
- Если для порта настроен наивысший приоритет, то пакеты для пересылки помещаются в очередь 3.
- Если для порта настроен режим сопоставления очередей на основе портов, полученные пакеты помещаются в очередь в соответствии с приоритетом порта по умолчанию. Сопоставление между приоритетом по умолчанию и очередями соответствует сопоставлению между приоритетом 802.1p и очередями.
- Значение DIFF зависит от DSCP в пакетах, тогда как значение TOS/DIFF зависит от TOS/DSCP в пакетах. Вы можете настроить сопоставление между приоритетом и очередями. ¬ Когда пакет помечен, значение 802.1p зависит от приоритета 802.1Q в пакет. Когда пакет не помечен, значение 802.1p зависит от приоритета порта по умолчанию. Вы можете настроить сопоставление между приоритетом 802.1p и

очередями. При пересылке данных порт использует режим планирования для планирования данных четырех очередей и пропускной способности каждой очереди. Коммутатор поддерживает два режима планирования: взвешенный циклический алгоритм (WRR), режим Hq-вытеснения и режим STRICT.

- В режиме WRR потоки данных планируются на основе коэффициента веса. Очереди получают свою пропускную способность исходя из соотношения их веса. WRR отдает приоритет очередям с высоким соотношением веса. Больше пропускной способности выделяется очередям с более высоким коэффициентом веса.
- В режиме Hq-preempt приоритетно 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.
- В режиме STRICT предпочтительнее 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.

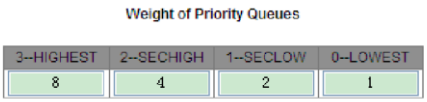
5.17.1. Конфигурирование

Настройте режим QoS, как показано на следующем рисунке.



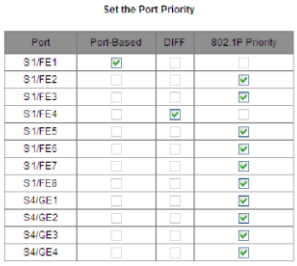
- **Qos Mode**
  Варианты: Disable/WRR/STRICT
  По умолчанию: STRICT
  Функция: Настройка режима планирования порта.

Настройте коэффициент веса очереди, как показано на следующем рисунке.



- **{3-HIGHEST, 2-SECHIGH, 1-SECLOW, 0-LOWEST}**
  Диапазон: {1~55, 1~55, 1~55, 1~55}
  По умолчанию: {8, 4, 2, 1}
  Функция: настроить коэффициент веса очереди, соблюдая следующие правила: Вес очереди 3 ≥ 2 × Вес очереди 2, Вес очереди 2 ≥ 2 × Вес очереди 1, Вес очереди 1 ≥ 2 × Вес очереди 0

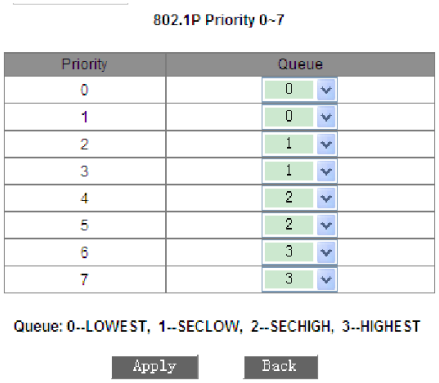
Настройте режим сопоставления приоритетов портов QoS, как показано на следующем рисунке.



- **Set the Port Priority**
  Опции: Port-Based/DIFF/802.1P Priority
  По умолчанию: 802.1P Priority.
  Функция: Настройка режима отображения приоритета портов.
  Описание: Для каждого порта можно выбрать только один режим отображения приоритета.

Настройте отображение приоритетной очереди на основе портов/802.1p.

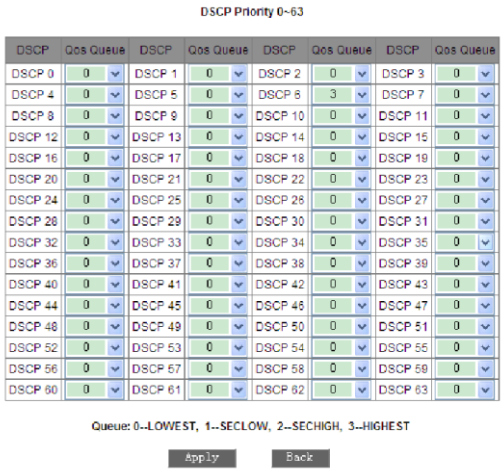
Отображение очереди в режиме на основе портов согласуется с отображением очереди в режиме приоритета 802.1p. Если вы хотите настроить любой из двух режимов, задайте параметры в таблице сопоставления приоритетов 802.1p, как показано на следующем рисунке. Нажмите <802.1p Priority>, отобразится следующая страница.



- **802.1P Priority**
  Портфолио: {Приоритет, Очередь}
  Диапазон: {0~7, 0~3}
  По умолчанию: приоритеты 0 и 1 сопоставляются с очередью 0; приоритеты 2 и 3 сопоставляются с очередью 1.
  Приоритеты 4 и 5 сопоставляются с очередью 2; приоритеты 6 и 7 сопоставляются с очередью 3.
  Функция: настройка сопоставления между приоритетом 802.1p и очередью.

Настройте сопоставление очереди приоритетов DSCP.

Щелкните <DSCP Priority >, чтобы настроить сопоставление очереди приоритетов DSCP, как показано на следующем рисунке.



- **DSCP Priority**
  Портфолио: {DSCP, Qos Queue}
  Диапазон: {0~63, 0~3}
  По умолчанию: приоритет от 0 до 63 сопоставляется с очередью 0.
  Функция: Настройка сопоставления между приоритетом DSCP и очередью.

1.1. MAC Address Aging Time

Порты коммутатора могут автоматически запоминать адреса. Коммутатор добавляет исходные адреса (MAC-адрес источника, номер порта коммутатора) полученных кадров в таблицу адресов. Время устаревания начинается с момента добавления динамического MAC-адреса в таблицу MAC-адресов. Если ни один порт не получает кадр с MAC-адресом в течение времени устаревания, в один-два раза превышающего время устаревания, коммутатор удаляет запись о MAC-адресе из таблицы адресов динамической пересылки. Статическая таблица MAC-адресов не включает понятие времени устаревания.

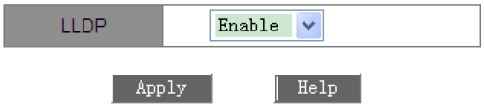
Настроить MAC address aging time можно, как показано на следующем рисунке.

- **MAC Aging Time**
  Диапазон: 15~3600 секунд
  По умолчанию: 300 секунд
  Описание: Вы можете настроить время старения по мере необходимости.

5.18. LLDP

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

Включите протокол LLDP, как показано на следующем рисунке.



- **LLDP**
  Опции: Enable/Disable
  По умолчанию: Enable
  Функция: включить/отключить протокол LLDP.
  Объяснение: Если LLDP включен, коммутатор будет отправлять сообщения LLDP своим соседним устройствам, в то же время получая и обрабатывая сообщения LLDP от соседних устройств. Если LLDP отключен, коммутатор не отправляет и не обрабатывает сообщения LLDP.

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

LLDP Information

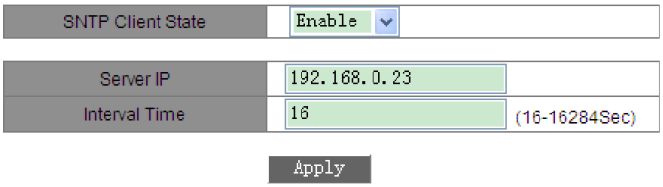
Local Port	Remote Port	Neighbor IP	Neighbor MAC
1/1	0/1	192.168.0.109	00:00:ee:ee:02:05

В информации LLDP вы можете просмотреть информацию о соседних устройствах, включая номер порта соседнего устройства, подключенного к локальному коммутатору, IP-адрес и MAC-адрес соседнего устройства.

5.19. SNTP

Simple Network Time Protocol (SNTP) синхронизирует время между сервером и клиентом с помощью запросов и ответов. Как клиент коммутатор синхронизирует время с сервером по пакетам сервера. В этом случае можно настроить максимум четыре SNTP-сервера, но только один из них может быть активен одновременно. Коммутатор также может служить сервером SNTP для обеспечения синхронизации времени для клиентов. Клиент SNTP отправляет запрос на каждый сервер один за другим через одноадресную рассылку. Сервер, ответивший первым, находится в активном состоянии. Остальные серверы находятся в неактивном состоянии.

Для включения SNTP выберите сервер и задайте соответствующие параметры, как показано на следующем рисунке.



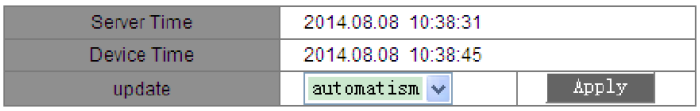
- **SNTP Client State**
  Опции: Enable/Disable
  По умолчанию: Disable
  Функция: Включить/Выключить SNTP.
- **Server IP**

Формат: A.B.C.D.

Функция: Установите IP-адрес сервера SNTP. Клиент синхронизирует время с сервером на основе пакетов, отправляемых сервером.

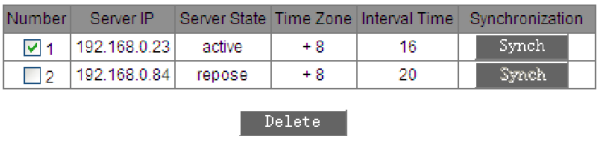
- **Interval Time**
  Диапазон: 16~16284c
  Функция: Настройка интервала отправки запросов на синхронизацию от SNTP-клиента на сервер.
- **time zone**
  Варианты: 0, +1, +2, +3, +4, +5, +6, +7, +8, +9, +10, +11, +12, +13, -1, -2, - 3, -4, -5, -6, -7, -8, -9, -10, -11, -12
  По умолчанию: 0
  Функция: выбор местного часового пояса.

Выберите режим синхронизации между клиентом и сервером, как показано на следующем рисунке.



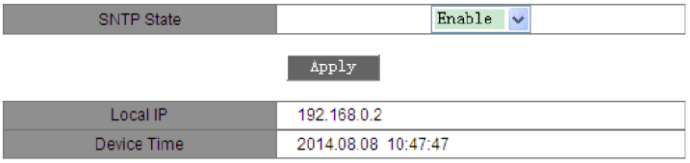
- **Server Time**
  Функция: отображение последнего времени устройства, полученного с сервера.
- **Device Time**
  Функция: отображение местного времени устройства.
- **update**
  Опции: automatism/manual
  По умолчанию: automatism
  Функция: выберите режим синхронизации времени между устройством и сервером.

Просмотреть конфигурацию SNTP можно, как показано на следующем рисунке. Вы можете установить флажок сервера SNTP и нажать <Delete>, чтобы удалить его.



- **Server State**
  Опции: active/repose
  Описание: Активный сервер предоставляет время SNTP для клиента. Одновременно в активном состоянии может находиться только один сервер.
- **Synchronization**
  Чтобы синхронизировать время вручную, нажмите < Synch>.

Настройте коммутатор в качестве сервера SNTP, как показано на следующем рисунке.



- **SNTP State**
  Опции: Enable/Disable
  По умолчанию: Disable
  Функция: Включите или отключите функцию сервера SNTP.
- **time zone**
  Варианты: 0, +1, +2, +3, +4, +5, +6, +7, +8, +9, +10, +11, +12, +13, -1, -2, - 3, -4, -5, -6, -7, -8, -9, -10, -11, -12
  По умолчанию: +8
  Функция: выбор местного часового пояса.

5.20. Port Isolate

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

Включите изоляцию портов, можно как показано на рисунке

Port	Isolate Enable
S1/FE1	☑
S1/FE2	☑
S1/FE3	☑
S1/FE4	☐
S1/FE5	☐
S1/FE6	☐
S1/FE7	☐
S1/FE8	☐
S2/FE1	☐

- **Isolate Enable**
  Опции: Enable/Disable
  По умолчанию: Disable
  Функция: Включить или отключить изоляцию порта.

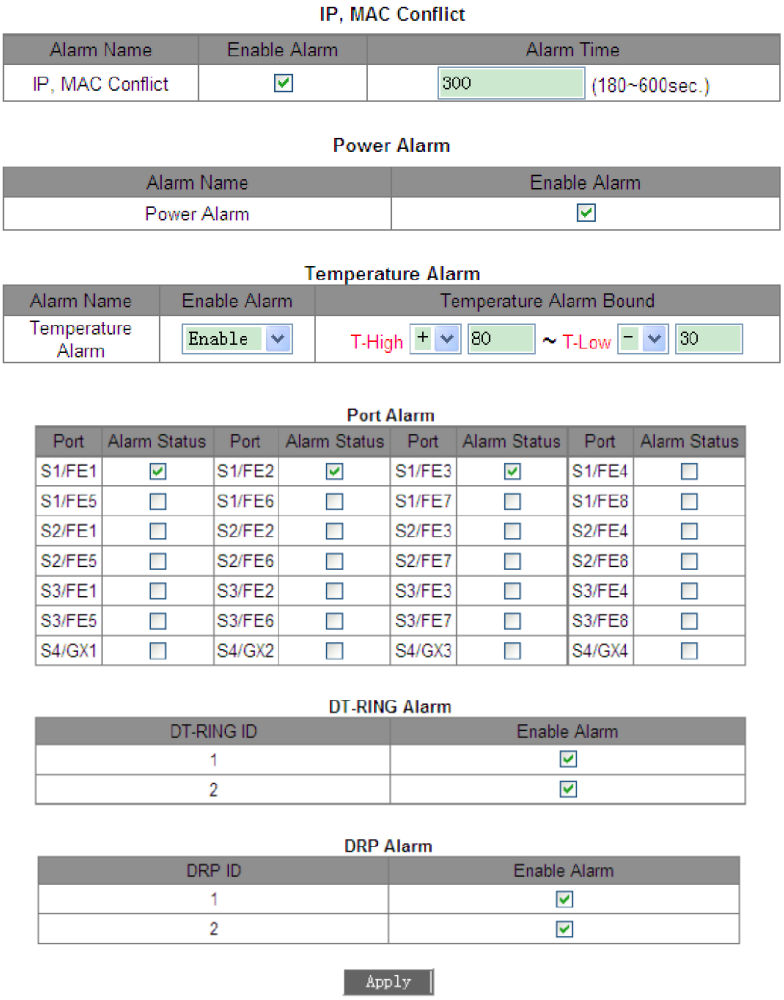
5.21. Аварийная сигнализация

Коммутаторы этой серии поддерживают следующие типы аварийных сигналов:

- Аварийный сигнал мощности: если функция включена, то аварийный сигнал будет сгенерирован для одного источника питания. вход.
- Аварийный сигнал температуры: если функция включена, то аварийный сигнал будет сгенерирован, когда температура будет равна или ниже нижнего предела или равна или выше верхнего предела.

- Аварийный сигнал конфликта IP/MAC: если функция включена, то для Конфликт IP/MAC.
- Аварийный сигнал порта: если функция включена, то для порта, находящегося в состоянии отсутствия связи, будет сгенерирован аварийный сигнал.
- Аварийный сигнал кольцевой топологии: Если функция включена, то при разомкнутом звонке будет сгенерирован сигнал тревоги.

Установить параметры тревоги, как показано на следующих рисунках.



- **IP, MAC Conflict**
  Опции: select/deselect
  По умолчанию: select
  Функция: включение или отключение оповещения о конфликте IP/MAC.
- **Alarm Time**
  Диапазон: 180~600 с
  По умолчанию: 300 с
  Функция: настройка интервала обнаружения конфликтов IP/MAC.
- **Power Alarm**
  Опции: select/deselect
  По умолчанию: select
  Функция: Включить или отключить сигнализацию питания.
- **Temperature Alarm (Alarm Enable, T-High~T-Low)**
  Диапазон: {Enable/Disable, +150℃~-55℃}

По умолчанию: { Disable, +80℃~-30℃}

Функция: включение или выключение аварийного сигнала температуры и настройка верхнего и нижнего пределов.

- **Port Alarm**

  Опции: select/deselect

  По умолчанию: deselect

  Функция: включить или выключить тревогу порта.

- **ST-RING/DRP Alarm**

  Опции: select/deselect

  По умолчанию: deselect

  Функция: включение или выключение функции тревоги ST-Ring/DRP.

После включения функции тревоги информация о тревоге выглядит следующим образом:

Basic Vision

Alarm Title	Alarm Status
power	WARN
temperature	NONE
IP Alarm	Normal
MAC Alarm	Normal

Port Alarm

Port	Alarm Status	Port	Alarm Status	Port	Alarm Status	Port	Alarm Status
S1/FE1	Link Up	S1/FE2	Link Up	S1/FE3	Link Down	S1/FE4	-
S1/FE5	-	S1/FE6	-	S1/FE7	-	S1/FE8	-
S2/FE1	-	S2/FE2	-	S2/FE3	-	S2/FE4	-
S2/FE5	-	S2/FE6	-	S2/FE7	-	S2/FE8	-
S3/FE1	-	S3/FE2	-	S3/FE3	-	S3/FE4	-
S3/FE5	-	S3/FE6	-	S3/FE7	-	S3/FE8	-
S4/GX1	-	S4/GX2	-	S4/GX3	-	S4/GX4	-

DT-RING Alarm

DT-RING ID	Alarm Status
2	Ring Open
1	Ring Close

DRP Alarm

DRP ID	Alarm Status
1	Normal
2	Alarm

- **Power**

  Опции: Normal/WARN

  Описание: После включения аварийного сигнала питания для двух входов питания отображается «Нормальный», а для одного входа питания отображается «ПРЕДУПРЕЖДЕНИЕ».

- **temperature**

  Опции: NONE/HIGH/LOW

  Описание: Когда температура переключателя равна или превышает верхний предел, отображается HIGH; когда температура переключателя равна или ниже нижнего предела, отображается LOW; в противном случае отображается Обычный.

- **IP/MAC AlarmТревога**

  Опции: Normal/Alarm

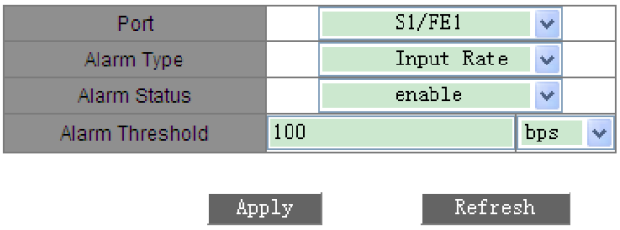
Описание: При возникновении конфликта IP/MAC отображается сигнал тревоги; в противном случае отображается Обычный.

- **Port Alarm**
  Опции: Link Up/Link Down
  Описание: После включения тревоги порта отображается Link Up для правильно подключенного порта. Link Down отображается для порта, отключенного или неправильно подключенного.
- **ST-RING/DRP Alarm**
  Опции: IST-Ring: Ring Open/Ring Close
  Варианты DRP: Normal/Alarm
  Описание: После включения уведомления кольцевой топология отображается Ring Open/Alarm, а Ring Close/Normal для замкнутого звонка.

5.22. Port Traffic Alarm

С помощью функции оповещения о трафике портов коммутатор генерирует оповещение, если скорость трафика порта превышает указанный порог или возникает ошибка CRC.

Настройте аварийный сигнал трафика порта, как показано на следующем рисунке.



- **Port**
  Опции: все порты коммутатора
  Функция: Выберите порты для оповещения о дорожном движении.
- **Alarm Type**
  Параметры: Input Rate/Output Rate/CRC Error
  Функция: Настройка типа сигнала тревоги трафика порта.
- **Alarm Status**
  Опции: enable/disable
  По умолчанию: disable
  Функция: включение или выключение типа тревоги.
  Порог тревоги Диапазон: 1 ~ 1000000000 бит/с или 1 ~ 1000000 кбит/с Функция: настройка порогового значения тревоги трафика порта.

Просмотреть информацию об аварийном сигнале трафика порта, как показано на следующем рисунке.

Port	Input Rate		Alarm Status	Output Rate		Alarm Status	Error CRC	Alarm Status
S1/FE1	enable	100bps	alarm	enable	1000bps	alarm	enable	alarm
S1/FE2	enable	100kbps	normal	enable	100bps	normal	enable	normal
S1/FE3	disable	-	-	disable	-	-	disable	-
S1/FE4	disable	-	-	disable	-	-	disable	-
S1/FE5	disable	-	-	disable	-	-	disable	-
S1/FE6	disable	-	-	disable	-	-	disable	-
S1/FE7	disable	-	-	disable	-	-	disable	-
S1/FE8	disable	-	-	disable	-	-	disable	-
S4/GE1	disable	-	-	disable	-	-	disable	-
S4/GE2	disable	-	-	disable	-	-	disable	-
S4/GE3	disable	-	-	disable	-	-	disable	-
S4/GE4	disable	-	-	disable	-	-	disable	-

5.23. Конфигурация и запрос GMRP

5.23.1. GARP

Generic Attribute Registration Protocol (GARP) используется для распространения, регистрации и отмены определенной информации (VLAN, многоадресный адрес) между коммутаторами в одной сети. Приложения GARP включают GVRP и GMRP.

При использовании GARP информация о конфигурации члена GARP будет распространяться по всей коммутационной сети. Член GARP инструктирует других членов GARP зарегистрировать или отменить свою собственную информацию о конфигурации посредством сообщения о присоединении/отключении 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: «Присоединиться», «Выйти» и «Выйти все» (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 еще не зарегистрированного атрибута.
- Когда объект приложения GARP хочет аннулировать свою собственную информацию о других коммутаторах, объект отправляет сообщение Leave.
- После запуска объекта GARP он запускает таймер LeaveAll. Когда таймер истекает, объект отправляет сообщение LeaveAll.

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

Hold Timer (Таймер удержания): при получении регистрационного сообщения объект GARP не сразу отправляет сообщение о присоединении, а запускает таймер удержания. Когда таймер истекает, объект отправляет все регистрационные сообщения, полученные в течение предшествующего периода, в одном сообщении о присоединении, сокращая отправку пакетов для повышения стабильности сети.

Join Timer (Таймер присоединения): чтобы гарантировать получение сообщений присоединения другими объектами приложения, объект приложения GARP запускает таймер присоединения после отправки сообщения присоединения. Если сообщение о присоединении не получено до истечения таймера присоединения, объект снова отправляет сообщение о присоединении. При получении сообщения JoinIn до истечения таймера объект не отправляет второе сообщение Join.

Leave Timer (Таймер выхода): когда объект приложения GARP хочет отменить информацию об атрибуте, объект отправляет сообщение «Выход». Объект, получивший сообщение, запускает таймер выхода. Если сообщение о присоединении не получено до истечения таймера, то объект, получивший сообщение, отменяет информацию об атрибуте.

LeaveAll Timer (Таймер выхода всем): Когда объект приложения GARP запускается, он запускает таймер LeaveAll. Когда таймер истекает, объект отправляет сообщение LeaveAll, чтобы другие объекты приложения GARP перерегистрировали все атрибуты. Затем объект снова запускает таймер LeaveAll для нового цикла.

5.23.2. GMRP

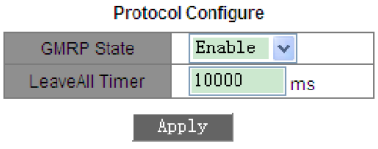
GARP Multicast Registration Protocol (GMRP) — это протокол регистрации многоадресной рассылки, основанный на GARP. Он используется для поддержки регистрационной информации многоадресной рассылки коммутаторов. Все коммутаторы с поддержкой GMRP могут получать информацию о регистрации многоадресной рассылки от других коммутаторов, динамически обновлять информацию о регистрации локальной многоадресной рассылки и распространять информацию о регистрации локальной многоадресной рассылки на другие коммутаторы. Этот механизм обмена информацией обеспечивает согласованность многоадресной информации, поддерживаемой всеми коммутаторами с поддержкой GMRP в сети.

Если коммутатор или терминал хочет присоединиться к группе многоадресной рассылки или выйти из нее, то порт с поддержкой GMRP передает информацию на все порты в той же VLAN.

Описание

Agent port (Порт агента): указывает порт, на котором включены GMRP и функция агента.
Propagation port (Порт распространения): указывает порт, на котором включен только GMRP, но не функция агента.
Динамически изученная многоадресная запись GMRP и запись агента перенаправляются портом распространения на порты распространения устройств более низкого уровня.
Все таймеры GMRP в одной сети должны поддерживать согласованность во избежание взаимных помех. Таймеры должны соответствовать следующим правилам: Hold timer<Join timer, 2*Join timer<Leave timer, и Leave timer<LeaveAll timer.

Включите глобальный протокол GMRP можно, как показано на следующем рисунке.

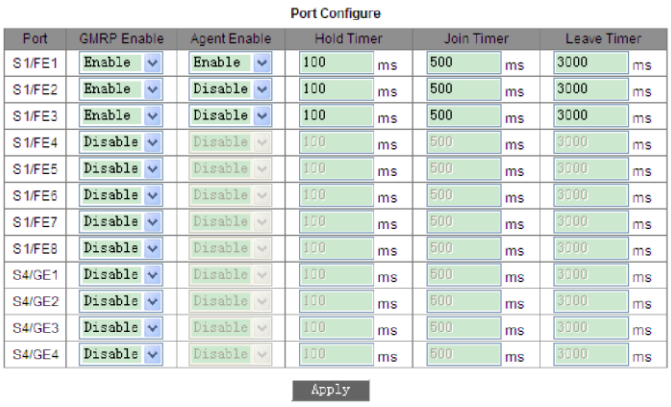


- **GMRP State**
  Опции: Enable/Disable
  По умолчанию: Disable

Функция: Включить или отключить глобальную функцию GMRP. Функцию и IGMP Snooping нельзя использовать одновременно.

- **LeaveAll Timer**
  Диапазон: 100 мс~327600 мс
  По умолчанию: 10000 мс
  Функция: Установите интервал для отправки сообщений LeaveAll. Значение должно быть кратно 100.
  Описание: Если таймеры LeaveAll на разных устройствах истекают одновременно, несколько сообщений LeaveAll будут отправлены одновременно, что приведет к увеличению количества ненужных пакетов. Чтобы предотвратить эту проблему, фактический тайм-аут таймера LeaveAll представляет собой случайное значение между указанным значением и значением, умноженным на 1,5 указанного значения.

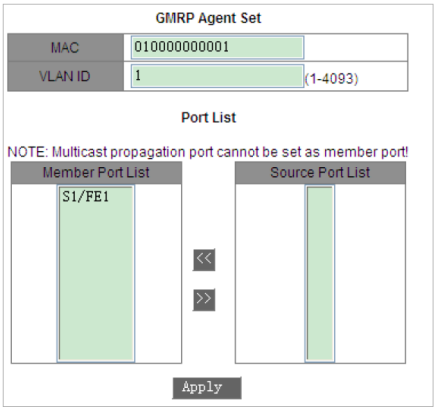
Настроить функцию GMPR на каждом порту можно, как показано на следующем рисунке.



- **GMRP Enable**
  Опции: Enable/Disable
  По умолчанию: Disable
  Функция: включение или выключение функции GMRP на порту.
- **Agent Enable**
  Опции: Enable/Disable
  По умолчанию: Disable
  Функция: включение или выключение функции агента GMRP на порту.
- **Hold Timer**
  Диапазон: 100 мс~327600 мс
  По умолчанию: 100 мс Описание: это значение должно быть кратно 100. Лучше установить таймеры удержания на всех портах с поддержкой GMRP на одно и то же время.
- **Join Timer**
  Диапазон: 100 мс~327600 мс
  По умолчанию: 500 мс
  Описание: это значение должно быть кратно 100. Лучше установить таймеры присоединения на всех портах с поддержкой GMRP на одно и то же время.
- **Leave Timer**
  Диапазон: 100 мс~327600 мс
  По умолчанию: 3000 мс

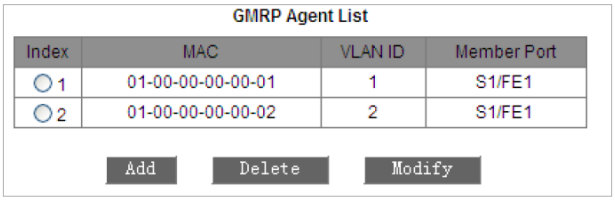
Описание: Это значение должно быть кратно 100. Лучше установить таймеры выхода на всех портах с поддержкой GMRP на одно и то же время.

Добавить запись агента GMRP можно, как показано на следующем рисунке.



- **AC**
  Формат: HHHHHHHHHHHH (H — шестнадцатеричное число.)
  Функция: Настройка MAC-адреса группы многоадресной рассылки. Младший бит первого байта равен 1.
- **VLAN ID**
  Опции: все созданные номера VLAN
  Функция: Настройте идентификатор VLAN для записи агента GMRP.
  Описание: Запись агента GMRP может быть перенаправлена только из порта распространения с идентификатором VLAN, совпадающим с идентификатором VLAN этой записи.
- **Member Port List**
  Выберите порт участника для записи агента. Порт можно выбрать только из портов с поддержкой агента GMRP.
- **Source Port List**
  Варианты: все порты с поддержкой агента GMRP

Просмотреть, изменить или удалить запись агента GMRP можно, как показано на следующем рисунке.

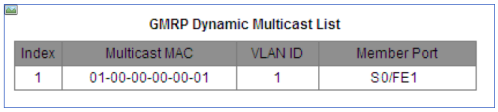


Запись агента GMRP состоит из MAC-адреса, идентификатора VLAN и порта участника. Чтобы удалить запись, выберите запись и нажмите <Delete>. Чтобы изменить запись, выберите запись и нажмите <Modify>.

Просмотрите участников многоадресной рассылки этой записи агента на подключенном соседнем устройстве, как показано на следующем рисунке.

Должны быть соблюдены следующие условия.

- GMRP включен на взаимосвязанных устройствах.
- Два порта, соединяющие устройства, должны быть propagation ports, а идентификатор VLAN порта распространения на локальном устройстве должен совпадать с идентификатором в записи агента.



GMRP Dynamic Multicast List

Index	Multicast MAC	VLAN ID	Member Port
1	01-00-00-00-00-01	1	S0/FE1

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

5.24. RMON

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

RMON в основном обеспечивает статистику и функции сигнализации. С помощью функции статистики Агенты могут периодически собирать статистику по различным типам трафика на этих портах, например, по количеству 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 заданного значения), агент может автоматически записывать события тревоги в журнал RMON или отправлять сообщение Trap на управляющее устройство.

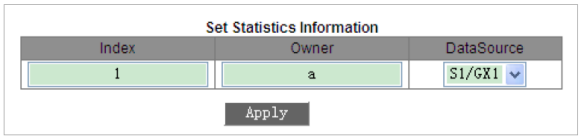
RMON (RFC2819) определяет несколько групп RMON. Устройства серии поддерживают группу статистики, группу истории, группу событий и группу сигналов тревоги в общедоступной MIB. Каждая группа поддерживает до 32 записей.

- Statistics group
  С помощью группы статистики система собирает статистику по всем типам трафика на портах и сохраняет статистику в таблице статистики Ethernet для дальнейшего запроса управляющим устройством. Статистика включает в себя количество сетевых коллизий, пакетов с ошибками CRC, пакетов меньшего или большего размера, широковещательных и многоадресных пакетов, полученных байтов и полученных пакетов. После успешного создания записи статистики на указанном порту группа статистики подсчитывает количество пакетов на порту, и статистика представляет собой постоянно накапливаемое значение.
- History group
  History group требует, чтобы система периодически отбирала все виды трафика на портах и сохраняла значения выборки в таблице записей истории для дальнейшего запроса устройством управления. Группа истории подсчитывает статистические значения всех видов данных в интервале выборки.
- Event group
  Группа событий используется для определения индексов событий и методов обработки событий. События, определенные в группе событий, используются в элементе конфигурации группы тревог. Событие запускается, когда контролируемое устройство соответствует условию тревоги.
  События рассматриваются следующими способами:

Log: регистрирует событие и связанную с ним информацию в таблице журнала событий.
Trap: отправляет сообщение Trap в NMS и информирует NMS о событии.
Log-Trap: регистрирует событие и отправляет сообщение Trap в NMS.
None: указывает на отсутствие действий.

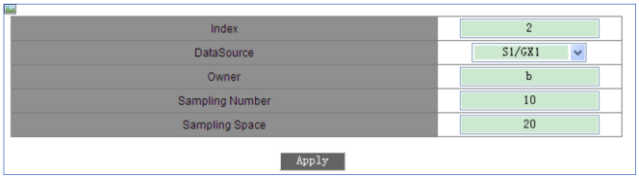
- Alarm group
  Управление аварийными сигналами RMON может отслеживать указанные переменные аварийных сигналов. После того, как записи сигналов тревоги определены, система получит значения контролируемых переменных сигналов тревоги за определенный период. Когда значение переменной тревоги больше или равно верхнему пределу, инициируется нарастающее событие тревоги. Когда значение тревожной переменной меньше или равно нижнему пределу, запускается падающее тревожное событие. Аварийные сигналы будут обрабатываться в соответствии с определением события.

Настройте таблицу статистики, как показано на следующем рисунке.



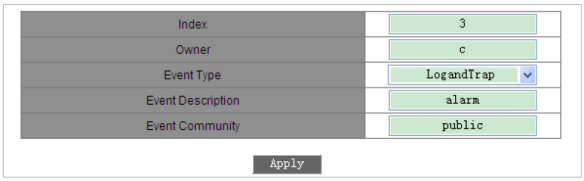
- **Index**
  Диапазон: 1~65535
  Функция: Настройка номера записи статистики.
- **Owner**
  Диапазон: 1~32 символа
  Функция: Настройка имени записи статистики.
- **Data source**
  Функция: Выберите порт, статистика которого должна быть собрана.

Настроить таблицу истории можно, как показано на следующем рисунке.



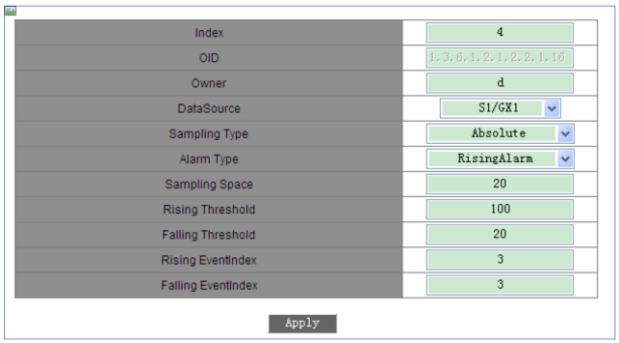
- **Index**
  Диапазон: 1~65535
  Функция: Настройка номера записи истории.
- **Data Source**
  Функция: Выберите порт, информация которого должна быть запрошена.
- **Owner**
  Диапазон: 1~32 символа Функция: Настройка имени записи истории.
- **Sampling Number**
  Диапазон: 1~65535 Функция: настроить время выборки порта.
- **Sampling Space**
  Диапазон: 1~3600 с Функция: Настройка периода выборки порта.

Настройте таблицу событий, как показано на следующем рисунке.



- **Index**
  Диапазон: 1~65535
  Функция: Настройка порядкового номера записи события.
- **Owner**
  Диапазон: 1~32 символа
  Функция: Настройка имени записи события.
- **Event type**
  Тип события Варианты: NONE/LOG/Snmp-Trap/Log and Trap
  По умолчанию: NONE
  Функция: Настроить тип события для аварийных сигналов, то есть режим обработки аварийных сигналов.
- **Event Description**
  Диапазон: 1~127 символов
  Функция: Опишите событие.
- **Event Community**
  Диапазон: 1~127 символов Функция: настроить имя сообщества для отправки события ловушки. Значение должно быть таким же, как в SNMP.

Настройте таблицу аварийных сигналов, как показано на следующих рисунках.



- **Index**
  Диапазон: 1~65535
  Функция: Настройка номера записи тревоги.
- **OID**
  Указывает OID текущего узла MIB.
- **Owner**
  Диапазон: 1~32 символа
  Функция: Настройка имени записи тревоги.
- **Data Source**
  Функция: Выберите порт, информация о котором должна отслеживаться.
- **Sampling Type**
  Опции: Absolute/Delta
  По умолчанию: Absolute
  Функция: Absolute указывает на выборку на основе абсолютного значения. Значение переменной извлекается напрямую, когда приближается конец периода выборки. Дельта указывает выборку на основе изменения значения. Значение

изменения переменной в периоде выборки извлекается, когда приближается конец периода.

- **Alarm Type**
  Опции: RisingAlarm/FallingAlarm/RisOrFallAlarm
  По умолчанию: RisingAlarm
  Функция: Выберите тип тревоги, включая тревогу по нарастающему фронту, тревогу по заднему фронту, а также тревогу по нарастающему и заднему фронту.
- **Sampling Space**
  Диапазон: 1~65535
  Функция: Настройка периода выборки. Значение должно совпадать со значением в таблице истории.
- **Rising Threshold**
  Диапазон: 0~65535
  Функция: Настройка порога нарастания фронта. Когда значение выборки превышает пороговое значение, а тип сигнала тревоги установлен на RisingAlarm или RisOrFallAlarm, генерируется сигнал тревоги и запускается индекс события нарастания.
- **Falling Threshold**
  Диапазон: 0~65535
  Функция: Настройка порога заднего фронта. Когда значение выборки ниже порогового значения, а тип сигнала тревоги установлен на FallingAlarm или RisOrFallAlarm, генерируется сигнал тревоги и запускается индекс события падения.
- **Rising Event Index**
  Диапазон: 0~65535
  Функция: Настройте индекс нарастающего события, т. е. режим обработки сигналов тревоги нарастающего фронта.
- **Falling Event Index**
  Функция: Сконфигурируйте индекс падающего события, т. е. режим обработки аварийных сигналов заднего фронта.

5.25. Log Query

Функция журнала записывает информацию о работе коммутатора, помогая администратору читать и управлять пакетами журнала, а также обнаруживать неисправности. Запуск журнала охватывает:

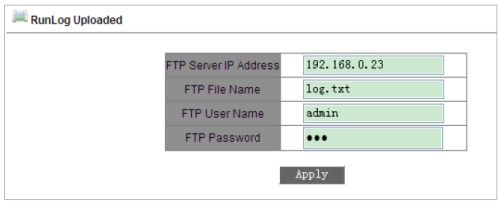
- Аварийный сигнал питания, аварийный сигнал температуры, аварийный сигнал конфликта IP/MAC, аварийный сигнал порта, аварийный сигнал IST-Ring и аварийный сигнал трафика порта
- Broadcast storm
- Программный перезапуск системы

Журнал выполнения содержит не более 1024 записей. Когда настроено более 1024 записей, новые записи перезаписывают старые записи.

Включить функцию журнала можно, как показано на следующем рисунке.

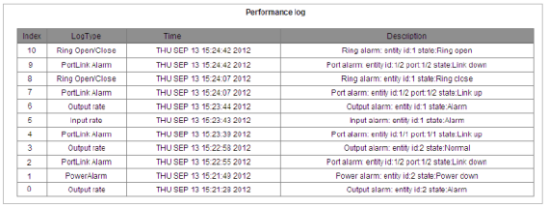
- **Enable Runlog**
  Опции: Enable/Disable
  По умолчанию: Enable
  Функция: включение или отключение функции журнала работы. Если функция включена, информация о работе будет записана.

Настроить загрузку текущего журнала можно, как показано на следующем рисунке.



- **FTP Server IP Address**
  Формат: A.B.C.D.
  Функция: Установите IP-адрес FTP-сервера.
- **FTP File Name**
  Диапазон: 1~20 символов
  Функция: Установите имя файла журнала, сохраненного на сервере.
- **FTP User Name**
  Диапазон: 1~20 символов
  Функция: Установите имя пользователя FTP.
- **FTP Password**
  Диапазон: 1~20 символов
  Функция: Установите пароль FTP.

Просмотреть журнал выполнения можно, как показано на следующем рисунке.



- **Performance log**
  Портфолио: {Index, LogType, Time, Description}
  Функция: Показать текущий рабочий журнал.

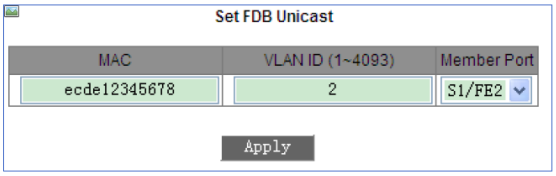
5.26. Unicast Address Configuration and Query

При пересылке пакета коммутатор ищет порт пересылки в таблице MAC-адресов на основе MAC-адреса получателя пакета.
MAC-адрес может быть, как статическим, так и динамическим.

Статический MAC-адрес настроен. Они имеют наивысший приоритет (не переопределяются динамическими MAC-адресами) и действуют постоянно.

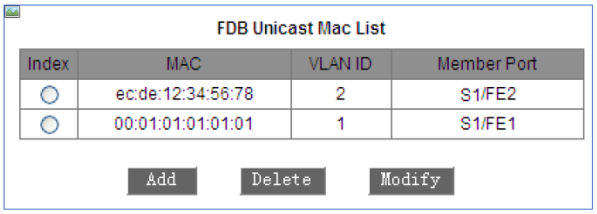
Динамические MAC-адреса узнаются коммутатором при пересылке данных и действительны только в течение определенного периода времени. Коммутатор периодически обновляет свою таблицу MAC-адресов. При получении кадра данных для пересылки коммутатор узнает исходный MAC-адрес кадра, устанавливает сопоставление с принимающим портом и запрашивает порт пересылки в таблице MAC-адресов на основе MAC-адреса получателя кадра. Если совпадение найдено, коммутатор пересылает фрейм данных с соответствующего порта. Если совпадений не найдено, коммутатор передает кадр в своем широковещательном домене.
Коммутатор поддерживает до 256 статических одноадресных записей.

Добавить запись статического MAC-адреса можно, как показано на следующем рисунке.



- **MAC**
  Формат: HHHHHHHHHHHH (H — шестнадцатеричное число.)
  Функция: Настройка одноадресного MAC-адреса. Младший бит в первом байте равен 0.
- **VLAN ID**
  Параметры: все созданные идентификаторы VLAN.
- **Member Port**
  Опции: все порты коммутатора
  Функция: выберите порт для пересылки пакетов, предназначенных для MAC-адреса. Порт должен находиться в указанной VLAN.

Просмотреть список статических одноадресных адресов можно, как показано на следующем рисунке.



Выберите запись. Вы можете удалить или изменить запись.

Просмотреть динамический список одноадресных адресов можно, как показано на следующем рисунке.

Dynamic Unicast Mac List

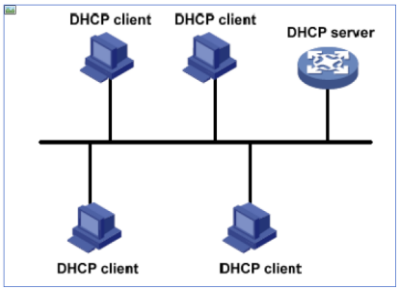
Index	MAC	VLAN ID	Member Port
1	ac:16:2d:03:a7:22	1	S1/FE2
2	70:71:bc:95:cc:22	1	S1/FE2
3	d0:67:e5:29:82:6e	1	S1/FE2
4	d4:be:d9:b9:47:ce	1	S1/FE2
5	c8:9c:dc:57:3e:96	1	S1/FE2
6	00:00:00:98:00:54	1	S1/FE2
7	40:16:9f:f0:b0:0e	1	S1/FE2
8	d0:67:e5:19:71:e2	1	S1/FE2
9	80:c1:6e:e0:5b:9a	1	S1/FE2
10	d0:27:88:70:5b:cd	1	S1/FE2
11	d4:be:d9:b9:46:fb	1	S1/FE2
12	d4:be:d9:b9:46:bb	1	S1/FE2
13	44:87:fc:40:02:be	1	S1/FE2
14	c8:3a:35:d3:cc:2a	1	S1/FE2
15	d0:27:88:45:ff:25	1	S1/FE2
16	00:1e:cd:17:83:6d	1	S1/FE2

Clear

5.27. DHCP

С постоянным расширением масштаба сети и ростом сложности сети, в условиях частого перемещения компьютеров (таких как ноутбуки или беспроводная сеть) и количества компьютеров, превышающих выделяемые IP-адреса, протокол BOOTP, специально предназначенный для статического хоста. конфигурация становится все более неспособной удовлетворить фактические потребности. Для быстрого доступа и выхода из сети и улучшения коэффициента использования ресурсов IP-адресов нам необходимо разработать автоматический механизм на основе BOOTP для назначения IP-адресов. DHCP (протокол динамической конфигурации хоста) был введен для решения этих проблем.

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



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. Этот механизм распределения содержит привязку IP-адреса порта и привязку MAC-адреса.

Динамическое распределение: 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.

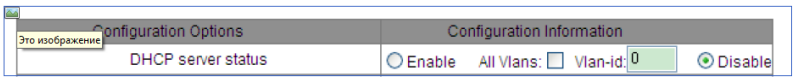
DHCP-сервер — поставщик услуг DHCP. Он использует DHCP-сообщения для связи с DHCP-клиентом, чтобы выделить клиенту, подходящий IP-адрес и при необходимости назначить ему другие сетевые параметры. В следующих случаях DHCP-сервер обычно используется для выделения IP-адресов.

- 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.
- Лишь нескольким хостам в сети нужны фиксированные IP-адреса.

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

- IP-адрес, статически связанный с MAC-адресом клиента или идентификатором порта, подключающегося к серверу.
- 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.

Включите DHCP-сервер можно, как показано на рисунке.



- **DHCP server status**
  Опции: Enable/Disable
  По умолчанию: Disable
  Функция: выберите текущий коммутатор для DHCP-сервера, чтобы выделить IP-адрес клиенту или нет. Если при включении выбран идентификатор VLAN, DHCP-сервер выделяет IP-адрес только клиенту, отправляющему запрос в этой VLAN. Если выбраны все VLAN, DHCP-сервер выделяет IP-адреса всем клиентам, отправляющим запрос.
  Объяснение: При выборе идентификатора VLAN можно выбрать только один идентификатор VLAN.

Выберите режим DHCP-сервера, как показано на рисунке.

- **DHCP server mode**
  Опции: Common-Mode/Port-Mode
  По умолчанию: Port-Mode
  Объяснение: Общий режим включает динамическое выделение IP-адреса и привязку статического MAC-адреса. Режим порта означает желаемую настройку IP порта.

Port-Mode конфигурация

При выборе Port-mode в режиме DHCP-сервера назначьте портам статические IP-адреса привязки, как показано на рисунке.

Port	IP
S1/FE1	
S1/FE2	
S1/FE3	192.168.0.6
S1/FE4	
S1/FE5	
S1/FE6	
S1/FE7	
S1/FE8	
S2/FE1	

Желаемый IP-адрес порта — это статическая настройка IP-адреса на порт. Когда порт получает сообщение запроса от клиента, IP-адрес, связанный с портом, будет выделен клиенту. Этот режим выделения IP-адресов имеет наивысший приоритет, а период аренды составляет 1000 дней 23 часа 59 минут.

Когда для назначения IP-адресов выбран режим порта, необходимо настроить DHCP-сервер, как показано на рисунке.

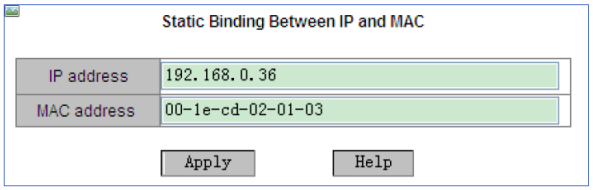
Configuration Options		Configuration Information
DHCP server status		Enable All Vlans: Vlan-id: Disable
DHCP server mode		Common-Mode Port-Mode
DHCP server IP-pool name		pool
The domain name for the IP-Pool		domain
The starting IP address of the IP-Pool		
The ending IP address of the IP-Pool		
The subnet mask of the network-address		255.255.255.0
The default lease time of the IP address		Infinite: 0 Days 1 Hours 0 Minutes
The maximum lease time of the IP address		1 Days 0 Hours 0 Minutes
The routers on the IP-Pool's subnet	IP Address 1:	
	IP Address 2:	
The dns-server for the IP-Pool's subnet	DNS1:	
	DNS2:	
Run		Run

Apply Help

- **DHCP server IP-pool name**
  Диапазон: 1~15 символов
  Функция: настроить имя пула IP-адресов.
- **The domain name for the IP-Pool**
  Диапазон: 1~60 символов
  Функция: настроить доменное имя пула IP-адресов.
- **The subnet mask of the network-address**
  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.

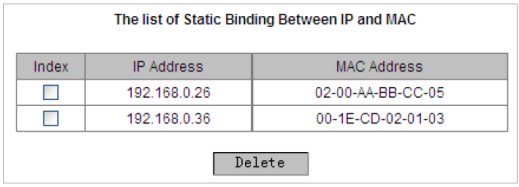
Port-Mode конфигурация

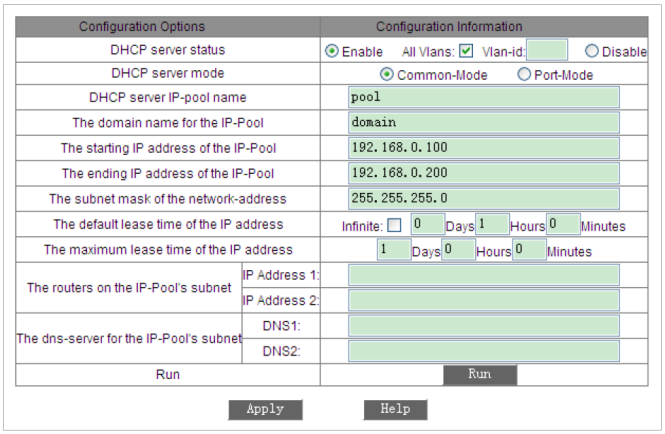
Когда режим DHCP-сервера установлен на Common-Mode, он содержит привязку статического MAC-адреса и динамическое выделение IP-адреса. При статической привязке MAC-адреса система предпочтительно выделяет IP-адрес, привязанный к MAC-адресу; в противном случае динамически выделяйте IP-адреса в пуле адресов. Конфигурация привязки статического MAC-адреса показана на рис. 166 и рис. 167; конфигурация динамического распределения IP-адресов показана на рисунке.



Статическая привязка MAC-адреса предназначена для привязки MAC-адреса клиента к IP-адресу. Когда сервер получает сообщение с запросом IP-адреса, исходным MAC-адресом которого является установленный здесь MAC-адрес, IP-адрес, связанный с этим MAC-адресом, будет выделен клиенту. Для такого режима распределения IP-адресов требуется конфигурация сервера, как показано на рисунке.

После настройки список «Статическая привязка между IP и MAC» показывает статически настроенные отношения привязки MAC-адресов и IP-адресов. Отметьте поле Индекса, чтобы удалить соответствующую запись привязки.





- **DHCP server IP-pool name**
  Диапазон: 1-15 символов
  Функция: настроить имя пула IP-адресов
- **The domain name for the IP-Pool**
  Диапазон: 1-60 символов
  Функция: настроить доменное имя пула IP-адресов
- **The starting IP address of the IP-Pool/The ending IP address of the IP-Pool**
  Формат: A.B.C.D (начальный IP-адрес и конечный IP-адрес должны быть в одном сегменте).
- **The subnet mask of the network-address**
  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. При динамическом распределении адресов необходимо установить диапазон пула IP-адресов, а диапазон адресов определяется маской подсети.
- **The default lease time of the IP address**
  Диапазон: 0 дней 0 часов 1 минута – 1000 дней 23 часа 59 минут/бесконечно
  По умолчанию: 0 дней 1 час 0 минут

Объяснение: Если сообщение с запросом IP-адреса, отправленное клиентом, не содержит действительного времени аренды, срок аренды IP-адреса, который сервер выделяет клиенту, является значением по умолчанию.

- **The maximum lease time of the IP address**
  Диапазон: 0 дней 0 часов 1 минута – 1000 дней 23 часа 59 минут
  По умолчанию: 1 день 0 часов 0 минут
  Объяснение: Когда клиент отправляет на сервер сообщение с запросом IP-адреса, время аренды сообщения не может превышать максимальное время аренды IP-адреса. Для разных пулов адресов сервер DHCP может установить разное время аренды адреса, но адреса в одном пуле адресов DHCP имеют одинаковое время аренды.
- **The routers on the IP-Pool's subnet**
  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 два адреса шлюза.
- **The dns-server for the IP-Pool's subnet**
  При посещении сетевого узла через доменное имя доменное имя должно быть преобразовано в IP-адрес, который реализуется DNS. 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 два адреса DNS.