Промышленный Ethernet-коммутатор серии SICOM3024P/SICOM3048/SICOM3024

Руководство пользователя по программной части

Версия 2.3

Сайт: https://kyland-rus.ru/
Эл. почта: sales@kyland-rus.ru
support@kyland-rus.ru

KYLAND

Содержание

Предисловие

В этом руководстве в основном представлены методы доступа и функции программного обеспечения промышленных Ethernet-коммутаторов серий SICOM3024P/SICOM3048/SICOM3024, а также подробно описаны методы настройки через веб-интерфейс.

Структура:

Руководство пользователя содержит следующий материал:

Глава	Содержание
1. Введение	Обзор Модели изделия Функции программного обеспечения
2. Доступ к коммутатору	Варианты представления Доступ через консольный порт Доступ через Telnet Доступ через веб-интерфейс
3. Управление устройством	> Перезапуск > Выход
4. Состояние устройства	Основные сведения Состояние порта Статистика порта Информация о системе
5. Основные настройки	IP-адрес Основные сведения Настройка порта Смена пароля Обновление программного обеспечения (FTP) Запрос версии программного обеспечения Выгрузка/загрузка конфигурации
6. Расширенные настройки	Ограничение скорости порта PVLAN Зеркалирование портов Агрегация портов Проверка канала связи Статическая многоадресная рассылка IGMP Snooping ACL ARP SNMP DT-Ring RSTP/STP Прозрачная передача RSTP/STP DRP# QoS Время старения MAC-адреса LLDP SNTP Настройка изоляции порта Аварийная сигнализация Аварийная сигнализация по трафику порта Настройка и запрос GMRP RMON Запрос журнала Настройка и запрос адреса одноадресной рассылки

	DHCP

	**Примечание:** * указывает, что функция недоступна в устройствах SICOM3048/SICOM3024 # указывает, что функция недоступна в устройствах SICOM3048.

Условные обозначения в руководстве

1. Условные обозначения в тексте

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

2. Условные обозначения в командной строке

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

3. Символы

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

1 Введение

1.1 Обзор

Коммутаторы серии применяются в энергетике, на железнодорожном транспорте, в угледобывающей промышленности и многих других отраслях и могут работать должным образом в суровых условиях. Коммутаторы поддерживают протоколы резервирования RSTP, DT-Ring и IEC62439-6, гарантируя надежную работу системы. В коммутаторах серии используется модульная конструкция, обеспечивающая гибкое расширение. Они соответствуют стандартам IEC61850-3 и IEEE1613.

1.2 Модели изделия

В серию входят:
SICOM3048
SICOM3024P

1.3 Функции программного обеспечения

Коммутаторы серии предоставляют обширный набор функций программного обеспечения, удовлетворяющих различные потребности заказчиков.
Протоколы резервирования: RSTP/STP, DT-Ring и IEC62439-6
Многоадресные протоколы: IGMP Snooping, GMRP и статическая многоадресная рассылка
Атрибуты коммутации: VLAN, PVLAN, QoS и ARP
Управление пропускной способностью: агрегация портов, ограничение скорости порта
Безопасность: ACL, изоляция портов
Протокол синхронизации: SNTP
Управление устройством: Обновление программного обеспечения по FTP, выгрузка/загрузка конфигурации
Диагностика устройства: зеркалирование портов, LLDP, проверка канала.
Функция аварийной сигнализации: сигнализация порта, сигнализация питания, сигнализация кольца, сигнализация конфликта IP/MAC адресов, сигнализация температуры, сигнализация низкой температуры, сигнализация трафика порта
Управление сетью: командная строка, Telnet, веб-интерфейс и ПО Kyvision, мониторинг SNMP

2 Доступ к коммутатору

Доступ к коммутатору осуществляется через:

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

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

2.1 Варианты представления

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

Таблица 1 Варианты представления

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

При настройке коммутатора через интерфейс командной строки для получения справки по командам можно использовать «?». В справочной информации используются различные форматы описания параметров. Например, <1, 255> означает числовой диапазон; <H.H.H.H> означает IP-адрес; <H:H:H:H:H:H> означает MAC address; word<1,31> означает диапазон строк. Кроме того, символы ↑ и ↓ могут использоваться для просмотра недавно использованных команд.

2.2 Доступ через консольный порт

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

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

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

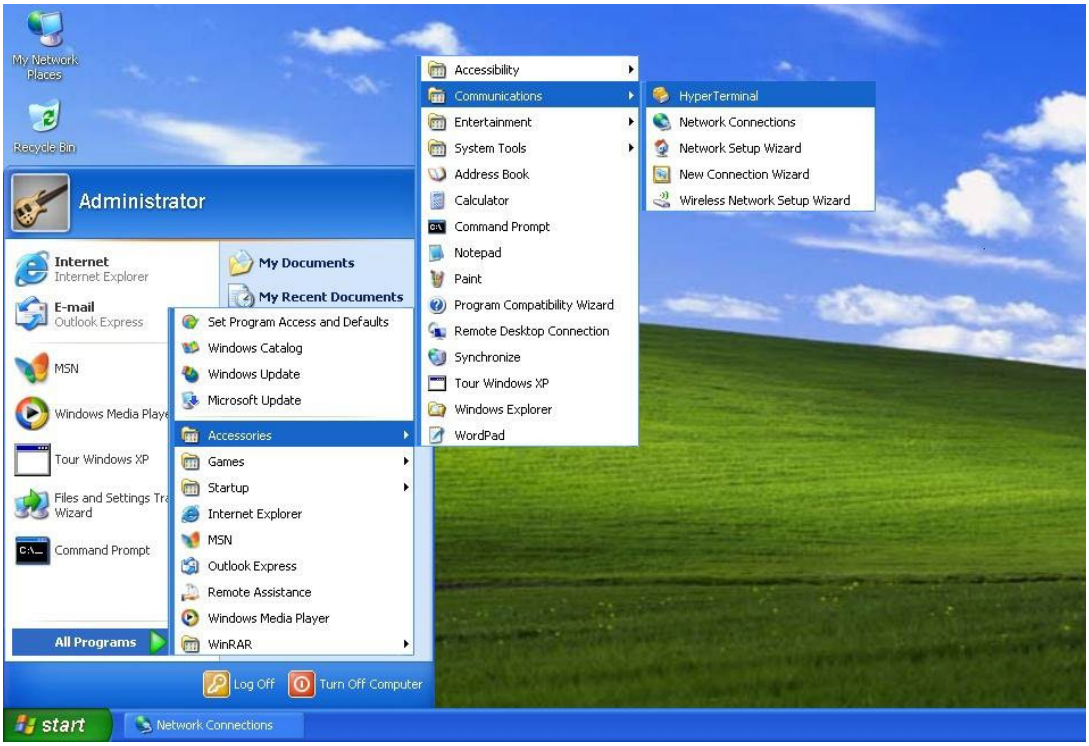

Рисунок 1 Запуск Hyper Terminal

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

Рисунок 2 Создание нового подключения

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

Рисунок 3 Выбор порта для подключения

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

5. Настройте параметры порта (Bits per second: 9600, Data bits: 8, Parity: None, Stop bits: 1, Flow control: None), как показано на рисунке ниже.

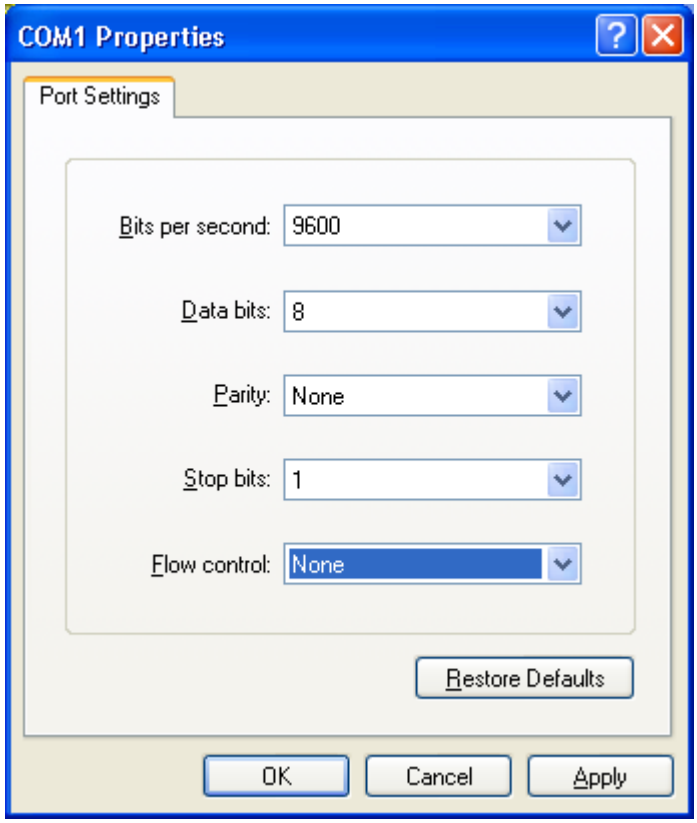

Рисунок 4 Настройка параметров порта

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

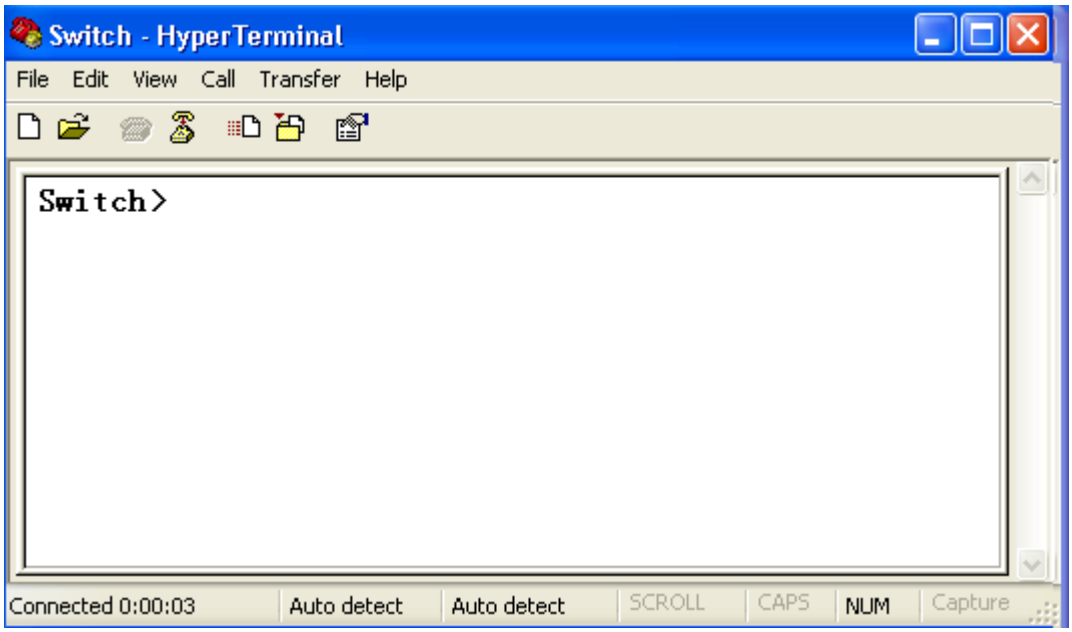

Рисунок 5 Интерфейс командной строки

2.3 Доступ через Telnet

Предварительным условием доступа к коммутатору по протоколу Telnet является нормальная связь между ПК и коммутатором.
1. Введите telnet IP address в диалоговом окне Run, как показано на следующем рисунке.

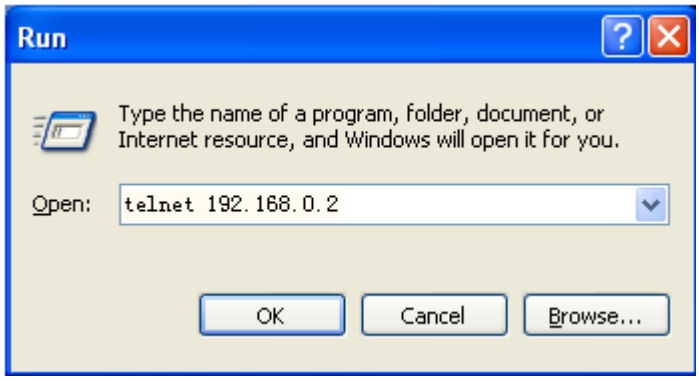

Рисунок 6 Доступ по Telnet

NOTE	**Примечание:** Для подтверждения IP-адреса обратитесь к разделу 5.1 Настройка IP.

2. В интерфейсе Telnet введите admin в поле User и 123 в поле Password. Нажмите <ENTER> для входа в коммутатор, как показано на рисунке ниже.

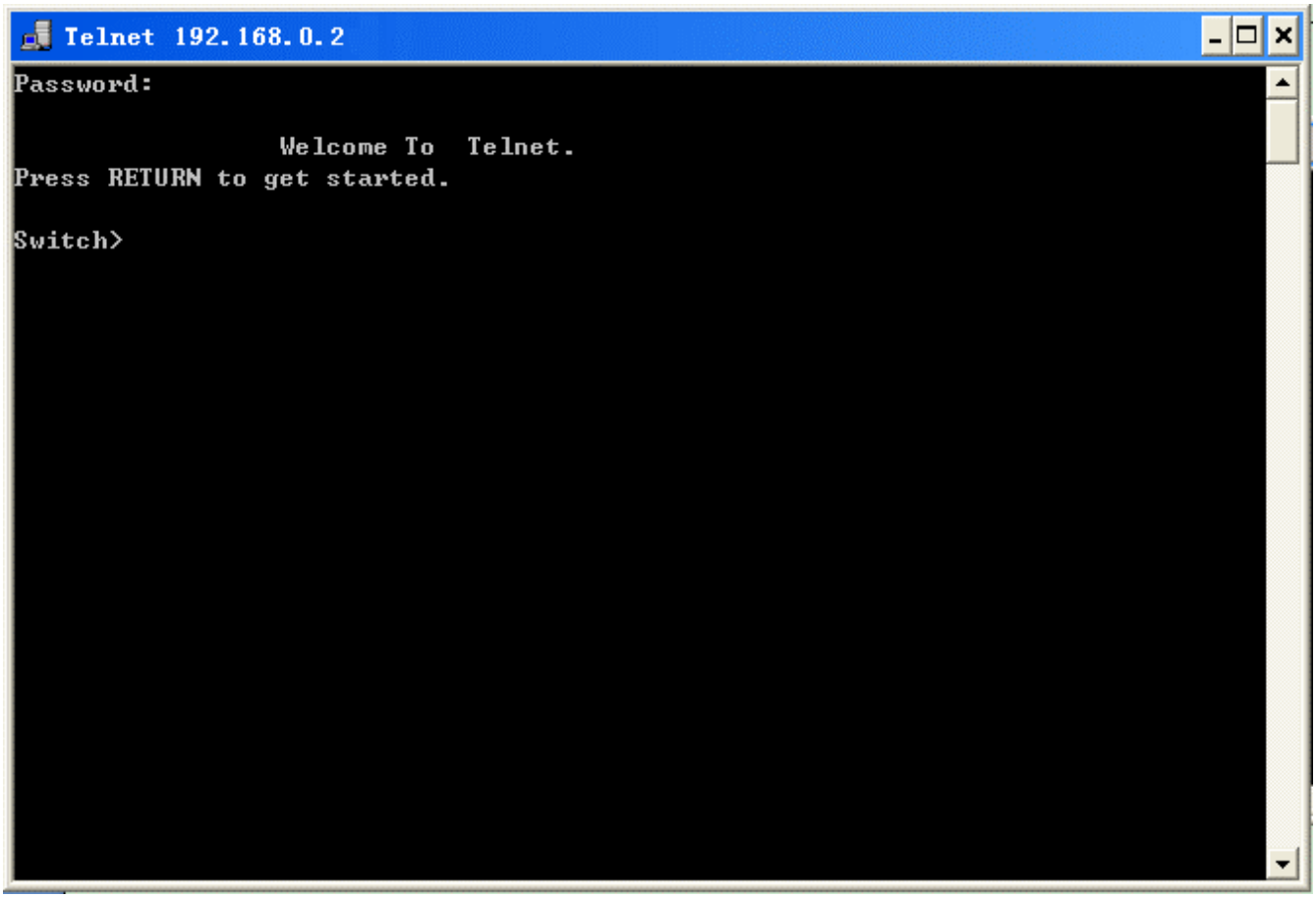

Рисунок 7 Интерфейс Telnet

2.4 Доступ через веб-интерфейс

Предварительным условием доступа к коммутатору через веб-интерфейс является нормальная связь между ПК и коммутатором.
Для наилучшего отображения доступа через веб-интерфейс рекомендуется использовать браузер IE8.0 или более позднюю версию.
1. Введите IP-адрес в адресной строке браузера. Отображается интерфейс для входа, как показано на рисунке ниже. Введите имя пользователя по умолчанию admin, пароль 123. Щелкните <Login>.

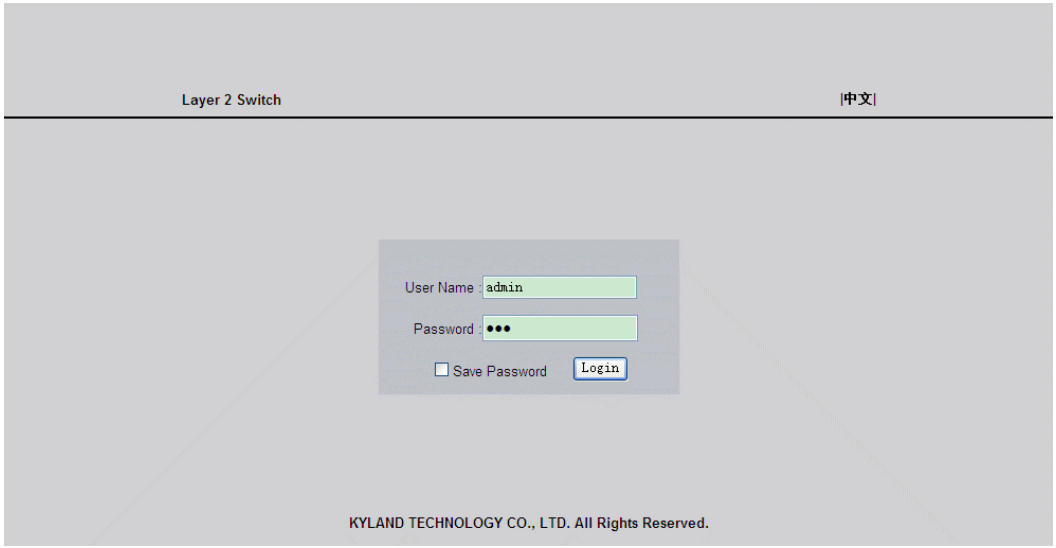

Рисунок 8 Вход через веб-интерфейс

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

NOTE	**Примечание:** Для подтверждения IP-адреса обратитесь к разделу 5.1 Настройка IP.

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

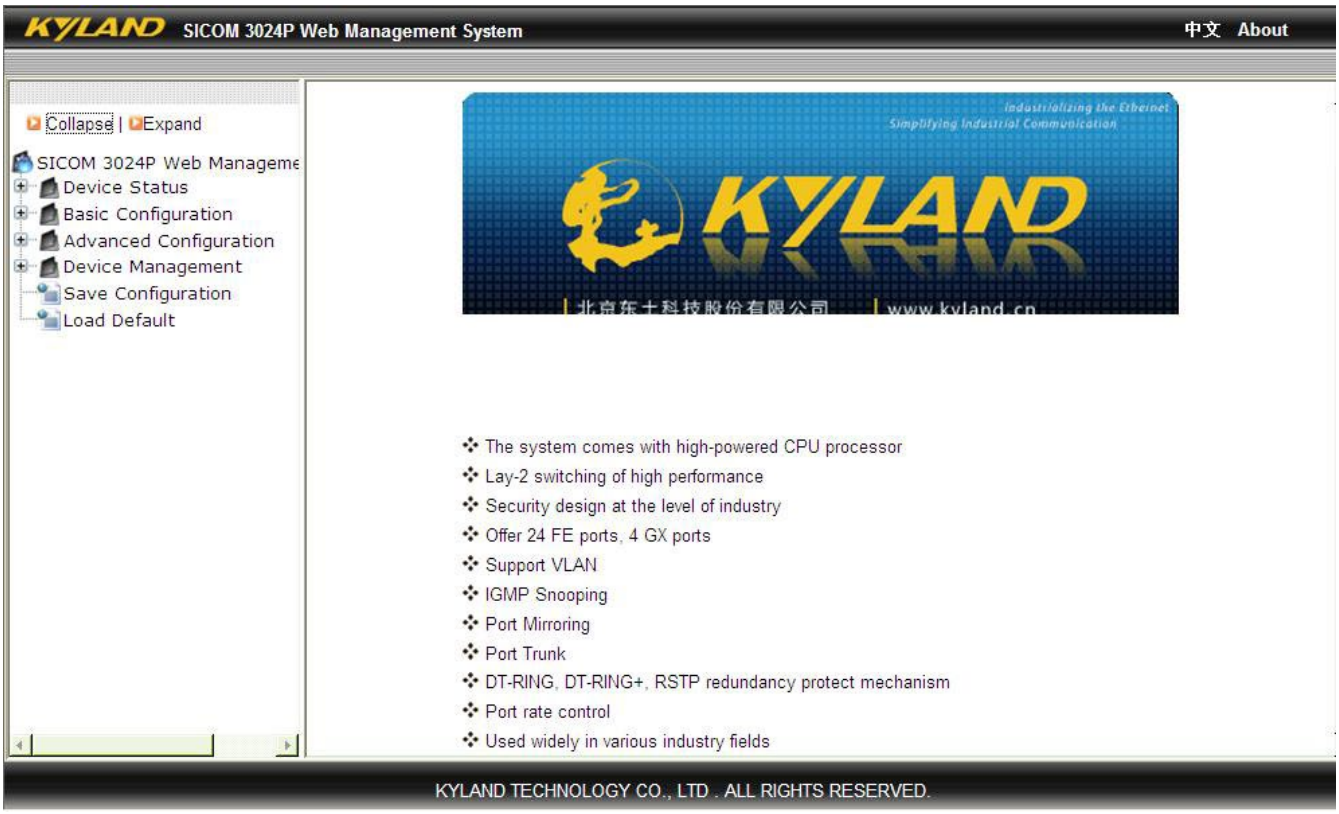

Рисунок 9 Веб-интерфейс

Щелкнув <Expand> или <Collapse> в верхней части дерева навигации, можно развернуть или свернуть дерево навигации. Можно выполнить соответствующие операции, щелкнув [Save Configuration] или [Load Default] в верхнем меню. В правом верхнем углу можно щелкнуть <中文>, чтобы изменить язык интерфейса на китайский.

CAUTION	**Предупреждение:** После восстановления настроек по умолчанию необходимо перезагрузить устройство, чтобы настройки вступили в силу.

3 Управление устройством

Щелкните [Device Management] ^ [Reboot]/ [Logout]. Можно перезагрузить устройство или выйти из веб-интерфейса. Перед перезагрузкой устройства необходимо сохранить текущие настройки должным образом. Если настройки сохранены, коммутатор после перезапуска автоматически использует их для настройки. Если настройки не сохранены, после перезапуска коммутатор восстановит заводские настройки по умолчанию.

4 Состояние устройства

4.1 Основные сведения

Основные сведения о коммутаторе включают в себя 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

Рисунок 10 Основные сведения

4.2 Состояние порта

На странице состояния порта отображается номер порта, статус 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	---	---	---	---	---

Рисунок 11 Состояние порта

Port ID

Отображается тип и ID портов.

Port ID имеет формат Sα/β.

α указывает номер слота, в котором находится плата. В SICOM3048, S0 указывает фиксированный порт устройства (не на плате);

β указывает тип порта и ID платы/панели, где находится порт.

FE/FX/GE/GX указывают тип порта.

FE: порт 10/100Base-TX RJ45

FX: Порт 100Base-FX

GE: порт 10/100/1000Base-TX RJ45
GX: гигабитный слот SFP

Administration Status

Отображение административного статуса для портов.
Enable: Порт включен и разрешает передачу данных.
Disable: Порт заблокирован без передачи данных.

Operation Status

Отображение состояния работы портов.

Link

Отображение статуса соединения для портов.
Up: Порт находится в состоянии LinkUp и может нормально передавать данные.
Down: Порт находится в состоянии LinkDown и не может нормально передавать данные.

Speed

Отображение скорости связи портов в состоянии LinkUp.

Duplex

Отображение режима дуплекса портов в состоянии LinkUp.
Full-duplex: Порт может одновременно принимать и передавать данные.
Half-duplex: Порт либо принимает, либо передает данные.

Flow Control

Отображение состояния управления потоком портов в состоянии LinkUp.

RX

Варианты: Enable/Disable
Enable: Порт может принимать данные.
Disable: Порт не может принимать данные.

TX

Варианты: Enable/Disable
Enable: Порт может передавать данные.
Disable: Порт не может передавать данные.

NOTE	**Примечание:** Подробности о настройках портов см. в разделе 5.3 Настройка портов.

4.3 Статистика порта

Статистика порта включает в себя количество байтов/пакетов, которые каждый порт отправляет/получает, ошибки CRC и количество пакетов длиной менее 64 байтов, 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

Рисунок 12 Статистика порта

Чтобы перезапустить сбор статистики, щелкните <Reset>.

4.4 Информация о работе системы

Информация о работе системы включает в себя время работы устройства, загрузку 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

Рисунок 13 Информация о работе системы (SICOM3024P)

Device Operating	
Device Operating Time:	0Days,5H:25M:41S
CPU:	5%(short-term), 5%(long-term)

Рисунок 14 Информация о работе системы (SICOM3048)

Device Operating	
Device Operating Time:	0Days,20H:3M:37S
CPU Usage:	3%(30 seconds), 1%(5 minutes)
Memory Usage:	70%
Device Time:	2014.08.08 10:10:26 Friday

Рисунок 15 Информация о работе системы (SICOM3024)

5 Основные настройки

5.1 IP-адрес

1. Просмотр IP-адреса коммутатора через консольный порт.
Войдите в интерфейс командной строки через консольный порт. Выполните команду show interface в привилегированном режиме, чтобы увидеть IP-адрес коммутатора. На рисунке ниже IP-адрес обведен красным.

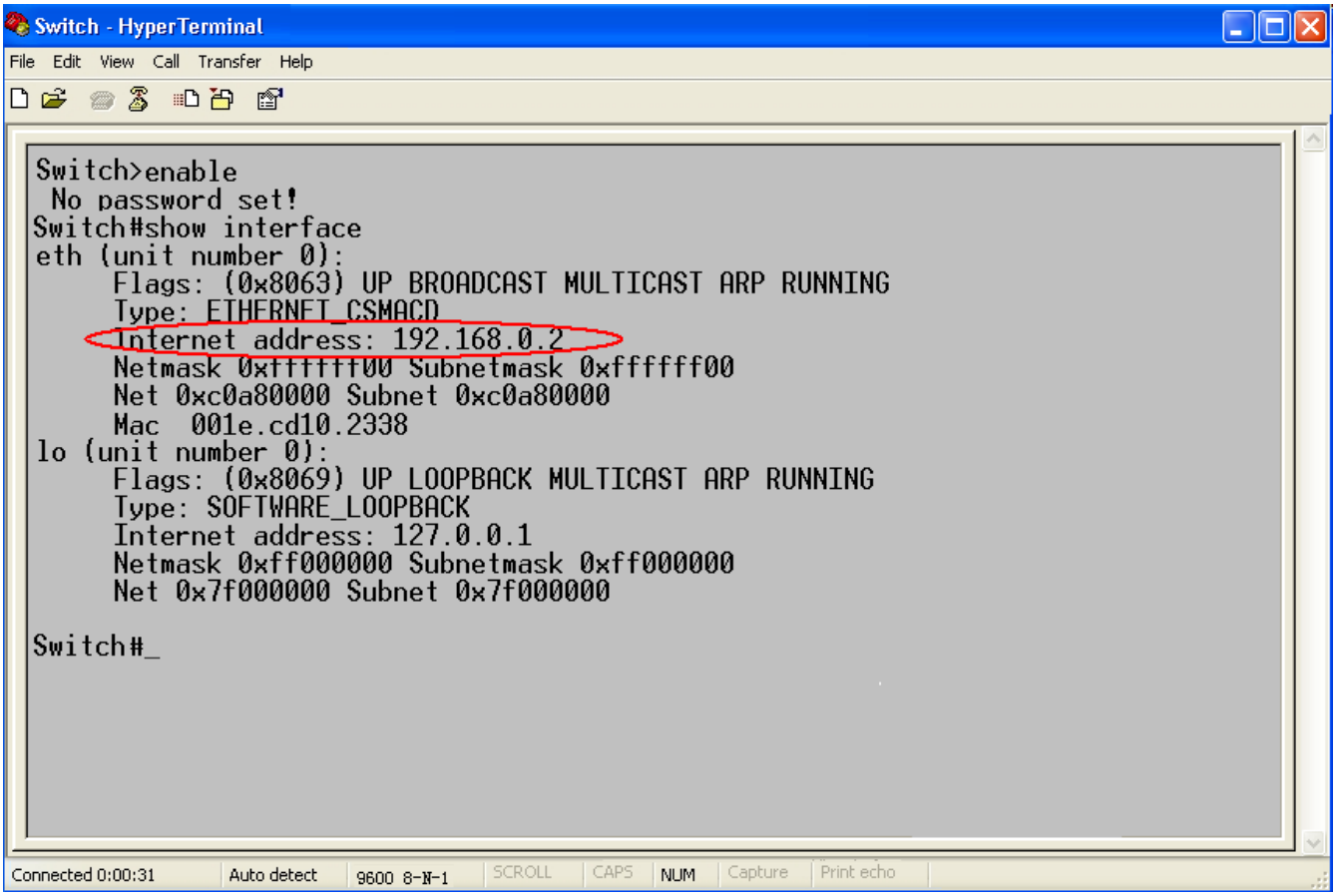

Рисунок 16 Просмотр IP-адреса

2. Настройка IP-адреса сервера.
IP-адрес коммутатора и шлюз можно настроить вручную, как показано на рисунке ниже.

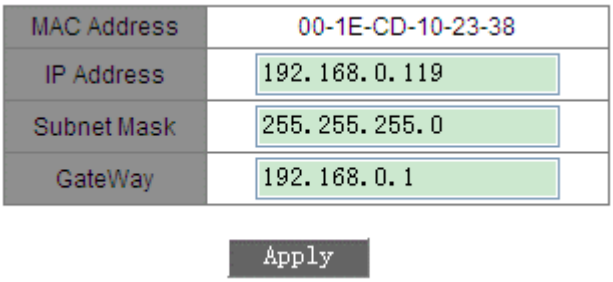

Рисунок 17 IP-адрес

CAUTION	**Предупреждение:** > IP-адрес и шлюз должны находиться в одном сегменте сети; в противном случае IP-адрес нельзя изменить. > Для коммутаторов этой серии изменение IP-адреса вступает в силу сразу после изменения без необходимости перезагрузки.

5.2 Основные сведения

Основные сведения включают в себя название проекта, имя системы, часовой пояс, местоположение, контактные данные и системное время, как показано на следующих рисунках.

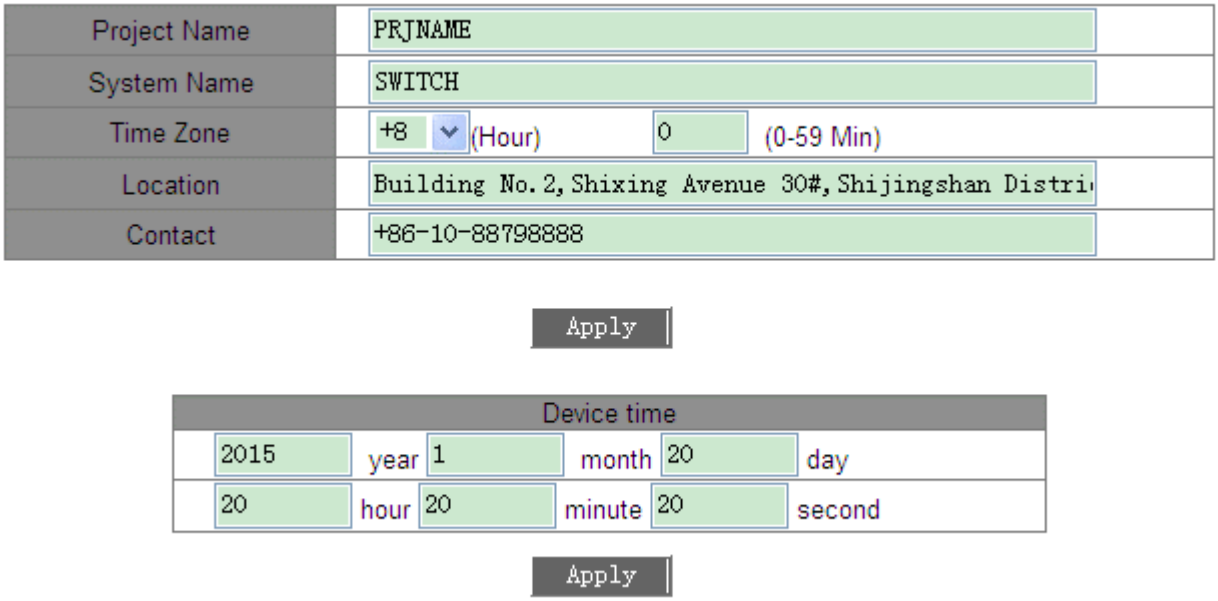

Рисунок 18 Информация об устройстве (SICOM3024P)

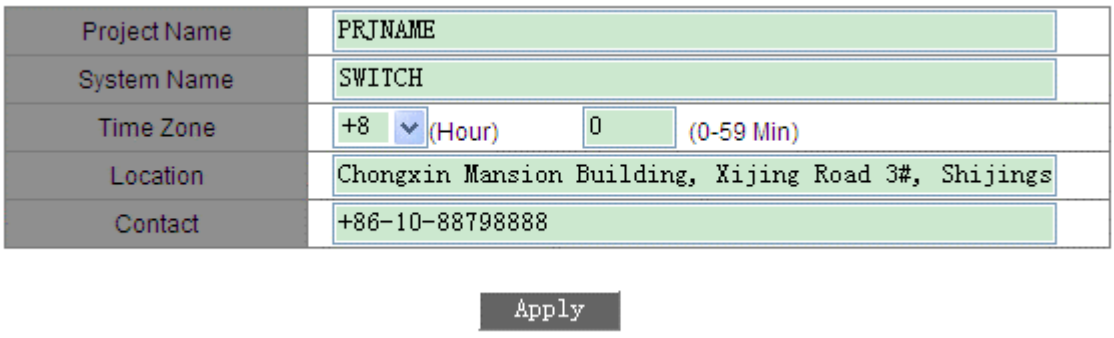

Рисунок 19 Информация об устройстве (SICOM3024)

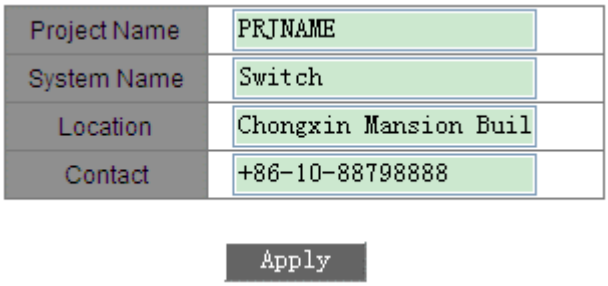

Рисунок 20 Информация об устройстве (SICOM3048)

Project Name
Диапазон: 1~64 символа
System Name
Диапазон: 1~32 символа
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 час.
0~59 мин.
По умолчанию: 0 часов 0 минут
Функция: Выбор местного часового пояса.
Location
Значение: Английские/китайские символы
Диапазон: 1~255 символов (один китайский символ занимает место двух английских символов)
Contact
Значение: Английские/китайские символы
Диапазон: 1~32 символа (один китайский символ занимает место двух английских символов)
Device Time
Состав: {YYYY, MM, DD, HH, MM, SS}
Диапазон: YYYY (год) от 2000 до 2099, MM (месяц) от 1 до 12, DD (день) от 1 до 31, HH (часы) от 0 до 23 и MM (минуты) и SS (секунды) от 0 до 59.
Функция: Настройка системной даты и времени. Коммутатор продолжает отсчет времени после выключения питания.

5.3 Настройка портов

В разделе настройки портов можно настроить состояние порта, скорость порта, управление потоком и другую информацию, как показано на рисунке ниже.

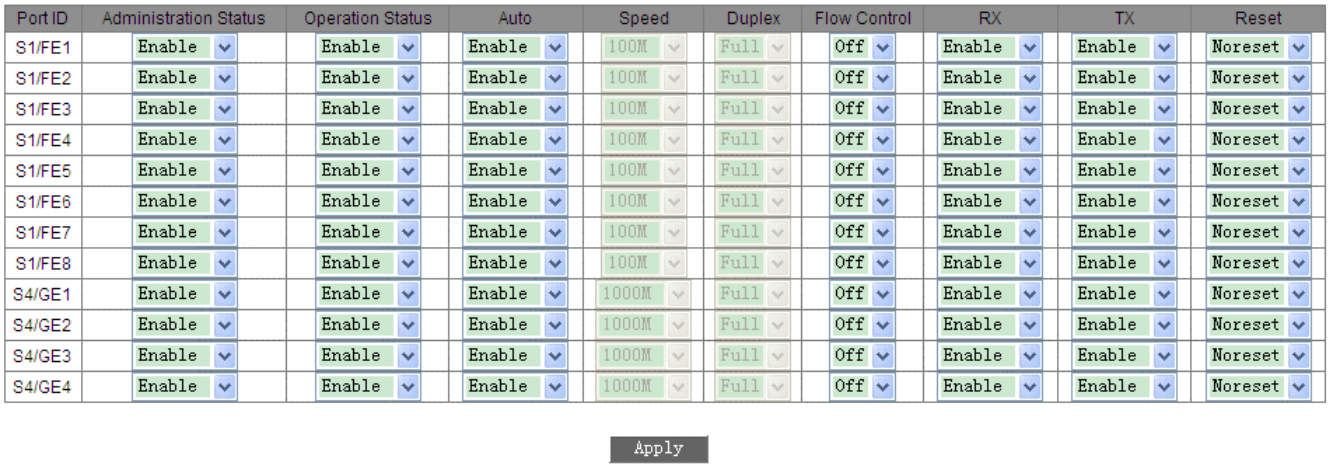

Рисунок 21 Настройка порта

Administration Status
Варианты: Enable/Disable
По умолчанию: Enable
Функция: Запрет/разрешение передачи данных через порт.
Описание: Enable указывает на то, что порт включен и разрешает передачу данных; Disable указывает на то, что порт отключен и запрещает передачу данных. Эта опция напрямую влияет на аппаратное состояние порта и запускает аварийные сигналы порта.
Operation Status
Описание: Когда для administration status задано значение Enable, для operation status значение enable

устанавливается принудительно; когда для administration status задано значение Disable, для operation status значение Disable устанавливается принудительно.

Auto

Варианты: Enable/Disable

По умолчанию: Enable

Функция: Настройка автосогласования состояния портов.

Описание: Если для Auto установлено значение Enable, скорость порта и режим дуплекса будут автоматически согласовываться в соответствии со статусом подключения порта. Если для Auto установлено значение Disable, скорость порта и режим дуплекса можно настроить.

	**Предупреждение:** > Для портов 10/100/1000Base-T(X) Enable устанавливается принудительно. > Для портов 100Base-FX Disable устанавливается принудительно.

Speed

Варианты: 10M/100M/1000M

Функция: Принудительная настройка скорости портов.

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

Duplex

Варианты: Half/Full

Функция: Настройка дуплексного режима портов.

Описание: Если для Auto установлено значение Disable, режим дуплекса можно настроить.

	**Предупреждение:** > Порты 10/100Base-T(X) можно настроить в режим автосогласования, режим 10M&full duplex, 10M&half duplex, 100M&full duplex или 100M&half duplex. > Для портов 100Base-FX режим 100M&full duplex устанавливается принудительно. > Для портов 10/100/1000Base-T(X) режим автосогласования устанавливается принудительно. > Волоконнооптические порты 1000M можно настроить в режим автосогласования и режим 10000M&full duplex.

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

Варианты: Off/On

По умолчанию: Off

Функция: Включение/выключение функции управления потоком на назначенном порту.

Описание: Как только функция управления потоком включена, порт сообщит отправителю о снижении скорости передачи, чтобы по алгоритму или протоколу избежать потери пакетов, когда поток, полученный портом, превышает размер кэша порта. Если устройства работают в разных дуплексных режимах (полу/полный), управление потоком у них реализуется по-разному. Если устройства работают в полнодуплексном режиме, принимающая сторона отправит специальный кадр (Pause frame), 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 методом обратного давления. Принимающая сторона создает конфликт или сигнал несущей. Когда отправитель

обнаруживает конфликт или несущую, он формирует отсрочку, чтобы отложить передачу данных.
RX
Варианты: Enable/Disable
По умолчанию: Enable
Функция: Разрешение/запрет получения данных для порта.
Описание: Enable указывает, что порт может принимать данные; Disable указывает, что порт не может принимать данные.
TX
Варианты: Enable/Disable
По умолчанию: Enable
Функция: Разрешение/запрет получения данных для порта.
Описание: Enable указывает, что порт может передавать данные; Disable указывает, что порт не может передавать данные.
Reset
Варианты: Reset/Noreset
По умолчанию: Noreset
Функция: Выполнить или нет сброс порта.

5.4 Смена пароля

Можно изменить пароль для пользователя admin, как показано на рисунке ниже.

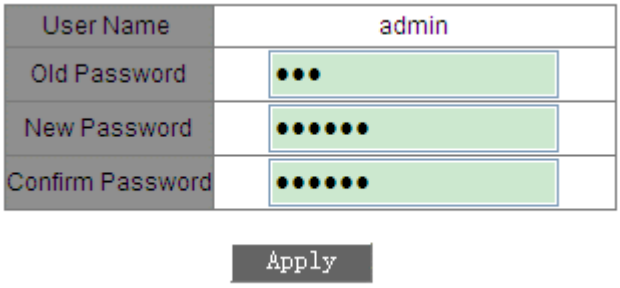

Рисунок 22 Смена пароля

5.5 Обновление программного обеспечения

Обновление программного обеспечения может помочь улучшить производительность коммутатора. Для коммутаторов этой серии обновление ПО включает в себя обновление версии загрузчика и обновление версии системного программного обеспечения. Версия загрузчика должна быть обновлена до обновления версии системного программного обеспечения. Если версия загрузчика не меняется, можно обновить только версию системного ПО.
Для обновления версии ПО требуется FTP-сервер.

5.5.1 Обновление программного обеспечения через FTP

Установите FTP-сервер. Ниже в качестве примера используется программное обеспечение WFTPD для ознакомления с конфигурацией FTP-сервера и обновлением программного обеспечения.
1. Щелкните [Security] ^ [Users/Rights]. Появится диалоговое окно Users/Rights Security Dialog. Щелкните <New User>, чтобы создать нового пользователя FTP, как показано на рисунке ниже. Создайте имя пользователя и пароль, например, имя пользователя admin и пароль 123. Щелкните <OK>.

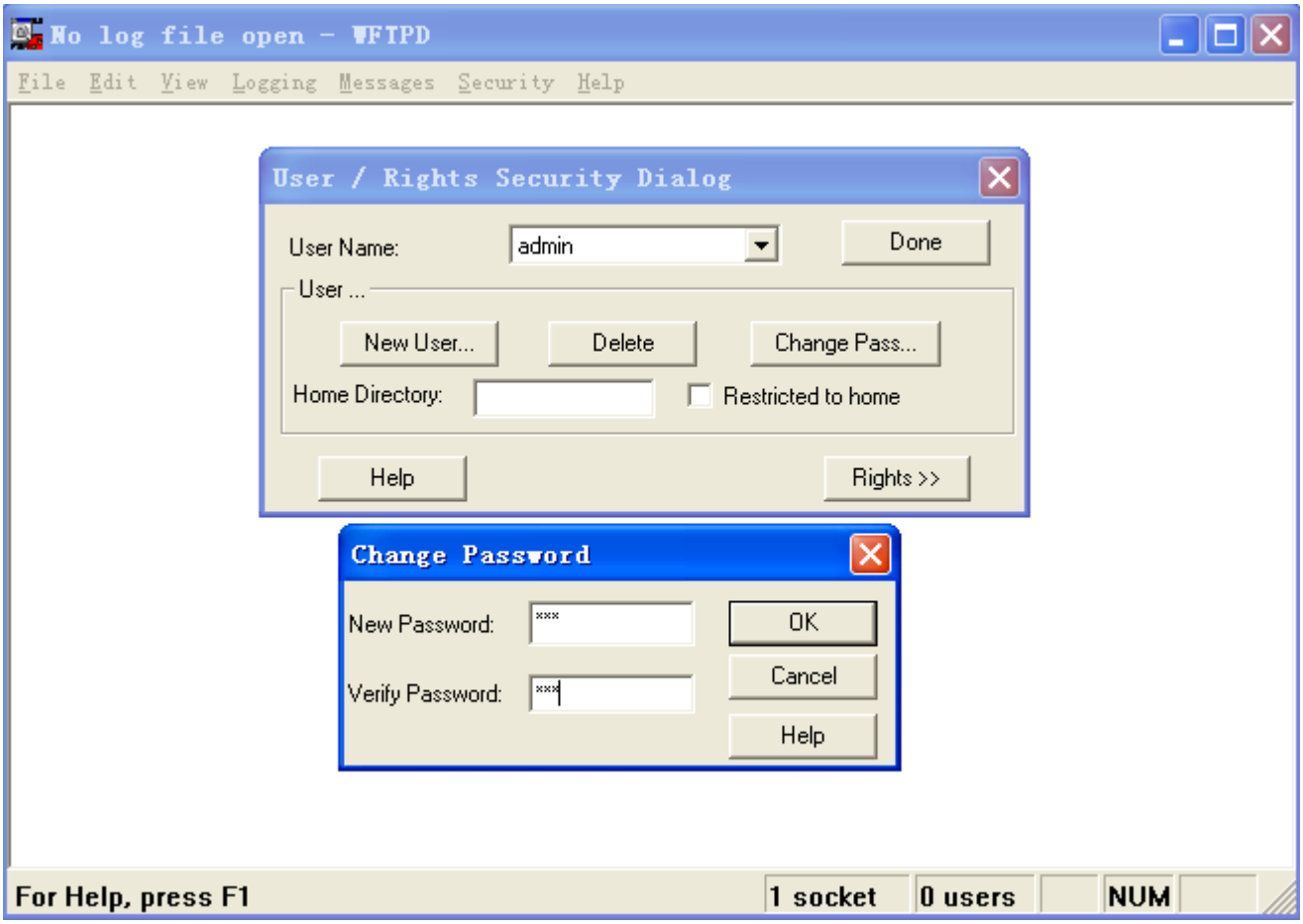

Рисунок 23 Создание нового пользователя FTP

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

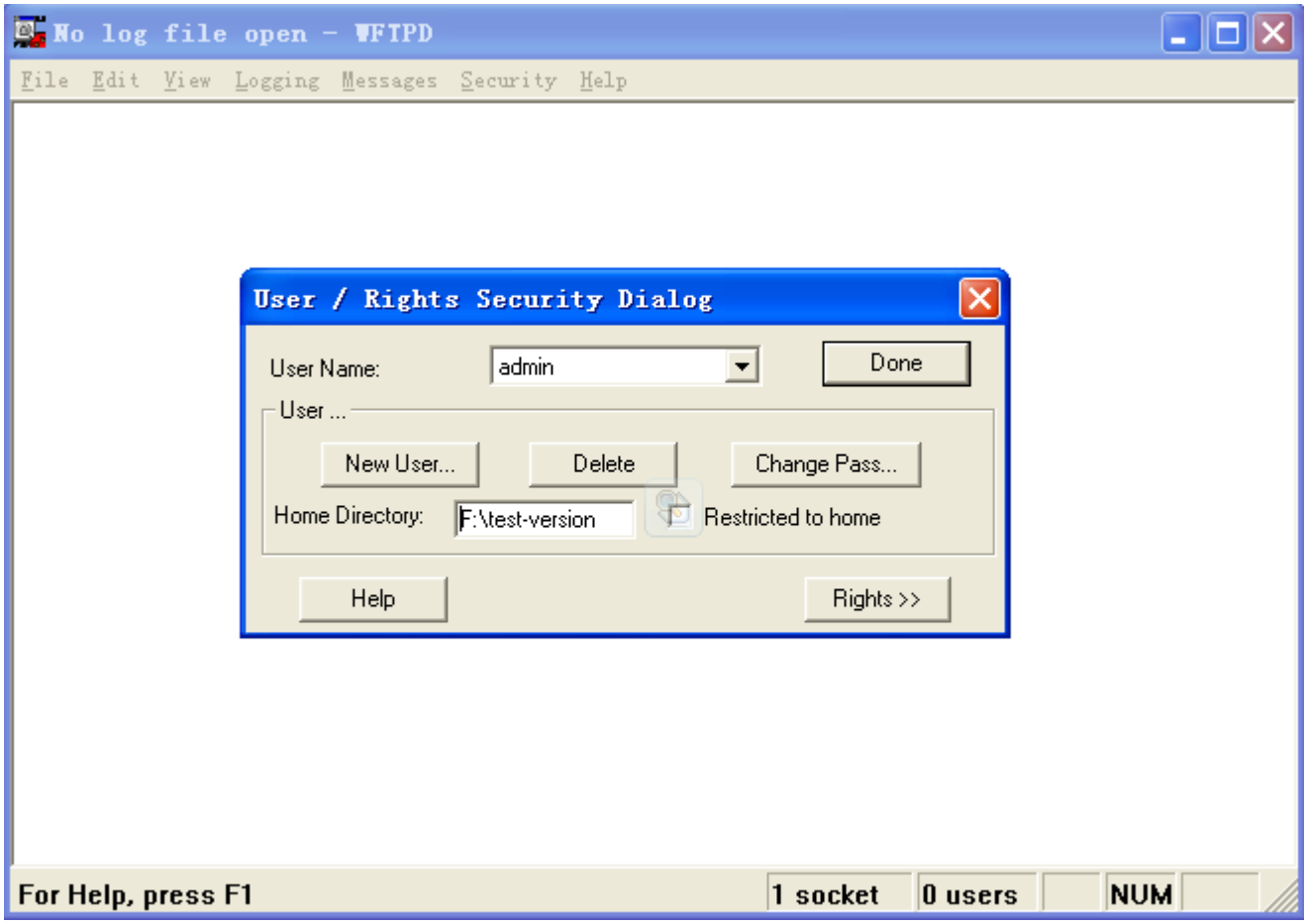

Рисунок 24 Местоположение файла

3. Для обновления BootROM введите в привилегированном режиме следующую команду. Switch#update bootrom File_name Ftp_server_ip_address User_name Password В таблице ниже приведено описание параметров.

Таблица 2 Параметры обновления BootROM через FTP

Параметр	**Описание**
File_name	Имя версии BootROM
Ftp_server_ip_address	IP-адрес сервера FTP
User_name	Созданное имя пользователя FTP.
Password	Созданный пароль FTP.

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

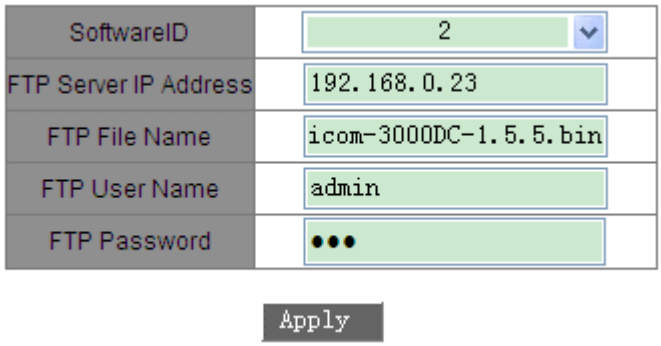

Рисунок 25 Обновление программного обеспечения через FTP

WARNING	**Внимание:** Имя файла должно содержать расширение. В противном случае обновление может пройти неудачно.

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

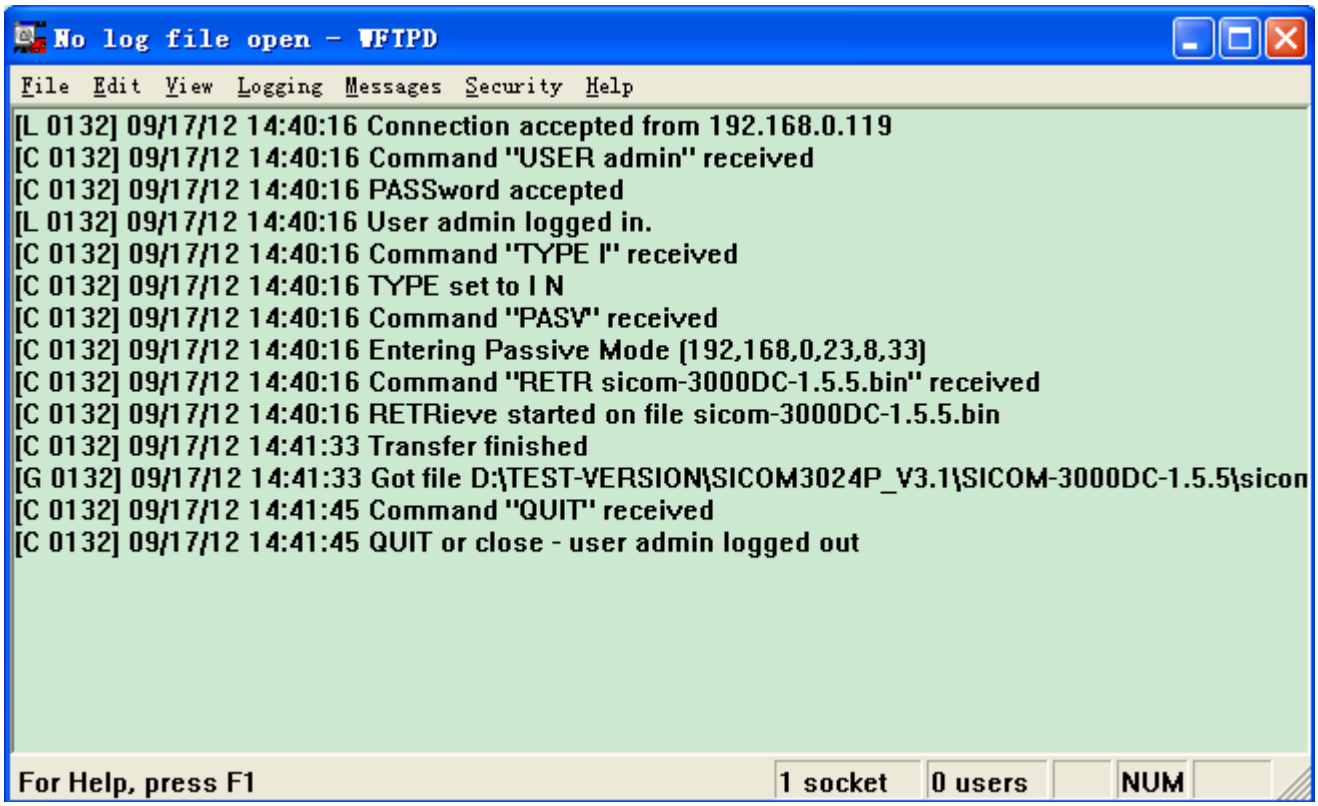

Рисунок 26 Нормальная связь между FTP-сервером и коммутатором

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

6. Когда обновление будет завершено, как показано на следующем рисунке, перезагрузите устройство и откройте страницу Switch Basic Information, чтобы проверить, успешно ли выполнено обновление и

активна ли новая версия.

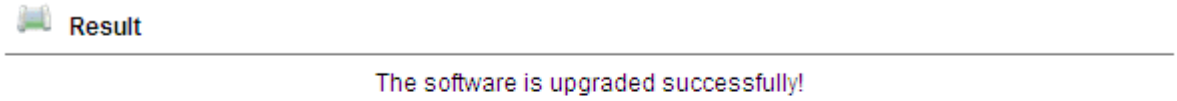

Рисунок 27 Успешное обновление программного обеспечения через FTP

WARNING	**Внимание:** > Во время обновления ПО не выключайте FTP-сервер. > По завершении обновления перезагрузите устройство для активации новой версии. > Если обновление не удалось, не перезагружайте устройство, чтобы избежать потери файла программного обеспечения и запуска с ошибкой.

5.6 Запрос версии программного обеспечения

В коммутатор можно загрузить две версии ПО, но только одна из них может быть активна.
Запросив версии программного обеспечения, можно узнать идентификаторы, даты выпуска и статусы двух версий, как показано на следующем рисунке.

ID	Version	Date	Status
1	R1004	2014-12-24 14:53	Active
2	R1003	2014-7-15 17:32	Inactive

Apply

Рисунок 28 Запрос версии программного обеспечения

5.7 Выгрузка/загрузка конфигурации

Функция резервного копирования конфигурации позволяет сохранять актуальные файлы конфигурации коммутатора на сервере. При изменении конфигурации коммутатора можно загрузить исходные файлы конфигурации с сервера на коммутатор через FTP.
Выгрузка файлов заключается в выгрузке файлов конфигурации коммутатора на сервер и сохранении их в файлах *.doc и *.txt. Загрузка файлов заключается в загрузке сохраненных файлов конфигурации с сервера на коммутатор, как показано на следующих рисунках.

CAUTION	**Предупреждение:** После загрузки файла конфигурации на коммутатор необходимо перезагрузить коммутатор, чтобы конфигурация вступила в силу.

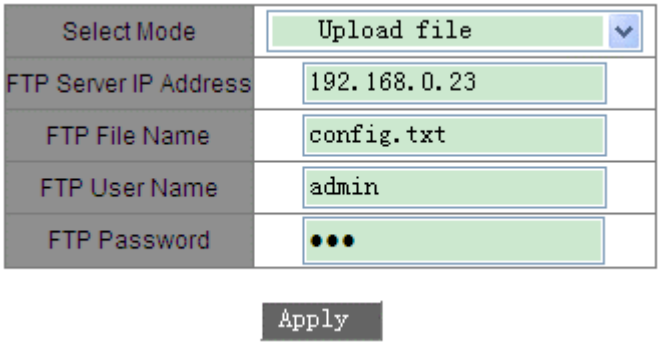

Рисунок 29 Выгрузка файла конфигурации

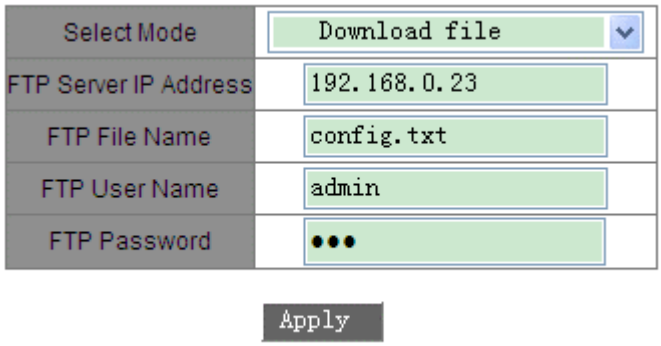

Рисунок 30 Загрузка файла конфигурации

6 Расширенные настройки

6.1 Ограничение скорости порта

6.1.1 Обзор

Ограничение скорости порта предназначено для ограничения скорости пакетов, принимаемых или передаваемых портом, и отбрасывания пакетов, скорость которых превышает пороговое значение. Эта функция действует на все пакеты на выходе, но только на определенные типы пакетов на входе. Следующие пакеты контролируются на входе.
Пакеты одноадресной рассылки: одноадресные пакеты, добавленные статически или исходные MAC-адреса которых изучены.
Пакеты многоадресной рассылки: пакеты, добавленные статически или полученные с помощью IGMP Snooping или GMRP.
Зарезервированные многоадресные пакеты: пакеты с MAC-адресами в диапазоне от 0x0180c2000000 до 0x0180c200002f.
Широковещательные пакеты: пакеты с MAC-адресом назначения FF:FF:FF:FF:FF:FF.
Неизвестные пакеты многоадресной рассылки: пакеты, которые не были добавлены статически и не изучены с помощью IGMP Snooping или GMRP.
Неизвестные одноадресные пакеты: пакеты, которые не были добавлены статически и MAC-адреса источника которых не изучены.
Пакеты неизвестного источника: пакеты с MAC-адресами неизвестного источника.

6.1.2 Настройка через веб-интерфейс

1. Выберите типы пакетов для контроля скорости, как показано на рисунке ниже.

The restricted speed is disabled when it is set to 0.

Set Packet Type for Rate Control

Type	Service	Broadcast	Remark
Unicast	☑	☐	Unicast packet type and address added staticly or learned.
Multicast	☑	☐	Multicast packet type and address added staticly or learned through IGMP Snooping.
RSVM	☐	☑	Mac control frame between 0x0180c2000000~0x0180c200002f.
Broadcast	☐	☑	Broadcast address.
MLF	☐	☑	Multicast packet and address not added staticly and not learned through IGMP Snooping.
DLF	☐	☑	Unicast packet type and address not added staticly and not through source MAC.
Unknown SA	☐	☑	Unknown source address in packet.

Рисунок 31 Типы пакетов для контроля скорости

Приемник разделяет управление скоростью на два типа: управление скоростью обслуживания и управление скоростью широковещательной передачи. Каждый пакет можно добавить только в один тип контроля скорости.

2 Настройте контроль скорости порта, как показано на рисунке ниже.

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

Рисунок 32 Контроль скорости порта

Service/Broadcast

Диапазон: 64~1000000 Кбит/с

Функция: Настройка контроля скорости для пакетов порта. Пакеты, скорость которых превышает указанное значение, 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: 64~1000000 Кбит/с

Функция: Ограничить скорость 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.

	**Предупреждение:** Если значение установлено равным 0, контроль скорости для порта отключен.

6.1.3 Пример типовой конфигурации

Установите порог скорости одноадресных и многоадресных пакетов на порту 2 до 70 Кбит/с, широковещательных пакетов до 80 Кбит/с и исходящей скорости до 90 Кбит/с.
Этапы настройки:
1. Выберите одноадресные и многоадресные пакеты в столбце Service и широковещательные пакеты в столбце Broadcast, как показано на рисунке 31.
2. На порту 2 установите порог скорости обслуживания 70 Кбит/с, порог скорости широковещательной передачи 80 Кбит/с и исходящую скорость 90 Кбит/с, как показано на рисунке 32.

6.2 VLAN

6.2.1 Обзор

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

6.2.2 Принцип работы

Чтобы сетевые устройства могли различать пакеты из разных VLAN, в пакеты необходимо добавить поля для идентификации VLAN. В настоящее время для идентификации VLAN чаще всего используется протокол IEEE802.1Q. В таблице показана структура кадра 802.1Q.
Таблица 3 Структура кадра 802.1Q

DA	SA	802.1Q Header				Length/Type	Data	FCS
		Type	PRI	CFI	VID			

4-байтовый заголовок 802.1Q в качестве тега VLAN добавляется к традиционному кадру данных Ethernet.
Тип 16 бит. Используется для идентификации кадра данных, несущего тег VLAN. Значение равно 0x8100.
PRI: три бита, определяющие приоритет пакета 802.1p.
CFI: один бит. 0 указывает на Ethernet, а 1 указывает на Token Ring.
VID: 12 бит, обозначающих номер VLAN. Диапазон значений от 1 до 4093. 0, 4094 и 4095 являются зарезервированными значениями.

NOTE	**Примечание**: > VLAN 1 является VLAN по умолчанию, и ее нельзя создать и/или удалить вручную. > Зарезервированные VLAN зарезервированы для реализации системой определенных функций и их нельзя создать и/или удалить вручную.

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

6.2.3 VLAN на основе порта

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

1. Тип порта

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

Нетегированный порт: Пересылаемые нетегированным портом пакеты не имеют тегов VLAN. Нетегированные порты обычно используются для подключения к терминалам, не поддерживающим 802.1Q. По умолчанию все порты коммутатора являются нетегированным портами и принадлежат VLAN1.

Тегированный порт: Все пересылаемые тегированным портом пакеты имеют тег VLAN. Тегированные порты обычно используются для подключения сетевых передающих устройств.

2. PVID

Каждый порт имеет PVID. При получении нетегированного пакета порт добавляет к пакету тег в соответствии с PVID.

PVID порта является VLAN ID для нетегированного порта. По умолчанию все PVID портов – VLAN 1.

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

Таблица 4 Различные режимы обработки пакетов

<table>
<tr><td colspan="2">Обработка полученных пакетов</td><td colspan="2">Обработка пакетов для пересылки</td></tr>
<tr><td>Нетегированные пакеты</td><td>Тегированные пакеты</td><td>Тип порта</td><td>Обработка пакетов</td></tr>
<tr><td rowspan="2">Добавить теги PVID в нетегированные пакеты</td><td rowspan="2">Если VLAN ID в пакете находится в списке разрешенных VLAN, принять пакет.
Если VLAN ID в пакете не находится в списке разрешенных VLAN, отклонить пакет.</td><td>Нетегированный</td><td>Переслать пакет после удаления тега.</td></tr>
<tr><td>Тегированный</td><td>Сохранить тег и переслать пакет.</td></tr>
</table>

6.2.4 Настройка через веб-интерфейс

Настройте режим прозрачной передачи VLAN, как показано на следующем рисунке.

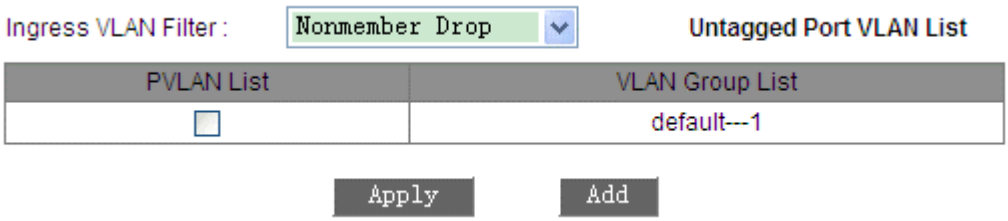

Рисунок 33 Настройка режима прозрачной передачи VLAN

Ingress VLAN
Варианты: Nonmember Drop/Nonmember Forward
По умолчанию: Nonmember Drop
Функция: Настройка режима прозрачной передачи VLAN.
Описание: Прозрачный режим передачи указывает, проверяет ли коммутатор входящие пакеты на порту. Если выбрано значение Nonmember Drop, пакет отбрасывается, если тег VLAN пакета отличается от VLAN порта. Если выбрано значение Nonmember Forward, пакет принимается, если тег VLAN пакета идентичен тегу любого другого подключенного порта коммутатора, в противном случае пакет отбрасывается.
2. Создайте VLAN.
Щелкните <Add> на рис. 33, чтобы создать VLAN. Как показано на рисунке ниже, выберите порты для добавления к VLAN и задайте параметры портов.

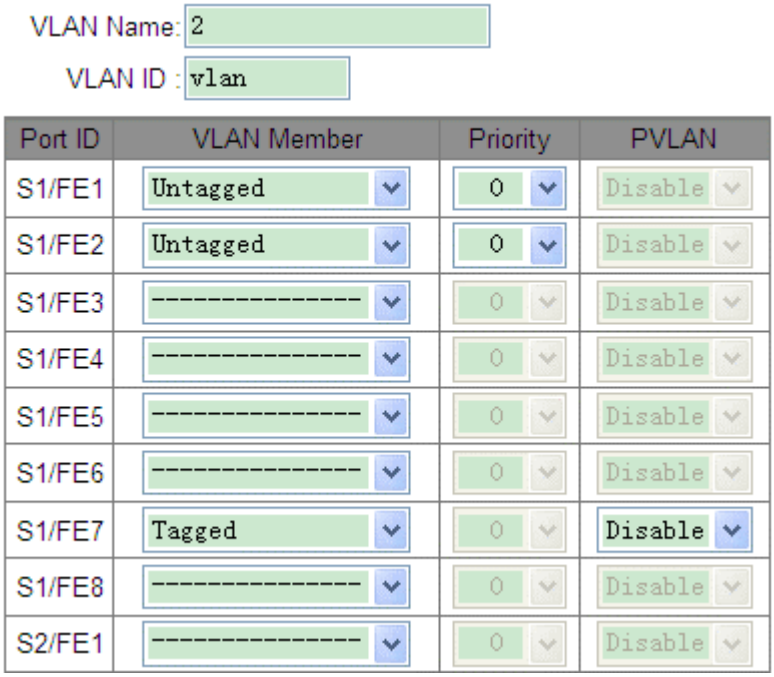

Рисунок 34 Настройка VLAN

VLAN Name
Диапазон: 1~31 символ
Функция: Задание имени VLAN.
VLAN ID
Диапазон: 2~4093
Функция: Настройка VLAN ID.
Описание: Идентификатор VLAN ID используется, чтобы различать разные VLAN. Коммутаторы серии поддерживают не более 256 VLAN.
VLAN Member
Варианты: Tagged/Untagged
Функция: Выбор типа порта в VLAN.
Priority

Диапазон: 0~7
По умолчанию: 0
Функция: Настройка приоритета по умолчанию для порта. При добавлении тега 802.1Q к нетегированному пакету значение поля PRI является приоритетом.

PVLAN

Варианты: Enable/Disable
По умолчанию: Disable
Функция: Для добавления тегированного порта в VLAN необходимо включить или выключить PVLAN. Дополнительную информацию
о PVLAN см. в следующей главе.

CAUTION	**Предупреждение:** Нетегированный порт можно добавить только в одну VLAN. VLAN ID является PVID для порта. Значение по умолчанию 1. Тегированный порт можно добавить в несколько VLAN.

3. Просмотрите список VLAN, как показано на рисунке ниже.

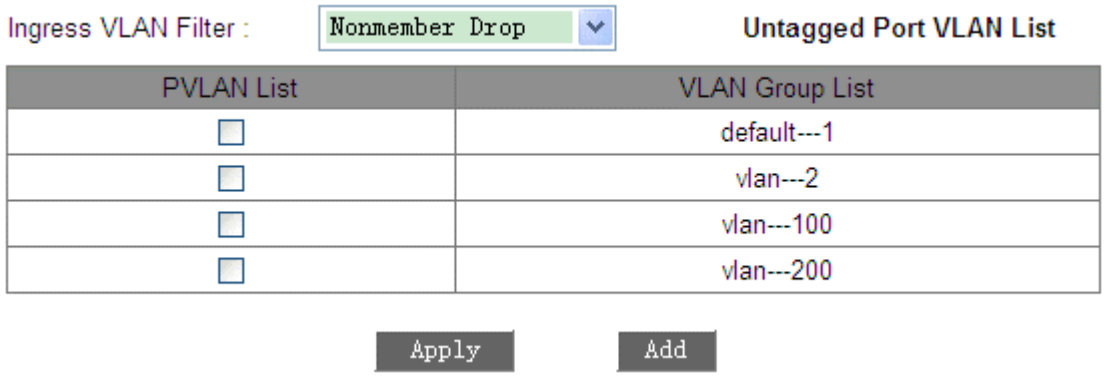

Рисунок 35 Просмотр списка VLAN

PVLAN List

Варианты: выбрать/отменить выбор
Функция: Включение или выключение функции PVLAN. Дополнительную информацию см. в следующей главе.
4. Просмотрите PVID портов.
Щелкните <Untagged Port VLAN List> на рисунке 35. Появится следующая страница.

Port ID	VLAN ID
S1/FE1	2
S1/FE2	2
S1/FE3	100
S1/FE4	100
S1/FE5	200
S1/FE6	200
S1/FE7	1
S1/FE8	1
S2/FE1	1
S2/FE2	1

Рисунок 36 Список PVID портов

CAUTION	**Предупреждение:** Каждый порт должен иметь атрибут Untag. Если он не установлен, порт с атрибутом Untag находится в VLAN 1 по умолчанию.

5. Изменение/удаление VLAN.
Щелкните список VLAN на рисунке 35. Можно изменить или удалить созданную VLAN. Щелкните <Delete> в нижней части экрана. Можно удалить VLAN напрямую, как показано на следующем рисунке.

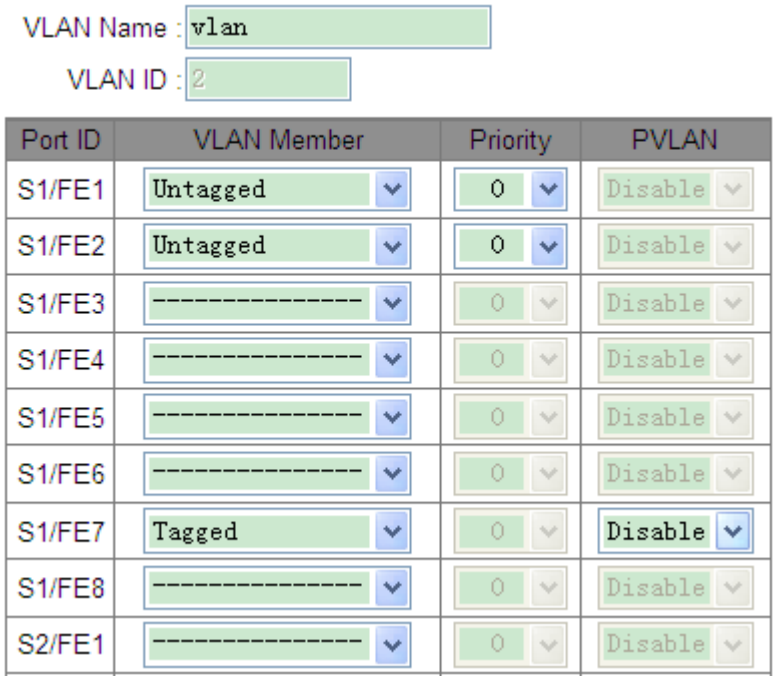

Рисунок 37 Изменение/удаление созданной VLAN

6.2.5 Пример типовой конфигурации

Как показано на следующем рисунке, сеть разделена на 3 VLAN: VLAN2, VLAN100 и VLAN200. Требуется,

чтобы устройства в одной VLAN могли осуществлять обмен данными друг с другом, но разные VLAN были изолированы. Терминальные ПК не могут различать тегированные пакеты, поэтому порты, соединяющие коммутатор A и коммутатор B с ПК, настроены на порт с атрибутом Untag. Пакеты VLAN2, VLAN100 и VLAN200 должны передаваться между коммутатором A и коммутатором B, поэтому порты, соединяющие коммутатор A и коммутатор B, должны быть настроены с атрибутом Tag, что позволит пропускать пакеты VLAN 2, VLAN 100 и VLAN 200. В таблице показана конкретная конфигурация.

Таблица 5 Конфигурация VLAN

Элемент	Настройка
VLAN2	Настройте порты 1 и 2 на коммутаторах A и B как нетегированные порты, а порт 7 как тегированный порт.
VLAN100	Настройте порты 3 и 4 на коммутаторах A и B как нетегированные порты, а порт 7 как тегированный порт.
VLAN200	Настройте порты 5 и 6 на коммутаторах A и B как нетегированные порты, а порт 7 как тегированный порт.

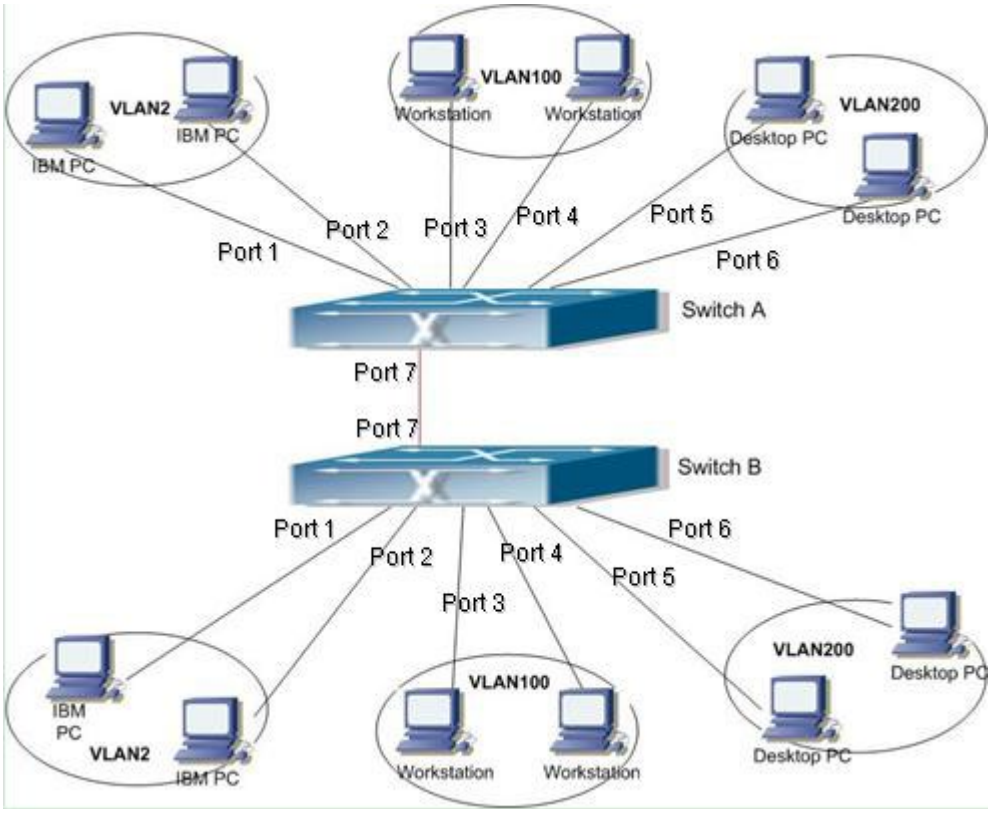

Рисунок 38 Использование VLAN

Конфигурация коммутатора A и коммутатора B:

1. Создайте VLAN 2, добавьте порт 1 и порт 2 в VLAN 2 как порты с атрибутом Untag и добавьте порт 7 в VLAN 2 как порт Tag, как показано на рисунке 34.
2. Создайте VLAN 100, добавьте порт 3 и порт 4 в VLAN 100 как порты с атрибутом Untag и добавьте порт 7 в VLAN 100 как порт Tag, как показано на рисунке 34.
3. Создайте VLAN 200, добавьте порт 5 и порт 6 в VLAN 200 как порты с атрибутом Untag и добавьте порт 7 в VLAN 200 как порт Tag, как показано на рисунке 34.

6.3 PVLAN

6.3.1 Обзор

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

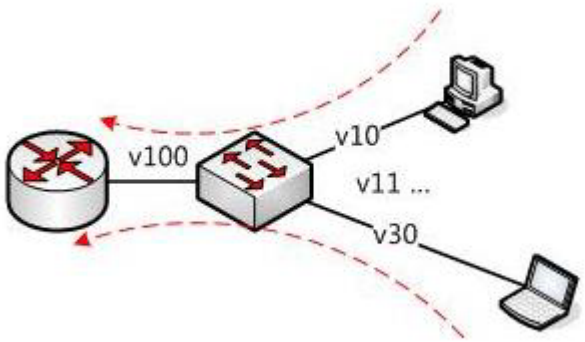

Рисунок 39 Использование PVLAN

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

NOTE	**Примечание:** Когда тегированный порт с поддержкой PVLAN пересылает кадр с тегом VLAN, тег VLAN удаляется.

6.3.2 Настройка через веб-интерфейс

1. Включите PVLAN дял порта, как показано на рисунке ниже.

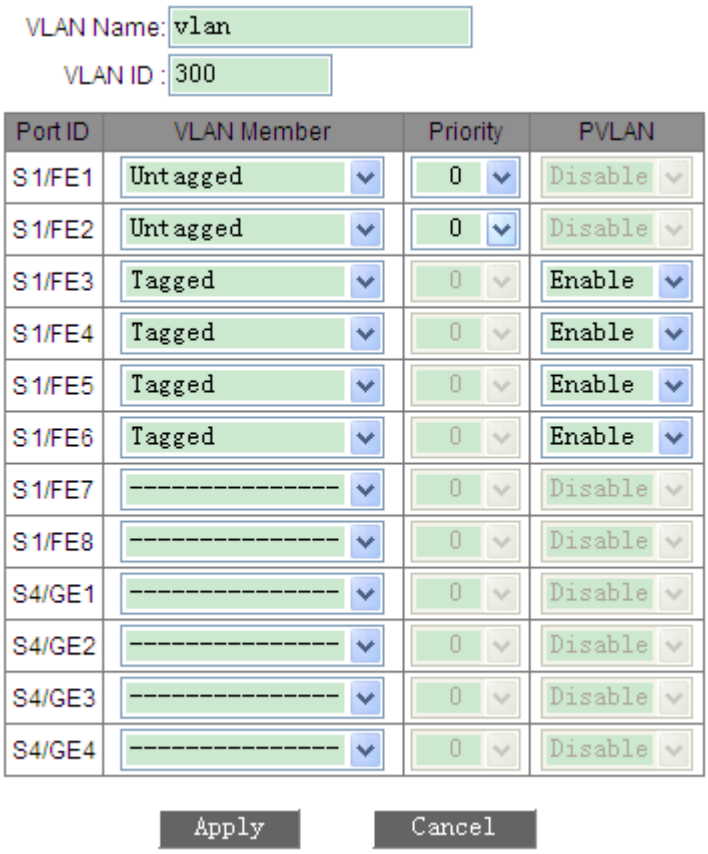

Рисунок 40 Включение PVLAN

Можно включить PVLAN на тегированном порту VLAN.
Если VLAN является общим доменом, порт восходящей линии связи является портом с атрибутом Untag, а порт нисходящей линии связи должен быть добавлен в VLAN в качестве порта атрибутом Tag.
Если VLAN является изолированным доменом, порт нисходящей линии связи является нетегированным, а порт восходящей линии связи должен быть добавлен в VLAN как тегированный .
2. Выберите VLAN, входящие в PVLAN, как показано на следующем рисунке.

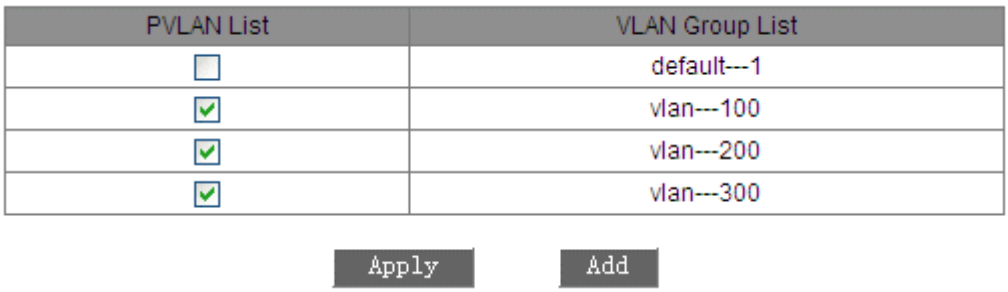

Рисунок 41 Выбор участников PVLAN

PVLAN List
Варианты: выбрать/отменить выбор
По умолчанию: отменить выбор
Функция: Выбор участников PVLAN

NOTE	**Примечание:** Как общие, так и изолированные домены являются VLAN, входящими в PVLAN.

6.3.3 Пример типовой конфигурации

Рисунок 42 показывает использование PVLAN. VLAN300 — это общий домен, а порты 1 и 2 — порты Uplink; VLAN100 и VLAN200 являются изолированными доменами, а порты 3, 4, 5 и 6 — портами Downlink.

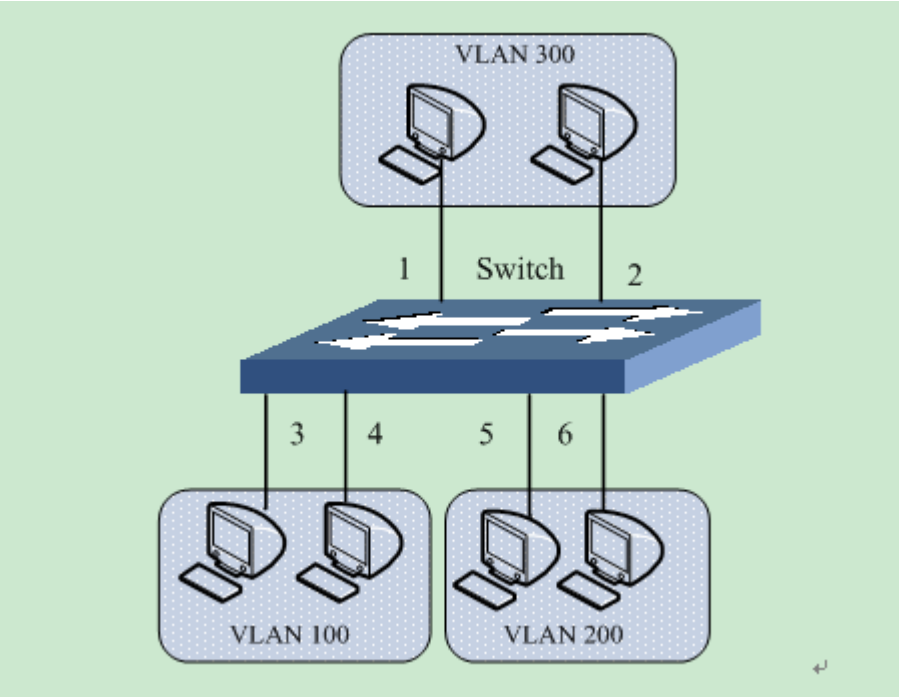

Рисунок 42 Пример настроек PVLAN

Этапы настройки:
1. Настройте общий домен, VLAN300, как показано на рисунке 40.
Настройте порт 1 и порт 2 как порты Untag и добавьте их в VLAN 300.
Настройте порт 3 и порт 4 как порты Tag и добавьте их в VLAN 300. Включите PVLAN на двух портах.
Настройте порт 5 и порт 6 как порты Tag и добавьте их в VLAN 300. Включите PVLAN на двух портах.
2. Настройте VLAN 100, изолированный домен, как показано на рисунке 40.
Настройте порт 1 и порт 2 как порты Tag и добавьте их в VLAN 100. Включите PVLAN на двух портах.
Настройте порт 3 и порт 4 как порты Untag и добавьте их в VLAN 100.
3. Настройте VLAN 200, изолированный домен, как показано на рисунке 40.
Настройте порт 1 и порт 2 как порты Tag и добавьте их в VLAN 200. Включите PVLAN на двух портах.
Настройте порт 5 и порт 6 как порты Untag и добавьте их в VLAN 200.
Настройте VLAN300, VLAN100 и VLAN200 в качестве участников PVLAN, как показано на рисунке 41.

6.4 Зеркалирование портов

6.4.1 Обзор

С функцией зеркалирования портов коммутатор копирует все полученные или переданные кадры данных в одном порту (исходный порт зеркалирования) на другой порт (порт назначения зеркалирования). Порт назначения зеркалирования подключается к анализатору протокола или монитору RMON для мониторинга сети, управления и диагностики неисправностей.
Описание

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

CAUTION	**Предупреждение:** > Порт источника или назначения зеркалирования не может быть добавлен в группу Trunk, а порт, добавленный в группу Trunk, не может быть установлен в качестве порта назначения или источника зеркалирования. > Порт источника или назначения зеркалирования не может быть установлен в качестве резервного порта, а резервный порт не может быть установлен в качестве порта источника или назначения зеркалирования.

6.4.3 Настройка через веб-интерфейс

1. Выберите порт назначения зеркалирования, как показано на рисунке ниже.

Рисунок 43 Выбор порта зеркалирования

Mirroring Port
Варианты: Disable/порт коммутатора
По умолчанию: Disable
Функция: Выбор порта, который будет портом назначения зеркалирования. Должен быть только один порт назначения зеркалирования.
2. Выберите порты источника зеркалирования и режим зеркалирования., как показано на рисунке ниже.

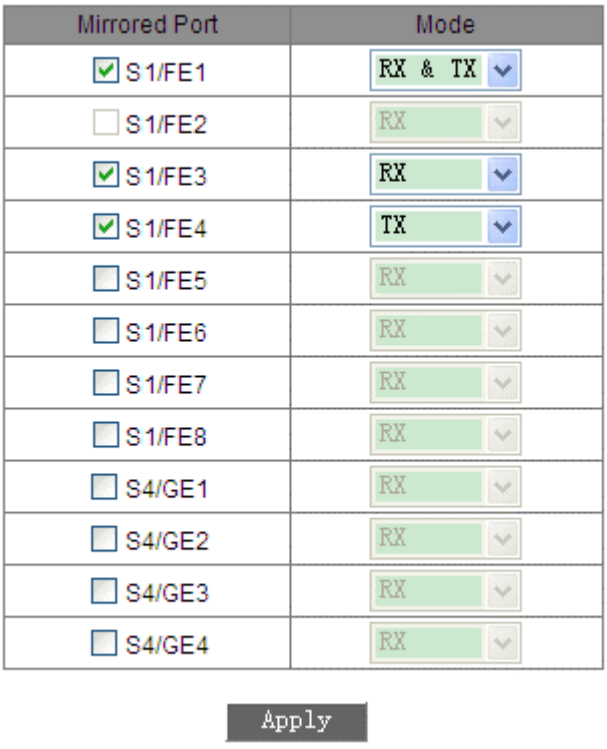

Рисунок 44 Порт источника зеркалирования

Mode
Варианты: RX/TX/RX & TX
Функция: Выбор данных для зеркалирования.
TX указывает, что в исходном порту зеркалируются только отправленные пакеты.
RXуказывает, что в исходном порту зеркалируются только полученные пакеты.
TX&RX указывает, что в исходном порту зеркалируются полученные и отправленные пакеты.

6.4.4 Пример типовой конфигурации

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

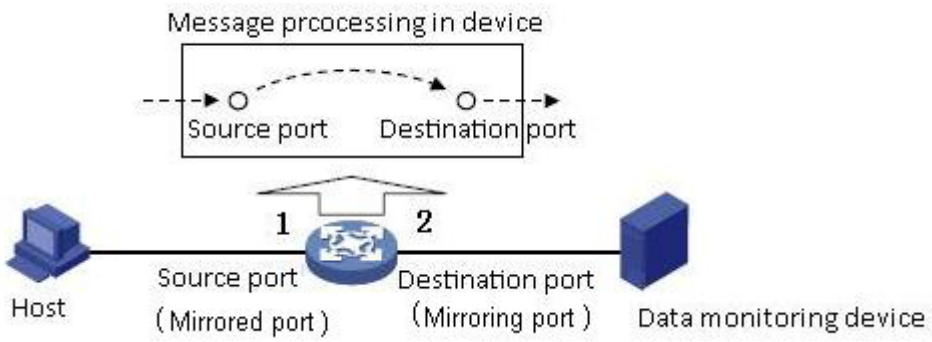

Рисунок 45 Пример зеркалирования порта

Этапы настройки:
1. Задайте порт 2 как порт назначения зеркалирования, как показано на рисунке 43.
2. Задайте порт 1 в качестве исходного порта зеркалирования, выберите режим зеркалирования TX&RX, как показано на рисунке 44.

6.5 Агрегация портов

6.5.1 Обзор

Агрегация портов предназначена для привязки группы физических портов с одинаковой конфигурацией к логическому порту. Порты в группе агрегации могут не только распределять нагрузку, но и выступать в качестве динамического резервного копирования друг для друга, повышая надежность соединения.

6.5.2 Реализация

Как показано на следующем рисунке, три порта коммутатора A объединяются в группу, а пропускная способность группы равна общей пропускной способности трех портов.

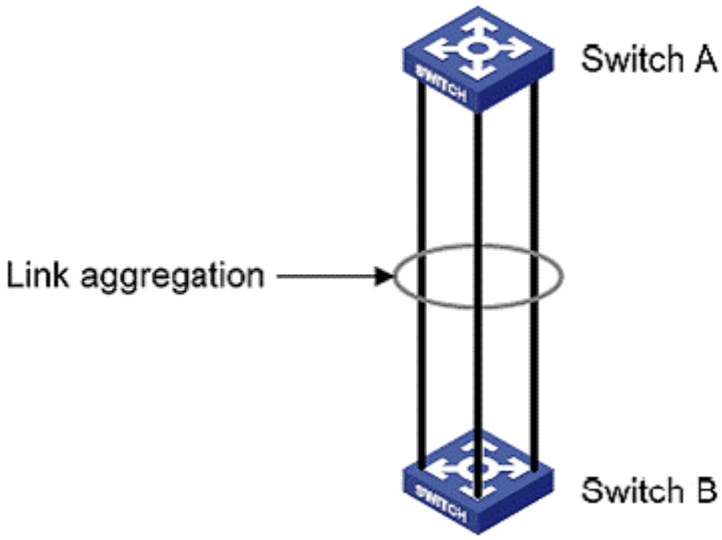

Рисунок 46 Агрегация портов

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

6.5.3 Описание

Агрегацию портов и следующие конфигурации портов нельзя использовать вместе:
Резервирование портов: Порт, добавленный в группу агрегации, портов нельзя настроить как резервный порт, а резервный порт нельзя добавить в группу агрегации.
Зеркалирование портов: Порт, добавленный в группу агрегации, портов нельзя настроить как порт назначения или источника зеркалирования, а порт назначения или источника зеркалирования нельзя добавить в группу агрегации.
DHCP Snooping: Порт, добавленный в группу агрегации, портов нельзя настроить как доверенный порт DHCP Snooping, а доверенный порт DHCP Snooping нельзя добавить в группу агрегации.
Кроме того, не рекомендованы следующие действия.
Включение GMRP на порту агрегации.
Добавление порта с включенным GMRP в группу агрегации.
Добавление порта агрегации к статической записи одноадресной/многоадресной рассылки.
Добавление порта из статической записи одноадресной/многоадресной рассылки в группу агрегации.
Предупреждение:
Гигабитные порты коммутаторов этой серии не поддерживают агрегацию портов.
Порт можно добавить только в одну группу портов.

CAUTION	**Предупреждение:** > Гигабитные порты коммутаторов этой серии не поддерживают агрегацию портов. > Порт можно добавить только в одну группу портов.

6.5.4 Настройка через веб-интерфейс

1. Добавьте группу портов.
Щелкните <Add>, чтобы добавить группу портов, как показано на рисунке ниже.

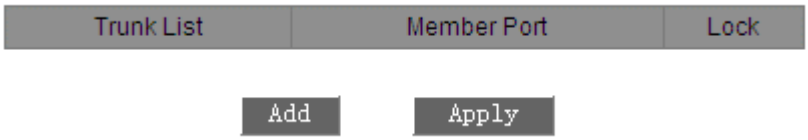

Рисунок 47 Добавление группы портов

2. Настройте группу портов, как показано на рисунке ниже.

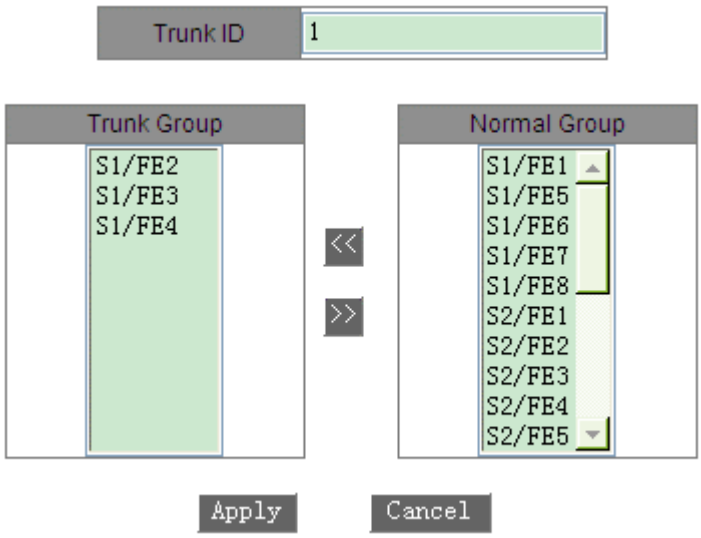

Рисунок 48 Настройка группы портов

Trunk ID (SICOM3024P/SICOM3024)
Диапазон: 1~14
Функция: Задание ID группы портов.
Описание: Коммутаторы серии поддерживают не более 14 групп агрегации. Каждая группа включает в себя не более 4 портов.
Trunk ID (SICOM3048)
Диапазон: 1~6
Функция: Задание ID группы портов.
Описание: Коммутаторы серии поддерживают не более 6 групп агрегации. Каждая группа включает в себя не более 4 портов.
Просмотрите список групп портов, как показано на рисунке ниже.

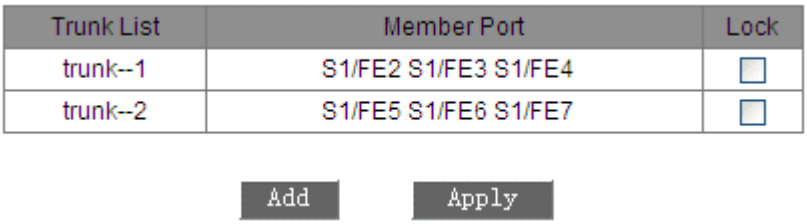

Рисунок 49 Список групп портов

Lock
Блокировка портов-участников в группе агрегации. После удаления заблокированных портов из группы агрегации необходимо вручную включить их, чтобы разблокировать.
Щелкните группу портов на рисунке 49. Можно изменить или удалить группу портов, как показано на рисунке ниже.

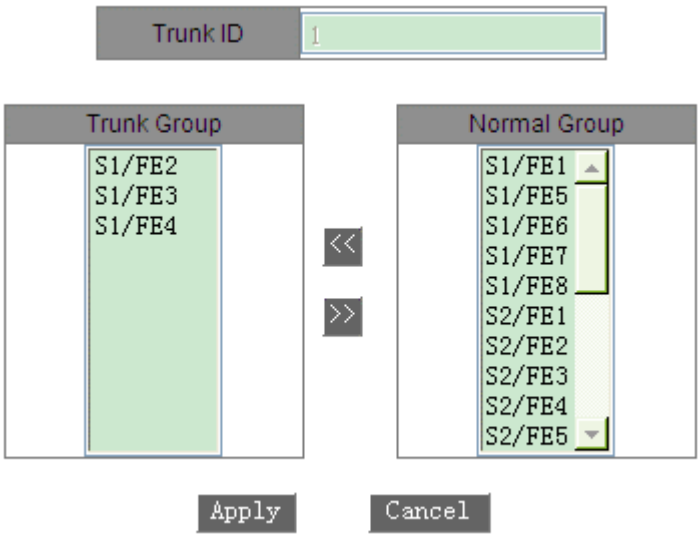

Рисунок 50 Изменение/удаление группы портов

После изменения настроек группы (добавления нового порта в группу или удаления порта из группы) щелкните <Apply>, чтобы изменения вступили в силу. Если щелкнуть <Delete>, можно удалить группу.

6.5.5 Пример типовой конфигурации

Как показано на рисунке 46, порт 2, порт 3 и порт 4 коммутатора A подключены к портам коммутатора B соответственно, образуя группу агрегации 1 для достижения балансировки нагрузки между портами.
Этапы настройки:
Создайте группу портов 1 на коммутаторе A и добавьте в группу порт 2, порт 3 и порт 4, как показано на рисунке 48.
1. Создайте группу портов 1 на коммутаторе B и добавьте в группу порт 2, порт 3 и порт 4, как показано на рисунке 48.
2. Создайте группу портов 1 на коммутаторе B и добавьте в группу порт 2, порт 3 и порт 4, как показано на рисунке 48.

6.6 Проверка канала связи

6.6.1 Обзор

Проверка канала использует периодическое взаимодействие пакетов протокола для оценки подключения канала и отображения состояния связи портов с поддержкой протокола 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 одноранговой стороны в течение времени ожидания приема (5 с), это означает, что канал неисправен, и порт отображает состояние ошибки получения. Если порт получает пакет проверки канала от одноранговой стороны, и пакет показывает, что пакет проверки канала получен от локального узла в течение периода ожидания приема (5 с), порт отображает нормальное состояние канала. Если порт получает пакет проверки канала от одноранговой стороны, но пакет показывает, что пакет проверки канала не получен от локального узла в течение периода ожидания приема (5 с), порт отображает состояние ошибки отправки.
Порт, для которого отключена проверка состояния канала, работает в пассивном режиме. Это значит, что он не отправляет пакет проверки связи в активном режиме. Однако после получения пакета проверки

канала от удаленного узла этот порт немедленно возвращает пакет проверки канала, чтобы проинформировать удаленный узел о том, что он получил пакет проверки канала.

NOTE	**Примечание:** > Функция действительна только для порта с поддержкой протокола резервирования. > Если кольцевой/резервный порт DRP, кольцевой/резервный порт DT-Ring, порт RSTP, для которого включена проверка канала, неисправен (например, прием ненормальный, отправка ненормальная), протокол резервирования заблокирует этот порт.

6.6.2 Настройка через веб-интерфейс

На следующем рисунке показана настройка проверки канала.

Link Check

Port	Administration Status	Run Status
S1/FE1	Enable	Normal Link
S1/FE2	Enable	Send Fault
S1/FE3	Enable	Receive Fault
S1/FE4	Disable	Disable
S1/FE5	Disable	Disable
S1/FE6	Disable	Disable
S1/FE7	Disable	Disable
S1/FE8	Disable	Disable
S4/GE1	Disable	Disable
S4/GE2	Disable	Disable
S4/GE3	Disable	Disable
S4/GE4	Disable	Disable

Apply

Рисунок 51 Настройка проверки канала связи

Administration Status
Варианты: Enable/Disable
По умолчанию: Enable
Описание: Включение/выключение проверки канала связи для порта.

CAUTION	**Предупреждение:** Если одноранговое устройство не поддерживает эту функцию, функция должна быть отключена на подключенном порту локального устройства.

Run Status
Варианты: Normal Link/Receive Fault/Disable/Send Fault
Описание: Если для кольцевого порта включена функция Link Check и порт нормально отправляет и принимает данные, отображается Normal Link. Если одноранговое устройство не получает пакеты обнаружения от устройства, отображается Send Fault. Если устройство не получает пакеты обнаружения от однорангового устройства, отображается Receive Fault. Если функция Link Check не включена для

порта, отображается Disable.

6.7 Статическая многоадресная рассылка

6.7.1 Обзор

Можно настроить статическую таблицу многоадресной рассылки. Запись в таблицу можно добавить в формате <multicast MAC address, VLAN ID, multicast member port>. При получении пакетов многоадресной рассылки коммутатор выполняет в таблице поиск соответствующего порта для пересылки пакетов. Устройство поддерживает до 256 записей многоадресной рассылки.

6.7.2 Настройка через веб-интерфейс

1. Включите статическую многоадресную рассылку, как показано на рисунке ниже.

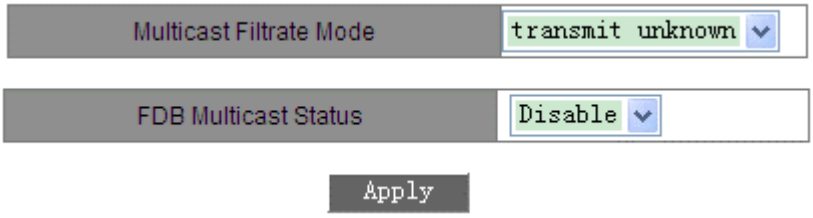

Рисунок 52 Включение статической многоадресной рассылки

Multicast Filtrate Mode
Варианты: transmit unknown/drop unknown
По умолчанию: transmit unknown
Функция: Настройка режима обработки неизвестных многоадресных пакетов.
Описание: Неизвестные пакеты многоадресной рассылки – пакеты, которые не были добавлены статически и не изучены с помощью IGMP Snooping или GMRP.
Transmit unknown указывает на то, что неизвестные многоадресные пакеты транслируются в соответствующих сетях VLAN; drop unknown указывает, что неизвестные многоадресные пакеты отбрасываются.
FDB Multicast Status
Варианты: Enable/Disable
По умолчанию: Disable
Функция: Включение или выключение статической многоадресной рассылки. Статическую многоадресную рассылку и IGMP Snooping нельзя включить одновременно.
2. Добавьте статическую запись многоадресной рассылки, как показано на рисунке ниже.

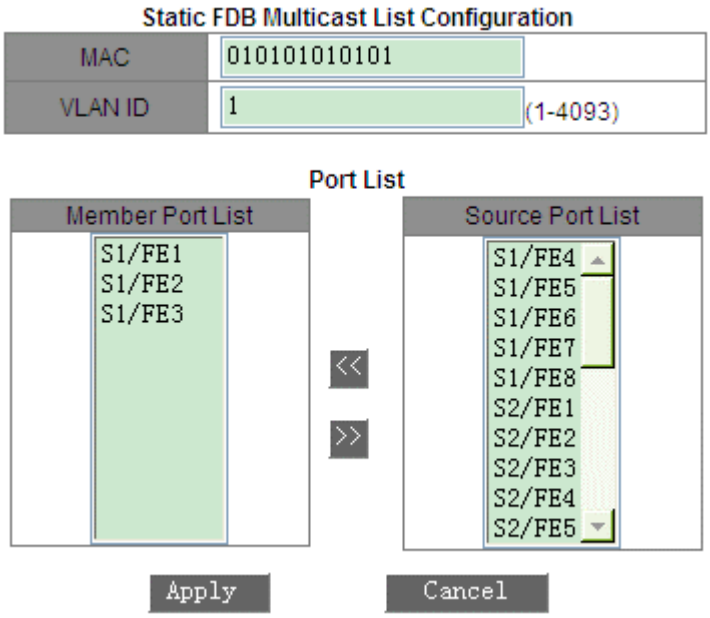

Рисунок 53 Добавление статической записи многоадресной рассылки

MAC
Состав: HHHHHHHHHHHH (H – шестнадцатеричное число.)
Функция: Настройка адреса группы многоадресной рассылки. Младший бит в старшем байте равен 1.
VLAN ID
Варианты: все существующие VLAN
Функция: Настройка VLAN ID для записи. Только порты-участники VLAN могут пересылать многоадресные пакеты.
Member Port List
Выбор портов многоадресной рассылки. Если хостам, подключенным к порту, необходимо получать пакеты с адреса многоадресной рассылки, можно настроить этот порт как порт-участник многоадресной рассылки.
3. Просмотрите, измените или удалите статическую запись многоадресной рассылки, как показано на рисунке ниже.

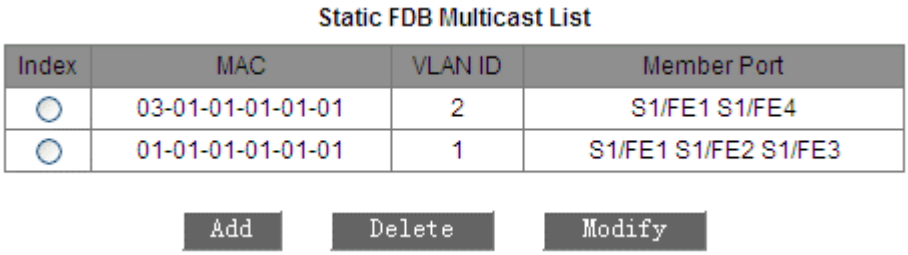

Рисунок 54 Действия со статической записью многоадресной рассылки

Список статических адресов многоадресной рассылки содержит MAC-адрес, идентификатор VLAN ID и порт-участник. Чтобы удалить запись, выберите запись и щелкните <Delete>. Чтобы изменить запись, выберите запись и щелкните <Modify>.

6.8 IGMP Snooping

6.8.1 Обзор

Отслеживание IGMP (Internet Group Management Protocol 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.

6.8.2 Основные понятия

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

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

6.8.3 Принцип работы

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

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

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

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

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

6.8.4 Настройка через веб-интерфейс

1. Включите IGMP Snooping, как показано на рисунке ниже.

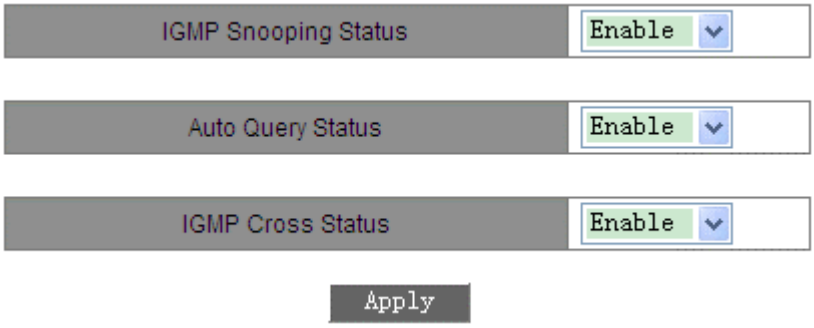

Рисунок 55 Включение IGMP Snooping

IGMP Snooping Status

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение или выключение IGMP Snooping. IGMP Snooping и статическую многоадресную рассылку/GMRP нельзя включить одновременно.

Auto Query Status

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение или выключение функции автоматического запроса.

Описание: Функция автоматического запроса может быть включена только при включенном IGMP Snooping.

CAUTION	**Предупреждение:** Функция автоматического запроса в сети должна быть включена хотя бы на одном коммутаторе.

IGMP Cross Status

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Если функция включена, пакеты отчетов и пакеты leave могут пересылаться через кольцевые порты DT.

2. Просмотрите список участников многоадресной рассылки, как показано на рисунке ниже.

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

Рисунок 56 Список участников IGMP Snooping

IGMP Member List

Комбинация: {MAC, VLAN ID, Member}

В таблице многоадресной рассылки FDB, динамически изучаемой посредством отслеживания IGMP, идентификатор VLAN — это идентификатор VLAN портов-участников.

6.8.5 Пример типовой конфигурации

Как показано на рисунке ниже, IGMP Snooping включен на коммутаторе 1, коммутаторе 2 и коммутаторе 3. Функция автоматического запроса включена на коммутаторе 2 и коммутаторе 3. IP-адрес коммутатора 2 192.168.1.2, а IP-адрес коммутатора 3 192.168.0.2, таким образом коммутатор 3 выбран в качестве генератора запросов.

1. Включите IGMP Snooping на коммутаторе 1.
2. Включите IGMP Snooping и функцию автоматического запроса на коммутаторе 2.
3. Включите IGMP Snooping и функцию автоматического запроса на коммутаторе 3.

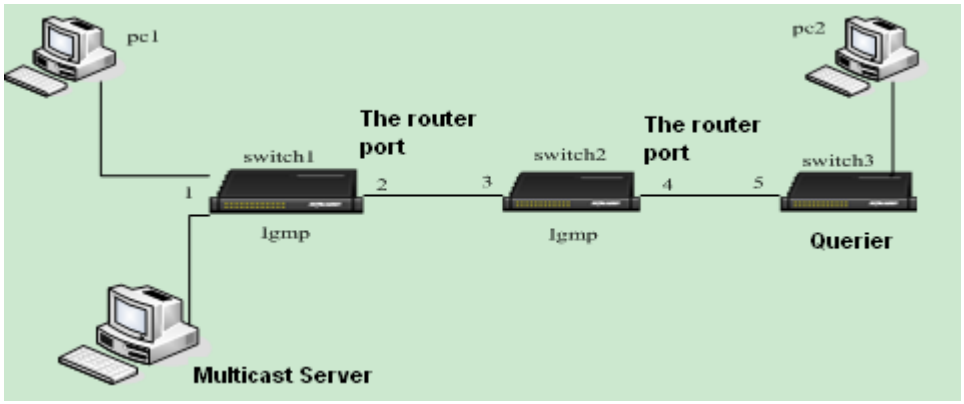

Рисунок 57 Пример настройки IGMP Snooping

Коммутатор 3 как генератор запросов периодически отправляет пакеты общего запроса. Порт 4 коммутатора 2 принимает пакеты и поэтому выбирается в качестве порта маршрутизации. Коммутатор 2 пересылает пакеты через порт 3. Порт 2 коммутатора 1 принимает пакеты и поэтому выбирается в качестве порта маршрутизации.
Когда ПК 1 добавляется в группу многоадресной рассылки 225.1.1.1 и отправляет пакеты отчетов IGMP, порт 1 и порт 2 (порт маршрутизации) коммутатора 1 добавляются в группу многоадресной рассылки 225.1.1.1. Пакеты отчетов IGMP пересылаются на коммутатор 2 через порт 2. Затем порт 3 и порт 4 коммутатора 2 добавляются в группу многоадресной рассылки 225.1.1.1. Коммутатор 2 пересылает пакеты отчетов IGMP на коммутатор 3 через порт 4. В результате порт 5 коммутатора 3 также добавляется в группу многоадресной рассылки 225.1.1.1.
При получении данных многоадресной рассылки коммутатор 1 пересылает данные на ПК 1 через порт 1. Поскольку порт 2 также является членом группы многоадресной рассылки, он также пересылает данные многоадресной рассылки. По ходу процесса многоадресные данные наконец достигают порта 5 коммутатора 3, поскольку дальнейший получатель недоступен. Если ПК 2 также добавлен в группу многоадресной рассылки 225.1.1.1, данные многоадресной рассылки также пересылаются на ПК 2.

6.9 ACL

6.9.1 Обзор

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

6.9.2 Реализация

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

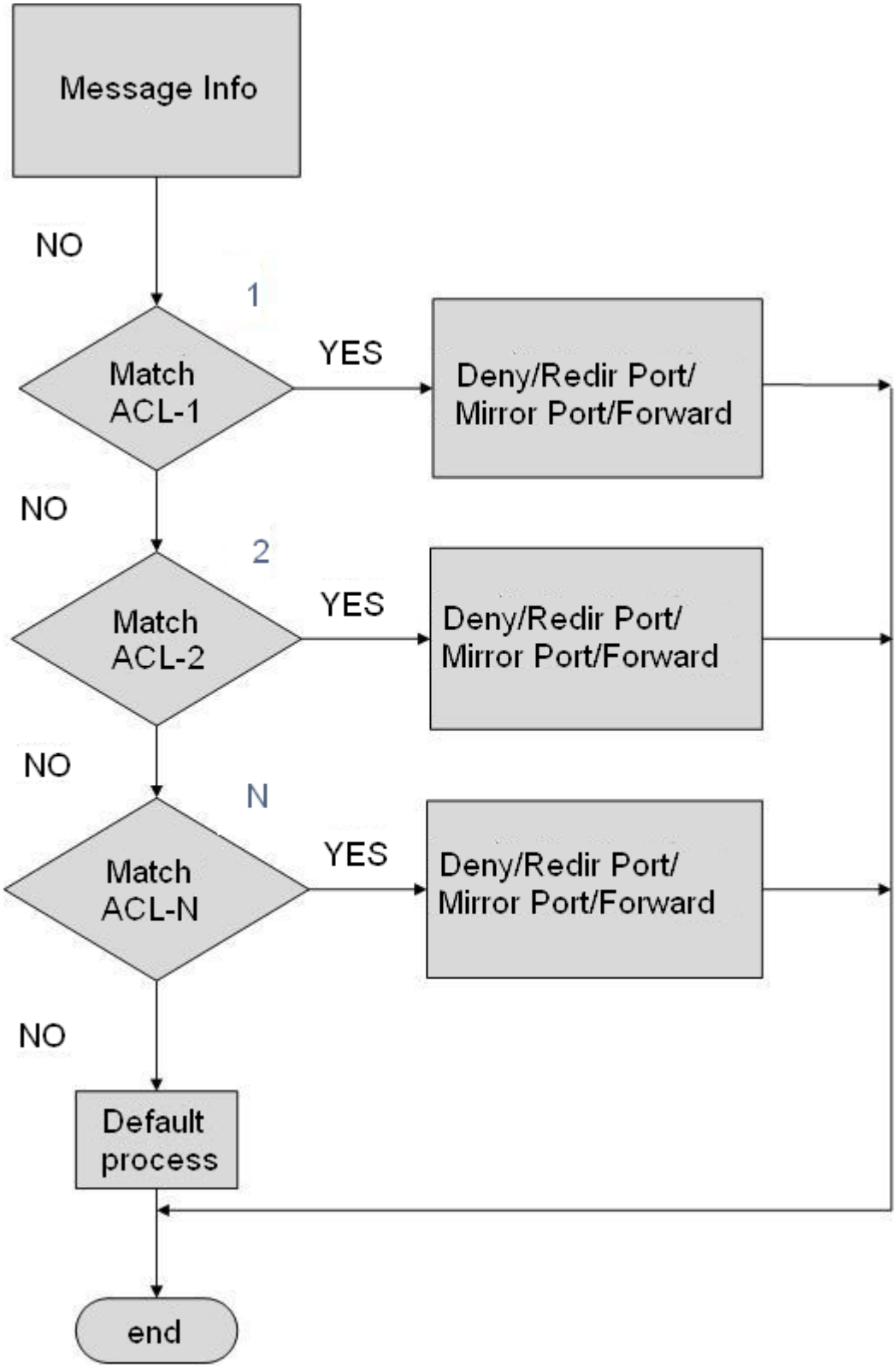

Рисунок 58 Схема обработки ACL

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

6.9.3 Настройка через веб-интерфейс (SICOM3024P/SICOM3024)

1. Добавьте запись ACL.
Щелкните <Add List>, чтобы добавить запись ACL, как показано на рисунке ниже.

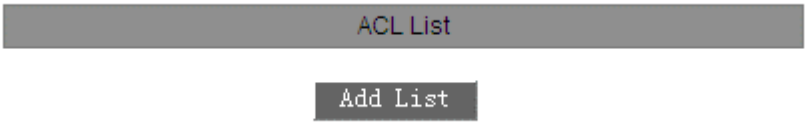

Рисунок 59 Добавление записи ACL

2. Задайте параметры записи ACL, как показано на следующем рисунке.

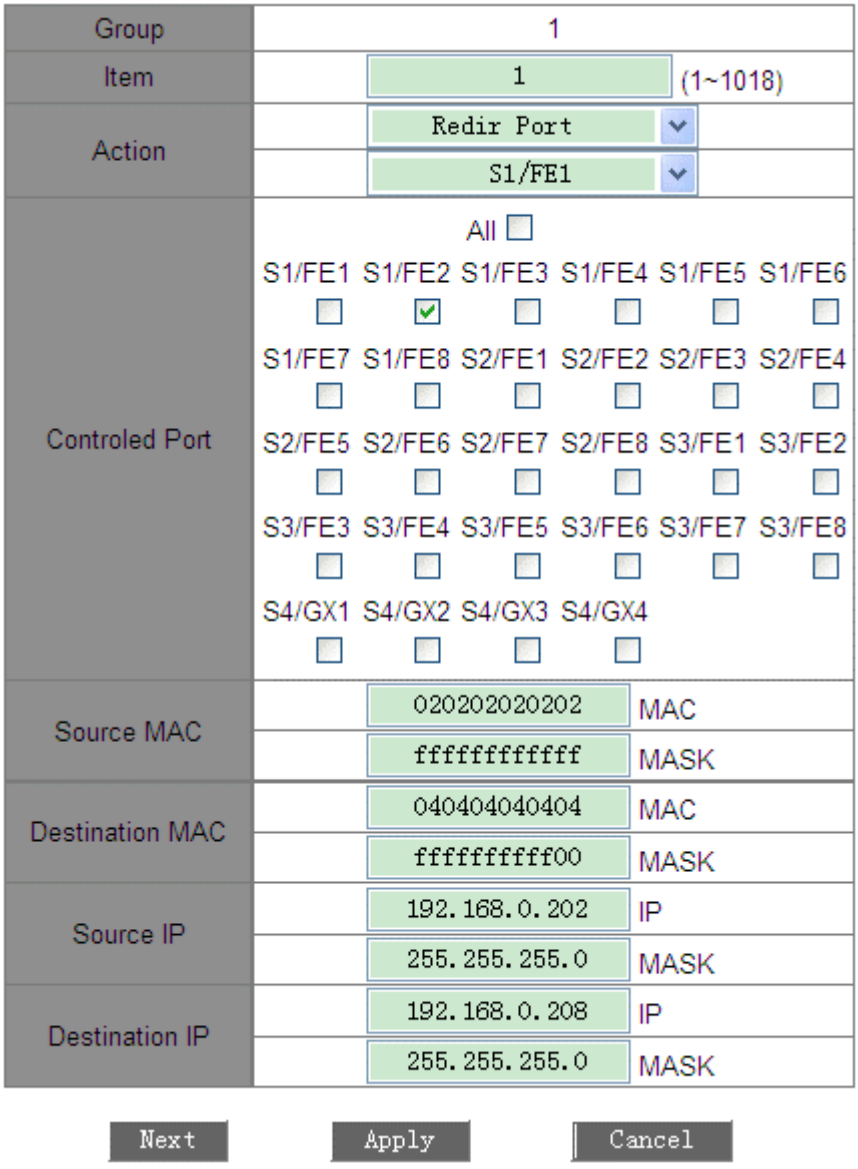

Рисунок 60 Задание параметров записи ACL 1

Коммутатор позволяет задать ряд параметров записи ACL. Для завершения настройки следует щелкнуть <Next>, как показано на рисунках ниже.

Configure Item

Ethernet Type	1537	(1537~65535)
TOS/DSCP	7	(0~255)
IP Protocol	6	(0~255)
IP TTL	2	(0~3)
Max ICMP	1000	(0~1023)
TCP Flag	60	(0~63)
ICMP Type Code	5000	(0~65535)
Vlan ID		(1~4093)
Vlan ID Range 0	5 ~ 16	(1~4093)
Vlan ID Range 1	~	(1~4093)
Vlan ID Range 2	~	(1~4093)
Vlan ID Range 3	~	(1~4093)

Back Next Apply Cancel

Рисунок 61 Задание параметров записи ACL 2

Configure Item

Source L4 Port	65000	(1~65535)
Src Port Range 0	~	(1~65535)
Src Port Range 1	~	(1~65535)
Src Port Range 2	~	(1~65535)
Src Port Range 3	~	(1~65535)
Destination L4 Port	21	(1~65535)
Dst Port Range 0	~	(1~65535)
Dst Port Range 1	~	(1~65535)
Dst Port Range 2	~	(1~65535)
Dst Port Range 3	~	(1~65535)
L2 Format	None	
L3 Format	None	
L4 Format	None	
Same IP	Disable	
Same L4 Port	Disable	
TCP Sequence Zero	Disable	

Back Next Apply Cancel

Рисунок 62 Задание параметров записи ACL 3

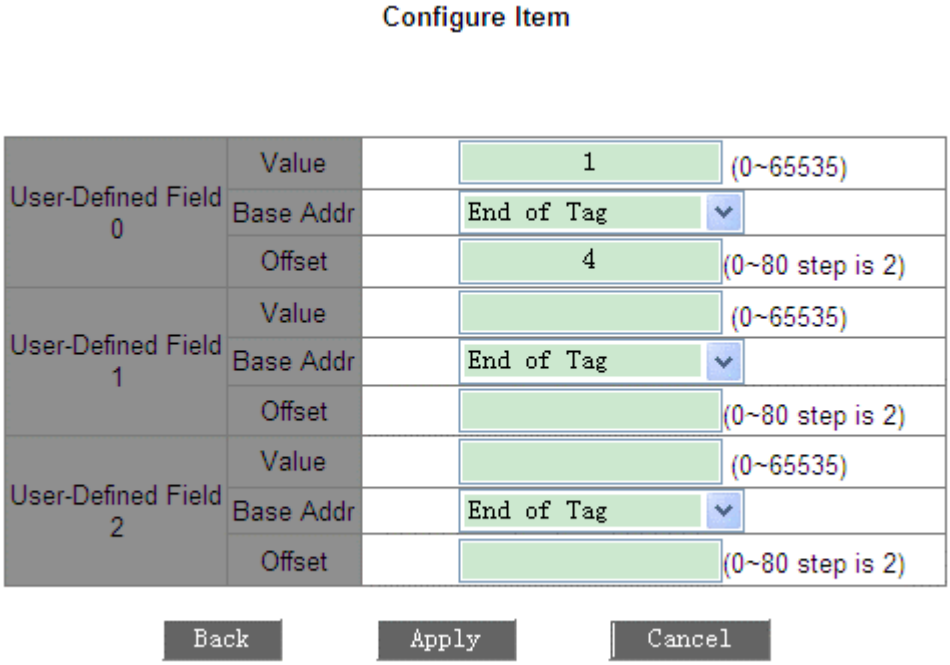

Рисунок 63 Задание параметров записи ACL 4

Group

Принудительная настройка: 1

Item

Диапазон: 1~1018

Функция: Задание ID записи ACL. Можно настроить не более 1023 записей ACL. Если настроено несколько записей ACL, они сравниваются с пакетами в порядке возрастания идентификаторов.

Action

Варианты: Deny/Redir Port/Mirror Port/Forward

По умолчанию: Deny

Функция: Настройка действия по отношению к пакету, который соответствует какой-либо записи ACL.

Deny: Пакеты, соответствующие какой-либо записи, будут отклонены.

Redir Port: Пакеты, соответствующие записи, будут перенаправлены на указанный порт. Необходимо указать порт в выпадающем списке.

Mirror Port: Пакеты, соответствующие записи, будут перенаправлены на порт назначения и на указанный в выпадающем списке порт.

Forward: Пакеты, соответствующие записи, будут перенаправлены на порт назначения.

Control Port

Варианты: all/один или несколько портов

Функция: Выбор порта, на котором действует ACL.

Source MAC

Состав: {MAC, MASK}

Формат: {HHHHHHHHHHHH, HHHHHHHHHHHH} (H – шестнадцатеричное число.)

Функция: Настройка MAC-адреса источника и маски подсети. Если MAC-адрес источника и маска подсети пакета совпадают со значением этого параметра, то условие выполнено.

Destination MAC

Состав: {MAC, MASK}

Формат: {HHHHHHHHHHHH, HHHHHHHHHHHH} (H – шестнадцатеричное число.)

Функция: Настройка MAC-адреса назначения и маски подсети. Если MAC-адрес назначения и маска подсети пакета совпадают со значением этого параметра, то условие выполнено.

Source IP

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

Destination IP

Состав: {IP, MASK}
Формат: {A.B.C.D, A.B.C.D}
Функция: Настройка IP-адреса назначения и маски подсети. Если IP-адрес назначения 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 совпадают 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 IP-протокола. Если соответствующее поле пакета совпадает со значением этого параметра, то условие выполнено.

IP TTL

Диапазон: 0~3
Функция: Настройка поля TTL. Если значение установлено равным 0, TTL соответствующего пакета должен быть равен 0; если значение установлено равным 1, TTL соответствующего пакета должен быть равен 1; если значение установлено равным 2, TTL сопоставленного пакета находится в диапазоне от 2 до 254; если установлено значение 3, TTL соответствующего пакета должен быть равен 255. Если соответствующее поле пакета отвечает этим правилам, то условие выполнено.

Max ICMP

Диапазон: 0~1023
Функция: Настройка значения Max 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 VLAN ID. Если соответствующее поле пакета совпадает со значением этого параметра, то условие выполнено.

Vlan ID Range (0~3)

Состав: {X~Y} (X и Y (X<Y) диапазон от 1 до 4093. X и Y указывают верхнюю и нижнюю границы Vlan ID соответственно.)
Функция: Настройка диапазона VLAN ID пакетов. Условие выполнено, если VLAN
ID пакета находится в указанном диапазоне.

Source L4 Port

Диапазон: 1~65535
Функция: Настройка номера исходного порта для пакетов протокола Layer-4. Если соответствующее поле пакета совпадает со значением этого параметра, то условие выполнено.

Src Port Range (0~3)

Состав: {X~Y} (X и Y (X<Y) диапазон от 1 до 65535. X и Y указывают верхнюю и нижнюю границы номеров портов Layer-4 соответственно.)
Функция: Настройка диапазона номеров исходного порта для пакетов протокола Layer-4. Если соответствующее поле пакета совпадает со значением этого параметра, то условие выполнено.

Destination L4 Port

Диапазон: 1~65535
Функция: Настройка номера порта назначения для пакетов протокола Layer-4. Если соответствующее поле пакета совпадает со значением этого параметра, то условие выполнено.

Dst Port Range (0~3)

Состав: {X~Y} (X и Y (X<Y) диапазон от 1 до 65535. X и Y указывают верхнюю и нижнюю границы номеров портов назначения Layer-4 соответственно.)
Функция: Настройка диапазона номеров порта назначения для пакетов протокола Layer-4. Если соответствующее поле пакета совпадает со значением этого параметра, то условие выполнено.

L2 Format

Варианты: None/L2_Others/Ethernet_II/IEEE_802_2_SNAP
По умолчанию: None
Функция: Настройка формата кадра Ethernet Layer-2. None указывает, что это правило не используется; L2_Others указывает все остальные форматы кадра Ethernet, кроме Ethernet_II и IEEE_802_2_SNAP. Если формат кадра Ethernet совпадает со значением этого параметра, то условие выполнено.

L3 Format

Варианты: None/L3_Others/IPV4_without_frag/IPV6_without_exten
По умолчанию: None
Функция: Настройка протокола Layer-3. None указывает, что это правило не используется; L3_Others указывает все протоколы Layer-3, кроме IPV4_without_frag и IPV6_without_exten. Если протокол Layer-3 совпадает со значением этого параметра, то условие выполнено.

L4 Format

Варианты: None/L4_Others/TCP/UDP/ (ICMP/IGMP)
По умолчанию: None
Функция: Настройка типа протокола Layer-4. None указывает, что это правило не используется; L4_Others указывает все протоколы, кроме TCP, UDP, ICMP и IGMP. Если протокол Layer-4 пакета совпадает со значением этого параметра, то условие выполнено.

Same IP

Варианты: Disable/False/True
По умолчанию: Disable
Функция: Проверка совпадения IP-адреса источника пакета с IP-адресом назначения.
Disable указывает, что это правило не используется;
Значение False указывает на то, что условие выполняется, если IP-адрес источника пакета отличается от IP-адреса назначения.
True указывает на то, что условие выполняется, если IP-адрес источника пакета совпадает с IP-адресом назначения.

Same L4 Port

Варианты: Disable/False/True
По умолчанию: Disable
Функция: Проверка совпадения номера порта Layer-4 источника пакета с номером порта назначения Layer-4.
Disable указывает, что это правило не используется;
Значение False указывает на то, что условие выполняется, если номер порта Layer-4 источника пакета отличается от номера порта назначения Layer-4.
True указывает на то, что условие выполняется, если номер порта Layer-4 источника пакета совпадает с номером порта назначения Layer-4.

TCP Sequence Zero

Варианты: Disable/False/True
По умолчанию: Disable
Функция: Проверка равенства 0 значения поля TCP Sequence пакета.

Disable указывает, что это правило не используется;
Значение False указывает на то, что условие выполняется, если значение поля TCP Sequence не равно 0. True указывает на то, что условие выполняется, если значение поля TCP Sequence равно 0.

User-Defined Field (0~2)

Состав: {Value, Base Addr, Offset}
Диапазон или варианты:
Value: 1~65535
Base Addr: End of Tag (по умолчанию)/End of EthType/End of IP Header
Offset: 0~80, с шагом 2
Функция: Задание поля как условия ACL. Value указывает значение, которое необходимо сопоставить; Base Addr указывает опорную точку пакета; End of Tag указывает, что конец поля тега является опорной точкой; End of EthType указывает, что конец поля EthType является опорной точкой; End of IP Header указывает, что конец поля IP-заголовка является опорной точкой; Offset указывает смещение сопоставляемого значения по сравнению с опорной точкой. Если Offset пакета по сравнению cBase Addr равно Value, то условие выполнено.

NOTE	**Примечание:** Не обязательно задавать все эти параметры, но необходимо задать хотя бы один параметр. Если требуется только один параметр, все остальные параметры остаются пустыми.

3. Просмотр ACL.

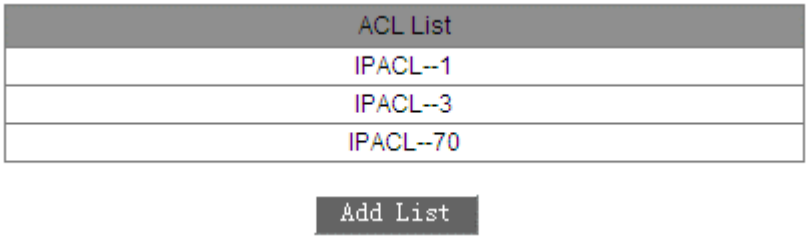

Рисунок 64 Записи ACL

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

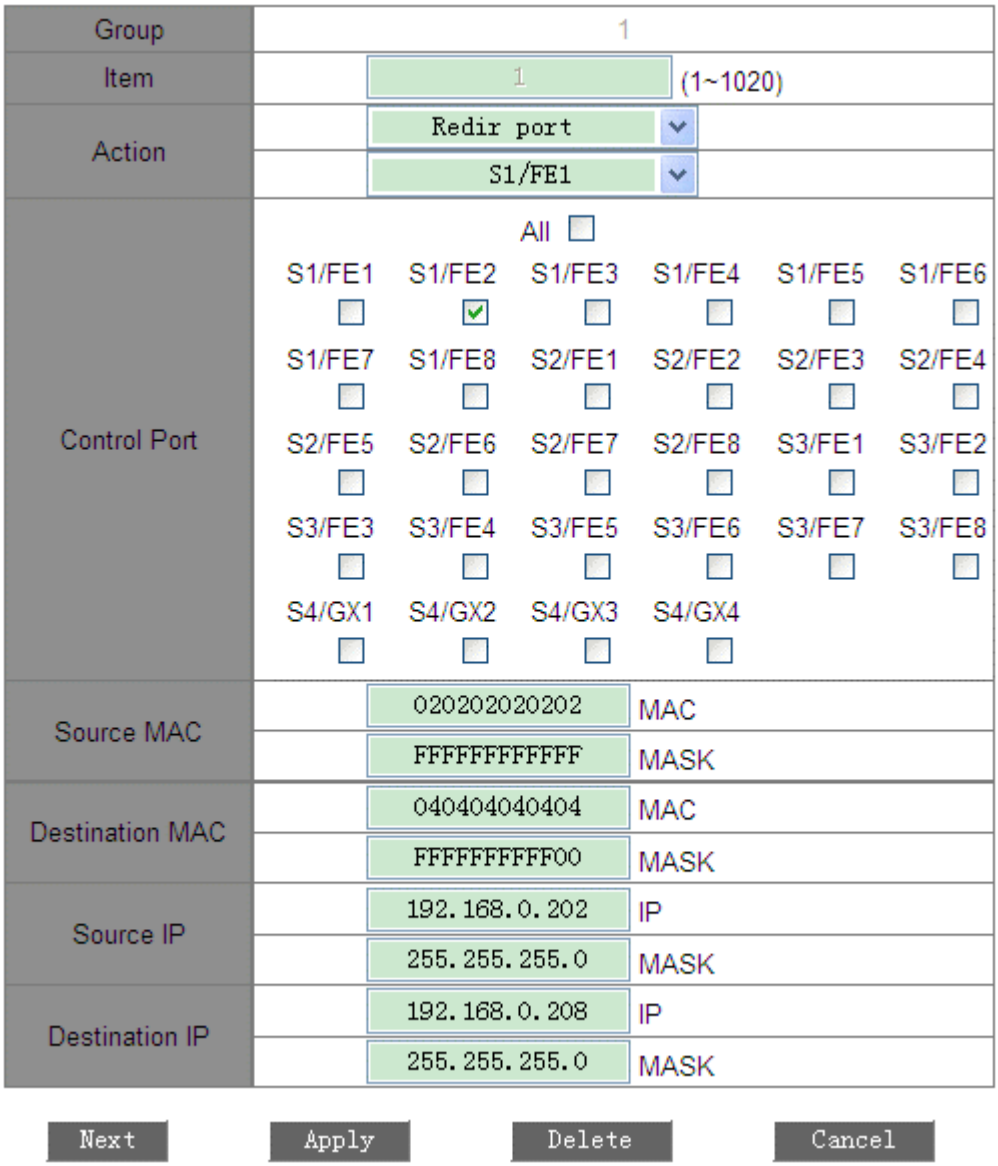

Рисунок 65 Изменение/удаление записи ACL

После внесения изменений щелкните <Apply>, чтобы внесенные изменения вступили в силу. Щелкните <Delete>, чтобы удалить запись ACL.

6.9.4 Настройка через веб-интерфейс (SICOM3048)

1. Добавьте запись ACL.

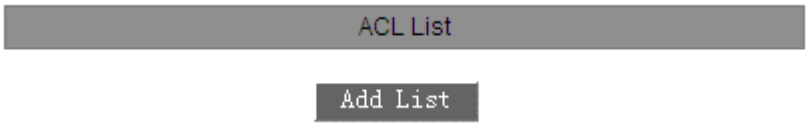

Рисунок 66 Добавление записи ACL

Щелкните <Add List> на предыдущем рисунке, чтобы добавить запись ACL. Разные идентификаторы групп соответствуют разным параметрам ACL, как показано на следующих рисунках.

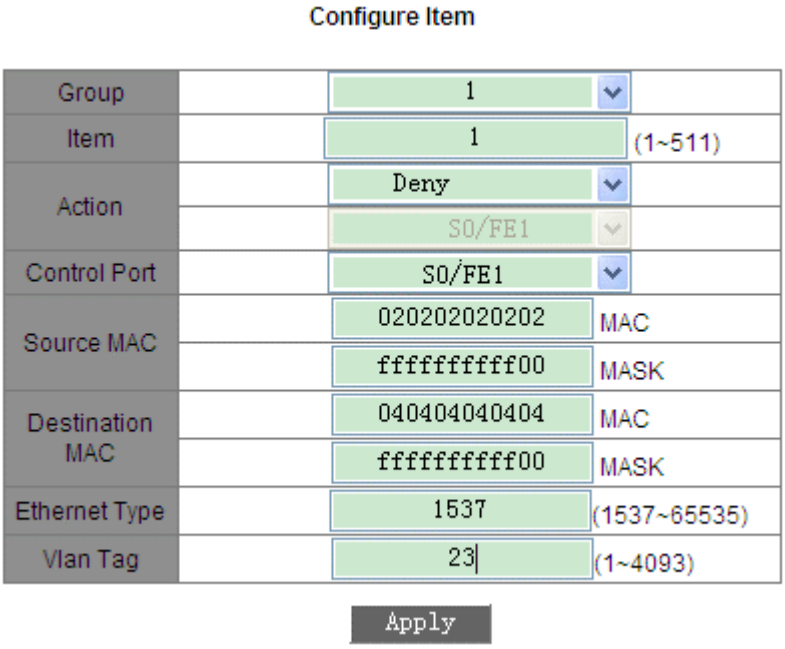

Рисунок 67 Задание параметров записи ACL – группа 1

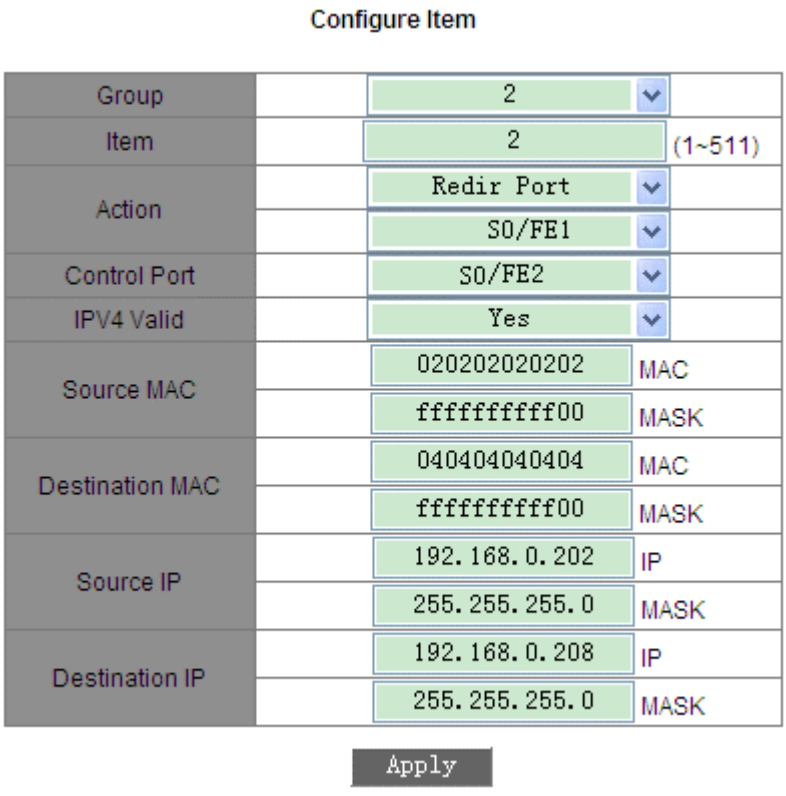

Рисунок 68 Задание параметров записи ACL – группа 2

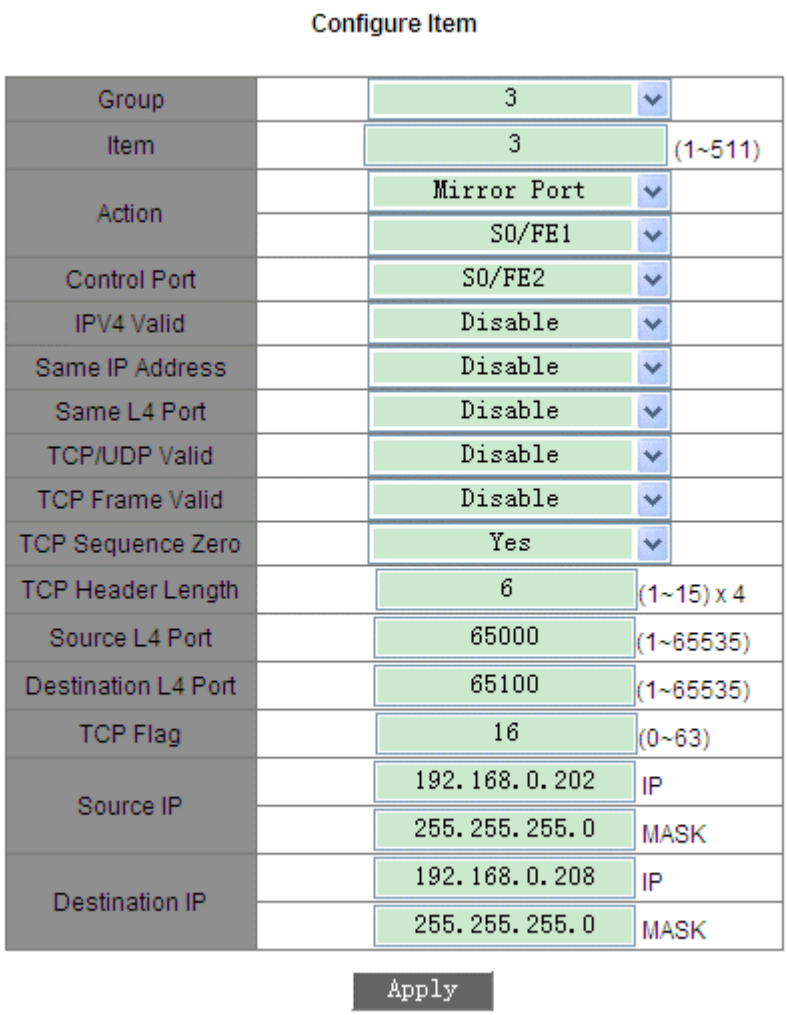

Рисунок 69 Задание параметров записи ACL – группа 3

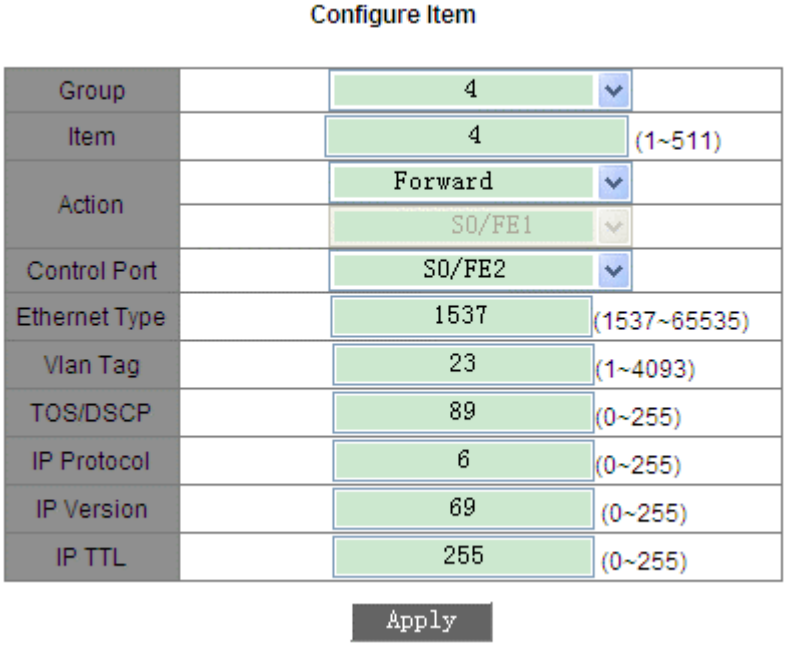

Рисунок 70 Задание параметров записи ACL – группа 4

Group
Варианты: 1~4
По умолчанию: 1

Функция: Настройка номера группы записи ACL.
Описание: Разные идентификаторы групп соответствуют разным параметрам ACL.

Item

Диапазон: 1~511
Функция: Задание ID записи ACL. Можно настроить не более 511 записей ACL. Если настроено несколько записей ACL, они сравниваются с пакетами в порядке возрастания идентификаторов.

Action

Варианты: Deny/Redir Port/Mirror Port/Forward
По умолчанию: Deny
Функция: Настройка действия по отношению к пакету, который соответствует какой-либо записи ACL.
Deny: Пакеты, соответствующие какой-либо записи, будут отклонены.
Redir Port: Пакеты, соответствующие записи, будут перенаправлены на указанный порт. Необходимо указать порт в выпадающем списке.
Mirror Port: Пакеты, соответствующие записи, будут перенаправлены на порт назначения и на указанный в выпадающем списке порт.

Control Port

Варианты: Все порты/любой указанный порт
Функция: Выбор порта, на котором действует ACL.

Source MAC

Состав: {MAC address, MAC subnet mask}
Формат: {HHHHHHHHHHHH, HHHHHHHHHHHH} (H – шестнадцатеричное число.)
Функция: Настройка MAC-адреса источника и маски подсети. Если MAC-адрес источника и маска подсети пакета совпадают со значением этого параметра, то условие выполнено.

Destination MAC

Состав: {MAC address, MAC subnet mask}
Формат: {HHHHHHHHHHHH, HHHHHHHHHHHH} (H – шестнадцатеричное число.)
Функция: Настройка MAC-адреса назначения и маски подсети. Если MAC-адрес назначения 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 совпадают со значением этого параметра, то условие выполнено.

Vlan Tag

Диапазон: 1~4093
Функция: Настройка VLAN ID. Если соответствующее поле пакета совпадает со значением этого параметра, то условие выполнено.

IPV4 Valid

Варианты: Disable/Yes/No
По умолчанию: Disable
Функция: Проверка, является ли полученный пакет действительным пакетом IPv4.
Disable указывает, что это правило не используется;
Yes указывает, что условие выполнено, если полученный пакет является действительным пакетом IPv4.
No указывает, что условие выполнено, если полученный пакет не является действительным пакетом IPv4.

Source IP

Состав: {IP address, IP subnet mask}
Формат: {A.B.C.D, A.B.C.D}
Функция: Настройка IP-адреса источника и маски подсети. Если IP-адрес источника и маска подсети пакета совпадают со значением этого параметра, то условие выполнено.

Destination IP

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

Same IP Address

Варианты: Disable/Yes/No
По умолчанию: Disable
Функция: Проверка совпадения IP-адреса источника пакета с IP-адресом назначения.
Disable указывает, что это правило не используется.
No указывает на то, что условие выполняется, если IP-адрес источника пакета отличается от IP-адреса назначения.
Yes указывает на то, что условие выполняется, если IP-адрес источника пакета совпадает с IP-адресом назначения.

Same L4 Port

Варианты: Disable/Yes/No
По умолчанию: Disable
Функция: Проверка совпадения номера порта Layer-4 источника пакета с номером порта назначения Layer-4.
Disable указывает, что это правило не используется.
No указывает на то, что условие выполняется, если номер порта Layer-4 источника пакета отличается от номера порта назначения Layer-4.
Yes указывает на то, что условие выполняется, если номер порта Layer-4 источника пакета совпадает с номером порта назначения Layer-4.

TCP/UDP Valid

Варианты: Disable/Yes/No
По умолчанию: Disable
Функция: Проверка, является ли полученный пакет пакетом TCP/UDP/
Disable указывает, что это правило не используется.
Yes указывает, что условие выполнено, если полученный пакет является действительным пакетом TCP/UDP.
No указывает, что условие выполнено, если полученный пакет не является действительным пакетом TCP/UDP.

TCP Frame Valid

Варианты: Disable/Yes/No По умолчанию: Disable
Функция: Проверка, является ли полученный пакет действительным кадром TCP.
Disable указывает, что это правило не используется.
Yes указывает, что условие выполнено, если полученный пакет является действительным кадром TCP.
No указывает, что условие выполнено, если полученный пакет не является действительным кадром TCP.

TCP Sequence Zero

Варианты: Disable/Yes/No
По умолчанию: Disable
Функция: Проверка равенства 0 значения поля TCP Sequence пакета.
Disable указывает, что это правило не используется.
No указывает на то, что условие выполняется, если значение поля TCP Sequence пакета не равно 0.
Yes указывает на то, что условие выполняется, если значение поля TCP Sequence пакета равно 0.

TCP Header Length

Диапазон: 1~15
Функция: Настройка длины заголовка TCP. Если соответствующее поле пакета меньше значения этого параметра, то условие выполнено.

Source L4 Port

Диапазон: 1~65535
Функция: Настройка номера исходного порта для пакетов протокола Layer-4. Если соответствующее поле пакета совпадает со значением этого параметра, то условие выполнено.

Destination L4 Port

Диапазон: 1~65535
Функция: Настройка номера порта назначения для пакетов протокола Layer-4. Если соответствующее поле пакета совпадает со значением этого параметра, то условие выполнено.

TCP Flag

Диапазон: 0~63

Функция: Настройка флага TCP. Если соответствующее поле 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 IP-протокола. Если соответствующее поле пакета совпадает со значением этого параметра, то условие выполнено.

IP Version

Диапазон: 0~255

Функция: Настройка значения версии протокола IP и длины заголовка. Если соответствующее поле пакета совпадает со значением этого параметра, то условие выполнено.

IP TTL

Диапазон: 0~255

Функция: Настройка поля TTL. Если соответствующее поле пакета совпадает со значением этого параметра, то условие выполнено.

NOTE	**Примечание:** Не обязательно задавать все эти параметры, но необходимо задать хотя бы один параметр. Если требуется только один параметр, все остальные параметры остаются пустыми.

2. Просмотр ACL.

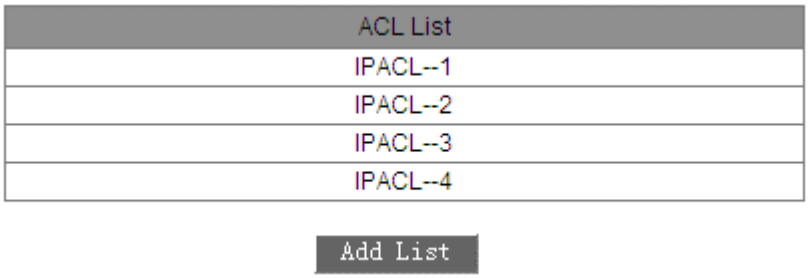

Рисунок 71 Записи ACL

Щелкните запись ACL на предыдущем рисунке. Можно изменить или удалить запись ACL, как показано на следующем рисунке.

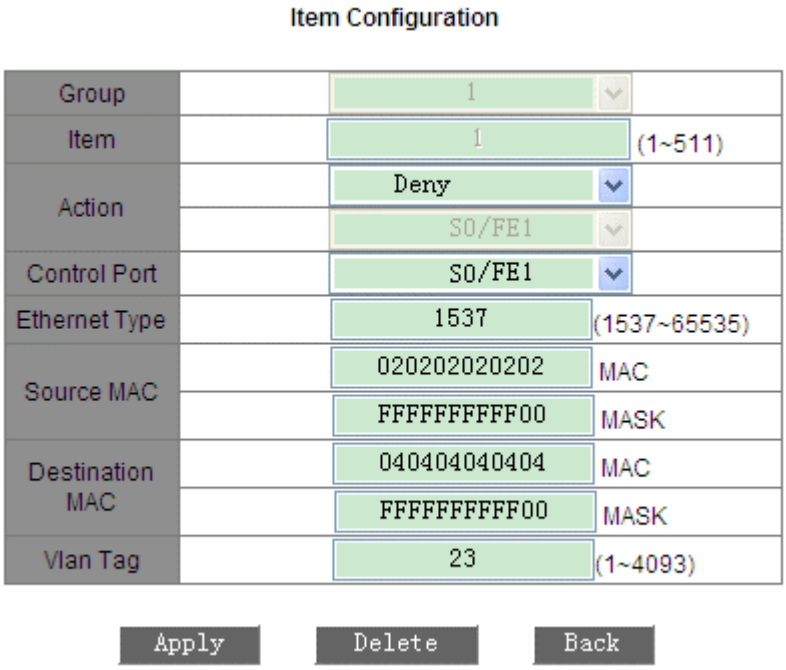

Рисунок 72 Изменение/удаление записи ACL

После внесения изменений щелкните <Apply>, чтобы внесенные изменения вступили в силу. Щелкните <Delete>, чтобы удалить запись ACL.

6.9.5 Пример типовой конфигурации

Далее используется SICOM3024P в качестве примера для описания настройки записи ACL.
Подключите порт 2 коммутатора. Настройте порт для получения пакетов только с исходного MAC-адреса 02-02-02-02-02-02 и пересылки пакетов через порт 1.
Этапы настройки:
1. Настройте действие для Redir Portи выберите порт 1 в выпадающем списке, как показано на рисунке 60.
2. Выберите FE2 в Control Port, как показано на рисунке 60.
3. Задайте MAC-адрес источника 020202020202 и маску подсети FFFFFFFFFFFF, как показано на рисунке 60.
4. Оставьте все остальные параметры пустыми.

6.10 ARP

6.10.1 Обзор

Протокол разрешения адресов (ARP) разрешает сопоставление между IP-адресами и MAC-адресами с помощью механизма запроса и ответа адреса. Коммутатор получает информацию о сопоставлении между IP-адресами и MAC-адресами других хостов в том же сегменте сети. Он также поддерживает статические записи ARP для определения соответствия между IP-адресами и MAC-адресами. Динамические записи ARP периодически устаревают, обеспечивая согласованность между записями ARP и реальными приложениями.
Коммутаторы этой серии обеспечивают не только функцию коммутации уровня Layer 2, но и функцию ARP для разрешения IP-адресов других хостов в том же сегменте сети, обеспечивая связь между NMS и управляемыми хостами.

6.10.2 Описание

Записи ARP делятся на динамические и статические.
Динамические записи генерируются и поддерживаются на основе обмена пакетами ARP. Динамические записи могут устаревать, обновляться новым пакетом ARP или перезаписываться статической записью ARP.
Статические записи настраиваются и поддерживаются вручную. Они никогда не устаревают и не перезаписываются динамическими записями ARP.
Коммутатор поддерживает до 512 записей ARP (максимум 256 статических). Когда количество записей ARP превышает 512, новые записи автоматически перезаписывают старые динамические записи.

6.10.3 Настройка через веб-интерфейс

1. Настройте время старения ARP, как показано на рисунке ниже.

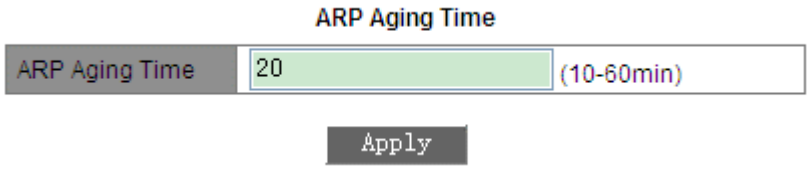

Рисунок 73 Настройка времени старения

ARP Aging Time
Диапазон: 10~60 минут
По умолчанию: 20 минут
Функция: Настройка времени устаревания ARP.
Описание: Время старения ARP — это промежуток с момента добавления динамической записи ARP в таблицу до момента удаления записи из таблицы.
2. Добавьте статическую запись ARP, как показано на рисунке ниже.

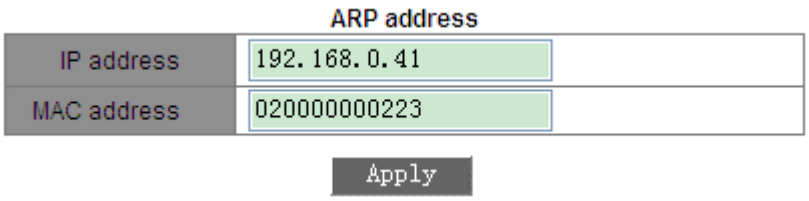

Рисунок 74 Добавление статической записи ARP

ARP address
Состав: {IP address, MAC address}
Формат: {A.B.C.D, HHHHHHHHHHHH} (H – шестнадцатеричное число.)
Функция: Настройка статической записи ARP.

CAUTION	**Предупреждение:** > 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. > Как правило, коммутатор автоматически запоминает записи ARP. Настройка вручную не требуется.

3. Просмотрите или удалите статическую запись ARP, как показано на рисунке ниже.

ARP address

Number	IP address	MAC address	Flags
○	192.168.0.23	90-FB-A6-3C-CA-7E	Dynamic
○	192.168.0.41	02-00-00-00-02-23	Static
○	192.168.0.94	00-00-AA-BB-CC-05	Dynamic
○	192.168.0.179	00-00-EE-EE-02-05	Dynamic

Add Delete

Рисунок 75 Таблица адресов ARP

ARP address
Состав: {IP address, MAC address, Flags}
Функция: Отображение записей ARP, включая статические и динамические записи.
Действие: Выберите статическую запись в столбце Number. Щелкните <Delete>, чтобы удалить запись.

CAUTION	**Предупреждение:** Нельзя удалить динамические записи ARP.

6.11 SNMP

6.11.1 Обзор

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

6.11.2 Реализация

SNMP использует режим станции управления/агента. Таким образом, SNMP включает в себя два типа сетевых элементов: NMS и агент.
Станция управления сетью (NMS) — это станция, на которой работает программный клиент управления сетью с поддержкой SNMP. Это ядро для управления сетью SNMP.
Агент — это процесс в управляемых сетевых устройствах. Он получает и обрабатывает пакеты запросов от NMS. Когда возникает сигнал тревоги, агент сообщает об этом в NMS.
NMS является средством управления сетью SNMP, а агент управляется сетью SNMP. NMS и агенты обмениваются пакетами управления через SNMP. SNMP включает в себя следующие основные операции:
> Get-Request
> Get-Response
> Get-Next-Request
> Set-Request
> Trap

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

6.11.3 Описание

Коммутаторы этой серии поддерживают SNMPv2. SNMPv2 совместим с SNMPv1.
SNMPv1 использует для аутентификации имя сообщества. Имя сообщества действует как пароль, ограничивая доступ NMS к агентам. Если имя сообщества, переносимое пакетом SNMP, не подтверждается коммутатором, пакет отбрасывается.
SNMPv2 также использует для аутентификации имя сообщества. Он совместим с SNMPv1 и расширяет функционал SNMPv1.
Чтобы обеспечить связь между NMS и агентом, их версии SNMP должны совпадать. Для агента можно настроить разные версии SNMP, чтобы он мог использовать разные версии для связи с разными NMS.

6.11.4 MIB

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

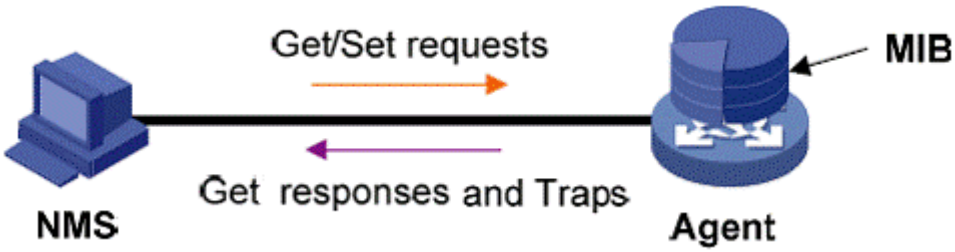

Рисунок 76 Взаимоотношения между NMS, агентом и MIB

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

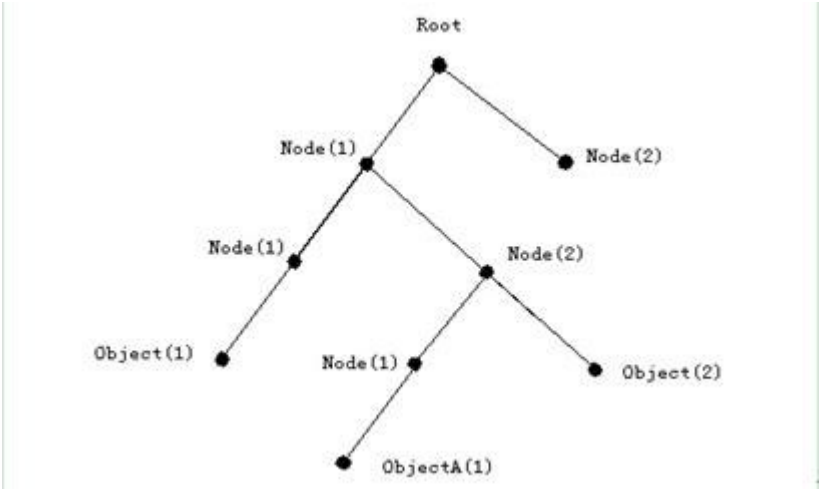

Рисунок 77 Структура дерева MIB

6.11.5 Настройка через веб-интерфейс

Включите SNMP, как показано на рисунке ниже.

Рисунок 78 Включение SNMP

SNMP status
Варианты: Enable/Disable
По умолчанию: Enable
Функция: Включение или выключение SNMP.
Настройте права доступа, как показано на рисунке ниже.

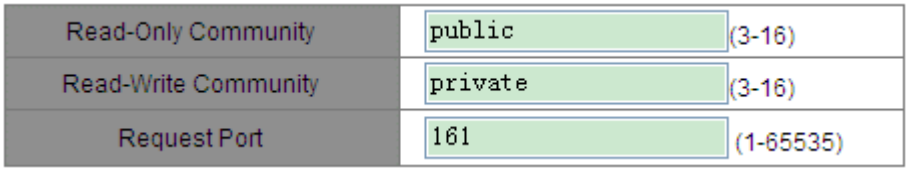

Рисунок 79 Настройка прав доступа

Read-Only Community
Диапазон: 3~16 символов
По умолчанию: public
Функция: Задание имени сообщества «Только чтение».
Описание: Информация MIB коммутатора может быть прочитана только в том случае, если имя сообщества, передаваемое пакетом SNMP, совпадает с именем, настроенным на коммутаторе.
Read-Write Community
Диапазон: 3~16 символов
По умолчанию: private
Функция: Задание имени сообщества «Чтение-запись».
Описание: Информация MIB коммутатора может быть прочитана и записана только в том случае, если имя сообщества, передаваемое пакетом SNMP, совпадает с именем, настроенным на коммутаторе.
Request Port
Диапазон: 1~65535
По умолчанию: 161
Функция: Настройка номера порта для получения запросов SNMP.
Задайте параметры Trap, как показано на рисунке ниже.

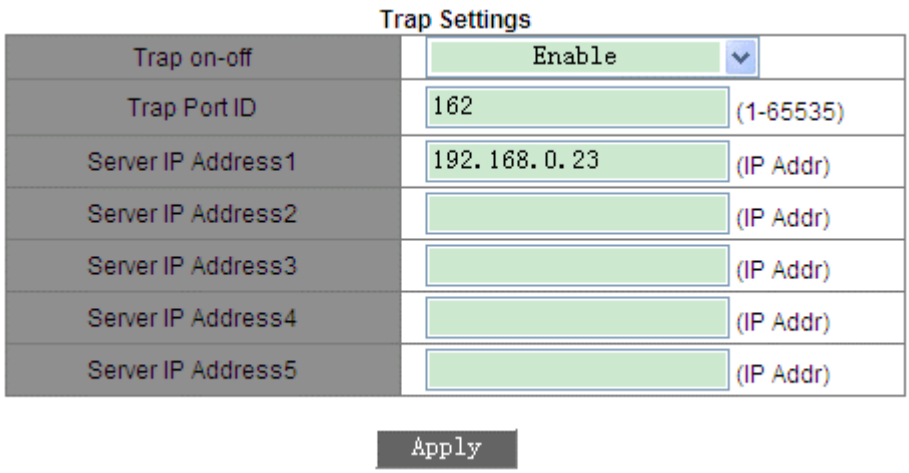

Рисунок 80 Настройка Trap

Trap on-off
Варианты: Enable/Disable
По умолчанию: Enable
Функция: Включение или выключение отправки Trap.
Trap Port ID
Варианты: 1~65535
По умолчанию: 162
Функция: Настройка номера порта для отправки сообщений Trap.
Server IP address
Формат: A.B.C.D
Функция: Настройка адреса сервера для приема сообщений Trap. Можно настроить не более пяти серверов.
4. Просмотрите IP-адрес управляющего сервера, как показано на следующем рисунке.

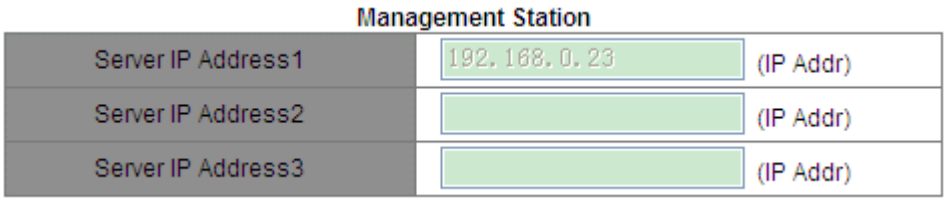

Рисунок 81 IP-адрес управляющего сервера

IP-адрес управляющего сервера не нужно настраивать вручную. Коммутатор автоматически отображает его только в том случае, если NMS работает на сервере и считывает и записывает информацию узла MIB устройства.

6.11.6 Пример типовой конфигурации

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

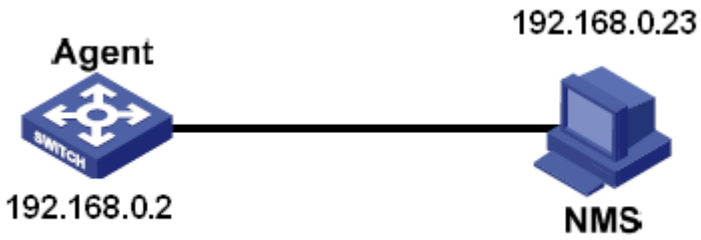

Рисунок 82 Пример настройки SNMP

Настройка агента:
1. Включите SNMP, как показано на рисунке 78.
2. Настройте права доступа. Установите имя сообщества «только чтение» public, имя сообщества «чтение и запись» private, а порт запроса — 161, как показано на рисунке 79.
3. Включите отправку trap, установите номер порта trap 162 и IP-адрес сервера 192.168.0.23, как показано на рисунке 80.
Для мониторинга и управления состоянием агента запустите на NMS программное обеспечение управления, например Kyvision.

Сведения о работе Kyvision приведены в Руководстве пользователя Kyvision.

6.12 DT-Ring

6.12.1 Обзор

DT-Ring и DT-Ring+ — это собственные протоколы резервирования компании Kyland. Они позволяют сети восстанавливаться в течение 50 мс при сбое канала, обеспечивая стабильную и надежную связь.
Кольца DT делятся на два типа: на основе портов (DT-Ring-Port) и на основе VLAN (DT-Ring-VLAN).
DT-Ring-Port: указывает порт для пересылки или блокировки пакетов.
DT-Ring-VLAN: указывает порт для пересылки или блокировки пакетов определенной VLAN. Это позволяет использовать несколько VLAN на общем порту, то есть один порт является частью разных резервных колец, основанных на разных VLAN.
DT-Ring-Port и DT-Ring-VLAN нельзя использовать вместе.

6.12.2 Основные понятия

Master: Одно кольцо может иметь только один узел в статусе Master. Узел в статусе Master отправляет пакеты протокола DT-Ring и определяет состояние кольца. Когда кольцо замкнуто, из двух портов, которые включены в кольцо, один находится в состоянии пересылки, а другой в состоянии блокировки, соответственно.
Основной порт: указывает кольцевой порт (для коммутатора Master), состояние которого настроено как принудительная переадресация пользователем, когда кольцо замкнуто.

Примечание:
Если для коммутатора Master не настроен основной порт, им будет первый порт, состояние связи которого изменилось на «работает» (когда кольцо замкнуто), и он будет в состоянии пересылки. Остальные кольцевые порты находятся в состоянии блокировки.

Slave: Кольцо может включать в себя несколько устройств Slave. Устройства Slave прослушивают и пересылают пакеты протокола DT-Ring и сообщают информацию об ошибках устройству Master.
Резервный порт: Порт для связи между кольцами DT называется резервным портом.
Резервный порт Master: Когда кольцо имеет несколько резервных портов, резервный порт с большим MAC-адресом является резервным портом Master. Он находится в состоянии пересылки.
Резервный порт Slave: Когда кольцо имеет несколько резервных портов, все резервные порты, кроме резервного порта Master, являются резервными портами Slave. Они находятся в состоянии блокировки.
Состояние пересылки: Если порт находится в состоянии пересылки, порт может и принимать, и отправлять данные.
Состояние блокировки: Если порт находится в состоянии блокировки, он может принимать и пересылать только пакеты протокола DT-Ring.

6.12.3 Реализация

Реализация DT-Ring-Port
Порт пересылки на устройстве Master периодически отправляет пакеты протокола DT-Ring для определения состояния кольца. Если блокирующий порт устройства Master получает пакеты, кольцо замкнуто; в противном случае кольцо разомкнуто.
Рабочий процесс коммутатора A, коммутатора B, коммутатора C и коммутатора D:
1. Настройте коммутатор A как Master, а остальные коммутаторы — как Slave.

2. Кольцевой порт 1 на Master находится в состоянии пересылки, а кольцевой порт 2 находится в состоянии блокировки. Оба порта на Slave находятся в состоянии пересылки.
3. Если линия связи CD неисправна, как показано на рисунке ниже.
a) когда линия связи CD неисправна, порт 6 и порт 7 на устройстве Slave находятся в состоянии блокировки. Порт 2 устройства Master переходит в состояние пересылки, обеспечивая работающую линию связи.
b) когда неисправность устранена, порт 6 и порт 7 устройства Slave находятся в состоянии пересылки. Порт 2 устройства Master переходит в состояние блокировки. Происходит переключение каналов, и каналы восстанавливаются до состояния, предшествующего отказу линии CD.

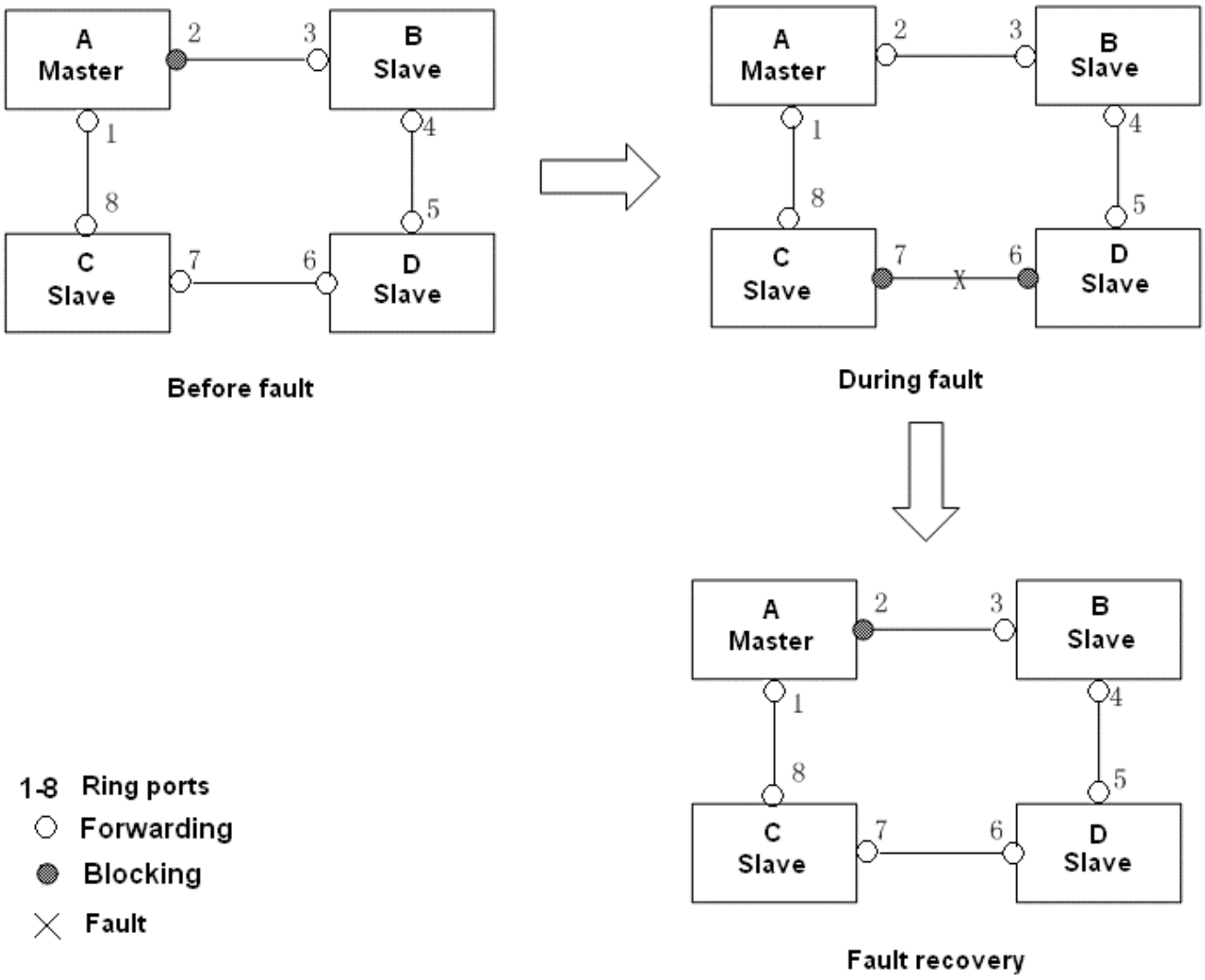

Рисунок 83 Отказ линии CD

NOTE	**Примечание:** Если порт 1 на устройстве Master A настроен как основной порт, процессы сбоя и восстановления после сбоя идентичны описанным выше.

4. Если линия связи AC неисправна, как показано на рисунке ниже:
a) Если линия связи AC неисправна, порт 1 находится в состоянии блокировки, а порт 2 переходит в состояние пересылки, обеспечивая работающую линию связи.

b) После устранения неисправности:
Если на устройстве Master A не настроен основной порт, порт 1 по-прежнему находится в состоянии блокировки, а порт 8 — в состоянии пересылки. Переключение не происходит.
Если порт 1 на устройстве Master A настроен как основной порт. Когда кольцо замкнуто, основной порт находится в состоянии пересылки. Порт 1 переходит в состояние пересылки. Порт 8 находится в состоянии пересылки, а порт 2 находится в состоянии блокировки. Переключение происходит.

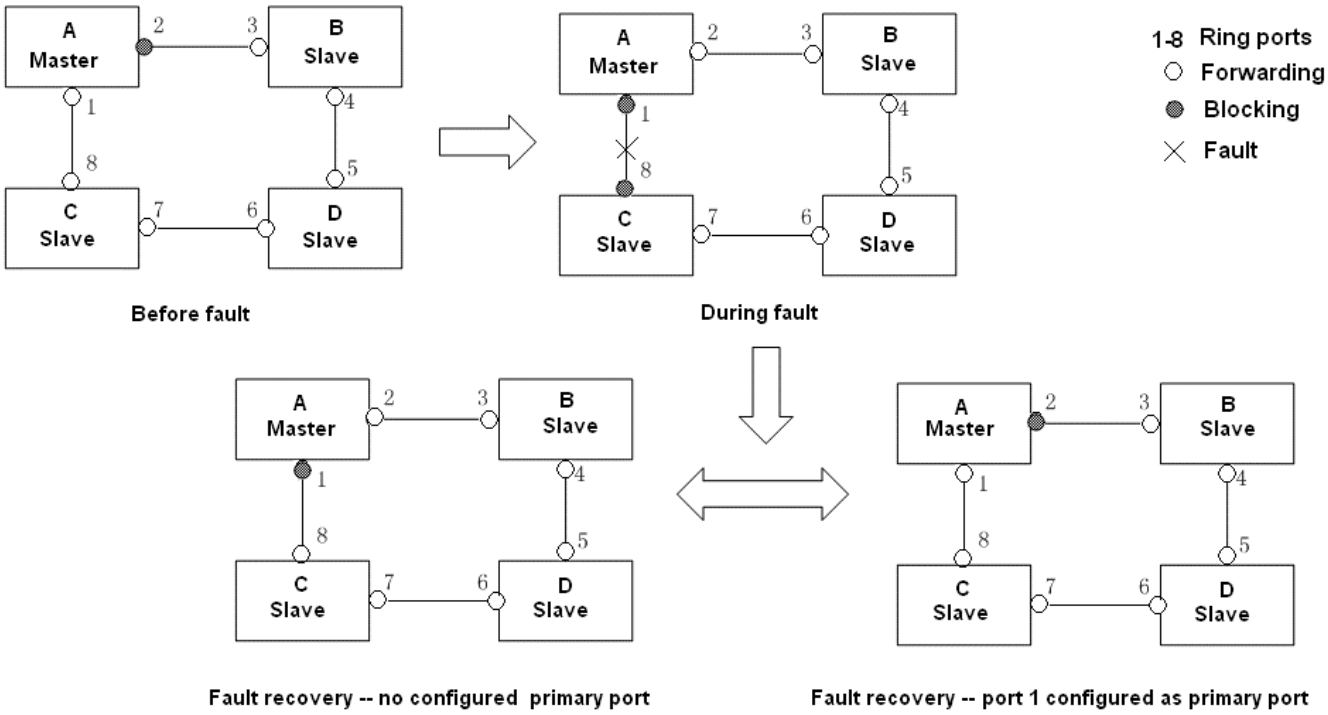

Рисунок 84 Отказ линии DT-Ring

CAUTION	**Предупреждение:** Изменение статуса соединения влияет на статус кольцевых портов.

Реализация DT-Ring-VLAN
DT-Ring-VLAN позволяет пересылать пакеты из разных VLAN по разным путям. Каждый путь пересылки для VLAN образует DT-Ring-VLAN. Различные DT-VLAN-Rings могут иметь разные устройства Master. Как показано на следующем рисунке, сконфигурированы две DT-Ring-VLAN. Линии связи DT-Ring-VLAN 10: AB-BC-CD-DE-EA.
Линии связи DT-Ring-VLAN 20: FB-BC-CD-DE-EF.
Два кольца соприкасаются линиями связи BC, CD и DE. Коммутатор C и коммутатор D используют одни и те же порты в двух кольцах, но используют разные логические каналы на основе VLAN.

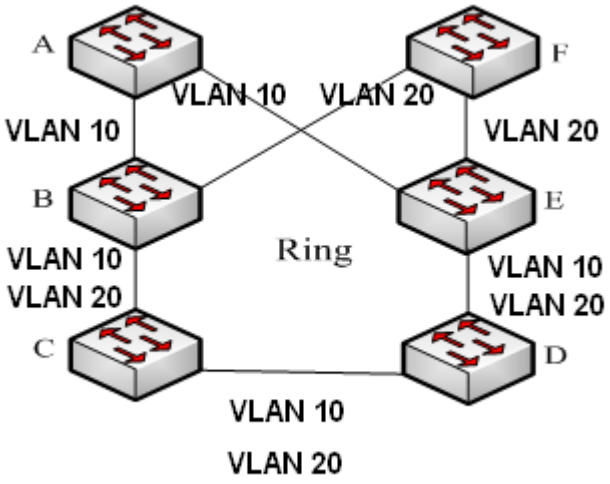

Рисунок 85 DT-Ring-VLAN

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

Реализация DT-Ring+

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

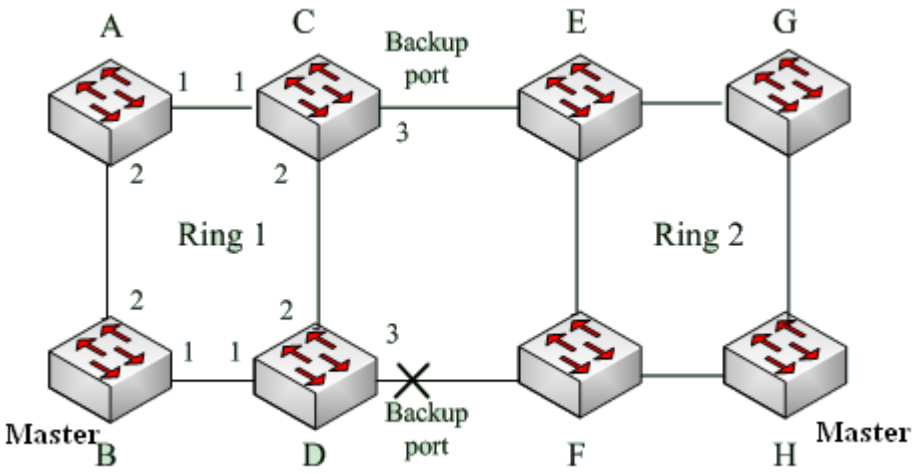

Рисунок 86 Топология DT-Ring+

CAUTION	**Предупреждение:** Изменение статуса соединения влияет на статус резервных портов.

6.12.4 Пояснения

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

6.12.5 Настройка через веб-интерфейс

1. Настройте режим резервирования, как показано на рисунке ниже.

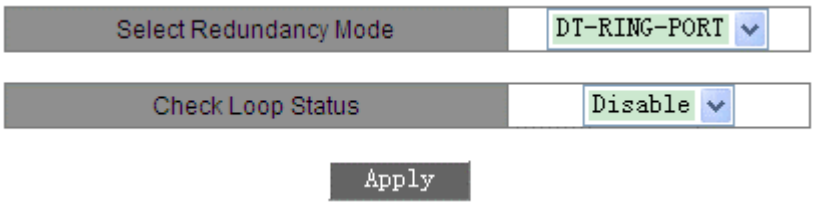

Рисунок 87 Настройка режима резервного кольца

Select Redundancy Mode
Варианты: DT-RING-PORT/DT-RING-VLAN
По умолчанию: DT-RING-PORT
Функция: Выбор режима резервирования.

CAUTION	**Предупреждение:** > К кольцевым протоколам на основе портов относятся RSTP, DT-Ring-Port и DRP-Port, а к протоколам на основе VLAN – DT-Ring-VLAN и DRP-VLAN. > Кольцевые протоколы на основе VLAN являются взаимоисключающими, и для одного устройства можно настроить только тип кольцевого протокола на основе VLAN. > Кольцевой протокол на основе порта и кольцевой протокол на основе VLAN являются взаимоисключающими, и для одного устройства можно выбрать только один режим кольцевого протокола.

Check Loop Status
Варианты: Disable/Enable
По умолчанию: Disable
Функция: Включение или выключение обнаружения состояния кольца.
Описание: После включения определения состояния кольца коммутатор автоматически определяет состояние кольца. При получении некольцевым портом пакетов DT-Ring, порт будет заблокирован. Используйте эту функцию с осторожностью.
2. Создайте DT Ring, как показано на рисунке ниже.

Рисунок 88 Создание DT Ring

Щелкните <Add> и настройте DT Ring.
3. Настройте DT-Ring и DT-VLAN-Ring, как показано на рисунке ниже.

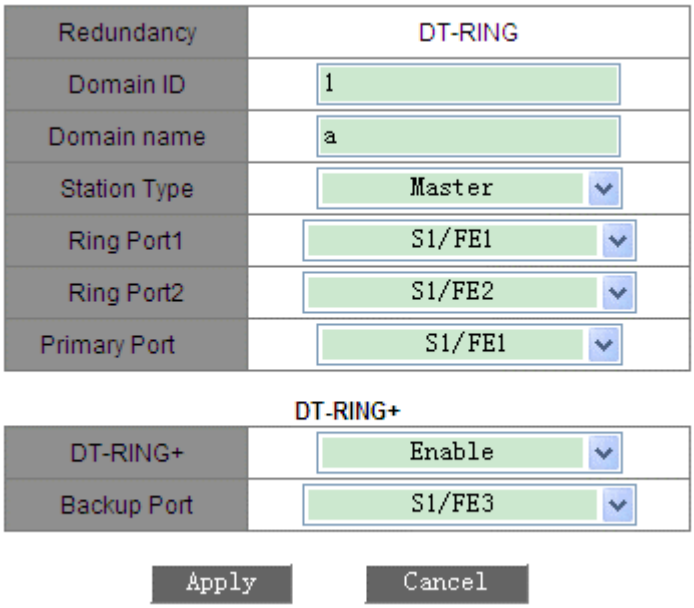

Рисунок 89 Конфигурация DT-Ring

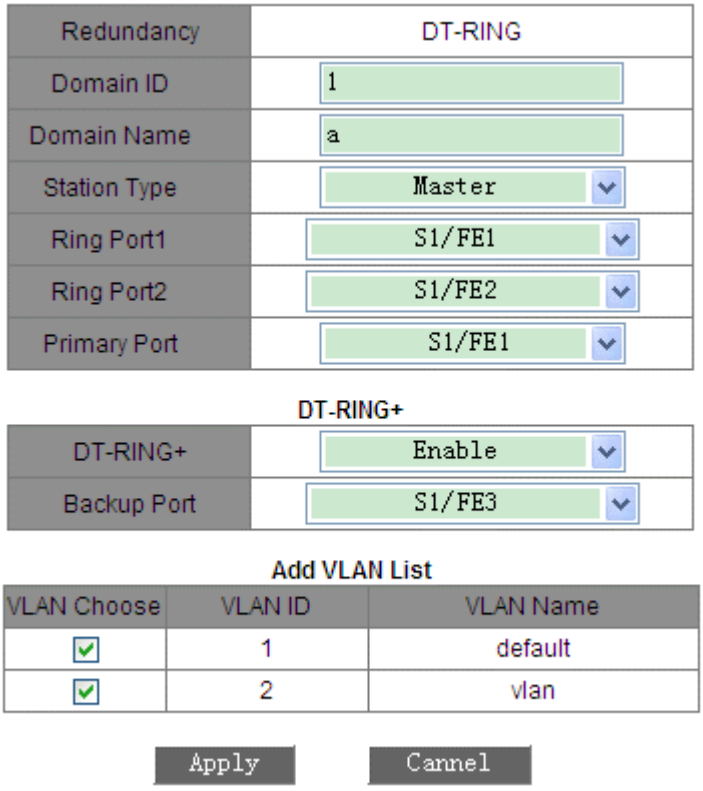

Рисунок 90 Конфигурация DT-VLAN-Ring

Redundancy
Принудительная конфигурация: DT-RING
Domain ID
Диапазон настройки: 1~32
Функция: Дифференцировать кольца. Один коммутатор поддерживает максимум 16 колец на основе портов или 8 колец на основе VLAN.
Domain Name
Диапазон: 1~31 символ
Функция: Задание доменного имени.
Station Type
Варианты: Master/Slave
По умолчанию: Master
Функция: Выбор роли коммутатора в текущем кольце.
Ring Port1/Ring Port2
Варианты: все порты коммутатора.
Функция: Выбор двух кольцевых портов.

CAUTION	**Предупреждение:** > Кольцевой порт DT-Ring или резервный порт не могут быть добавлены к группе агрегации. Порт, добавленный к группе агрегации, нельзя настроить как кольцевой порт DT-Ring или резервный порт. > Кольцевой порт DT-Ring или резервный порт нельзя настроить как исходный порт или порт назначения зеркалирования. Исходный порт или порт назначения зеркалирования нельзя настроить как кольцевой порт DT-Ring или резервный порт. > Кольцевые порты между кольцевыми протоколами на основе портов RSTP, DT-Ring-Port и DRP-Port являются взаимоисключающими, то есть кольцевой порт и резервный порт

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

Primary Port
Варианты: Disable/все порты коммутатора
По умолчанию: Disable
Функция: Настройка основного порта.
Описание: Когда кольцо замкнуто, основной порт коммутатора находится в состоянии пересылки.

CAUTION	**Предупреждение:** > Основной порт вступает в силу только тогда, когда кольцо замкнуто. > Основной порт должен быть одним из двух кольцевых портов устройства Master.

DT-RING+
Варианты: Enable/Disable
По умолчанию: Disable
Функция: Включение или выключение функции DT-Ring+.
Backup Port
Варианты: Все порты коммутатора
Функция: Выбор одного порта в качестве резервного порта.
Пояснение: Резервный порт можно настроить только после включения функции DT-Ring+.
Add VLAN List
Варианты: Все созданные VLAN
Функция: Выбор VLAN, управляемой данным кольцом DT-Ring-VLAN.

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

DT-RING List

Domain ID	Station Type	Ring Port(1,2)	Primary Port	DT-RING+ Status	Backup Port	Change times
a-1	Master	S1/FE1,S1/FE2	S1/FE1	Enable	S1/FE3	0
b-2	Slave	S1/FE4,S1/FE5	Disable	Enable	S1/FE6	0

Add

Рисунок 91 Список DT-Ring List

4. Просмотр и изменение конфигурации DT-Ring.
Щелкните опции DT-Ring на предыдущем рисунке. Можно просматривать и изменять настройки кольца, как показано на следующем рисунке.

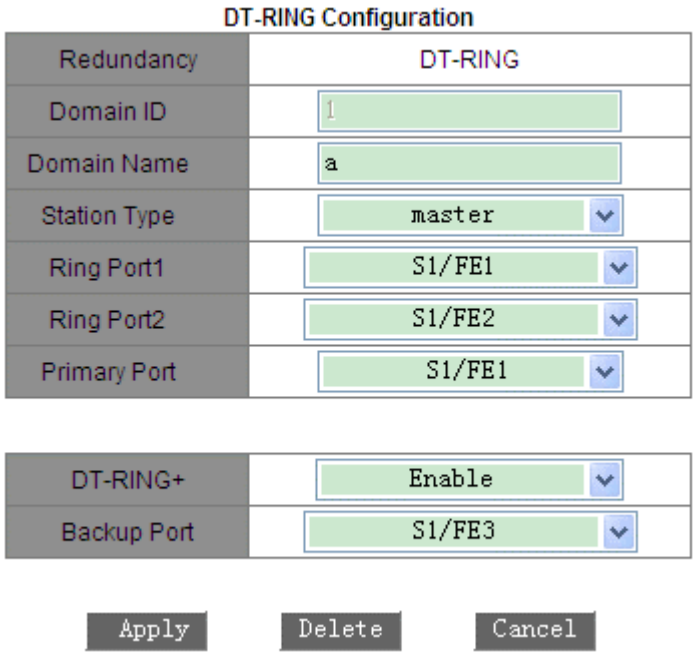

Рисунок 92 Конфигурация DT-Ring

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

5. Просмотрите состояние DT-Ring и порта, как показано на рисунке ниже.

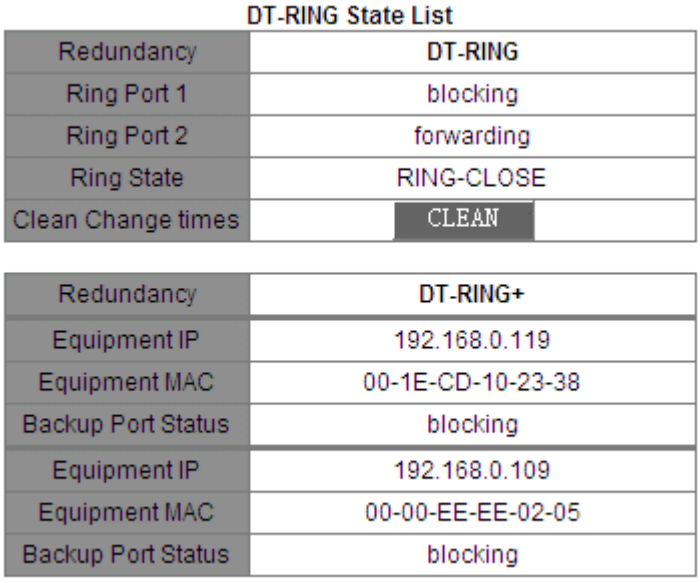

Рисунок 93 Состояние DT-Ring

6.12.6 Пример типовой конфигурации

Как показано на рисунке 86, коммутаторы A, B, C и D образуют кольцо 1; коммутаторы E, F, G и H образуют кольцо 2.

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

Конфигурация коммутатора A:

1. Domain ID: 1; Domain name: Ring; Ring port: port 1 и port 2; Station type: Slave; DT-Ring+: Disable; резервные порты не назначены, как показано на рисунке 89.

Конфигурация коммутатора B:
2. Domain ID: 1; Domain name: Ring; Ring port: port 1 и port 2, основного порта нет; Station type: Master; DT-Ring+: Disable; резервные порты не назначены, как показано на рисунке 89.
Конфигурация коммутатора C и коммутатора D:
3. Domain ID: 1; Domain name: Ring; Ring port: port 1 и port 2; Station type: Slave; DT-Ring+: Enable; Backup port: port 3, как показано на рисунке 89.
Конфигурация коммутатора E, коммутатора F и коммутатора G:
4. Domain ID: 2; Domain name: Ring; Ring port: port 1 и port 2; Station type: Slave; DT-Ring+: Disable; резервные порты не назначены, как показано на рисунке 89.
Конфигурация коммутатора H:
5. Domain ID: 2; Domain name: Ring; Ring port: port 1 и port 2, основного порта нет; Station type: Master; DT-Ring+: Disable; резервные порты не назначены, как показано на рисунке 89.

6.13 RSTP/STP

6.13.1 Обзор

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

6.13.2 Основные понятия

Корневой мост: служит корнем дерева. Сеть имеет только один корневой мост. Корневой мост меняется в зависимости от топологии сети. Корневой мост периодически отправляет BPDU другим устройствам, которые пересылают BPDU для обеспечения стабильности топологии.
Корневой порт: указывает наилучший порт для передачи от некорневых мостов к корневому мосту. Лучший порт — это порт с наименьшей стоимостью пути до корневого моста. Некорневой мост взаимодействует с корневым мостом через корневой порт. Некорневой мост имеет только один корневой порт. Корневой мост не имеет корневого порта.
Назначенный порт: указывает порт для пересылки BPDU на другие устройства или локальные сети. Все порты корневого моста являются назначенными портами.
Альтернативный порт: указывает резервный порт корневого порта. Если корневой порт выходит из строя, альтернативный порт становится новым корневым портом.
Резервный порт: указывает резервный порт назначенного порта. Когда назначенный порт выходит из строя, резервный порт становится новым назначенным портом и пересылает данные.

6.13.3 BPDU

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

Таблица 6 BPDU

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

ID корневого моста: приоритет корневого моста (2 байта) +MAC-адрес корневого моста (6 байт).
Стоимость корневого пути: стоимость пути к корневому мосту.
ID назначенного моста: приоритет назначенного моста (2 байта) +MAC-адрес назначенного моста (6 байт).
ID назначенного порта: приоритет порта+номер порта.
Возраст сообщения: продолжительность распространения BPDU по сети.
Макс. возраст: максимальная продолжительность хранения BPDU на устройстве. Когда возраст сообщения больше чем макс. возраст, BPDU отбрасывается.
Интервал Hello: интервал времени для отправки BPDU.
Задержка отправки: задержка изменения статуса (отбрасывание--обнаружение--пересылка).

6.13.4 Реализация

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 полученным.
Устройства сравнивают BPDU всех портов и определяют лучший BPDU. Принципы сравнения BPDU следующие:
BPDU с меньшим идентификатором корневого моста имеет более высокий приоритет.
Если идентификаторы корневого моста двух BPDU совпадают, сравнивается их стоимость корневого пути.
Если стоимость корневого пути в BPDU плюс стоимость пути локального порта меньше, приоритет BPDU выше.
Если стоимость корневого пути двух BPDU также одинакова, идентификаторы назначенного моста, идентификаторы назначенного порта и идентификаторы порта, получающего BPDU, дополнительно сравниваются по порядку. BPDU с меньшим идентификатором имеет более высокий приоритет. BPDU с меньшим идентификатором корневого моста имеет более высокий приоритет.
3. Выбор корневого моста Корневой мост связующего дерева — это мост с наименьшим идентификатором моста.
4. Выбор корневого порта Устройство без корневого моста выбирает порт, получающий лучший BPDU, в качестве корневого порта.
5. Расчет BPDU назначенного порта: На основе BPDU корневого порта и стоимости пути корневого порта устройство вычисляет BPDU назначенного порта для каждого порта следующим образом:
Идентификатор корневого моста заменяется идентификатором корневого моста BPDU корневого порта.
Стоимость корневого пути заменяется на стоимость корневого пути BPDU корневого порта плюс стоимость пути корневого порта.
Идентификатор назначенного моста заменяется идентификатором локального устройства.
Идентификатор назначенного порта заменяется идентификатором локального порта.
6. Выбор назначенного порта. Если рассчитанный BPDU лучше, то устройство выбирает порт в качестве назначенного порта, заменяет BPDU порта рассчитанным BPDU и отправляет рассчитанный BPDU. Если BPDU порта лучше, то устройство не обновляет BPDU порта и блокирует порт. Заблокированные порты

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

6.13.5 Настройка через веб-интерфейс

Включите STP/RSTP, как показано на рисунке ниже.

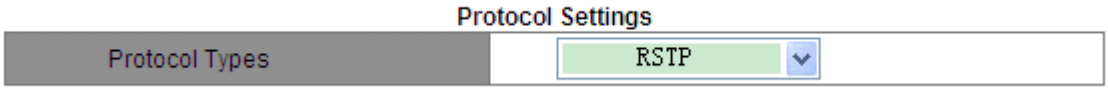

Рисунок 94 Включение RSTP/STP

Protocol Type
Варианты: Disable/RSTP/STP
По умолчанию: Disable
Функция: Включение или выключение RSTP или STP.

CAUTION	**Предупреждение:** > К кольцевым протоколам на основе портов относятся RSTP, DT-Ring-Port и DRP-Port, а к протоколам на основе VLAN – DT-Ring-VLAN и DRP-VLAN. > Кольцевой протокол на основе порта и кольцевой протокол на основе VLAN являются взаимоисключающими, и для одного устройства можно выбрать только один режим кольцевого протокола.

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

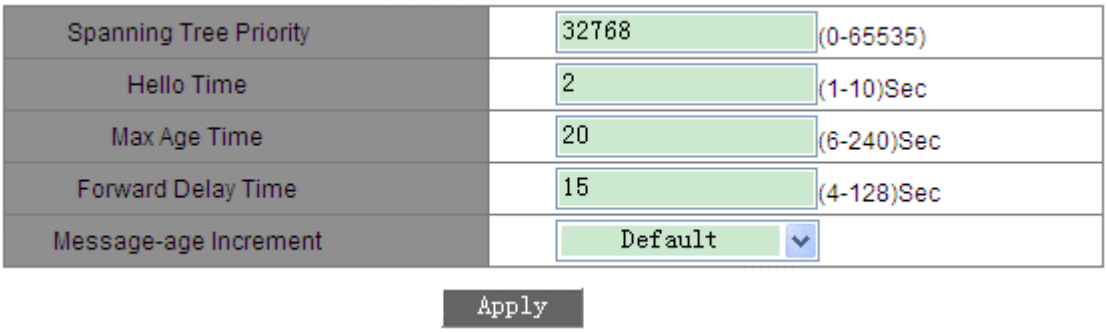

Рисунок 95 Задание параметров времени сетевого моста

Spanning Tree Priority
Диапазон: 0~65535 Шаг составляет 4096.
По умолчанию: 32768
Функция: Настройка приоритета сетевого моста.
Описание: Приоритет используется для выбора корневого моста. Чем меньше значение, тем выше приоритет.
Hello Time
Диапазон: 1~10 с
По умолчанию: 2 с
Функция: Настройка интервала времени для отправки BPDU.
Max Age Time
Диапазон: 6~240 с
По умолчанию: 20 с
Описание: Если значение возраста сообщения в BPDU больше указанного значения, то BPDU

отбрасывается.

Forward Delay Time

Диапазон: 4~128 с

По умолчанию: 15 с

Функция: Настройка времени изменения статуса с Discarding на Learning или с Learning на Forwarding.

Message-age Increment

Варианты: Compulsion/Default

По умолчанию: Default

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

Описание: В режиме Compulsion значение равно 1.

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

Значения Forward Delay Time, Max Age Time и Hello Time должны соответствовать следующим требованиям:

2 x (Forward Delay Time – 1,0 с) > Max Age Time;

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

Включите RSTP на портах, как показано на рисунке ниже.

Port Settings

Port	Protocol State	Port Priority(0~255)	Path Cost(1~200000000)	Cost Count
S1/FE1	Enable	128	200000	Yes
S1/FE2	Enable	128	2000000	No
S1/FE3	Enable	128	2000000	Yes
S1/FE4	Enable	128	2000000	No
S1/FE5	Disable	128	2000000	Yes
S1/FE6	Disable	128	2000000	Yes
S1/FE7	Disable	128	2000000	Yes
S1/FE8	Disable	128	2000000	Yes
S4/GE1	Disable	128	2000000	Yes
S4/GE2	Disable	128	2000000	Yes
S4/GE3	Disable	128	2000000	Yes
S4/GE4	Disable	128	2000000	Yes

Apply

Рисунок 96 Настройки портов

Protocol State

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение или выключение STP для портов.

CAUTION	**Предупреждение:** > Порт RSTP нельзя настроить как исходный порт или порт назначения зеркалирования. Исходный порт или порт назначения зеркалирования нельзя настроить как порт RSTP. > Порт RSTP нельзя добавить к группе агрегации. Порт, добавленный к группе агрегации, нельзя настроить как порт RSTP.

	> Кольцевые порты между кольцевыми протоколами на основе портов RSTP, DT-Ring-Port и DRP-Port являются взаимоисключающими, то есть порт RSTP нельзя настроить как кольцевой порт DT-Ring-Port/DRP-Port или резервный порт DT-Ring-Port/DRP-Port; Кольцевой порт DT-Ring-Port/DRP-Port и резервный порт DT-Ring-Port/DRP-Port не должны быть настроены как порт RSTP. > Не рекомендуется одновременно настраивать порты в изолированной группе как порты RSTP, а порты RSTP нельзя добавлять в изолированную группу.

Port Priority
Диапазон: 0~255 Шаг составляет 16.
По умолчанию: 128
Функция: Настройка приоритета порта, определяющего роли портов.
Path Cost
Диапазон: 1~200000000
По умолчанию: 2000000 (10M порт), 200000 (100M port), 20000 (1000M port)
Описание: Стоимость пути порта используется для расчета наилучшего пути. Значение параметра зависит от полосы пропускания. Чем больше значение, тем ниже стоимость. Можно изменить роль порта, изменив значение параметра стоимости пути. Чтобы настроить значение вручную, выберите значение No для параметра Cost Count.
Cost Count
Диапазон: Yes/No
По умолчанию: Yes
Описание: Yes указывает, что стоимость пути порта принимает значение по умолчанию. No означает, что можно настроить стоимость пути.
Просмотрите статус RSTP, как показано на рисунке ниже.

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

Рисунок 97 Информация о статусе RSTP

6.13.6 Пример типовой конфигурации

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

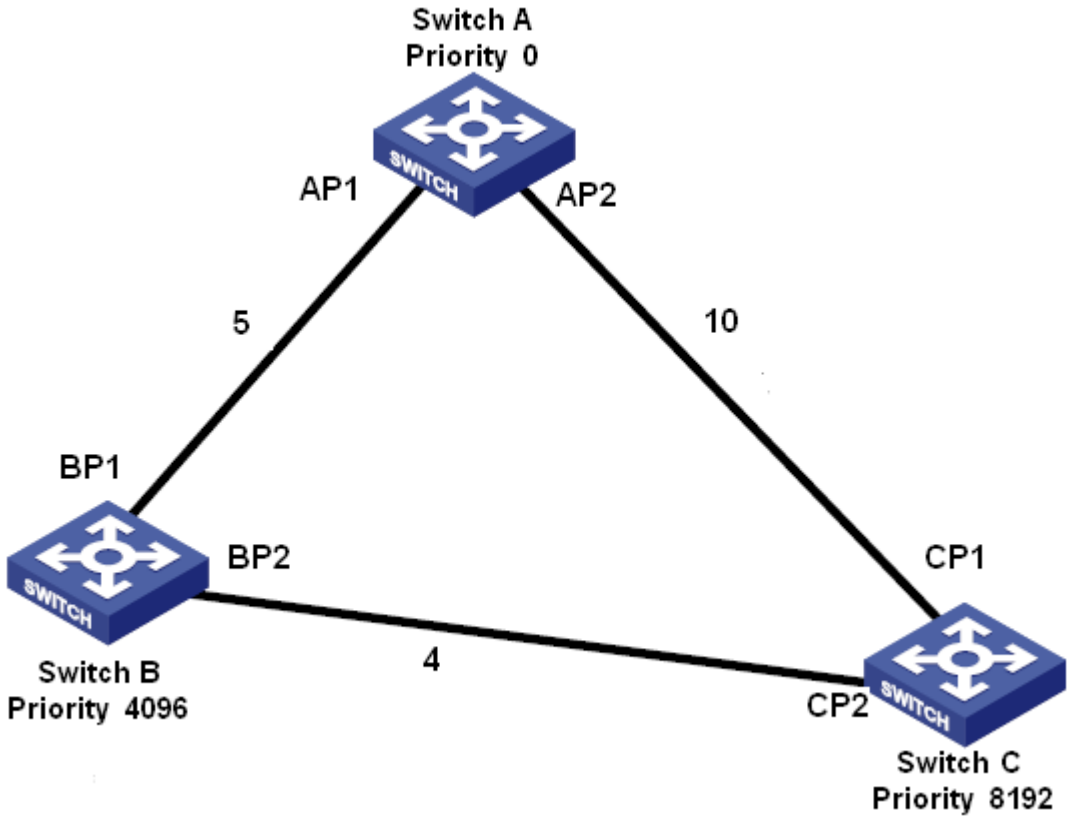

Рисунок 98 Пример конфигурации RSTP

Конфигурация коммутатора A:
1. Установите приоритет 0 и значения по умолчанию для временных параметров, как показано на рисунке 95.
2. Установите стоимость пути для порта 1 – 5 и для порта 2 – 10, как показано на рисунке 96.
Конфигурация коммутатора B:
1. Установите приоритет 4096 и значения по умолчанию для временных параметров, как показано на рисунке 95.
2. Установите стоимость пути для порта 1 – 5 и для порта 2 – 4, как показано на рисунке 96.
Конфигурация коммутатора C:
1. Установите приоритет 8192 и значения по умолчанию для временных параметров, как показано на рисунке 95.
2. Установите стоимость пути для порта 1 – 10 и для порта 2 – 4, как показано на рисунке 96.
Приоритет коммутатора A равен 0, а его корневой идентификатор наименьший. Таким образом, коммутатор A является корневым мостом.
Стоимость пути от AP1 к BP1 равна 5, а от AP2 к BP2 равна 14. Таким образом, BP1 является корневым портом.
Стоимость пути от AP1 к CP2 равна 9, а от AP2 к CP1 равна 10. Таким образом, CP2 является корневым портом, а BP2 является назначенным портом.

6.14 Режим прозрачной передачи RSTP/STP

6.14.1 Обзор

RSTP соответствует стандарту IEEE. DT-Ring/DRP — это проприетарный протокол резервной защиты Kyland, но он не может сосуществовать с RSTP в одной сети. Чтобы решить эту проблему, компания Kyland разработала функцию прозрачной передачи RSTP/STP. Эта функция позволяет коммутатору

использовать другие протоколы резервирования при прозрачной передаче пакетов RSTP, что соответствует требованиям промышленного обмена данными.
Коммутаторы, использующие другие резервные протоколы, могут получать и пересылать пакеты RSTP только в том случае, если включена функция прозрачной передачи RSTP. Коммутаторы с поддержкой прозрачной передачи RSTP можно рассматривать как прозрачный канал связи.
Как показано на следующем рисунке, коммутатор A, коммутатор B, коммутатор C и коммутатор D образуют DT-Ring. На этих четырех коммутаторах включена функция прозрачной передачи, поэтому коммутаторы E и F могут получать пакеты RSTP друг от друга.

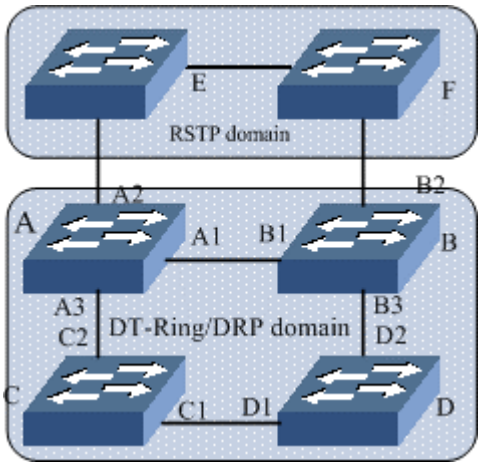

Рисунок 99 Прозрачная передача RSTP

6.14.2 Настройка через веб-интерфейс

Настройте прозрачную передачу RSTP на портах, как показано на рисунке ниже.

Port	RSTP Transparent Transmission
S1/FE1	Disable
S1/FE2	Disable
S1/FE3	Disable
S1/FE4	Disable
S1/FE5	Enable
S1/FE6	Enable
S1/FE7	Disable
S1/FE8	Disable
S4/GE1	Disable
S4/GE2	Disable
S4/GE3	Disable
S4/GE4	Disable

Apply

Рисунок 100 Настройка прозрачной передачи RSTP

RSTP Transparent Transmission

Варианты: Enable/Disable
По умолчанию: Disable
Функция: Включение или выключение режима прозрачной передачи RSTP для портов.

	**Предупреждение:** Прозрачную передачу RSTP нельзя включить для порта с поддержкой RSTP.

6.14.3 Пример типовой конфигурации

Как показано на рисунке 99, коммутатор A, коммутатор B, коммутатор C и коммутатор D образуют кольцо DT-Ring, а коммутатор E и коммутатор F образуют кольцо RSTP. В кольце RSTP все кольцо DT служит прозрачным каналом для пересылки пакетов RSTP на коммутаторы E и F.
Настройте коммутатор A, коммутатор B, коммутатор C и коммутатор D как DT-Ring. Подробности см. в разделе 6.12 DT-Ring.
Включите RSTP на задействованных портах коммутатора E и коммутатора F, как показано на рисунке 94 и рисунке 96.
Включите прозрачную передачу RSTP на портах A1, A2, A3, B1, B2, B3, C1, C2, D1 и D2, как показано на рисунке 100.

6.15 DRP

6.15.1 Обзор

Компания Kyland разрабатывает протокол распределенного резервирования (DRP) для передачи данных в сетях кольцевой топологии. Это может предотвратить широковещательные штормы для кольцевых сетей. Когда канал или узел неисправен, резервный канал может взять на себя обслуживание в режиме реального времени, чтобы обеспечить непрерывную передачу данных.
В соответствии со стандартом IEC 62439-6 DRP использует механизм выбора устройства Master без его фиксации. DRP обеспечивает следующие функции:
Время восстановления, не зависящее от масштаба сети.
DRP обеспечивает время восстановления, не зависящее от масштаба сети, за счет оптимизации механизма пересылки пакетов обнаружения кольца. DRP позволяет сетям восстанавливаться в течение 20 мс благодаря введению отчетов о прерывании в реальном времени, что повышает надежность передачи данных в реальном времени. Эта функция позволяет коммутаторам обеспечивать более высокую надежность для приложений в энергетике, железнодорожном транспорте и многих других отраслях, требующих управления в режиме реального времени.
Различные функции проверки линии связи
Для повышения стабильности сети DRP предоставляет разнообразные функции обнаружения каналов для типичных сетевых сбоев, включая обнаружение быстрого отключения, обнаружение однонаправленных каналов оптоволокна, проверку качества каналов и проверку работоспособности оборудования, обеспечивая правильную передачу данных.
Применимость к нескольким сетевым топологиям
Помимо быстрого восстановления для простых кольцевых сетей, DRP также поддерживает сложные кольцевые топологии, такие как пересекающиеся кольца и соприкасающиеся кольца. Кроме того, DRP поддерживает многовариантные решения на основе VLAN, что подходит для различных сетевых приложений с гибкой сетью.
Мощные функции диагностики и обслуживания
DRP предоставляет мощные механизмы запросов о состоянии и сигналов тревоги для диагностики и обслуживания сети, а также механизм предотвращения непреднамеренных операций и неправильных конфигураций, которые могут привести к кольцевым сетевым штормам.

6.15.2 Основные понятия

1. Режимы DRP
DRP имеет два режима: DRP-Port-Based и DRP-VLAN-Based.
DRP-Port-Based: перенаправляет или блокирует пакеты на основе определенных портов.
DRP-VLAN-Based: перенаправляет или блокирует пакеты на основе VLAN. Если порт находится в состоянии блокировки, блокируются только пакеты данных указанной VLAN. Таким образом, на портах соприкасающихся колец можно настроить несколько VLAN. Порт может принадлежать разным кольцам DRP в соответствии с конфигурациями VLAN.
2. Состояния порта DRP
Состояние пересылки: Если порт находится в состоянии пересылки, порт может и принимать, и отправлять пакеты данных. Состояние блокировки: Если порт находится в состоянии блокировки, порт может и принимать пакеты DRP, но не другие пакеты данных.

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

3. Режимы DRP
DRP определяет роли коммутаторов, пересылая пакеты Announce, предотвращая образование петель в кольцах резервирования.
INIT: указывает устройство, на котором включен DRP, а два кольцевых порта находятся в состоянии Link down.
INIT: указывает устройство, на котором включен DRP, а хотя бы один кольцевой порт находится в состоянии Link up. В кольце Root выбирается в соответствии с векторами пакетов Announce. Это может измениться в зависимости от топологии сети. Root периодически отправляет свои собственные пакеты Announce на другие устройства. Состояния кольцевых портов: Один кольцевой порт находится в состоянии пересылки, а другой — в состоянии блокировки. Получив пакет Announce от другого устройства, Root сравнивает вектор пакета с вектором своего собственного пакета Announce. Если вектор полученного пакета больше, Root меняет свою роль на Normal или B-Root в зависимости от состояния канала и ухудшения CRC портов.
B-Root: указывает устройство, на котором включен DRP, отвечающее хотя бы одному из следующих условий: один кольцевой порт находится в состоянии Link up, а другой — в состоянии Link down, деградация CRC, приоритет не менее 200. B-Root сравнивает и пересылает пакеты Announce. Если вектор полученного пакета Announce меньше вектора его собственного пакета Announce, B-Root меняет свою роль на Root; в противном случае он пересылает полученный пакет и не меняет свою роль. Состояния кольцевых портов: Один кольцевой порт находится в состоянии пересылки.
Normal: указывает устройство, на котором включен DRP, и оба кольцевых порта находятся в состоянии Link up без ухудшения CRC, а приоритет больше 200. Normal только пересылает пакеты Announce, но не проверяет содержимое пакетов. Состояния кольцевых портов: Оба кольцевых порта находятся в состоянии пересылки.

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

6.15.3 Реализация

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

Таблица 7 Вектор пакета Announce

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

Состояние канала: Значение устанавливается равным 1, если один кольцевой порт находится в состоянии Link down, и устанавливается в 0, если оба кольцевых порта находятся в состоянии Link up.
Состояние ухудшения CRC: Если ухудшение CRC происходит на одном порту, значение устанавливается равным 1. Если ухудшение CRC не происходит на двух кольцевых портах, значение устанавливается равным 0.
Скорость ухудшения CRC: Соотношение количества пакетов CRC и порогового значения за 15 минут.
Приоритет роли: Значение можно задать через веб-интерфейс.
Параметры в таблице 7 сравниваются в следующей процедуре:
1. Сначала проверяется значение состояния канала. Устройство с большим значением состояния канала считается имеющим больший вектор.

2. Если два сравниваемых устройства имеют одинаковое значение состояния канала, сравниваются значения состояния ухудшения CRC. Устройство с большим значением состояния ухудшения CRC считается имеющим больший вектор. Если значение состояния ухудшения CRC всех сравниваемых устройств равно 1, считается, что устройство с большим значением скорости ухудшения CRC имеет больший вектор.
3. Если два сравниваемых устройства имеют одинаковое значение состояния канала и значение ухудшения CRC, значения приоритета ролей, IP-адресов и MAC-адресов сравниваются последовательно. Устройство с большим значением считается имеющим больший вектор.
Устройство с большим вектором будет выбрано в качестве Root.

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

> Реализация режима DRP-Port-Based
Роли коммутаторов следующие:
1. При запуске все коммутаторы находятся в состоянии INIT. Когда состояние одного порта изменяется на Link up, коммутатор становится коммутатором Root и отправляет пакеты Announce другим коммутаторам в кольце для выбора.
2. Коммутатор с большим вектором пакета Announce будет выбран в качестве Root. Кольцевой порт, который первым на Root переходит в состояние Link up, находится в состоянии пересылки, а другой кольцевой порт находится в состоянии блокировки. Среди других коммутаторов в кольце коммутатор с одним кольцевым портом в состоянии Link down или ухудшения CRC является коммутатором B-Root. Коммутатор с обоими кольцевыми портами в состоянии Link up и без ухудшения CRC является коммутатором Normal.
Процедура устранения отказов следующая:
1. В исходной топологии A является Root; порт 1 находится в состоянии пересылки, а порт 2 в состоянии блокировки. B, C и D – коммутаторы Normal, и их кольцевые порты находятся в состоянии пересылки, как показано на рисунке ниже.

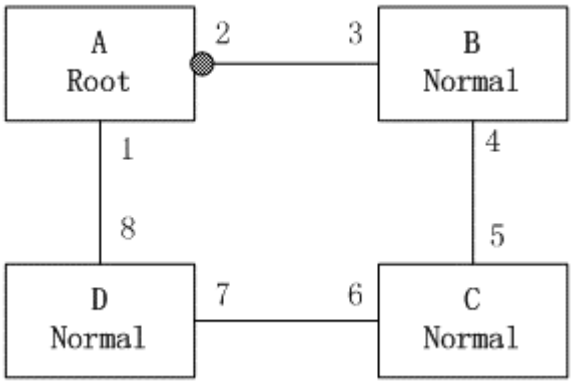

Рисунок 101 Топология DRP

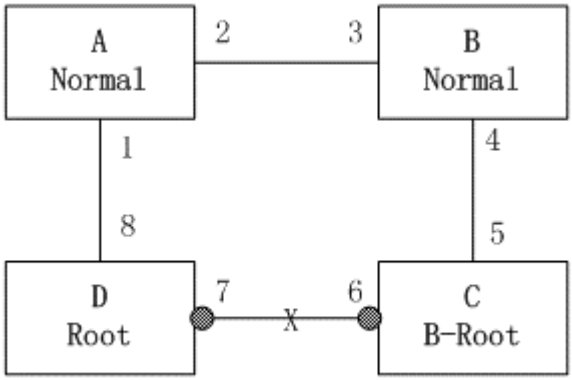

Рисунок 102 Отказ канала

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

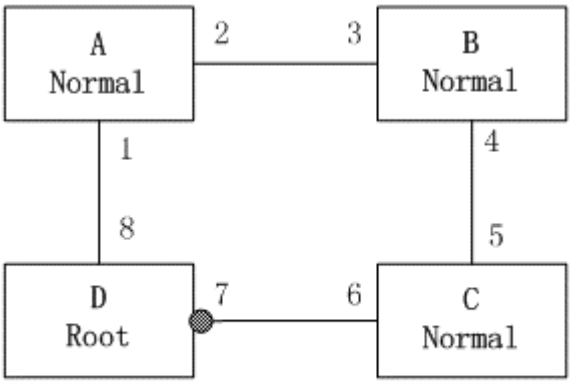

Рисунок 103 Восстановление канала

3. Когда связь CD восстанавливается, D по-прежнему является Root, 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, и DRP меняет статус порта 6 на пересылку. В результате C становится коммутатором Normal. Поэтому роли коммутаторов не меняются для восстановления связи.

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

> Реализация режима DRP-VLAN-Based

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

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

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

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

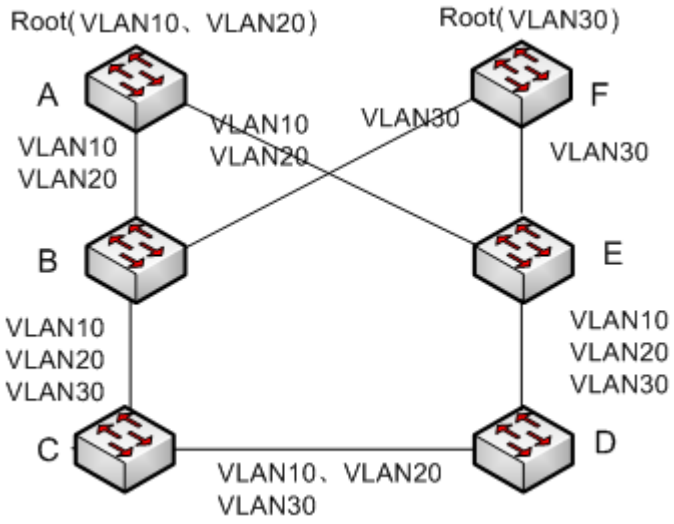

Рисунок 104 DRP-VLAN-Based

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

Резервирование DRP

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

Порт резервирования: указывает порт связи между кольцами DRP. Можно настроить несколько портов резервирования, но они должны находиться в одном кольце. Первый резервный порт в состоянии Link

up – это резервный порт Master, который находится в состоянии пересылки. Все остальные порты являются портами Slave. Они находятся в состоянии блокировки.
Как показано на следующем рисунке, на каждом коммутаторе можно настроить один резервный порт. Резервный порт Master находится в состоянии пересылки, а другие резервные порты — в состоянии блокировки. Если резервный порт Master или его канал выходят из строя, для пересылки данных будет выбран резервный порт Slave.

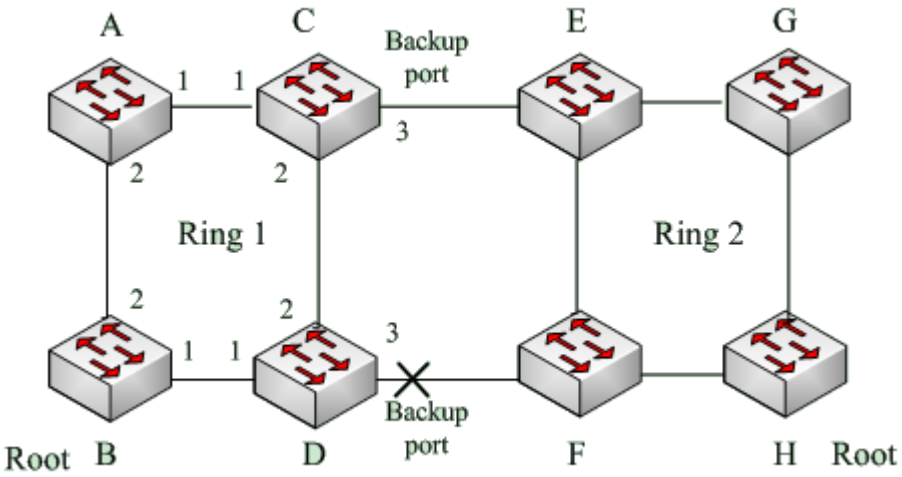

Рисунок 105 Резервирование DRP

CAUTION	**Предупреждение:** Изменение статуса соединения влияет на статус резервных портов.

6.16 DHP

6.16.1 Обзор

Как показано на следующем рисунке, коммутаторы A, B, C и D подключены к кольцу. Протокол Dual Homing (DHP) выполняет следующие функции, если он включен на A, B, C и D:
A, B, C и D могут взаимодействовать друг с другом, не влияя на правильную работу устройств в кольце. Если связь между A и B неисправна, A все еще может обмениваться данными с B, C и D через Устройство 1 и Устройство 2.

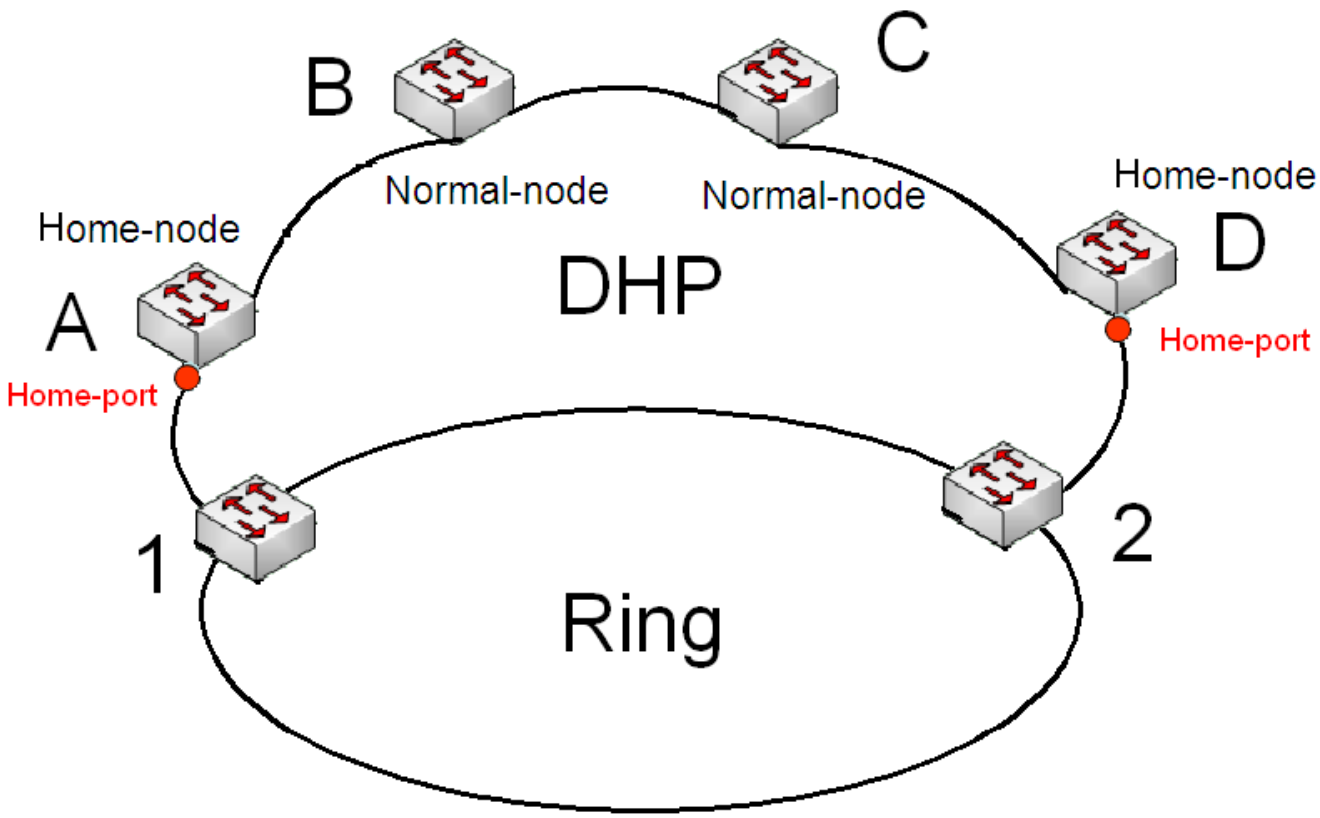

Рисунок 106 Использование DHP

6.16.2 Основные понятия

Реализация DHP основана на DRP. Механизм выбора и назначения ролей в DHP такой же, как и в DRP. DHP обеспечивает резервирование канала посредством настройки узла Home, узла Normal и порта Home.
Узел Home: указывает устройства на обоих концах канала DHP и завершает пакеты DRP. Порт Home: указывает порт, соединяющий узел Home с внешней сетью. Порт Home обеспечивает следующие функции:
Отправка ответных пакетов Root после получения пакетов Announce от Root. Если Root получает ответные пакеты, состояние кольца идентифицируется как замкнутое. Если Root получает не ответные пакеты, состояние кольца идентифицируется как разомкнутое.
Блокировка пакетов DRP внешних сетей и изоляция канала DHP от внешних сетей.
Отправка пакетов очистки входа на подключенные устройства во внешних сетях при изменении топологии канала DHP.
Узел Normal: указывает устройства в канале DHP, за исключением устройств на обоих концах. Узлы Normal передают ответные пакеты домашних узлов Home.

6.16.3 Реализация

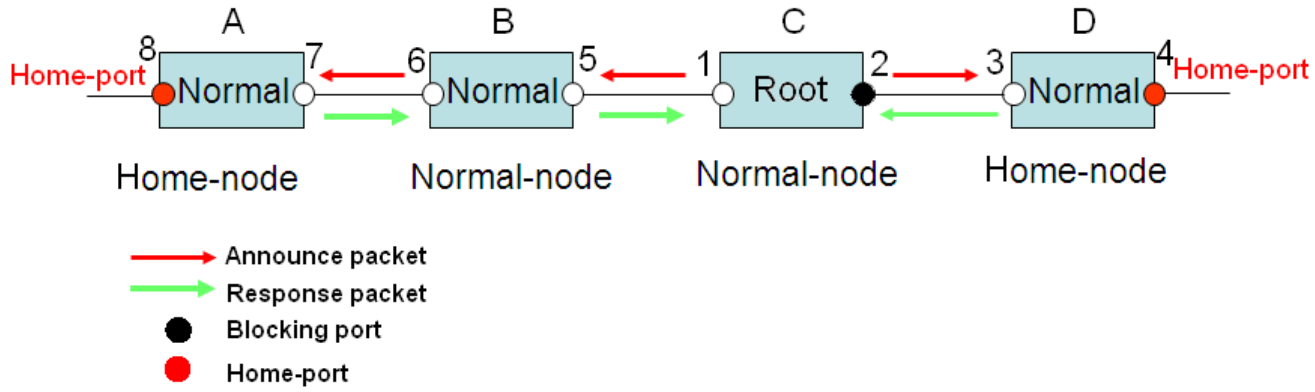

Рисунок 107 Конфигурация DHP

Как показано на предыдущем рисунке, конфигурации A, B, C и D на рисунке 6 следующие:
Конфигурация DRP: C — Root; порт 2 находится в состоянии блокировки; A, B и D являются узлами Normal; все остальные порты кольца находятся в состоянии пересылки.
Конфигурация DHP: A и D — узлы Home; порт 8 и порт 4 — порты Home; B и C являются узлами Normal.
Реализация:
1. C, Root, отправляет пакеты Announce через два своих кольцевых порта. Порт Home 8 и порт Home 4 завершают полученные пакеты Announce и отправляют ответные пакеты на C. C идентифицирует состояние кольца как замкнутое. Порт 2 находится в состоянии блокировки.
2. Когда канал между A и B заблокирован, топология включает два канала: A и B-C-D.
A выбран в качестве Root. Порт 7 находится в состоянии блокировки.
B в канале B-C-D B выбран в качестве Root. Порт 6 находится в состоянии блокировки. C становится узлом Normal. Порт 2 находится в состоянии пересылки. A может обмениваться данными с B, C и D через Устройство 1 и Устройство 2, как показано на следующем рисунке.

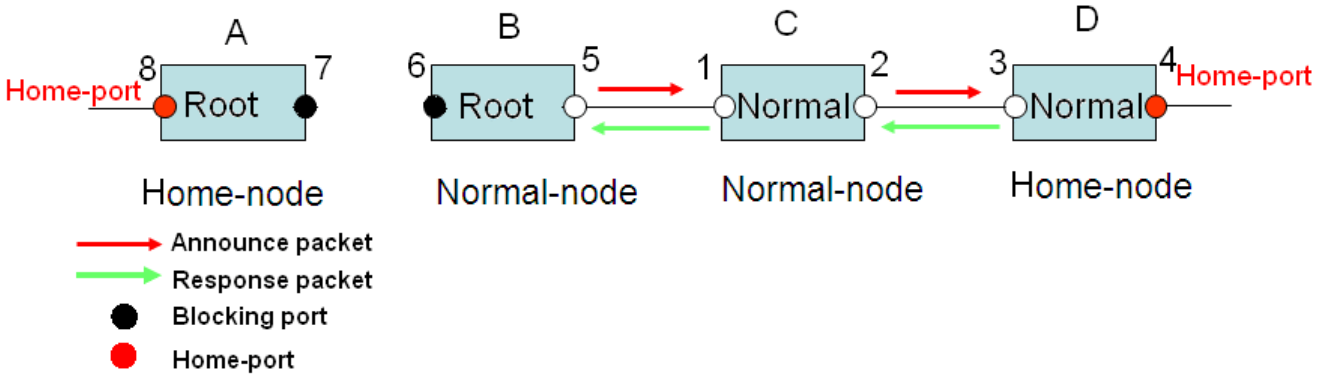

Рисунок 108 Устранение отказа DHP

6.16.4 Описание

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

6.16.5 Настройка через веб-интерфейс

Настройте режим DRP, как показано на следующем рисунке.

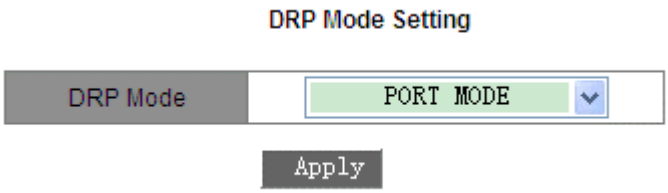

Рисунок 109 Настройка режима DPR

Режим DRP
Варианты: PORT MODE/VLAN MODE
По умолчанию: PORT MODE
Функция: Настройка режима DRP.

CAUTION	**Предупреждение:** > К кольцевым протоколам на основе портов относятся RSTP, DT-Ring-Port и DRP-Port, а к протоколам на основе VLAN – DT-Ring-VLAN и DRP-VLAN. > Кольцевые протоколы на основе VLAN являются взаимоисключающими, и для одного устройства можно настроить только тип кольцевого протокола на основе VLAN. > Кольцевой протокол на основе порта и кольцевой протокол на основе VLAN являются взаимоисключающими, и для одного устройства можно выбрать только один режим кольцевого протокола.

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

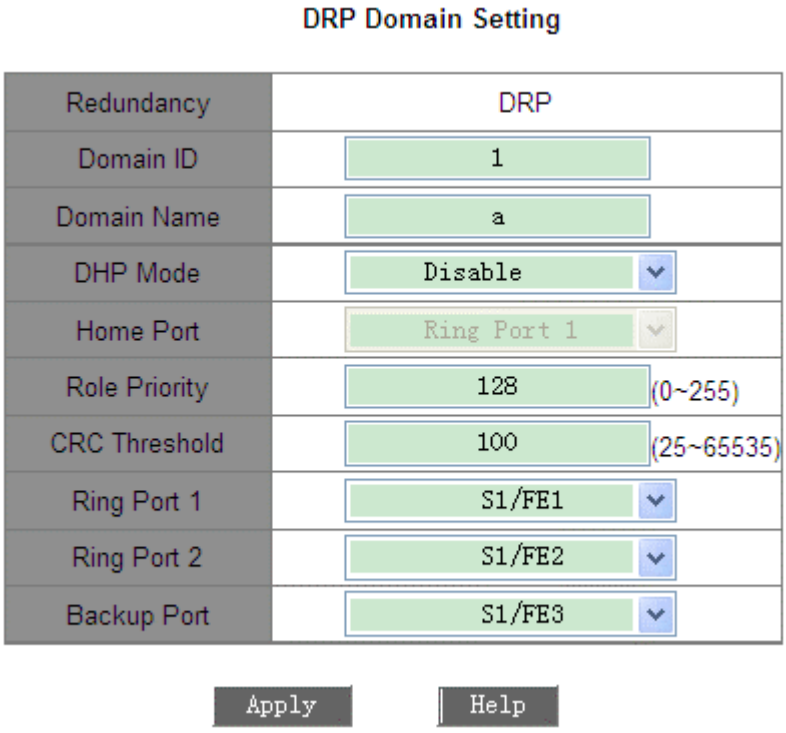

Рисунок 110 Настройка DRP-Port-Based

Redundancy
Обязательная настройка: DRP

Domain ID
Диапазон: 1~32
Функция: Каждое кольцо имеет уникальный идентификатор домена. На одном коммутаторе можно настроить не более 16 колец DRP-Port-Based.
Domain Name
Диапазон: 1~31 символ
Функция: Задание доменного имени.
DHP Mode
Варианты: Disable/Normal Node/Home Node
По умолчанию: Disable
Функция: Включение или отключение DHP или настройка режима DHP.

	**Предупреждение:** DHP доступен только в режиме DRP-Port-Based.

Home Port
Варианты: Ring Port 1/Ring Port 2/Ring Port 1-2
Функция: Настройка порта Home для узла Home DHP.
Описание: Если в канале DHP есть только одно устройство, оба кольцевых порта узла Home должны быть настроены как порты Home.
Role Priority
Диапазон: 0~255
По умолчанию: 128
Функция: Настройка приоритета коммутатора.
CRC Threshold
Диапазон: 25~65535
По умолчанию: 100
Функция: Настройка порогового значения CRC.
Описание: Этот параметр используется при выборе коммутатора Root. Система подсчитывает количество полученных CRC. Если количество CRC одного кольцевого порта превышает пороговое значение, система считает, что порт имеет ухудшение CRC. В результате в векторе пакета Announce порта значение ухудшения CRC устанавливается равным 1.
Ring Port 1/Ring Port 2
Варианты: все порты коммутатора.
Функция: Выбор двух кольцевых портов.
Backup Port
Варианты: все порты коммутатора.
Функция: Настройка резервного порта.

	**Предупреждение:** Не следует настраивать кольцевой порт в качестве резервного.

После завершения настройки созданные кольца будут отображаться 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

Рисунок 111 Список DRP-Port-Based

CAUTION	**Предупреждение:** > Кольцевой порт DRP или резервный порт не могут быть добавлены к группе агрегации. Порт, добавленный к группе агрегации, нельзя настроить как кольцевой порт DRP или резервный порт. > Кольцевой порт DRP или резервный порт нельзя настроить как исходный порт или порт назначения зеркалирования. Исходный порт или порт назначения зеркалирования нельзя настроить как кольцевой порт DRP или резервный порт. > Кольцевые порты между кольцевыми протоколами на основе портов RSTP, DT-Ring-Port и DRP-Port являются взаимоисключающими, то есть кольцевой порт и резервный порт DRP-Port не могут быть настроены как порт RSTP, DRP-Port. кольцевой порт DT-Ring-Port или резервный порт DT-Ring-Port; Порт RSTP, кольцевой порт DT-Ring-Port и резервный порт DT-Ring-Port нельзя настроить как кольцевой порт DRP-Port или резервный порт. > Не рекомендуется одновременно настраивать порты в изолированной группе как порты DRP и резервные порты, а порты DRP и резервные порты нельзя добавлять в изолированную группу.

> Просмотр настроек параметров DRP-Port-Based.
Щелкните запись DRP на рисунке 111. Можно просматривать и изменять 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

Рисунок 112 Запрос и изменение записи DRP-Port-Based.

После внесения изменений щелкните <Apply>, чтобы внесенные изменения вступили в силу. Можно

удалить запись DRP, щелкнув <Delete>.
> Просмотрите роли и статус порта кольца DRP, как показано на следующем рисунке.

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

Рисунок 113 Запрос статуса DRP-Port-Based

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

DRP Domain 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
Protocol Vlan	2 (1~4093)
Service Vlan	2-4 (e.g. 1,2,3,6-8)

Apply Help

Рисунок 114 Настройка DRP-VLAN-Based

Redundancy
Обязательная настройка: DRP
Domain ID
Диапазон: 1~32
Функция: Каждое кольцо имеет уникальный идентификатор домена. На одном коммутаторе можно настроить не более 8 колец DRP-VLAN-Based.

Domain Name

Диапазон: 1~31 символ
Функция: Задание доменного имени.

Role Priority

Диапазон: 0~255
По умолчанию: 128
Функция: Настройка приоритета коммутатора.

CRC Threshold

Диапазон: 25~65535
По умолчанию: 100
Функция: Настройка порогового значения CRC.
Описание: Этот параметр используется при выборе коммутатора Root. Система подсчитывает количество полученных CRC. Если количество CRC одного кольцевого порта превышает пороговое значение, система считает, что порт имеет ухудшение CRC. В результате в векторе пакета Announce порта значение ухудшения CRC устанавливается равным 1.

Ring Port 1/Ring Port 2

Варианты: все порты коммутатора.
Функция: Выбор двух кольцевых портов.

Backup Port

Варианты: все порты коммутатора.
Функция: Настройка резервного порта.

	**Предупреждение:** Не следует настраивать кольцевой порт в качестве резервного.

	**Предупреждение:** > Кольцевой порт DRP или резервный порт не могут быть добавлены к группе агрегации. Порт, добавленный к группе агрегации, нельзя настроить как кольцевой порт DRP или резервный порт. > Кольцевой порт DRP или резервный порт нельзя настроить как исходный порт или порт назначения зеркалирования. Исходный порт или порт назначения зеркалирования нельзя настроить как кольцевой порт DRP или резервный порт. > Не рекомендуется одновременно настраивать порты в изолированной группе как порты DRP и резервные порты, а порты DRP и резервные порты нельзя добавлять в изолированную группу.

Protocol VLAN

Диапазон: 1~4093
Описание: VLAN ID должен быть идентификатором сервисной VLAN.
Функция: Пакеты DRP с VLAN ID служат основой для диагностики и обслуживания кольца DRP-VLAN-Based.

Service VLAN

Варианты: Все созданные VLAN
Функция: Выбор VLAN, управляемой данным кольцом DRP-VLAN-Based.

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

DRP List

Domain ID	Role Status	Ring Port(1,2)	Backup Port	Ring Status	Protocol Vlan	Service Vlan
1-a	ROOT	S1/FE1,S1/FE2	S1/FE3	Ring-Close	2	2-4

Рисунок 115 Список DRP-VLAN-Based

> Просмотр настроек параметров DRP-VLAN-Based.
Щелкните запись DRP на рисунке 115. Можно просматривать и изменять 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
Protocol Vlan	2
Service Vlan	2-4

Apply Delete Cancel Help

Рисунок 116 Запрос и изменение записи DRP-VLAN-Based.

После внесения изменений щелкните <Apply>, чтобы внесенные изменения вступили в силу. Можно удалить запись DRP, щелкнув <Delete>.
Просмотрите роли и статус порта кольца DRP, как показано на следующем рисунке.

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

Рисунок 117 Запрос статуса DRP-VLAN-Based

6.16.6 Пример типовой конфигурации

Как показано на рисунке 105, A, B, C и D образуют кольцо 1; E, F, G и H образуют кольцо 2; CE и DF являются резервными каналами Ring 1 и Ring 2.

Конфигурация коммутатора A и коммутатора B:

1. Установите Domain ID 1 и Domain name Ring. Выберите кольцевой порт 1 и кольцевой порт 2. Сохраните значения по умолчанию для приоритета роли и резервного порта, как показано на рисунке 110.

Конфигурация коммутатора C и коммутатора D:

2. Установите Domain ID 1, Domain name Ring, резервный порт 3. Выберите кольцевой порт 1 и кольцевой порт 2. Сохраните значения по умолчанию для приоритета роли, как показано на рисунке 110.

Конфигурация коммутаторов E, F, G и H:

3. Установите Domain ID 2 и Domain name Ring. Выберите кольцевой порт 1 и кольцевой порт 2. Сохраните значения по умолчанию для приоритета роли и резервного порта, как показано на рисунке 110.

6.17 QoS

6.17.1 Обзор

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

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

Идентификация служб: Объекты идентифицируются на основе определенных правил соответствия. Например, объекты могут быть тегами приоритета, переносимыми пакетами, приоритетом, отображаемым портами и VLAN, или другой информацией о приоритете. Идентификация служб предварительным условием для QoS. Управление перегрузками: Это обязательно для решения проблемы конкуренции за ресурсы. Управление перегрузками кэширует пакеты в очередях и определяет последовательность пересылки пакетов на основе определенного алгоритма планирования, обеспечивая приоритетную пересылку для ключевых служб. Предотвращение перегрузки: Чрезмерная перегрузка может привести к повреждению сетевых ресурсов. Функция предотвращения перегрузки отслеживает использование сетевых ресурсов. При обнаружении увеличения перегрузки функция использует упреждающее отбрасывание пакетов и настраивает объем трафика для устранения перегрузки.

6.17.2 Принцип работы

Каждый порт коммутаторов этой серии поддерживает четыре очереди кэширования, от 0 до 3 в порядке возрастания приоритета.

Можно настроить сопоставление между приоритетом и очередями. Когда кадр достигает порта, коммутатор определяет очередь для кадра в соответствии с информацией в заголовке кадра.

Коммутатор поддерживает пять режимов сопоставления очередей для определения приоритета: наивысший приоритет, на основе порта, DIFF, TOS/DIFF и 802.1p.

Если для порта настроен наивысший приоритет, то пересылаемые пакеты помещаются в очередь 3.

Если для порта настроен режим сопоставления очередей на основе порта, полученные пакеты ставятся 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.

Можно настроить сопоставление между приоритетом и очередями.
Когда пакет тегирован, значение 802.1p зависит от приоритета 802.1Q в пакете. Когда пакет не тегирован, значение 802.1p зависит от приоритета порта. Можно настроить сопоставление между приоритетом 802.1p и очередями.

При пересылке данных порт использует режим планирования для планирования данных в четырех очередях и пропускной способности каждой очереди. Коммутатор поддерживает два режима планирования: Weighted Round Robin (WRR), режим Hq-preempt и режим STRICT.
WRR планирует потоки данных на основе соотношения весов. Очереди получают свою пропускную способность на основе соотношения весов. WRR отдает приоритет очередям с высоким весом. Больше пропускной способности выделяется очередям с более высоким весовым коэффициентом.
В режиме Hq-preempt преимущественно пересылаются высокоприоритетные пакеты. Он в основном используется для передачи чувствительных сигналов. Если кадр поступает в очередь с высоким приоритетом, коммутатор прекращает планирование очередей с низким приоритетом и начинает обрабатывать данные очереди с высоким приоритетом. Когда очередь с высоким приоритетом не содержит данных, коммутатор начинает обрабатывать данные из очереди с более низким приоритетом.
В режиме STRICT преимущественно пересылаются высокоприоритетные пакеты. Он в основном используется для передачи чувствительных сигналов. Если кадр поступает в очередь с высоким приоритетом, коммутатор прекращает планирование очередей с низким приоритетом и начинает обрабатывать данные очереди с высоким приоритетом. Когда очередь с высоким приоритетом не содержит данных, коммутатор начинает обрабатывать данные из очереди с более низким приоритетом.

6.17.3 Настройка через веб-интерфейс (SICOM3024P/SICOM3024)

1. Настройте режим QoS, как показано на следующем рисунке.

Рисунок 118 Режим QoS

Qos Mode
Варианты: Disable/WRR/STRICT
По умолчанию: STRICT
Функция: Настройка режима планирования для порта.
Настройте весовой коэффициент очереди, как показано на следующем рисунке.

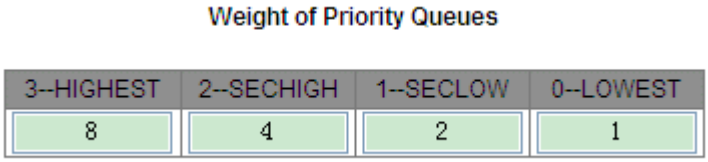

Рисунок 119 Настройка весового коэффициента очереди

{3-HIGHEST, 2-SECHIGH, 1-SECLOW, 0-LOWEST}
Диапазон: {1~55, 1~55, 1~55, 1~55}
По умолчанию: {8, 4, 2, 1}
Функция: Настройка весового коэффициента очереди по следующим правилам:
Вес очереди 3 > 2 x Вес очереди 2, Вес очереди 2 > 2 x Вес очереди 1,
Вес очереди 1 > 2 x Вес очереди 0
3. Настройте режим сопоставления приоритетов портов QoS, как показано на следующем рисунке.

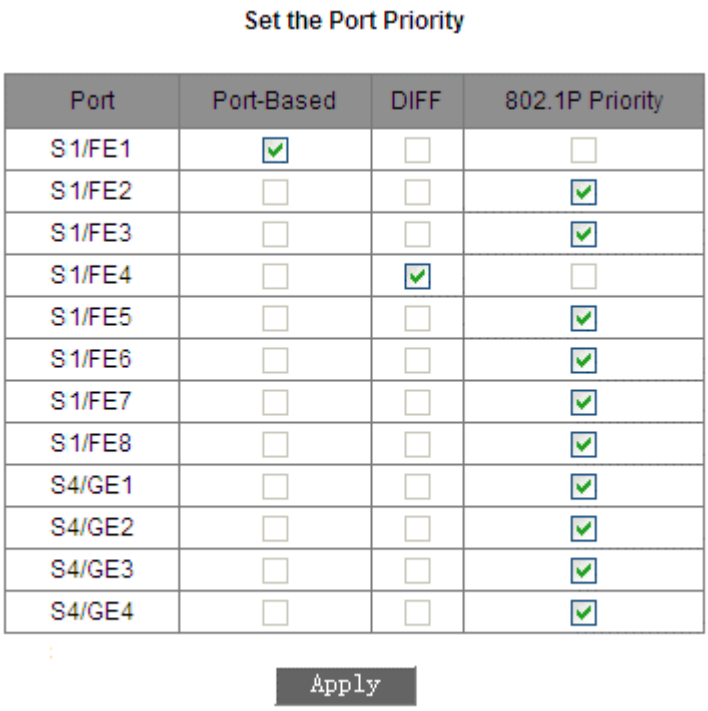

Рисунок 120 Настройка режима сопоставления приоритетов портов QoS

Set the Port Priority
Варианты: Port-Based/DIFF/802.1P Priority
По умолчанию: 802.1P Priority
Функция: Настройка режима сопоставления приоритетов портов.
Описание: Для каждого порта можно выбрать только один режим сопоставления приоритетов.
4. Настройте сопоставление очереди и приоритетов на основе портов/802.1p.
Сопоставление очередей в режиме на основе порта соответствует сопоставлению очереди в режиме приоритета 802.1p. Если требуется настроить любой из двух режимов, установите параметры в таблице сопоставления приоритетов 802.1p, как показано на следующем рисунке.
Щелкните <802.1p Priority> на рисунке 118. Появится следующая страница.

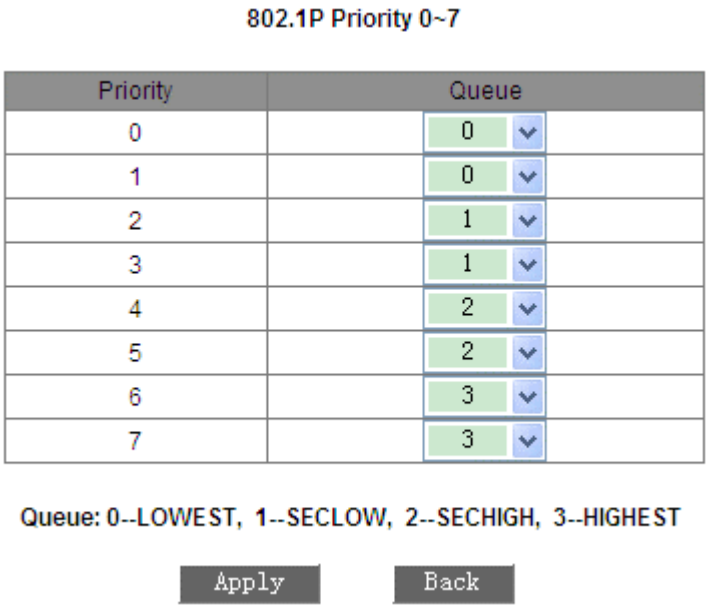

Рисунок 121 Сопоставление приоритета 802.1p и очереди

802.1P Priority
Состав: {Priority, Queue}
Диапазон: {0~7, 0~3}

По умолчанию: Приоритеты 0 и 1 сопоставлены очереди 0; приоритеты 2 и 3 сопоставлены очереди 1. Приоритеты 4 и 5 сопоставлены очереди 2; приоритеты 6 и 7 сопоставлены очереди 3.
Функция: Настройка сопоставления между приоритетом 802.1p и очередью.
5. Настройте сопоставление приоритета DSCP и очереди.
Щелкните <DSCP Priority> на рисунке 118, чтобы настроить сопоставление приоритета DSCP и очереди, как показано на следующем рисунке.

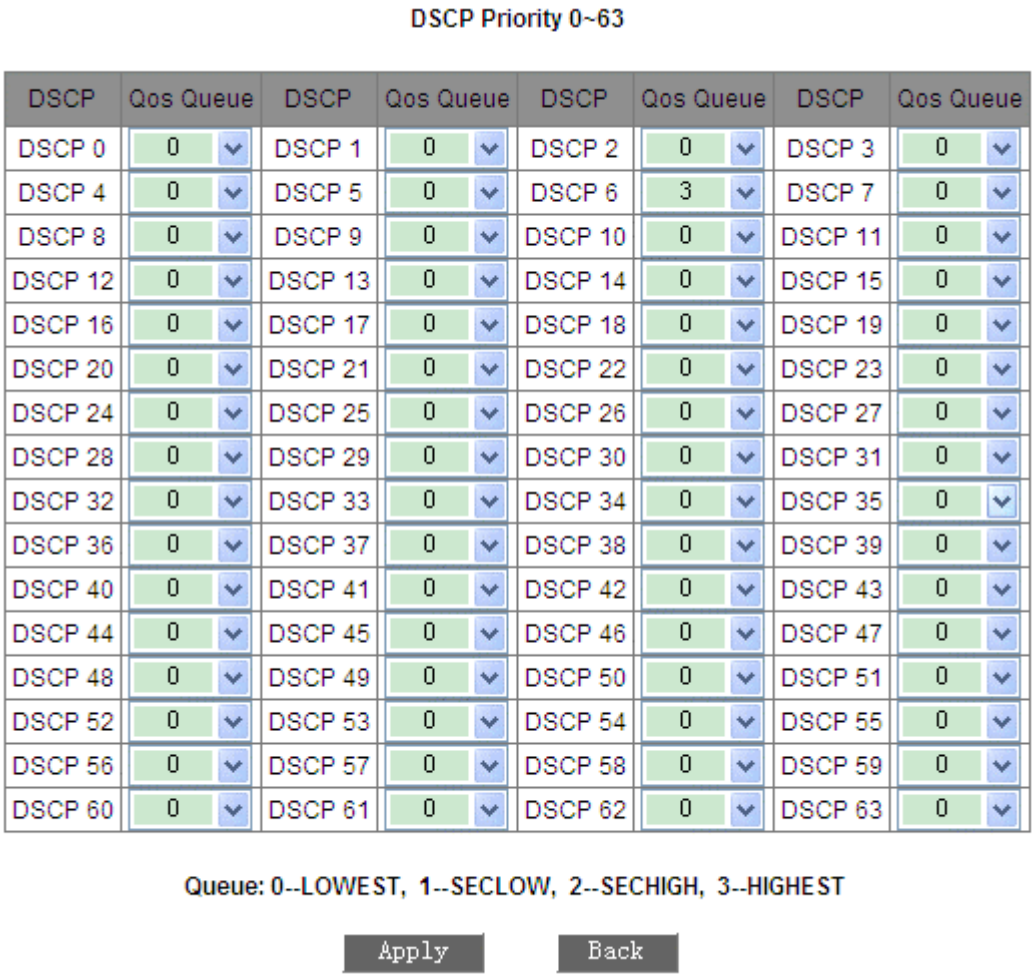

Рисунок 122 Сопоставление приоритета DSCP и очереди

DSCP Priority
Состав: {DSCP, Qos Queue}
Диапазон: {0~63, 0~3}
По умолчанию: Приоритет от 0 до 63 сопоставляется очереди 0.
Функция: Настройка сопоставления между приоритетом DSCP и очередью.

6.17.4 Настройка через веб-интерфейс (SICOM3048)

Настройте режим QoS, как показано на следующем рисунке.

Рисунок 123 Режим QoS

Qos Mode
Варианты: Disable/WRR/Hq-preempt
По умолчанию: Hq-preempt
Функция: Настройка режима планирования для порта.
IP TOS/DSCP
Варианты: DSCP MODE/IPTOS MODE
По умолчанию: DSCP MODE
Функция: Если выбран вариант TOS/DIFF, для этого параметра нужно выбрать IP TOS или DSCP. Режим DSCP указывает режим сопоставления очереди и приоритетов DSCP, а режим IP TOS указывает режим сопоставления очереди и приоритетов IP TOS.
2. Настройте весовой коэффициент очереди, как показано на следующем рисунке.

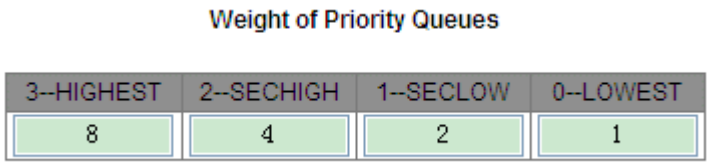

Рисунок 124 Настройка весового коэффициента очереди

{3-HIGHEST, 2-SECHIGH, 1-SECLOW, 0-LOWEST}
Диапазон: {1~55, 1~55, 1~55, 1~55}
По умолчанию: {8, 4, 2, 1}
Функция: Настройка весового коэффициента очереди по следующим правилам:
Вес очереди 3 > 2 x Вес очереди 2, Вес очереди 2 > 2 x Вес очереди 1,
Вес очереди 1 > 2 x Вес очереди 0
3. Настройте режим сопоставления приоритетов портов QoS, как показано на следующем рисунке.

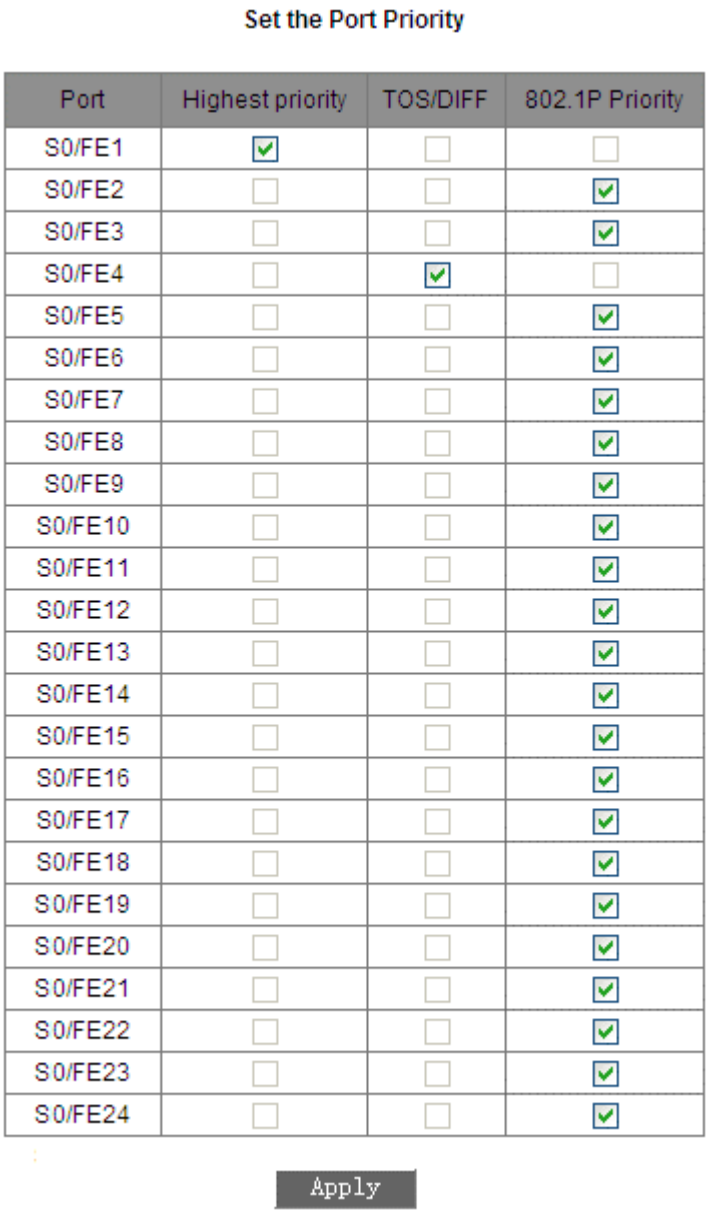

Рисунок 125 Настройка режима сопоставления приоритетов портов QoS

Set the Port Priority
Варианты: Highest priority/TOS/DIFF/802.1P Priority
По умолчанию: 802.1P Priority
Функция: Настройка режима сопоставления приоритетов портов.
Описание: Для каждого порта можно выбрать только один режим сопоставления приоритетов.
4. Настройте сопоставление приоритета 802.1p и очереди
Щелкните <802.1p Priority> на рисунке 123. Появится следующая страница.

802.1P Priority 0~7

Priority	Queue
0	0
1	0
2	1
3	1
4	2
5	2
6	3
7	3

Queue: 0--LOWEST, 1--SECLOW, 2--SECHIGH, 3--HIGHEST

Apply Back

Рисунок 126 Сопоставление приоритета 802.1p и очереди

802.1P Priority
Состав: {Priority, Queue}
Диапазон: {0~7, 0~3}
По умолчанию: Приоритеты 0 и 1 сопоставлены очереди 0; приоритеты 2 и 3 сопоставлены очереди 1. Приоритеты 4 и 5 сопоставлены очереди 2; приоритеты 6 и 7 сопоставлены очереди 3.
Функция: Настройка сопоставления между приоритетом 802.1p и очередью.
5. Настройте сопоставление приоритета IP TOS и очереди.
Щелкните <IP TOS Priority> на рисунке 123, чтобы настроить сопоставление приоритета IP TOS и очереди, как показано на следующем рисунке.

IP TOS Priority 0~7

Priority	Queue
IP TOS 0	0
IP TOS 1	0
IP TOS 2	0
IP TOS 3	0
IP TOS 4	0
IP TOS 5	0
IP TOS 6	0
IP TOS 7	0

Queue: 0--LOWEST, 1--SECLOW, 2--SECHIGH, 3--HIGHEST

Apply Back

Рисунок 127 Настройка сопоставления приоритета IP TOS и очереди.

IP TOS Priority
Состав: {Priority, Queue}

Диапазон: {0~7, 0~3}
По умолчанию: Приоритет от 0 до 7 сопоставляется очереди 0.
Функция: Настройка сопоставления между приоритетом IP TOS и очередью.
6. Настройте сопоставление приоритета DSCP и очереди.
Щелкните <DSCP Priority> на рисунке 123, чтобы настроить сопоставление приоритета DSCP и очереди, как показано на следующем рисунке.

DSCP Priority 0~63

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

Queue: 0--LOWEST, 1--SECLOW, 2--SECHIGH, 3--HIGHEST

Apply Back

Рисунок 128 Сопоставление приоритета DSCP и очереди

DSCP Priority
Состав: {DSCP, Qos Queue}
Диапазон: {0~63, 0~3}
По умолчанию: Приоритет от 0 до 63 сопоставляется очереди 0.
Функция: Настройка сопоставления между приоритетом DSCP и очередью.

6.17.5 Пример типовой конфигурации

Далее используется SICOM3024P в качестве примера для описания настройки QoS .
Как показано на рисунке ниже, порты 1, 2, 3 и 4 пересылают пакеты на порт 5.
Режим на основе порта настроен на порт 1. Приоритет по умолчанию для порта 1 равен 6. Пакеты от порта сопоставляются с очередью 3. Приоритет 802.1p, передаваемый пакетами из порта 2, равен 2 и сопоставляется с очередью 1
. Приоритет 802.1p, передаваемый пакетами из порта 3, равен 4 и сопоставляется с очередью 2. Приоритет DSCP, передаваемый пакетами из порта 4, равен 6 и сопоставляется с очередью 3. Порт 5 использует режим планирования WRR.

Этапы настройки:
1. Выберите WRR для режима QoS и сохраните значения по умолчанию для весового коэффициента очереди WRR, как показано на рисунках 118 и 119.

2. Настройте сопоставление очереди с высшим приоритетом на порту 1, 802.1p на портах 2 и 3, а также DIFF на порту 4, как показано на рисунке 120.

3. Настройте сопоставление приоритетов 802.1p 6, 2 и 4 с очередями 3, 1 и 2 соответственно, как показано на рисунке 121.

4. Настройте сопоставление приоритета DSCP 6 с очередью 3, как показано на рисунке 122.

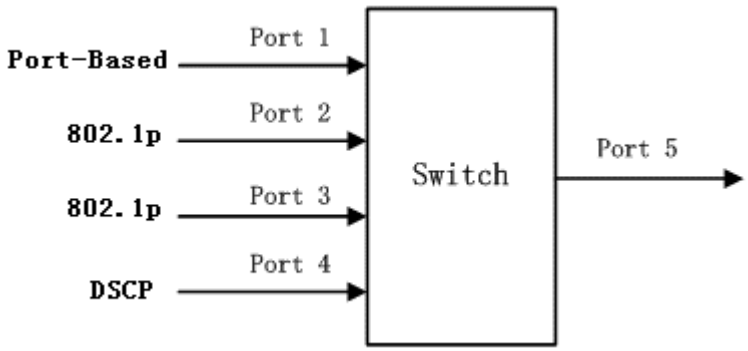

Рисунок 129 Пример настройки QoS

Пакеты, полученные через порт 1 и порт 4, помещаются в очередь 3; пакеты, полученные через порт 2, помещаются в очередь 1; пакеты, полученные через порт 3, помещаются в очередь 2. Согласно сопоставлению между очередью и весом, вес очереди 1 равен 2, вес очереди 2 равен 4, а вес очереди 3 равен 8. В результате пакеты в очереди 1 получают пропускную способность 2/(2+4+8), пакеты в очереди 2 — 4/(2+4+8), а пакеты в очереди 3 — 8/(2+4+8). Пакеты, полученные через порт 1 и порт 4, помещаются в очередь 3 и пересылаются в соответствии с механизмом FIFO. Общая доля пропускной способности порта 1 и порта 4 составляет 8/(2+4+8).

6.18 Время старения MAC-адреса

6.18.1 Обзор

Порты коммутатора могут автоматически узнавать адреса. Коммутатор добавляет адреса источников (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, в 1-2 раза превышающего время устаревания, коммутатор удаляет запись MAC-адреса из таблицы динамических адресов пересылки. Статические MAC-адреса не включают понятие времени устаревания.

6.18.2 Настройка через веб-интерфейс

Настройте время старения MAC-адреса, как показано на рисунке ниже.

Рисунок 130 Время старения MAC-адреса

MAC Aging Time
Диапазон: 15~3600 секунд
По умолчанию: 300 секунд
Описание: При необходимости можно настроить время старения.

6.19 LLDP

6.19.1 Обзор

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

6.19.2 Настройка через веб-интерфейс

1. Включите LLDP, как показано на рисунке ниже.

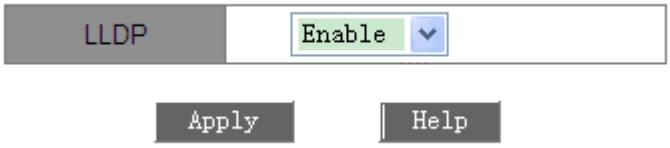

Рисунок 131 Включение LLDP

LLDP
Варианты: Enable/Disable
По умолчанию: Enable
Функция: Включение/отключение протокола LLDP
Пояснение: Если LLDP включен, коммутатор будет отправлять сообщения LLDP своим соседним устройствам, одновременно получая и обрабатывая сообщения LLDP от соседних устройств. Если LLDP отключен, коммутатор не отправляет и не обрабатывает сообщения LLDP.
2. Просмотрите информацию о соединениях LLDP, как показано на рисунке ниже.

LLDP Information

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

Рисунок 132 Информация LLDP

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

CAUTION	**Предупреждение:** Для отображения информации LLDP необходимо включить LLDP на двух подключенных устройствах. LLDP — это протокол обнаружения канального уровня, включенный по умолчанию.

6.20 SNTP

6.20.1 Обзор

Простой протокол сетевого времени (SNTP) синхронизирует время между сервером и клиентом путем запросов и ответов. Как клиент коммутатор синхронизирует время с сервером по пакетам сервера. Для одного коммутатора можно не более четырех серверов SNTP, но активным может быть только один. Коммутатор может также выступать в качестве сервера SNTP для обеспечения синхронизации времени для клиентов.
Клиент SNTP отправляет запрос на каждый сервер один за другим через одноадресную рассылку. Сервер, который отвечает первым, находится в активном состоянии. Остальные серверы находятся в неактивном состоянии.

CAUTION	**Предупреждение:** > Для синхронизации времени по SNTP необходим активный SNTP-сервер. > Вся информация о времени, передаваемая в протоколе SNTP, является стандартной информацией о времени часового пояса 0.

6.20.2 Настройка через веб-интерфейс

1. Включите SNTP. Выберите сервер и задайте соответствующие параметры, как показано на рисунке ниже.

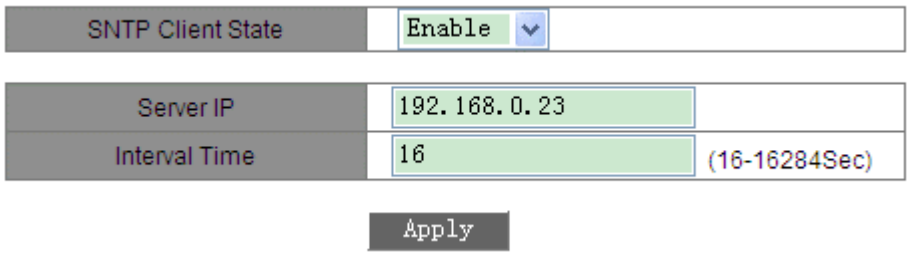

Рисунок 133 Настройка SNTP (SICOM3024P/SICOM3024)

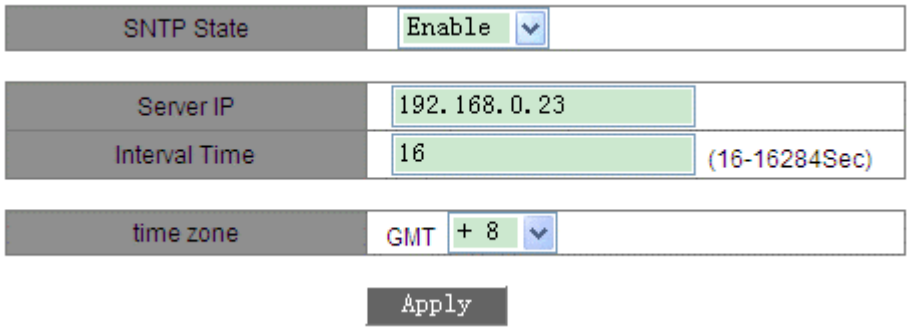

Рисунок 134 Настройка SNTP (SICOM3048)

SNTP Client State
Варианты: Enable/Disable
По умолчанию: Disable
Функция: Включение/выключение SNTP.
Server IP
Формат: A.B.C.D
Функция: Настройка IP-адреса сервера SNTP. Клиент синхронизирует время с сервера на основе пакетов, отправленных сервером.
Interval Time
Диапазон: 16~16284 с
Функция: Настройка интервала для отправки запросов синхронизации от клиента SNTP серверу.
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.
2. Выберите режим синхронизации между клиентом и сервером, как показано на следующем рисунке.

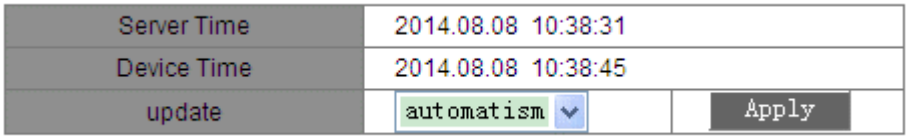

Рисунок 135 Режим синхронизации времени

Server Time
Функция: Отображение последнего времени устройства, полученного с сервера.
Device Time
Функция: Отображение местного времени устройства.
update
Варианты: automatism/manual
По умолчанию: automatism
Функция: Выбор режима синхронизации между клиентом и сервером.
3. Просмотрите конфигурацию SNTP, как показано на рисунке ниже. Можно установить флажок сервера SNTP и щелкнуть <Delete>, чтобы удалить его.

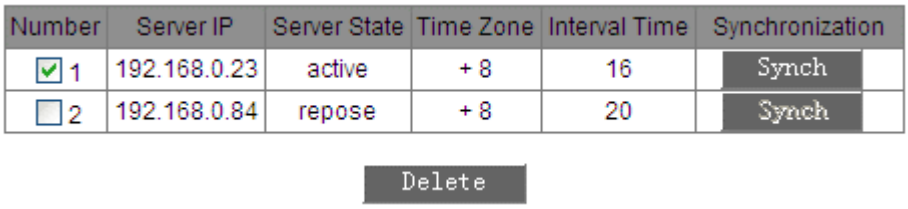

Рисунок 136 Настройка SNTP

Server State
Варианты: active/repose
Описание: Активный сервер предоставляет клиенту время SNTP. В данный момент в активном состоянии может находиться только один сервер.
Synchronization
Для синхронизации времени вручную щелкните <Synch>.
4. Настройте коммутатор как сервер SNTP, как показано на следующем рисунке.

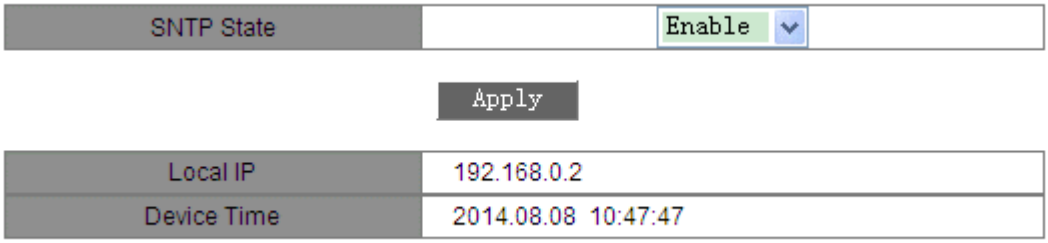

Рисунок 137 Настройка коммутатора как сервера SNTP (SICOM3024P/SICOM3024)

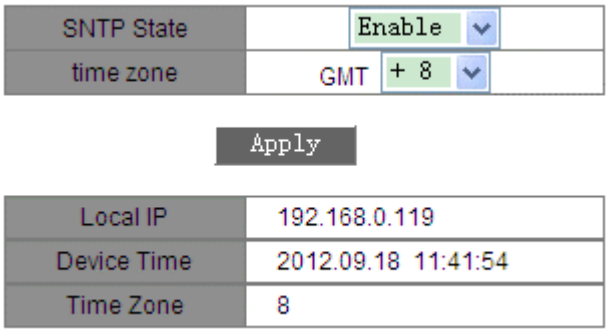

Рисунок 138 Настройка коммутатора как сервера SNTP (SICOM3048)

SNTP State
Варианты: Enable/Disable
По умолчанию: Disable Функция: Включение/выключение функции 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 и -12
По умолчанию: +8
Функция: Выбор часового пояса сервера.

6.21 Изоляция портов

6.21.1 Обзор

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

NOTE	**Примечание:** > Порты группы изоляции могут быть только портами одного и того же коммутатора. > После настройки группы изоляции невозможен обмен пакетами только между портами группы изоляции, обмен данными между порами внутри группы изоляции и портами вне группы не затронут.

6.21.2 Настройка через веб-интерфейс

Включите изоляцию портов, как показано на рисунке 139.

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

Рисунок 139 Настройка изоляции портов

Isolate Enable
Варианты: Enable/Disable
По умолчанию: Disable
Функция: Включение или выключение изоляции портов.

NOTE	**Примечание:** Устройство поддерживает только одну группу изоляции, что означает, что порты с включенной изоляцией портов не могут обмениваться информацией друг с другом, в то время как связь между портами с включенной изоляцией портов и портами с отключенной изоляцией портов не будет осуществляться.

6.21.3 Пример типовой конфигурации

Требования к сети:
Подключите ПК1, ПК2 и ПК3 к портам Ethernet 1, 2 и 3 коммутатора, а порт 4 подключите к внешней сети. ПК1, ПК2 и ПК3 не могут обмениваться данными друг с другом, но имеют доступ к внешней сети, как показано на рисунке 140.

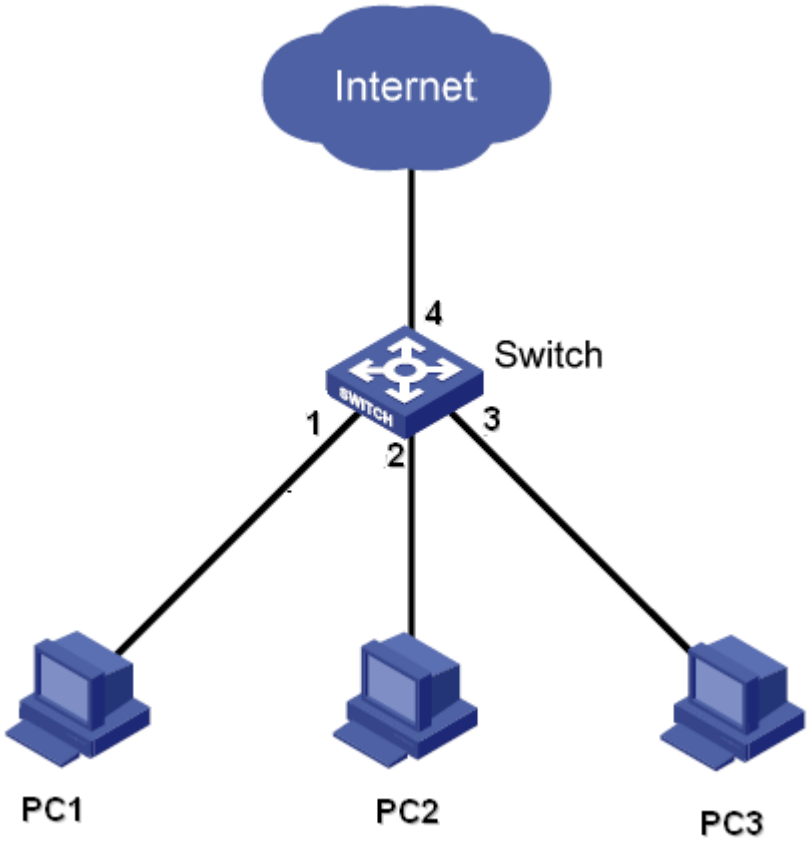

Рисунок 140 Экземпляр конфигурации изоляции портов

Конкретная конфигурация:
Добавьте порты 1, 2 и 3 в группу изоляции, чтобы изолировать ПК1, ПК2 и ПК3, как показано на рисунке 139.

6.22 Аварийная сигнализация

6.22.1 Обзор

Коммутаторы этой серии поддерживают следующие типы аварийной сигнализации:
Аварийная сигнализация по электропитанию: Если функция включена, то для отдельного источника питания будет генерироваться аварийный сигнал.
Аварийная сигнализация по температуре: Если функция включена, то сигнал тревоги будет генерироваться, когда температура равна или ниже нижнего предела или равна или выше верхнего предела.
Аварийная сигнализация по конфликту IP/MAC: Если функция включена, то будет генерироваться аварийный сигнал при возникновении конфликта IP/MAC-адресов.
Аварийная сигнализация по порту: Если функция включена, то будет генерироваться аварийный сигнал для порта в состоянии Link Down.

Аварийная сигнализация по кольцу: Если функция включена, то будет генерироваться аварийный сигнал для разомкнутого кольца.

CAUTION	**Предупреждение:** > Функцию аварийной сигнализации по кольцу поддерживают только Master в DT-Ring и корневое устройство DRP.

	> SICOM3024P поддерживает сигнализацию по питанию, сигнализацию по температуре, сигнализацию конфликта IP/MAC адресов, сигнализацию порта и сигнализацию по кольцу. > SICOM3048 поддерживает сигнализацию конфликта IP/MAC адресов, сигнализацию порта и сигнализацию по кольцу. > SICOM3024 поддерживает сигнализацию по питанию, сигнализацию конфликта IP/MAC адресов, сигнализацию порта и сигнализацию по кольцу.

6.22.2 Настройка через веб-интерфейс

1. Задайте параметры сигнализации, как показано на рисунке ниже.

IP, MAC Conflict

Alarm Name	Enable Alarm	Alarm Time
IP, MAC Conflict	☑	300 (180~600sec.)

Power Alarm

Alarm Name	Enable Alarm
Power Alarm	☑

Temperature Alarm

Alarm Name	Enable Alarm	Temperature Alarm Bound
Temperature Alarm	Enable	T-High + 80 ~ T-Low - 30

Port Alarm

Port	Alarm Status	Port	Alarm Status	Port	Alarm Status	Port	Alarm Status
S1/FE1	☑	S1/FE2	☑	S1/FE3	☑	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	Enable Alarm
1	☑
2	☑

DRP Alarm

DRP ID	Enable Alarm
1	☑
2	☑

Apply

Рисунок 141 Настройка аварийной сигнализация

IP, MAC Conflict
Варианты: выбрать/отменить выбор
По умолчанию: выбрать
Функция: Включение или выключение аварийной сигнализации по конфликту IP/MAC.
Alarm Time
Диапазон: 180~600 с
По умолчанию: 300 с
Функция: Настройка интервала времени для обнаружения конфликтов IP/MAC.
Power Alarm
Варианты: выбрать/отменить выбор
По умолчанию: выбрать
Функция: Включение или выключение аварийной сигнализации по питанию.
Temperature Alarm (Alarm Enable, T-High~T-Low)
Диапазон: {Enable/Disable, +150C~-55C}
По умолчанию: {Disable, +80C~-30C}
Функция: Включение или выключение аварийной сигнализации по температуре и задание верхнего и нижнего предельных значений.
Port Alarm
Варианты: выбрать/отменить выбор
По умолчанию: отменить выбор
Функция: Включение или выключение аварийной сигнализации по порту.
DT-RING/DRP Alarm
Варианты: выбрать/отменить выбор
По умолчанию: отменить выбор
Функция: Включение или выключение аварийной сигнализации DT-Ring/DRP.
2. После включения функции аварийной сигнализации предоставляется следующая информация:

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

Рисунок 142 Информация аварийной сигнализации

power
Варианты: Normal/WARN
Описание: После включения аварийной сигнализации по питанию Normal отображается для двух входов питания, а WARN отображается для одного входа питания.
temperature
Варианты: NONE/HIGH/LOW
Описание: Когда температура коммутатора равна верхнему пределу или превышает его, отображается HIGH; когда температура коммутатора равна или ниже нижнего предела, отображается LOW; в иных случаях отображается Normal.
IP/MAC Alarm
Варианты: Normal/Alarm
Описание: Когда возникает конфликт IP/MAC, отображается Alarm, в противном случае отображается Normal.
Port Alarm
Варианты: Link up/ Link down
Описание: После включения сигнализации для порта, подключенного правильно, отображается Link Up. Link Down отображается для отключенного или подключенного ненормально порта.
DT-RING/DRP Alarm
Варианты DT-Ring: Ring Open/Ring Close
Варианты DRP: Normal/Alarm
Описание: После включения сигнализации для разомкнутого кольца отображается Ring Open/Alarm, а для замкнутого кольца – Close/Normal.

6.23 Сигнализация по трафику порта

6.23.1 Обзор

С функцией сигнализации по трафику порта коммутатор генерирует сигнал тревоги, если скорость трафика порта превышает указанный порог или возникает ошибка CRC.

CAUTION	**Предупреждение:** > Функция сигнализации по трафику действует для порта. Аварийный сигнал генерируется только если функция включена на порту. > Функция сигнализации по трафику учитывает направление. Входящий и исходящий трафик соответствуют разным сигналам. > При возникновении ошибки CRC генерируется сигнал ошибки CRC.

6.23.2 Настройка через веб-интерфейс

1. Настройте сигнализацию по трафику порта, как показано на рисунке ниже.

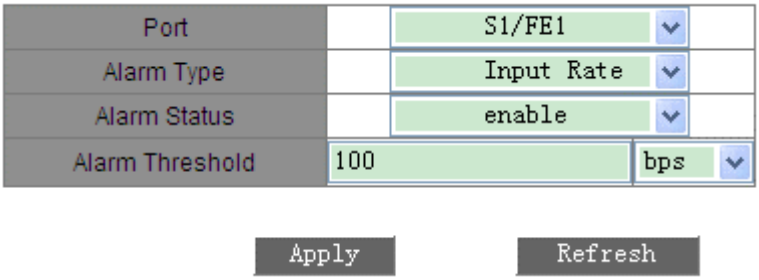

Рисунок 143 Настройка сигнализации по трафику порта

Port
Варианты: все порты коммутатора.
Функция: Выбор порта для сигнализации по трафику порта.
Alarm Type
Варианты: Input Rate/Output Rate/CRC Error
Функция: Настройка типа сигнализации по трафику порта.
Alarm Status
Варианты: Enable/Disable
По умолчанию: Disable
Функция: Включение или выключение типа сигнализации.
Alarm Threshold
Диапазон: 1~1000000000 бит/с или 1~1000000 Кбит/с
Функция: Настройка порога сигнализации по трафику порта.
2. Просмотрите информацию сигнализации по трафику порта, как показано на рисунке ниже.

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	-

Рисунок 144 Информация сигнализации по трафику порта

6.24 Настройка и запрос GMRP

6.24.1 GARP

Протокол GARP (Generic Attribute Registration Protocol) используется для распространения, регистрации и отмены определенной информации (VLAN, адрес многоадресной рассылки) между коммутаторами в одной сети. Приложения GARP включают в себя GVRP и GMRP.
При использовании GARP информация о конфигурации участника GARP будет распространяться по всей сети коммутатора. Устройства, поддерживающие GARP, передают друг другу инструкции о регистрации или отмене тех или иных настроек путём отправки соответствующих сообщений join/leave. Участник также регистрирует или отменяет информацию о конфигурации других участников на основе сообщений join/leave, отправленных другими участниками.
GARP включает в себя три типа сообщений: Join, Leave и LeaveAll.
Когда прикладной объект GARP хочет зарегистрировать свою собственную информацию на других коммутаторах, объект отправляет сообщение Join. Сообщения Join делятся на два типа: JoinEmpty и JoinIn. Сообщение JoinIn отправляется для объявления зарегистрированного атрибута, а сообщение JoinEmpty отправляется для объявления еще не зарегистрированного атрибута.
Когда прикладной объект GARP хочет удалить свою собственную информацию на других коммутаторах, объект отправляет сообщение Leave.
После запуска объекта GARP он запускает таймер LeaveAll. Когда период таймера истекает, объект отправляет сообщение LeaveAll.

Примечание:
Прикладной объект указывает порт с поддержкой GARP.

Таймеры GARP – это таймер Hold, таймер Join, таймер Leave и таймер LeaveAll.
Hold Timer: При получении регистрационного сообщения объект GARP не сразу отправляет сообщение о присоединении, а запускает таймер Hold. Когда период таймера истекает, объект отправляет все регистрационные сообщения, полученные в течение предшествующего периода, в одном сообщении о присоединении, сокращая отправку пакетов для повышения стабильности сети.
Join Timer: Чтобы гарантировать получение сообщений Join другими прикладными объектами, прикладной объект GARP запускает таймер Join после отправки сообщения Join. Если сообщение JoinIn не получено до истечения периода таймера Join, объект снова отправляет сообщение Join. Если сообщение JoinIn получено до истечения периода таймера Join, объект не отправляет второе сообщение Join.
Leave Timer: Когда прикладной объект GARP хочет удалить информацию об атрибуте, объект отправляет

сообщение Leave. Объект, получивший сообщение, запускает таймер Leave. Если сообщение Join не получено до истечения периода таймера, объект, получивший сообщение, удаляет информацию об атрибуте.
LeaveAll Timer: После запуска объекта GARP он запускает таймер LeaveAll. Когда период таймера истекает, объект отправляет сообщение LeaveAll, чтобы другие прикладные объекты GARP перерегистрировали все атрибуты. Затем объект снова запускает таймер LeaveAll для нового цикла.

6.24.2 GMRP

GARP Multicast Registration Protocol (GMRP) – это протокол регистрации многоадресной передачи, основанный на GARP. Он используется для поддержки регистрационной информации многоадресной рассылки коммутаторов. Все коммутаторы с поддержкой GMRP могут получать информацию о регистрации многоадресной рассылки от других коммутаторов, динамически обновлять информацию о регистрации локальной многоадресной рассылки и распространять информацию о регистрации локальной многоадресной рассылки на другие коммутаторы. Этот механизм обмена информацией обеспечивает согласованность многоадресной информации, поддерживаемой всеми коммутаторами с поддержкой GMRP в сети.
Если коммутатор или терминал хочет присоединиться к группе многоадресной рассылки или выйти из нее, порт с поддержкой GMRP передает информацию на все порты в той же VLAN.

6.24.3 Описание

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

6.24.4 Настройка через веб-интерфейс

Включите глобальный протокол GMRP, как показано на рисунке ниже.

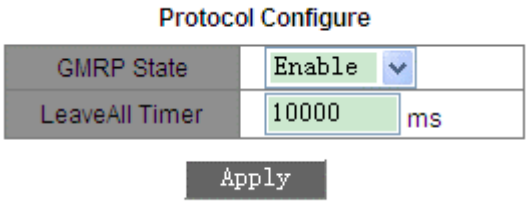

Рисунок 145 Глобальная настройка GMRP

GMRP State
Варианты: Enable/Disable
По умолчанию: Disable
Функция: Включение или выключение глобальной функции GMRP. Функцию и IGMP Snooping нельзя включить одновременно.
LeaveAll Timer
Диапазон: 100 мс~327600 мс
По умолчанию: 10000 мс
Функция: Настройка интервала времени для отправки сообщений LeaveAll. Значение должно быть кратно 100.

Описание: Если таймеры LeaveAll разных устройств истекают одновременно, одновременно будет отправлено несколько сообщений LeaveAll, что приведет к увеличению количества ненужных пакетов. Чтобы предотвратить эту проблему, фактический интервал таймера LeaveAll представляет собой случайное значение между указанным значением и указанным значением, умноженным на 1,5.
2. Настройте функцию GMPR на каждом порту, как показано на рисунке ниже.

Port Configure

Port	GMRP Enable	Agent Enable	Hold Timer	Join Timer	Leave Timer
S1/FE1	Enable	Enable	100 ms	500 ms	3000 ms
S1/FE2	Enable	Disable	100 ms	500 ms	3000 ms
S1/FE3	Enable	Disable	100 ms	500 ms	3000 ms
S1/FE4	Disable	Disable	100 ms	500 ms	3000 ms
S1/FE5	Disable	Disable	100 ms	500 ms	3000 ms
S1/FE6	Disable	Disable	100 ms	500 ms	3000 ms
S1/FE7	Disable	Disable	100 ms	500 ms	3000 ms
S1/FE8	Disable	Disable	100 ms	500 ms	3000 ms
S4/GE1	Disable	Disable	100 ms	500 ms	3000 ms
S4/GE2	Disable	Disable	100 ms	500 ms	3000 ms
S4/GE3	Disable	Disable	100 ms	500 ms	3000 ms
S4/GE4	Disable	Disable	100 ms	500 ms	3000 ms

Apply

Рисунок 146 Настройка функции GMPR на порту

GMRP Enable
Варианты: Enable/Disable
По умолчанию: Disable
Функция: Включение или выключение GMRP на порту.
Agent Enable
Варианты: Enable/Disable
По умолчанию: Disable
Функция: Включение или выключение функции агента GMRP на порту.

CAUTION	**Предупреждение:** > Порт агента не может распространять запись агента. > Чтобы включить функцию агента GMRP на порту, необходимо сначала включить функцию GMRP.

Hold Timer
Диапазон: 100 мс~327600 мс
По умолчанию: 100 мс
Описание: Значение должно быть кратно 100. Лучше установить одинаковое время таймеров Hold на всех портах с поддержкой GMRP.
Join Timer
Диапазон: 100 мс~327600 мс
По умолчанию: 500 мс
Описание: Значение должно быть кратно 100. Лучше установить одинаковое время таймеров Join на всех

портах с поддержкой GMRP.

Leave Timer
Диапазон: 100 мс~327600 мс
По умолчанию: 3000 мс
Описание: Значение должно быть кратно 100. Лучше установить одинаковое время таймеров Leave на всех портах с поддержкой GMRP.

3. Добавьте запись агента GMRP, как показано на рисунке ниже.

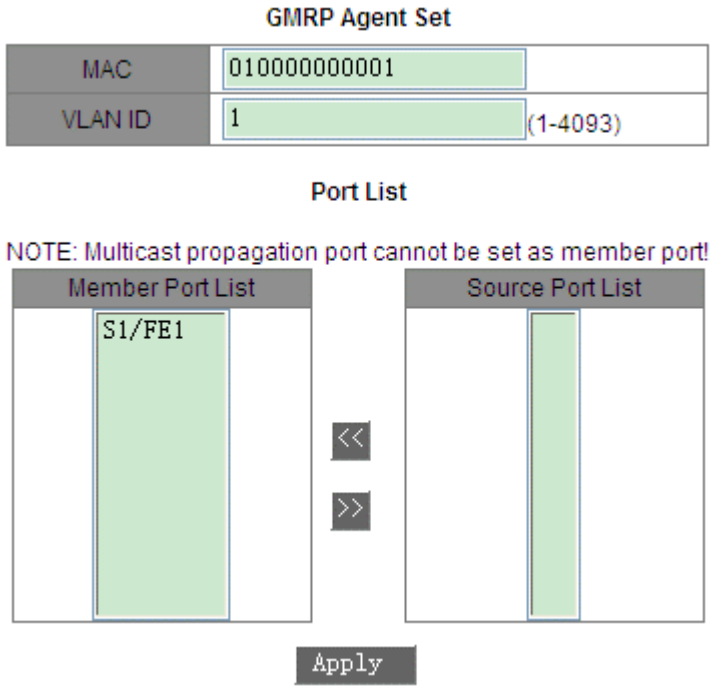

Рисунок 147 Настройка записи агента GMRP

MAC
Формат: HHHHHHHHHHHH (H – шестнадцатеричное число.)
Функция: Настройка MAC-адреса многоадресной группы. Младший бит в первом байте равен 1.
VLAN ID
Варианты: все созданные номера VLAN
Функция: Настройка VLAN ID для записи агента GMRP.
Описание: Запись агента GMRP может быть перенаправлена только из порта распространения с идентификатором VLAN, совпадающим с идентификатором VLAN этой записи.
Member Port List
Выбор порта-участника для записи агента. Порт можно выбрать только из числа портов с поддержкой агента GMRP.
Source Port List
Варианты: все порты с поддержкой агента GMRP
4. Просмотрите, измените или удалите запись агента GMRP, как показано на рисунке ниже.

GMRP Agent List

Index	MAC	VLAN ID	Member Port
1	01-00-00-00-00-01	1	S1/FE1
2	01-00-00-00-00-02	2	S1/FE1

Add Delete Modify

Рисунок 148 Действия с записью агента GMRP

Запись агента GMRP содержит MAC-адрес, VLAN ID и порт участник. Чтобы удалить запись, выберите запись и щелкните <Delete>. Чтобы изменить запись, выберите запись и щелкните <Modify>.
5. Отображаются участники многоадресной рассылки этой записи агента на подключенном соседнем устройстве, как показано на рисунке ниже.
Должны быть соблюдены следующие условия.
> Функция GMRP включена на взаимосвязанных устройствах.
Два порта, которые соединяют устройства, должны быть портами распространения, а VLAN ID 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

Рисунок 149 Динамическая таблица многоадресной рассылки GMRP

GMRP Dynamic Multicast List
Состав: {Index, Multicast MAC, VLAN ID, Member Port}
Функция: Просмотр динамических записей многоадресной рассылки GMRP.

6.24.5 Пример типовой конфигурации

Как показано на рисунке ниже, коммутатор A и коммутатор B соединены через порты 2. Порт 1 коммутатора A настроен как порт-агент и содержит две записи многоадресной рассылки:
MAC-адрес: 01-00-00-00-00-01, VLAN: 1
MAC-адрес: 01-00-00-00-00-02, VLAN: 2
После настройки различных атрибутов VLAN на портах наблюдайте за динамической регистрацией между коммутаторами и обновлением информации о многоадресной рассылке.

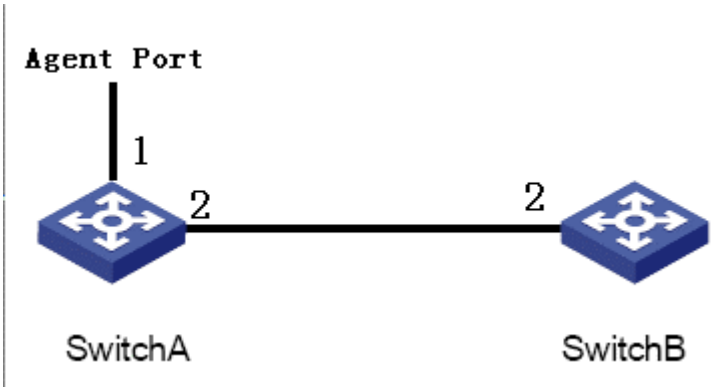

Рисунок 150 Сеть GMRP

Конфигурация коммутатора A:
1. Включите глобальную функцию GMRP на коммутаторе A; установите для таймера LeaveAll значение по умолчанию, как показано на рисунке 145.
2. Включите функцию GMRP и функцию агента на порту 1; включите только функцию GMRP на порту 2;

установите таймеры на значения по умолчанию, как показано на рисунке 146.
3. Настройте запись агента многоадресной рассылки. Установите <MACaddress, VLAN ID, Member port> <01-00-00-00-00-01, 1, 1> и <01-00-00-00-00-02, 2, 1>, как показано на рисунке 147.

Конфигурация коммутатора B:

1. Включите глобальную функцию GMRP на коммутаторе B; установите для таймера LeaveAll значение по умолчанию, как показано на рисунке 145.
2. Включите функцию GMRP на порту 2; установите таймеры на значения по умолчанию, как показано на рисунке 146.

В таблице перечислены динамически полученные записи многоадресной рассылки GMRP на коммутаторе B.

Таблица 8 Динамические записи многоадресной рассылки

Атрибуты порта 2 коммутатора A	Атрибуты порта 2 коммутатора B	Записи многоадресной рассылки, полученные на коммутаторе B
Untag1	Untag1	MAC: 01-00-00-00-00-01 VLAN ID: 1 Порт-участник 2
Untag2	Untag2	MAC: 01-00-00-00-00-02 VLAN ID: 2 Порт-участник 2
Untag1	Untag2	MAC: 01-00-00-00-00-01 VLAN ID: 2 Порт-участник 2

6.25 RMON

6.25.1 Обзор

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

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

6.25.2 Группы RMON

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

> Группа статистики

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

значение.
> Группа истории
Группа истории требует, чтобы система периодически отбирала все виды трафика на портах и сохраняла значения выборки в таблице записей истории для дальнейшего запроса устройством управления. Группа истории подсчитывает статистические значения всех видов данных в интервале выборки.
> Группа событий
Группа событий используется для определения индексов событий и методов обработки событий. События, определенные в группе событий, используются в элементе конфигурации группы тревог. Событие запускается, когда контролируемое устройство соответствует условию тревоги. События обрабатываются следующими способами:
Log: регистрирует события и соответствующую информацию в таблице журнала событий.
Trap: отправляет сообщение Trap в NMS и информирует NMS о событии.
Trap: отправляет сообщение Trap в NMS и информирует NMS о событии.
None: указывает на отсутствие действий.
> Группа тревоги
Управление сигналами тревоги RMON может отслеживать указанные переменные аварийных сигналов тревоги. После того, как записи сигналов тревоги определены, система получит значения контролируемых переменных сигналов тревоги за определенный период. Когда значение переменной тревоги больше или равно верхнему пределу, инициируется событие роста значения. Когда значение переменной тревоги меньше или равно нижнему пределу, инициируется событие падения значения. Сигналы тревоги будут обрабатываться в соответствии с определением события.

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

6.25.3 Настройка через веб-интерфейс

1. Настройте таблицу статистики, как показано на следующем рисунке.

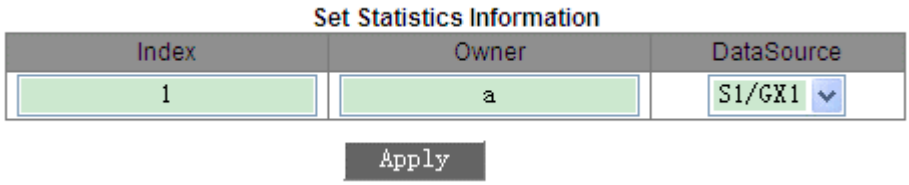

Рисунок 151 Статистика RMON

Index
Диапазон: 1~65535
Функция: Настройка номера записи статистики.
Owner
Диапазон: 1~32 символа
Функция: Настройка имени записи статистики.
Data Source
Функция: Выбор порта для сбора статистики.
2. Настройте таблицу истории, как показано на следующем рисунке.

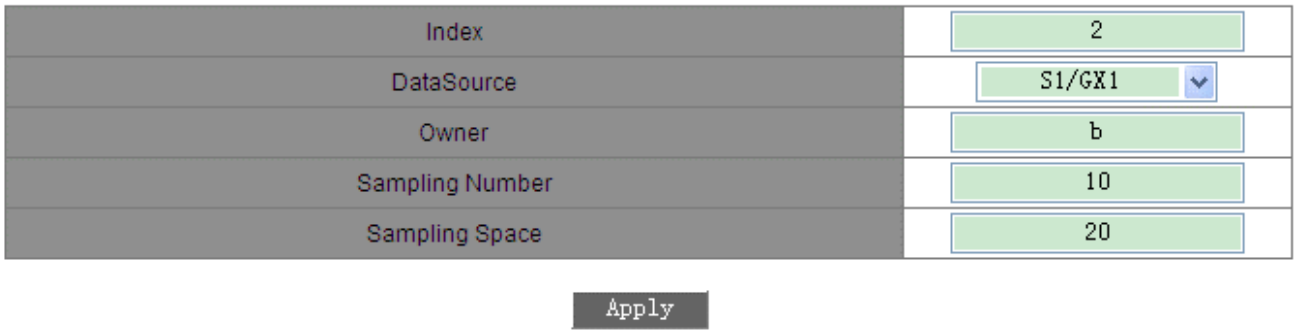

Рисунок 152 Таблица истории RMON

Index
Диапазон: 1~65535
Функция: Настройка номера записи истории.
Data Source
Функция: Выбор порта для сбора информации.
Owner
Диапазон: 1~32 символа
Функция: Настройка имени записи истории.
Sampling Number
Диапазон: 1~65535
Функция: Настройка количества выборок для порта.
Sampling Space
Диапазон: 1~3600 с
Функция: Настройка периода выборки для порта.

3. Настройте таблицу событий, как показано на следующем рисунке.

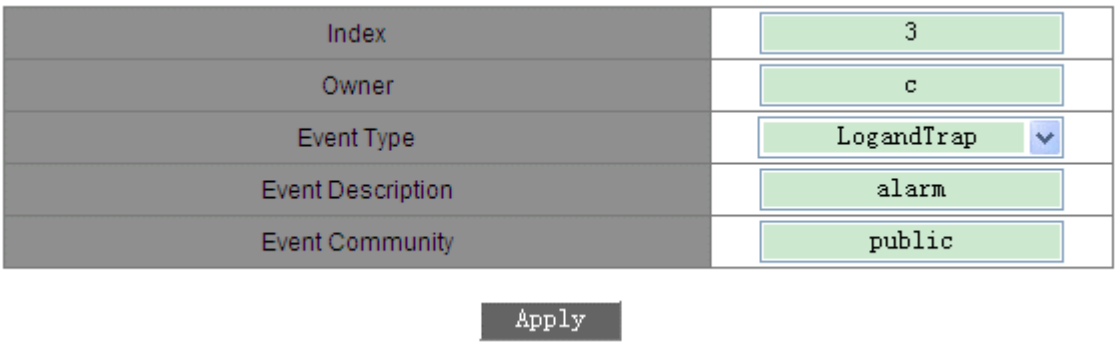

Рисунок 153 Таблица событий RMON

Index
Диапазон: 1~65535
Функция: Настройка порядкового номера записи событий.
Owner
Диапазон: 1~32 символа
Функция: Настройка имени записи события.
Event Type
Варианты: NONE/LOG/Snmp-Trap/Log and Trap
По умолчанию: NONE
Функция: Настройка типа события для сигналов тревоги, то есть режима обработки сигналов тревоги.
Event Description
Диапазон: 1~127 символов

Функция: Описание события.

Event Community

Диапазон: 1~127 символов

Функция: Задание имени сообщества для отправки события trap. Значение должно совпадать со значением в SNMP.

4. Настройте таблицу сигнализации, как показано на следующих рисунках.

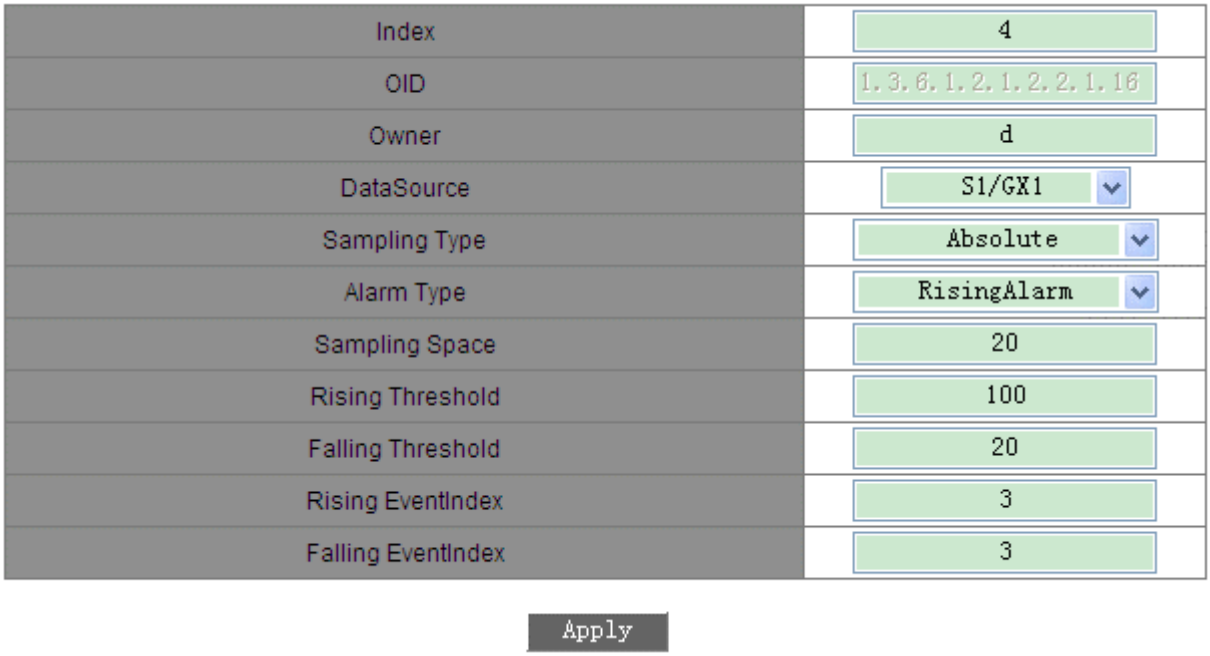

Рисунок 154 Таблица сигнализации RMON

Index

Диапазон: 1~65535

Функция: Настройка номера записи сигнала тревоги.

OID

Указание OID текущего узла MIB.

Owner

Диапазон: 1~32 символа

Функция: Настройка имени записи сигнала тревоги.

Data Source

Функция: Выбор порта для отслеживания информации.

Sampling Type

Варианты: Absolute/Delta

По умолчанию: Absolute

Функция: Absolute указывает на выборку на основе абсолютного значения. Значение переменной извлекается напрямую, когда приближается конец периода выборки. Delta указывает выборку на основе изменения значения. Значение изменения переменной за период выборки извлекается, когда приближается конец периода.

Alarm Type

Варианты: RisingAlarm/FallingAlarm/RisOrFallAlarm

По умолчанию: RisingAlarm

Функция: Выбор типа сигнала тревоги, включая сигнал по переднему фронту, сигнал по заднему фронту, а также сигнал по переднему и заднему фронту.

Sampling Space

Диапазон: 1~65535

Функция: Настройка периода выборки. Значение должно совпадать со значением в таблице истории.

Rising Threshold
Диапазон: 0~65535
Функция: Настройка порогового значения по нарастанию. Когда значение выборки превышает порог повышения и типом тревоги является RisingAlarm или RisOrFallAlarm, срабатывает тревога и активируется индекс событий повышения.
Falling Threshold
Диапазон: 0~65535
Функция: Настройка порогового значения по понижению. Когда значение выборки ниже порога понижения и типом тревоги является FallingAlarm или RisOrFallAlarm, срабатывает тревога и активируется индекс событий понижения.
Rising Event Index
Диапазон: 0~65535
Функция: Настройте индекс события нарастания, то есть режим обработки сигналов тревоги по нарастанию.
Falling Event Index
Функция: Настройте индекс события убывания, то есть режим обработки сигналов тревоги по убыванию.

6.26 Запрос журнала

6.26.1 Обзор

Функция журнала записывает информацию о работе коммутатора, помогая администратору читать и управлять пакетами журналов и обнаруживать неисправности.
Журнал работы охватывает:
Сигнализацию по питанию, сигнализацию по температуре, сигнализацию конфликта IP/MAC адресов, сигнализацию порта, сигнализацию DT-Ring и сигнализацию по трафику порта
Широковещательный шторм
Перезагрузку

6.26.2 Описание

Жрнал содержит максимум 1024 записи. Если настроено более 1024 записей, новые записи перезаписывают старые записи.

6.26.3 Настройка через веб-интерфейс

Включите функцию журнала, как показано на рисунке ниже.

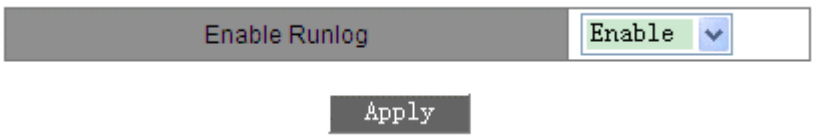

Рисунок 155 Настройка состояния журнала

Enable Runlog
Варианты: Enable/Disable
По умолчанию: Enable
Функция: Включение или выключение функции журнала. Если функция включена, информация о работе будет записана.
2. Настройте выгрузку журнала, как показано на рисунке ниже.

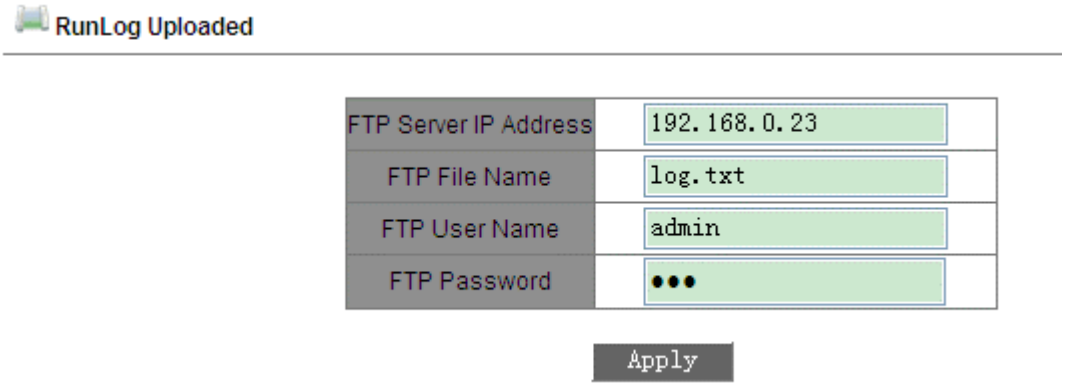

Рисунок 156 Выгрузка журнала

FTP Server IP Address
Формат: A.B.C.D
Функция: Настройка IP-адреса сервера FTP.
FTP File Name
Диапазон: 1~20 символов
Функция: Задание имени файла журнала, сохраненного на сервере.
FTP User Name
Диапазон: 1~20 символов
Функция: Задание имени пользователя FTP.
Рисунок 156 Выгрузка журнала
FTP Password
Диапазон: 1~20 символов
Функция: Задание пароля FTP.

CAUTION	**Предупреждение:** В процессе выгрузки журнала ПО сервера должно работать.

3. Просмотрите журнал, как показано на рисунке ниже.

Performance log

Index	LogType	Time	Description
10	Ring Open/Close	THU SEP 13 15:24:42 2012	Ring alarm: entity id:1 state:Ring open
9	PortLink Alarm	THU SEP 13 15:24:42 2012	Port alarm: entity id:1/2 port:1/2 state:Link down
8	Ring Open/Close	THU SEP 13 15:24:07 2012	Ring alarm: entity id:1 state:Ring close
7	PortLink Alarm	THU SEP 13 15:24:07 2012	Port alarm: entity id:1/2 port:1/2 state:Link up
6	Output rate	THU SEP 13 15:23:44 2012	Output alarm: entity id:1 state:Alarm
5	Input rate	THU SEP 13 15:23:43 2012	Input alarm: entity id:1 state:Alarm
4	PortLink Alarm	THU SEP 13 15:23:39 2012	Port alarm: entity id:1/1 port:1/1 state:Link up
3	Output rate	THU SEP 13 15:22:58 2012	Output alarm: entity id:2 state:Normal
2	PortLink Alarm	THU SEP 13 15:22:55 2012	Port alarm: entity id:1/2 port:1/2 state:Link down
1	PowerAlarm	THU SEP 13 15:21:49 2012	Power alarm: entity id:2 state:Power down
0	Output rate	THU SEP 13 15:21:28 2012	Output alarm: entity id:2 state:Alarm

Рисунок 157 Запрос журнала

Performance log
Состав: {Index, LogType, Time, Description}
Функция: Отображение текущего журнала

6.27 Настройка и запрос адреса одноадресной рассылки

6.27.1 Обзор

При пересылке пакета коммутатор ищет порт пересылки в таблице MAC-адресов на основе MAC-адреса получателя пакета.
MAC-адрес может быть как статическим, так и динамическим.
Статический MAC-адрес настраивается. Он имеет наивысший приоритет (не переопределяется динамическими MAC-адресами) и действует постоянно.
Динамические MAC-адреса коммутатор узнает при пересылке данных, они действуют только на определенный период. Коммутатор периодически обновляет свою таблицу MAC-адресов. При получении кадра данных для пересылки коммутатор узнает исходный MAC-адрес кадра, устанавливает сопоставление с принимающим портом и запрашивает порт пересылки в таблице MAC-адресов на основе MAC-адреса получателя кадра. Если совпадение найдено, коммутатор пересылает кадр данных с соответствующего порта. Если совпадений не найдено, коммутатор передает кадр в своем широковещательном домене.
Коммутатор поддерживает не более 256 статических одноадресных записей.

6.27.2 Настройка через веб-интерфейс

1. Добавьте статическую запись MAC-адреса, как показано на рисунке ниже.

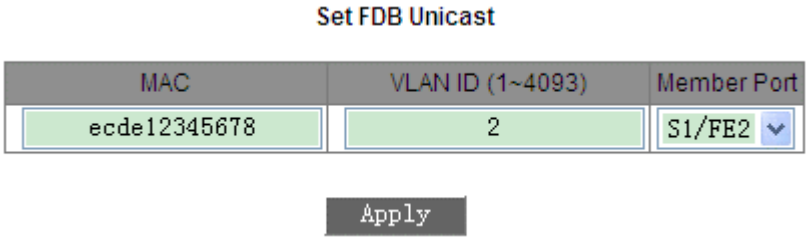

Рисунок 158 Добавление статической одноадресной записи FDB

MAC
Формат: HHHHHHHHHHHH (H – шестнадцатеричное число.) Функция: Настройка MAC-адреса

одноадресной рассылки. Младший бит в первом байте равен 0.

VLAN ID

Варианты: все созданные VLAN ID

Member Port

Варианты: все порты коммутатора.

Функция: Выберите порт для пересылки пакетов, предназначенных для MAC-адреса. Порт должен находиться в указанной VLAN.

2. Просмотрите список адресов одноадресной рассылки, как показано на рисунке ниже.

FDB Unicast Mac List

Index	MAC	VLAN ID	Member Port
○	ec:de:12:34:56:78	2	S1/FE2
○	00:01:01:01:01:01	1	S1/FE1

Add Delete Modify

Рисунок 159 Просмотр статической таблицы FDB

Выберите запись. Можно удалить или изменить запись.

3. Просмотрите динамический список адресов одноадресной рассылки, как показано на рисунке ниже.

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

Рисунок 160 Динамическая таблица одноадресной рассылки FDB

6.28 DHCP

С непрерывным расширением масштаба и ростом сложности сети, в условиях частого перемещения компьютеров (таких как ноутбуки или беспроводная сеть) и числа компьютеров, превышающего выделяемые IP-адреса, протокол BootP, специально предназначенный для статической конфигурации

хоста, оказывается неспособным удовлетворить фактические потребности. Для быстрого доступа и выхода из сети и улучшения коэффициента использования ресурсов IP-адресов нам необходимо разработать автоматический механизм на основе BootP для назначения IP-адресов. Для решения этих проблем был введен DHCP (протокол динамической конфигурации хоста).
DHCP использует модель взаимодействия клиент-сервер. Клиент отправляет запрос конфигурации на сервер, а затем сервер отправляет параметры конфигурации, такие как IP-адрес, клиенту, достигая динамической конфигурации IP-адресов. Структура типичного использования DHCP показана на рисунке 161.

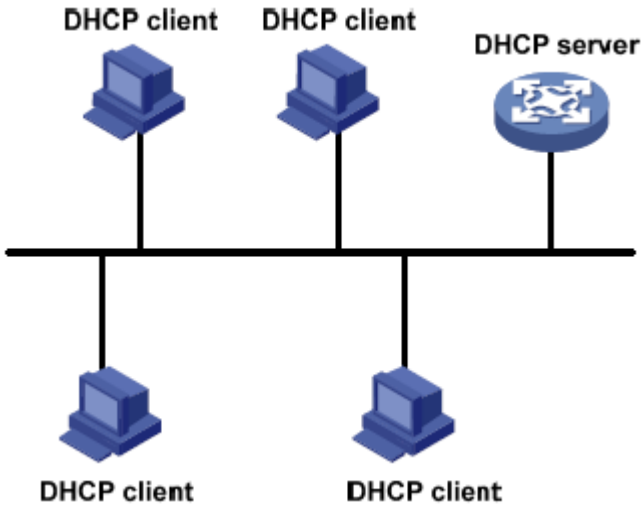

Рисунок 161 Типичное использование DHCP

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

DHCP поддерживает два типа механизмов распределения IP-адресов.
Статическое распределение: сетевой администратор статически привязывает фиксированные IP-адреса к нескольким конкретным клиентам, таким как WWW-сервер, и отправляет привязанные IP-адреса клиентам по DHCP. Этот механизм распределения содержит привязку IP-адреса порта и привязку MAC-адреса.
Динамическое распределение: Сервер DHCP динамически выделяет IP-адрес клиенту. Этот механизм выделения может выделить клиенту постоянный IP-адрес или IP-адрес с ограниченным сроком аренды. Когда срок аренды истекает, клиенту необходимо повторно запросить IP-адрес. Сетевой администратор может выбрать механизм распределения DHCP для каждого клиента.

6.28.1 Настройка сервера DHCP

6.28.1.1 Введение

DHCP-сервер — поставщик услуг DHCP. Он использует DHCP-сообщения для связи с DHCP-клиентом, чтобы выделить клиенту подходящий IP-адрес и при необходимости назначить ему другие сетевые параметры. DHCP-сервер обычно используется для выделения IP-адресов в следующих случаях.
> Большой масштаб сети. Трудоемкость ручной настройки велика, и трудно управлять всей сетью.

> Количество хостов превышает количество назначаемых IP-адресов, и нет возможности выделить фиксированный IP-адрес каждому хосту.
> Лишь несколько хостов в сети нуждаются в фиксированных IP-адресах.

6.28.1.2 Пул адресов DHCP

DHCP-сервер выбирает IP-адрес из пула адресов и выделяет его клиенту вместе с другими параметрами. Последовательность распределения IP-адресов следующая:
1. IP-адрес статически привязан к MAC-адресу клиента или идентификатору порта, подключенного к серверу.
2. Записанный на DHCP-сервере IP-адрес, который когда-либо был выделен клиенту.
3. IP-адрес, указанный в сообщении запроса, отправленном от клиента.
4. Первый доступный IP-адрес, найденный в пуле адресов.
5. Если нет доступного IP адреса, проверяется IP адрес, срок действия которого истекает, и у которого были конфликты в процессе использования. Если такой IP адрес найден, он присваивается клиенту. Если нет, то ничего не происходит.

6.28.1.3 Настройка через веб-интерфейс

1. Запустите сервер DHCP, как показано на рисунке 162.

Рисунок 162 Состояние сервера DHCP

DHCP server status
Варианты: Enable/Disable
По умолчанию: Disable
Функция: Выбор текущего коммутатора как сервера DHCP, чтобы выделить или не выделять IP-адрес клиенту. Если во время включения выбран идентификатор VLAN, DHCP-сервер выделяет IP-адрес только клиенту, отправляющему запрос в эту VLAN. Если выбраны все VLAN, DHCP-сервер выделяет IP-адреса всем клиентам, отправляющим запрос.
Пояснение: При выборе идентификатора VLAN можно выбрать только один идентификатор VLAN.
2. Выберите режим сервера DHCP, как показано на рисунке 163.

Рисунок 163 Режим сервера DHCP

DHCP server mode
Варианты: Common-Mode/Port-Mode
По умолчанию: Port-Mode
Пояснение: Режим Common-Mode содержит динамическое выделение IP-адреса и статическую привязку MAC-адреса. Режим Port-Mode означает желаемую настройку IP-адреса порта.
3. Настройка Port-Mode
При выборе режима Port-Mode в режиме DHCP-сервера назначьте портам IP-адреса со статической привязкой, как показано на рисунке 164.

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

Рисунок 164 Желаемая настройка IP-адреса порта

Желаемая настройка IP-адреса порта предназначена для статической настройки IP-адреса порта. Когда порт получает сообщение запроса от клиента, IP-адрес, привязанный к порту, будет выделен клиенту. Этот режим выделения IP имеет наивысший приоритет, а срок аренды составляет 1000 дней 23 часа 59 минут.

CAUTION	**Предупреждение:** IP-адрес, привязанный к порту, и DHCP-сервер должны находиться в одном сегменте.

Если для назначения IP выбран режим порта, необходимо настроить DHCP-сервер, как показано на рисунке 165.

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

Рисунок 165 Настройка сервера для режима Port-Mode

DHCP server IP-pool name
Диапазон: 1~15 символов
Функция: задание имени пула IP-адресов.
The domain name for the IP-Pool
Диапазон: 1~60 символов
Функция: задание доменного имени 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. Значение обычно настроено как 255.255.255.0.

CAUTION	**Предупреждение:** > После настройки нажмите кнопку <Run>, чтобы назначить клиентам правильные IP-адреса. > После изменения конфигурации снова нажмите кнопку <Run>, чтобы назначить клиентам правильные IP-адреса.

4. Настройка Common-Mode
Когда для DHCP-сервера выбран режим Common-Mode, он содержит статическую привязку MAC-адреса и динамическое выделение IP-адреса. При статической привязке MAC-адреса система предпочтительно выделяет IP-адрес, привязанный к MAC-адресу; в противном следует динамически выделять IP-адреса в пуле адресов. Конфигурация привязки статического MAC-адреса показана на рисунках 166 и 167; Конфигурация динамического выделения IP-адресов показана на рисунке 168.

Static Binding Between IP and MAC

IP address	192.168.0.36
MAC address	00-1e-cd-02-01-03

Apply Help

Рисунок 166 Статическая привязка MAC-адреса

Статическая привязка MAC-адреса заключается в привязке MAC-адреса клиента к IP-адресу. Когда сервер получает сообщение с запросом IP-адреса, MAC-адрес источника которого является MAC-адресом, установленным здесь, IP-адрес, привязанный к этому MAC-адресу, будет выделен клиенту. Этот вариант режима выделения IP требует настройки сервера, как показано на рисунке 168.
После настройки список Static Binding between IP and MAC показывает статически настроенные привязки MAC-адресов и IP-адресов. Установите флажок в поле Index, чтобы удалить соответствующую запись привязки.

The list of Static Binding Between IP and MAC

Index	IP Address	MAC Address
☐	192.168.0.26	02-00-AA-BB-CC-05
☐	192.168.0.36	00-1E-CD-02-01-03

Delete

Рисунок 167 Список привязки статического MAC-адреса

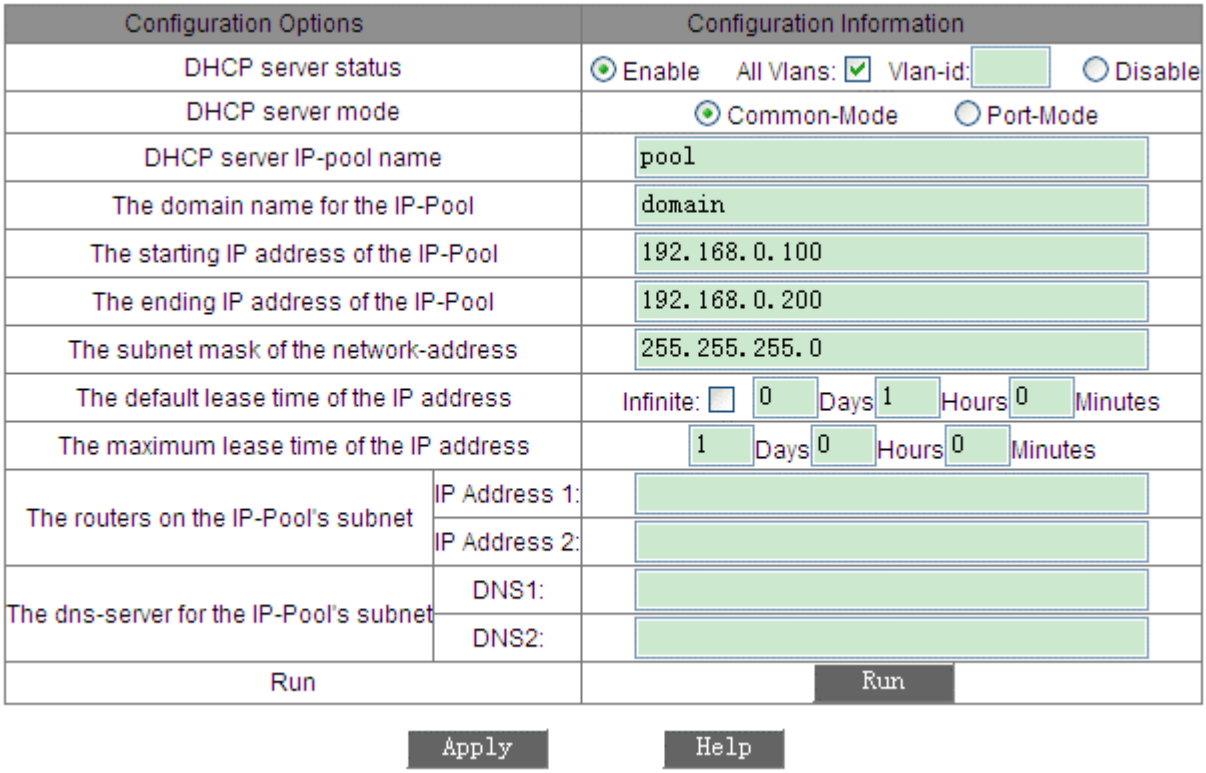

Рисунок 168 Настройка сервера для режима Common

DHCP server IP-pool name
Диапазон: 1~15 символов
Функция: задание имени пула IP-адресов.
The domain name for the IP-Pool
Диапазон: 1~60 символов
Функция: задание доменного имени 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 и конечный IP-адреса должны находиться 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. Значение обычно настроено как 255.255.255.0. При динамическом выделении адресов необходимо задать 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
Пояснение: Если сообщение с запросом IP-адреса, отправленное от клиента, не содержит действительного времени аренды, время 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
Пояснение: Когда клиент отправляет сообщение запроса IP-адреса на сервер, 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
Пояснение: когда DHCP-клиент посещает хост, находящийся в другом сегменте, данные должны пересылаться через шлюзы. Когда DHCP-сервер выделяет клиентам IP-адреса, он может одновременно

указывать адреса шлюза. Для пула адресов DHCP можно настроить не более двух шлюзов.

The dns-server for the IP-Pool's subnet

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

CAUTION	**Предупреждение:** > Настройте правильную подсеть на основе топологии сети клиента. > После настройки нажмите кнопку <Run>, чтобы назначить клиентам правильные IP-адреса. > После изменения конфигурации снова нажмите кнопку <Run>, чтобы назначить клиентам правильные IP-адреса.

6.28.1.4 Пример типовой конфигурации

Как показано на рисунке 169, коммутатор A работает как сервер DHCP, а коммутатор B работает как DHCP-клиент. Порт 3 коммутатора A подключается к порту 4 коммутатора B. Клиент отправляет сообщения с запросом IP-адреса, и сервер может выделить IP-адрес клиенту тремя способами.

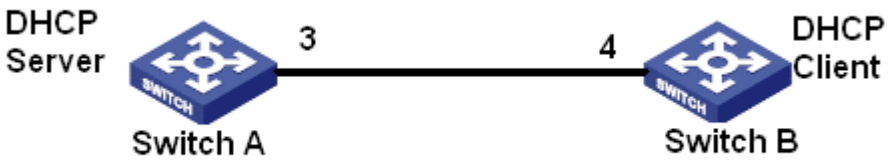

Рисунок 169 Пример типовой конфигурации DHCP

Port IP binding

> Конфигурация коммутатора A:

1. Установите статус сервера DHCP в состояние Enable, как показано на рисунке 162.
2. Выберите режим сервера DHCP Port-Mode, как показано на рисунке 163.
3. Установите для IP-pool name значение pool, для the domain name for the IP- pool значение domain, установите для the subnet mask значение 255.255.255.0, как показано на рисунке 165.
4. Порт 3 привязан к IP-адресу 192.168.0.6, как показано на рисунке 164.
5. Щелкните кнопку <Run> в интерфейсе конфигурации сервера, чтобы запустить сервер.

> Конфигурация коммутатора B:

1. Как клиент DHCP, коммутатор B автоматически получает IP-адрес.
2. Коммутатор B получает IP-адрес 192.168.0.6 и маску подсети 255.255.255.0 от DHCP-сервера, как показано на рисунке 170.

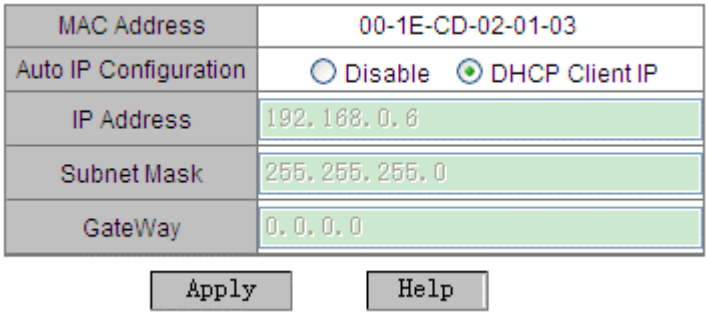

Рисунок 170 Клиент DHCP получает IP-адрес-1

Статическая привязка MAC-адреса

> Конфигурация коммутатора A:

1. Установите статус сервера DHCP в состояние Enable, как показано на рисунке 162.
2. Выберите режим сервера DHCP Common-Mode, как показано на рисунке 163.
3. Установите для IP-pool name значение pool, для the domain name for the IP- pool значение domain, для the starting IP address of the IP-pool значение 192.168.0.3, для the ending IP address of the IP-pool значение 192.168.0.201, установите для the subnet mask значение 255.255.255.0, для lease time используйте значения по умолчанию, как показано на рисунке 168.
4. Привяжите MAC-адрес коммутатора B 00-1E-CD-02-01-03 к IP-адресу 192.168.0.36, как показано на рисунке 166.
5. Щелкните кнопку <Run> в интерфейсе конфигурации сервера, чтобы запустить сервер.

> Конфигурация коммутатора B:

1. Как клиент DHCP, коммутатор B автоматически получает IP-адрес.
2. Коммутатор B получает IP-адрес 192.168.0.36 и маску подсети 255.255.255.0 от DHCP-сервера, как показано на рисунке 171.

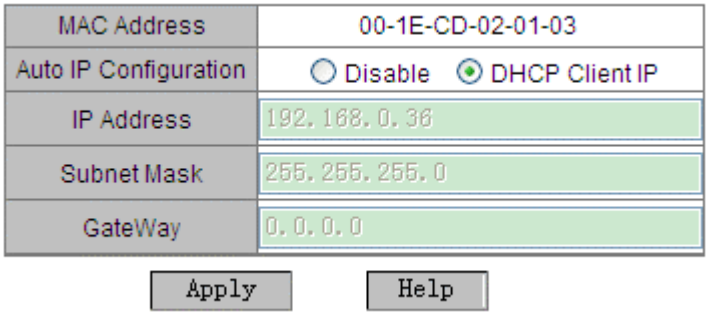

Рисунок 171 Клиент DHCP получает-адрес-2

Динамическое получение IP-адреса в пуле адресов

> Конфигурация коммутатора A:

1. Установите статус сервера DHCP в состояние Enable, как показано на рисунке 162.
2. Выберите режим сервера DHCP Common-Mode, как показано на рисунке 163.
3. Установите для IP-pool name значение pool, для the domain name for the IP- pool значение domain, для the starting IP address of the IP-pool значение 192.168.0.3, для the ending IP address of the IP-pool значение 192.168.0.201, установите для the subnet mask значение 255.255.255.0, для lease time используйте значения по умолчанию, как показано на рисунке 168.
4. Щелкните кнопку <Run> на экране конфигурации сервера, чтобы запустить сервер.

> Конфигурация коммутатора B:

1. Как клиент DHCP, коммутатор B автоматически получает IP-адрес.
2. DHCP-сервер ищет доступные IP-адреса в пуле адресов по порядку и выделяет первый найденный доступный IP-адрес и другие сетевые параметры коммутатору B. Маска подсети 255.255.255.0, как показано на рисунке 172.

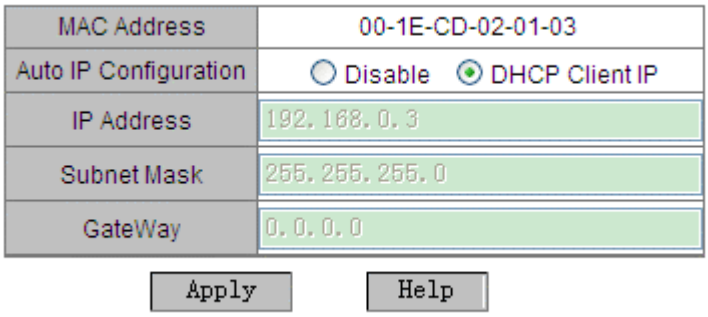

Рисунок 172 Клиент DHCP получает IP-адрес-3

6.28.2 DHCP Snooping

6.28.2.1 Введение

Отслеживание DHCP — это функция мониторинга служб DHCP на уровне 2 и функция безопасности DHCP, обеспечивающая дополнительную безопасность клиента. Механизм безопасности DHCP Snooping может контролировать, что только доверенный порт может пересылать сообщение запроса DHCP-клиента на легальный сервер, в то же время он может контролировать источник ответного сообщения DHCP-сервера, гарантируя, что клиент получит IP-адрес от действительного сервера, и предотвращая выделения IP-адресов или других параметров конфигурации другим хостам поддельным или недействительным DHCP-сервером.
Механизм безопасности DHCP Snooping делит порты на доверенные и ненадежные.
Доверенный порт: порт, который прямо или косвенно подключается к действительному DHCP-серверу. Доверенный порт пересылает сообщения запросов DHCP-клиентов и ответные сообщения DHCP-серверов, чтобы гарантировать, что DHCP-клиенты могут получить допустимые IP-адреса. Ненадежный порт: это порт, который подключается к недействительному DHCP-серверу. Ненадежный порт не пересылает сообщения запросов DHCP-клиентов и ответные сообщения DHCP-серверов, чтобы предотвратить получение DHCP-клиентами недопустимых IP-адресов.

6.28.2.2 Настройка через веб-интерфейс

1. Включите функцию DHCP Snooping, как показано на рисунке 173.

Рисунок 173 Состояние функции DHCP Snooping

DHCP Snooping Status
Варианты: Enable/Disable
По умолчанию: Disable
Функция: Включение/выключение функции DHCP Snooping

CAUTION	**Предупреждение:** У коммутатора, который работает и как сервер DHCP и как клиент, нельзя включить функцию DHCP Snooping.

2. Настройте доверенные порты, как показано на рисунке 174.

Port	Protocol Status
S1/FE1	◉ Trust ○ Untrust
S1/FE2	○ Trust ◉ Untrust
S1/FE3	○ Trust ◉ Untrust
S1/FE4	○ Trust ◉ Untrust
S1/FE5	○ Trust ◉ Untrust
S1/FE6	○ Trust ◉ Untrust
S1/FE7	○ Trust ◉ Untrust
S1/FE8	○ Trust ◉ Untrust

Рисунок 174 Настройка доверенного порта

Protocol Status
Варианты: Trust/Untrust
По умолчанию: Untrust
Функция: настройка порта как доверенного или ненадежного. Порты, которые прямо или косвенно подключаются к действительному DHCP-серверу – это доверенные порты.

CAUTION	**Предупреждение:** Назначение порта доверенным и транковым является взаимоисключающим. Порт, входящий в транковую группу нельзя назначить доверенным. Доверенный порт не может входить в транковую группу.

6.28.2.3 Пример типовой конфигурации

Как показано на рисунке 175, DHCP-клиент запрашивает IP-адрес от сервера DHCP. В сети существует неавторизованный DHCP-сервер. Порт 1 настроен как доверенный порт с помощью DHCP Snooping, чтобы пересылать сообщение запроса DHCP-клиента на DHCP-сервер и пересылать ответное сообщение DHCP-сервера на DHCP-клиент. Порт 3 настроен в качестве ненадежного порта, который не может пересылать сообщение запроса DHCP-клиента и ответное сообщение неавторизованного DHCP-сервера, гарантируя, что клиент может получить действительный IP-адрес от действительного DHCP-сервера.

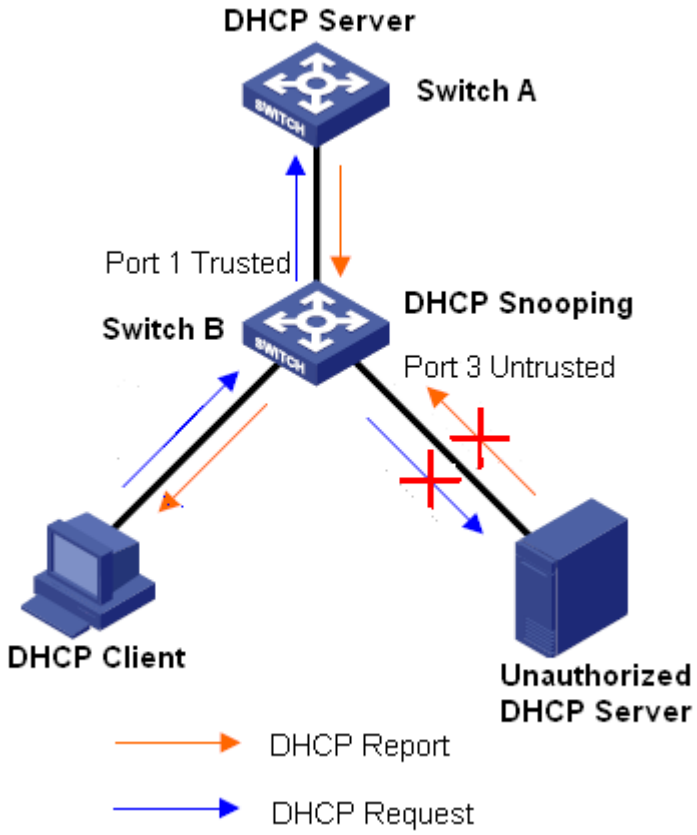

Рисунок 175 Пример типовой конфигурации DHCP Snooping

Конфигурация коммутатора B:
> Включите функцию DHCP Snooping, как показано на рисунке 173.
> Настройте порт 1 коммутатора B как доверенный порт, а порт 3 как ненадежный порт, как показано на рисунке 174.

6.28.3 Настройка Option 82

Функция Option 82 (запись информации об агенте ретрансляции) записывает информацию о клиенте. Когда DHCP Snooping, поддерживаемый Option 82, получает сообщение запроса от DHCP-клиента, в сообщения добавляется соответствующее поле Option 82, а затем сообщение пересылается на DHCP-сервер. Сервер, поддерживающий Option 82, может гибко распределять адреса в соответствии с сообщением Option 82.
После включения функции Option 82 поле Option 82 должно быть добавлено в сообщение. Поле Option82 коммутаторов этой серии содержит два параметра: параметр 1 (Circuit ID) и параметр 2 (Remote ID). Формат двух параметров показан ниже:
Параметр 1 содержит идентификатор VLAN ID и номер порта, который получает сообщение запроса от DHCP-клиента, как показано в Таблице 9.

Таблица 9 Формат поля параметра 1

Тип параметра（0x01）	Длина（0x04）	VLAN ID	Номер порта
Один байт	Один байт	Два байта	Два байта

Тип параметра: Тип параметра 1 – 1.
Длина: количество байтов, которые занимают идентификатор VLAN и номер порта.
VLAN ID: На устройстве DHCP Snooping — идентификатор VLAN порта, который получает сообщение запроса от DHCP-клиента.
Номер порта: На устройстве DHCP Snooping — номер порта, который получает сообщение запроса от

DHCP-клиента.
Параметр 2 содержит MAC-адрес устройства DHCP Snooping, которое получает сообщение запроса от DHCP-клиента, как показано в таблице 10, или строку символов, заданную пользователями, как показано в таблице 11.

Таблица 10 Формат поля параметра 2 – MAC-адрес

Тип параметра（ 0x02 ）	Длина （ 0x06)	MAC ???
Один байт	Один байт	6 байт

Таблица 10 Формат поля параметра 2 – строка символов

Тип параметра（ 0x02 ）	Длина (0x10)	Строка символов
Один байт	Один байт	16 байт

Тип параметра: Тип параметра 2 – 2.
Длина: количество байтов, которые занимает содержание параметра 2. MAC-адрес занимает 6 байт, а строка символов занимает 16 байт.
MAC-адрес: содержимое параметра 2 — это MAC-адрес устройства DHCP Snooping, которое получает сообщение запроса от DHCP-клиента.
Строка символов: содержание параметра 2 – 1~16 символов, заданных пользователями. (Символ задается кодом ASCII, каждый символ занимает один байт). Длина фиксирована и равна 16. Если настроенная длина строки символов меньше 16 байт, заполните недостающие символы 0.

6.28.3.1 DHCP Snooping с поддержкой функции Option 82

1. Введение
Если устройство DHCP Snooping поддерживает функцию Option 82, при получении DHCP Snooping сообщения запроса DHCP сообщение обрабатывается в соответствии с тем, содержит ли сообщение параметр 82 и политику клиента, а затем обработанное сообщение пересылается серверу DHCP. Метод обработки показан в таблице 12.

Таблица 12 Режимы обработки сообщений запроса (DHCP Snooping)

Получение сообщения запроса от DHCP-клиента.	Политика конфигурации	Обработка сообщения запроса на устройстве DHCP Snooping
Сообщение запроса содержит Option 82	Drop	Отклонить сообщение запроса
	Keep	Сохранить формат сообщения без изменений и переслать сообщение
	Replace	Заменить поле Option 82 в сообщении полем Option 82 устройства Snooping и переслать новое сообщение
Сообщение запроса не содержит Option 82	Drop/Keep/Replace	Добавить поле Option 82 устройства Snooping в сообщение и переслать его

Когда устройство DHCP Snooping получает сообщение запроса от DHCP-сервера, если сообщение содержит поле Option 82, удалить поле Option 82 и переслать сообщение клиенту. Если сообщение не содержит поля Option 82, обработать ответное сообщение в соответствии с политикой сервера, как

показано в Таблице 13.

Таблица 13 Режимы обработки сообщений ответа (DHCP Snooping)

Получение сообщения ответа от DHCP-сервера.	Политика конфигурации	Обработка сообщения ответа на устройстве DHCP Snooping
Сообщение ответа содержит поле Option 82	Drop/Keep	Удалить поле Option 82 в сообщении ответа и переслать сообщение
Сообщение ответа не содержит поле Option 82	Drop	Отбросить сообщение ответа
	Keep	Сохранить формат сообщения без изменений и переслать сообщение

2. Настройка через веб-интерфейс

Настройка DHCP Snooping Option 82 показана на рисунке 176.

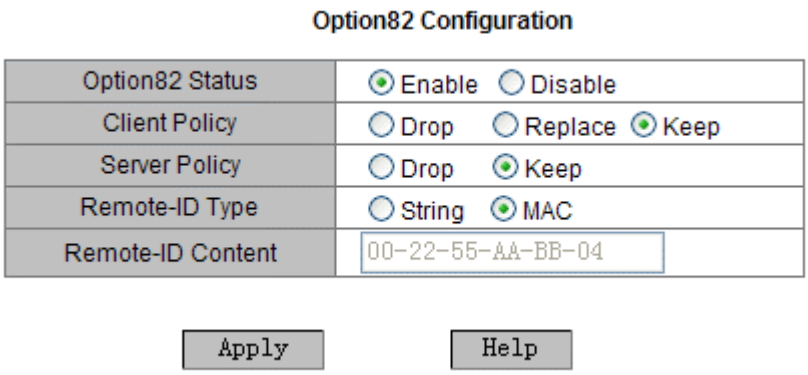

Рисунок 176 Настройка DHCP Snooping Option 82

Option82 Status

Варианты: Enable/Disable

По умолчанию: Disable

Функция: Включение/выключение функции Option82 на устройстве DHCP Snooping.

Client Policy

Варианты: Drop/Replace/Keep

По умолчанию: Keep

Функция: Настройка политики клиента. Устройство DHCP Snooping обрабатывает сообщение запроса, отправленное от клиента, в соответствии с политикой клиента, как показано в таблице 12.

Server Policy

Варианты: Drop/Keep

По умолчанию: Keep

Функция: Настройка политики сервера. Устройство DHCP Snooping обрабатывает сообщение запроса, отправленное от сервера, в соответствии с политикой сервера, как показано в таблице 13.

Remote-ID Type

Варианты: Строка/MAC

По умолчанию: MAC

Функция: настройка содержания параметра 2.

Пояснение: MAC означает, что содержимое параметра 2 — это MAC-адрес устройства DHCP Snooping, которое получает сообщение запроса от DHCP-клиента. String означает, что содержимое параметра 2 представляет собой строку символов, определенную пользователем.

Remote-ID Content

Варианты: MAC-адрес/1~16 символов
По умолчанию: MAC-адрес
Пояснение: когда для remote ID type установлено значение MAC, содержимое Remote ID принудительно переводится на MAC-адрес текущего устройства Snooping. Когда для remote ID type установлено значение String, содержимое Remote ID настраивается пользователем. Содержимое конфигурации составляет 1–16 символов (каждый символ занимает один байт).

6.28.3.2 DHCP Server с поддержкой функции Option 82 1. Введение

Если DHCP-сервер настроен на поддержку функции Option82, при получении DHCP-сервером запроса DHCP, он предоставляет разные решения по выделению адреса в зависимости от наличия в сообщении поля Option82 и конфигурации сервера.
DHCP-сервер включает в себя следующие переменные:
Class: для каждого DHCP-сервера можно настроить 32 класса. Каждый класс содержит три переменных: начальный и конечный IP-адрес и опцию match always and relay information.
Переменная relay information сопоставляется с полем Option 82. Если значение переменной совпадает со значением поля Option82, считается, что они совпадают, иначе они не совпадают.
Если параметр match always включен, предполагается, что значение параметра relay information всегда соответствует значению, указанному в поле Option82, без необходимости подтверждения. Если параметр match always выключен, необходимо проверить, соответствует ли значение relay information значению поля Option82.
В соответствии с конфигурацией вышеуказанных переменных сервер обрабатывает сообщение запроса, как показано в таблице 14.

Таблица 14 Режимы обработки сообщений запроса
(DHCP-сервер с поддержкой Option82)

<table>
<tr><td>Получение сообщения запроса от DHCP-клиента.</td><td colspan="2">Политика конфигурации</td><td>Обработка сообщения запроса сервером DHCP</td></tr>
<tr><td rowspan="3">Сообщение запроса содержит поле Option 82</td><td colspan="2">match always включен</td><td>Добавить поле Option82 в ответное сообщение и назначить клиенту IP-адрес и другие параметры.</td></tr>
<tr><td rowspan="2">match always выключен</td><td>Настроить relay information</td><td>Значение relay information совпадает с полем Option82: Добавить поле Option82 в ответное сообщение и назначить клиенту IP-адрес и другие параметры.
Значение relay information не совпадает с полем Option82: сервер не выделяет IP-адрес клиенту</td></tr>
<tr><td>Значение relay information не настроено</td><td>Сервер не выделяет клиенту IP-адрес.</td></tr>
<tr><td></td><td colspan="2"></td><td></td></tr>
<tr><td rowspan="2">Сообщение запроса не содержит поле Option 82</td><td colspan="2">Match always включен</td><td>Ответное сообщение не содержит поле Option82, назначить клиенту IP-адрес и другие параметры.</td></tr>
<tr><td colspan="2">Match always выключен</td><td>Сервер не выделяет клиенту IP-адрес.</td></tr>
</table>

Если DHCP-сервер не поддерживает функцию Option82, при получении DHCP-сервером сообщения, содержащего поле Option82, ответное сообщение не содержит поля Option82, и сервер может выделить клиенту IP-адрес и другие параметры. При таком условии сервер обрабатывает сообщение запроса, как

показано в таблице 15.

Таблица 15 Режимы обработки сообщений запроса
(DHCP-сервер без поддержки Option82)

Получение сообщения запроса от DHCP-клиента.	Обработка сообщения запроса сервером DHCP
Сообщение запроса содержит поле Option 82	Ответное сообщение не содержит поле Option82, сервер назначает клиенту IP-адрес и другие параметры.
Сообщение запроса не содержит поле Option 82	

2 Настройка через веб-интерфейс
Включите функцию Option82 на сервере DHCP, как показано на рисунке 177.

Рисунок 177 Состояние Option82 сервера DHCP

DHCP Server Option82 Enable
Варианты: Enable/Disable
По умолчанию: Disable
Функция: Включите или выключите функцию Option82 на сервере DHCP. Настройте Option82 для сервер DHCP, как показано на рисунке 178.

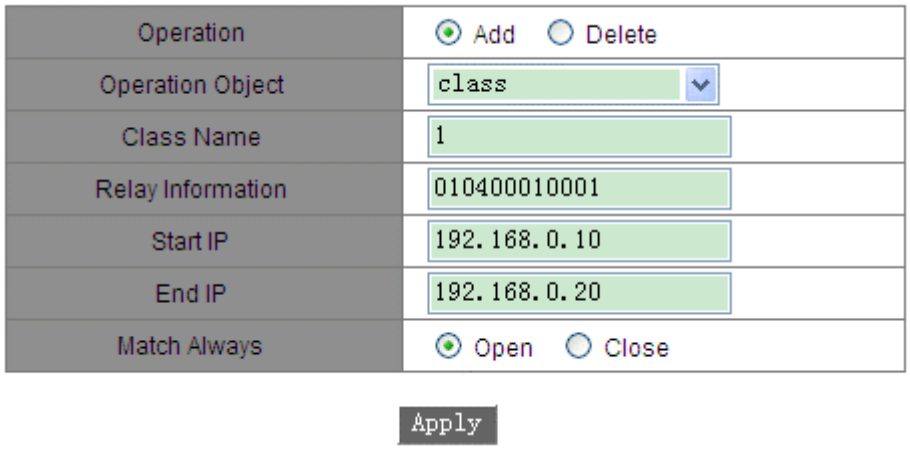

Рисунок 178 Настройка Option82 сервера DHCP

Operation
Варианты: Add/Delete
По умолчанию: Add
Функция: Добавить или удалить указанный класс.
Operation Object
Варианты: class/Relay Information/start & end ip/Match Always
По умолчанию: class
Описание: При добавлении класса можно настроить следующие параметры. При удалении класса необходимо указать только имя класса. Можно добавить несколько значений relay information к уже

созданному указанному классу. Start & end IP/ match always добавляются для изменения конфигурации связанных параметров уже созданного указанного класса. При удалении relay information, можно удалить указанное значение relay information в текущем классе.

Class Name

Диапазон: 1~15 символов

Функция: Настройка имени класса.

Relay information

Диапазон: 12~60 шестнадцатеричное число

Функция: Настройка relay information класса.

Start IP/ End IP

Формат: A.B.C.D

Функция: Настройка начального/конечного IP-адреса класса Диапазон должен быть выбран из пула адресов сервера DHCP.

Match Always

Варианты: Open/Close

Функция: Включение или выключение опции match always. Если параметр match always включен, предполагается, что значение параметра relay information всегда соответствует значению, указанному в поле Option82, без необходимости подтверждения. Если параметр match always выключен, необходимо проверить, соответствует ли значение relay information значению поля Option82.

CAUTION	**Предупреждение:** При создании нескольких классов DHCP-сервер выделяет IP-адрес клиенту на основе информации о классе с совпадающим значением relay information. Если несколько классов имеют совпадающее значение relay information, сервер DHCP выделяет клиенту IP-адрес на основе информации класса, созданного первым.

Запросите класс Option82 сервера DHCP, как показано на рисунке 179.

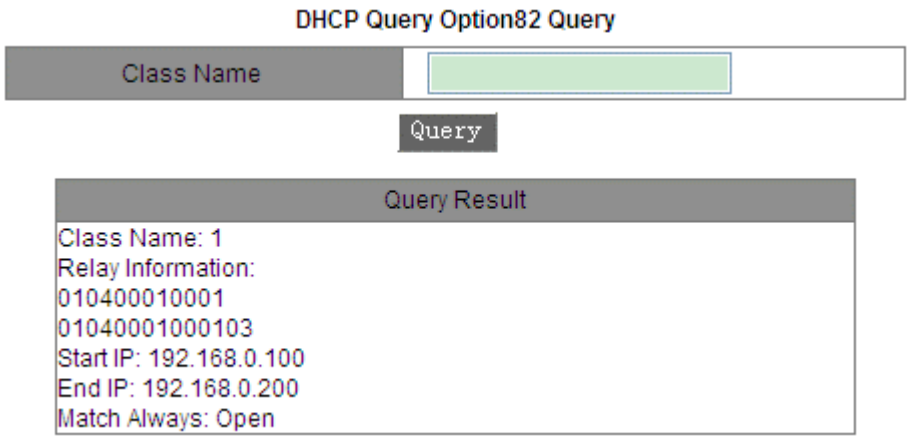

Рисунок 179 Запрос класса Option82 сервера DHCP

Приложение: Аббревиатуры

Аббревиатура	Полное написание
ACL	Access Control List
ARP	Address Resolution Protocol
BPDU	Bridge Protocol Data Unit
CLI	Command Line Interface
CRC	Cyclic Redundancy Check
DHCP	Dynamic Host Configuration Protocol
DHP	Dual Homing Protocol
DRP	Distributed Redundancy Protocol
DSCP	Differentiated Services Code Point
FTP	File Transfer Protocol
GARP	Generic Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
IGMP	Internet Group Management Protocol
IGMP Snooping	Internet Group Management Protocol Snooping
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
MAC	Media Access Control
MIB	Management Information Base
NMS	Network Management Station
OID	Object Identifier
PVLAN	Private VLAN
QoS	Quality of Service
RMON	Remote Network Monitoring
RSTP	Rapid Spanning Tree Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
ToS	Type of Service

VLAN	Virtual Local Area Network
WRR	Weighted Round Robin

Контакты

Для получения технической поддержки пишите на наш адрес электронной почты: *support@kyland-rus.ru*
Офис продаж: *sales@kyland-rus.ru*

Для получения информации об оборудовании, документации, актуальной информации обращайтесь на сайт: *https://kyland-rus.ru/*