SYMANITRON

Инновационные
промышленные сети

# Руководство по настройке коммутаторов серии SEWM312G-D

# Оглавление

## Введение

Данный документ содержит информацию о настройках и возможностях программного обеспечения коммутаторов серии SEWM312G-D. Кроме того, в документе приводится детальная информация по настройке коммутаторов с помощью WEB-интерфейса.

## Структура документа

Данное руководство включает следующую информацию:

| Основная информация | Описание |
|---|---|
| 1. Информация о продукте | • Описание продукта<br>• Возможности программного обеспечения |
| 2. Способы подключения к устройству | • Варианты просмотра и отображения<br>• Подключение через консольный порт<br>• Подключение с использованием Telnet<br>• Подключение через Web-интерфейс |
| 3. Информация об устройстве | • Основная информация о коммутаторе |
| 4. Управление | • Перезагрузка<br>• Обновление прошивки (через FTP или TFTP) |
| 5. Базовые настройки | • Основные настройки<br>• Настройки управления пользователями<br>• Настройка портов<br>• Настройка VLAN<br>• Настройка PVLAN<br>• Зеркалирование портов<br>• Подавление штомов<br>• Изоляция портов<br>• Агрегация портов<br>• Настройка сервера Telnet<br>• Настройка сервера SSH<br>• Настройка SSL<br>• Передача файлов (сервис TFTP, сервис FTP)<br>• Настройка таблицы MAC-адресов<br>• Отладка базовой окнфигурации |
| 6. Расширенные настройки | • Настройка ARP<br>• Настройка интерфейса L3<br>• SNMP v2c, SNMP v3<br>• Sy2-Ring<br>• Sy2-RP<br>• STP/RSTP<br>• MSTP<br>• Тревожная сигнализация<br>• Системный журнал<br>• Статическая маршрутизация<br>• Настройка RIP |

| | |
|---|---|
| | • Настройка OSPF<br>• Настройка сервера DHCP<br>• Настройка QoS<br>• Настройка МЭК61850<br>• IGMP Snooping<br>• GMRP<br>• LLDP<br>• VRRP<br>• Настройка SNTP<br>• Настройка NTP<br>• Настройка TACACS+<br>• Настройка RADIUS<br>• Настройка IEEE802.1x<br>• Настройка аутентификации<br>• Проверка связи (Link check)<br>• Настройка функции обнаружения петель (Loop Detect)<br>• Настройка защиты CRC |

## Условные обозначения

### 1. Условные обозначения в тексте

| Формат | Описание |
|---|---|
| < > | Скобки < > обозначают «кнопки». Например, нажмите кнопку <Apply>. |
| [ ] | Скобки [ ] обозначают имя окна или имя меню. Например, нажмите пункт меню [File]. |
| { } | Скобки { } обозначают группу. Например, {IP address, MAC address} означает, что IP адрес и MAC адрес составляют группу и могут быть настроены и показаны вместе. |
| → | Мультиуровневое меню разделяется посредством знака «→». Например, Start→AllPrograms→Accessories. Нажмите меню [Start], войдите в подменю [All programs], затем войдите в подменю [Accessories]. |
| / | Выбор одной, двух или более опций при помощи символа «/». Например, «Add/Subtract» означает добавить или удалить. |
| ~ | Знак «~» обозначает диапазон значений. Например, «1~255» указывает на диапазон от 1 до 255. |

### 2. Условные обозначения CLI

| Формат | Описание |
|---|---|
| **Bold** | Означает команды и ключевые слова. Например, **show version** будет показываться с использованием шрифта **Bold.** |
| *Italic* | Параметры, для которых вы указываете значения с помощью шрифта *italic.* Например, для команды **show vlan** *vlan id* указывается актуальное |

| | |
|---|---|
| | значение команды *vlan id* посредством шрифта *italic.* |
| [ ] | Элементы (ключевые слова или аргументы) в [ ] являются необязательными. |
| {x\|y\|……} | Альтернативные элементы сгруппированы в { } и разделены вертикальными чертами. Выбирается один. |
| [x\|y\|……] | Необязательные альтернативные элементы сгруппированы в [ ] и разделены вертикальными чертами. Выбирается один или более. |
| <x\|y\|……> | Альтернативные элементы сгруппированы в < > и разделены вертикальными чертами. Можно выбрать минимум один или максимум все. |
| // | Строка, начинающаяся со знака //, является комментарием. |

3. Условные символы

| Символ | Описание |
|---|---|
| **Предостережение** | Эти вопросы требуют внимания во время работы с устройством при настройке, а также дают дополнительную информацию. |
| **Заметка** | Необходимые пояснения к содержимому выполняемых операций с устройством. |
| **Внимание** | Вопросы, требующие особого внимания. Некорректная работа с устройством может привести к потере данных или повреждению. |

# 1. Информация об устройстве

## 1.1 Основная информация о коммутаторе

Промышленные коммутаторы серии SEWM312G-D могут использоваться в различных областях промышленности: системах передачи данных в энергетике, на транспорте, в горнодобывающей промышленности и т.д. Данная серия коммутаторов представляет собой коммутатор уровня 3 (L3), который поддерживает протоколы маршрутизации, а также протоколы MSTP, RSTP, и проприетарный протокол Sy2-Ring, гарантируя надежную работу системы.

## 1.2 Функциональные возможности ПО

Программное обеспечение серии коммутаторов SEWM312G-D поддерживает множество различных функций:

- Протоколы кольцевого резервирования: Sy2-RP, STP/RSTP, VRRP и MSTP;
- Протоколы маршрутизации: статическая маршрутизация, RIP, OSPFv2;
- Протоколы многоадресной рассылки (Multicast): IMGP Snooping, GMRP, PIM-SM и PIM-DM;

- Функции коммутации: VLAN, PVLAN, QoS, ARP;
- Управление пропускной способностью: статическая агрегация портов, ограничение скорости порта и подавление широковещательных штормов;
- Протоколы синхронизации времени: SNTP, NTP;
- Безопасность: IEEE802.1x, TACACS+, RADIUS, SSH, SSL, ACL, привязка MAC-адресов, изоляция портов и управление пользователями;
- Управление устройством: обновление программного обеспечения и передача файлов при помощи FTP/TFTP, запись и выгрузка системного журнала;
- Диагностика устройства: зеркалирование портов (port mirroring), LLDP, проверка канала связи, обнаружение петель, защита CRC;
- Аварийная сигнализация: ошибка порта (port alarm), ошибка питания (power alarm), ошибка кольца (ring alarm), оповещения о высокой или низкой температуре, оповещения о проблемах с трафиком на портах;
- Сетевой доступ к устройству и управление: CLI, Telnet, Web, NMS Symanitron, DHCP, SNMP v1/v2/v2 и мониторинг сети IEC61850.

# 2. Подключение к устройству

Устройство можно настраивать одним из четырех нижеперечисленных способов:

- через консольный порт;
- посредством Telnet;
- с использованием WEB-интерфейса;
- с помощью программы Symanitron NMS.

## 2.1 Варианты просмотра и отображения

Когда пользователь (администратор сети) подключается к устройству посредством CLI через консольный порт или Telnet, он имеет возможность, используя различные команды, получать информацию о состоянии устройства и выполнять настройки коммутатора:

Таблица 1

| Подсказка | Тип отображения | Функция | Команда |
|---|---|---|---|
| Switch > | Основной режим | • Отображение даты и Времени<br>• Отображение версии ПО | Введите **«enable»** для входа в привилегированный режим |
| Switch # | Привилегированный режим | • Настройка даты и времени<br>• Передача файла и обновление ПО<br>• Удаление файла<br>• Отображение конфигурации коммутатора и системной информации | Введите «**config**» для переключения из привилегированного режима в режим настройки<br><br>Введите «**exit**» для возврата в основной режим |

| | | | |
|---|---|---|---|
| | | • Восстановление конфигурации по умолчанию<br>• Запись текущих настроек<br>• Перезагрузка коммутатора | |
| Switch (config) # | Режим настройки | Настроить все функциональные возможности коммутатора | Введите «**exit**» для возврата в привилегированный режим |

Когда выполняется настройка коммутатора при помощи командной строки (CLI), символ «?» может использоваться для получения помощи по используемым командам. Для получения помощи, нужно ввести описание параметров, например, <1,255> означает диапазон чисел, <H.H.H.H> означает IP адрес, <xx:xx:xx:xx:xx:xx> означает MAC адрес, <word31> означает диапазон строк 1~31. Также символы ↑ и ↓ могут использоваться для просмотра недавно использованных команд.

## 2.2 Подключение через консольный порт

Пользователь может подключиться к устройству посредством консольного порта с помощью HyperTerminal операционной системы Windows или с помощью другого программного обеспечения, которое поддерживает подключение по последовательному порту, например, HTT3.3. В примере ниже показано, как использовать консольный порт и HyperTerminal для доступа к коммутатору.

1. Подключите кабель DB9-M12 к ПК и консольному интерфейсу устройства.

2. Запустите HyperTerminal в основном окне Windows, нажмите [Start] → [All Programs] → [Accessories] → [Communications] → [Hyper Terminal] (см. рисунок 1).

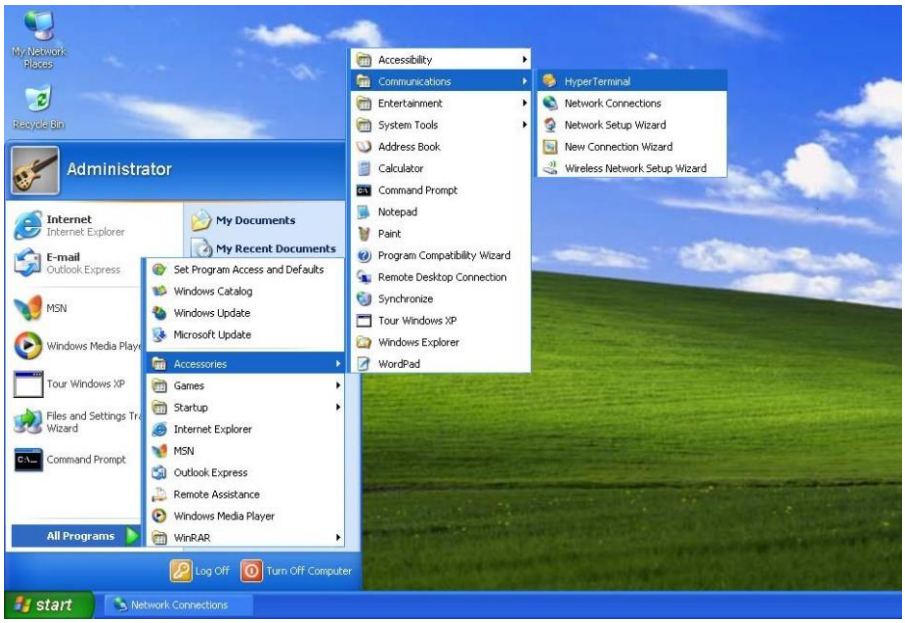



Рисунок 1 – Запуск HyperTerminal

3. Создайте новое подключение, например, с именем «Switch» (см. рисунок 2).


Рисунок 2 – Создание нового подключения

4. Выберите COM-порт для подключения.


Рисунок 3 – Выбор COM порта для подключения

Чтобы убедиться, что консольный порт выбран верно, проверьте его статус в Диспетчере устройств Windows.

5. Настройте параметры COM порта. Скорость (Bits per second): 115200, Биты данных (Data bits): 8, Чётность (Parity): None, Стоповые биты (Stop bits): 1, Контроль потока (Flow control): None.

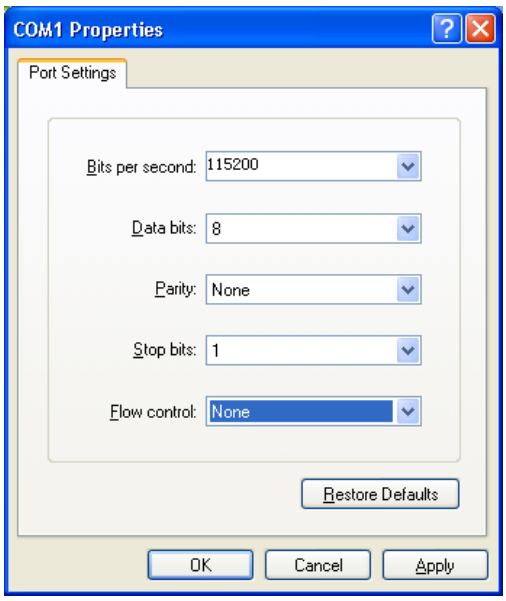



Рисунок 4 – Настройка параметров COM порта

6. Нажмите <OK> для входа в командную строку CLI. Нажмите <Enter> для входа в основной режим. Введите имя пользователя по умолчанию «admin» и пароль «123», чтобы войти в основной режим.

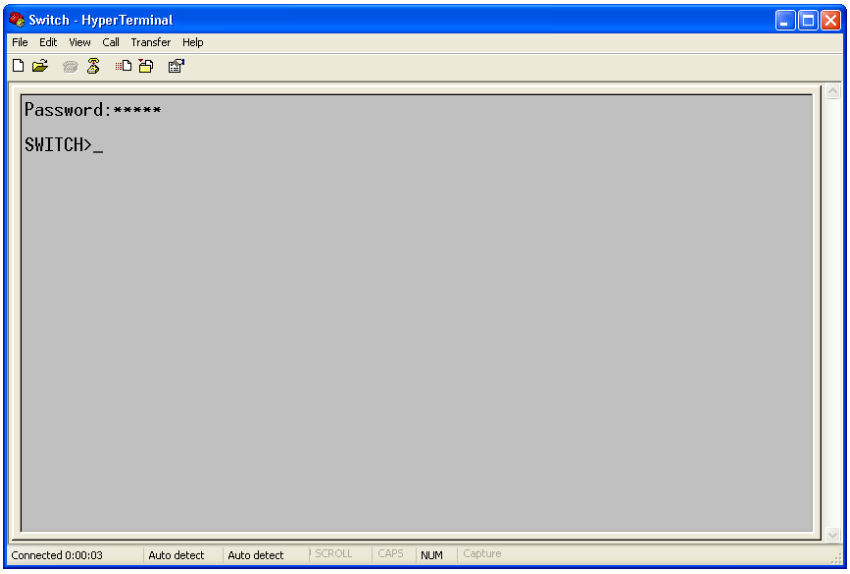



Рисунок 5 – Экран CLI

7. Введите команду «enable», имя пользователя по умолчанию «admin» и пароль «123» для входа в привилегированный режим. Вы также можете ввести данные других созданных пользователей.

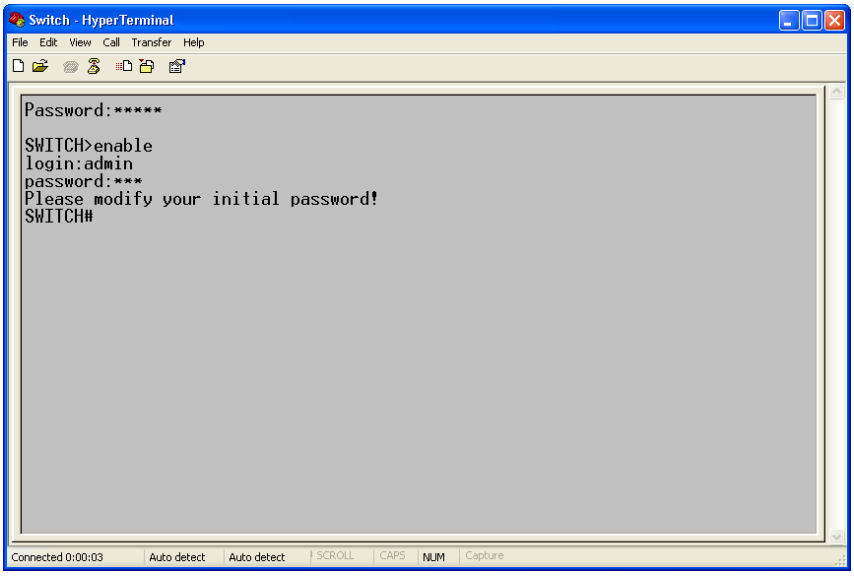



Рисунок 6 – Привилегированный режим

## 2.3 Подключение к коммутатору при помощи Telnet

1. Подключите любой RJ45 порт коммутатора к Ethernet порту ПК.

2. Откройте диалоговое окно <Выполнить> на ПК, там введите «telnet *IP-адрес*»; по умолчанию IP-адрес – 192.168.0.2.

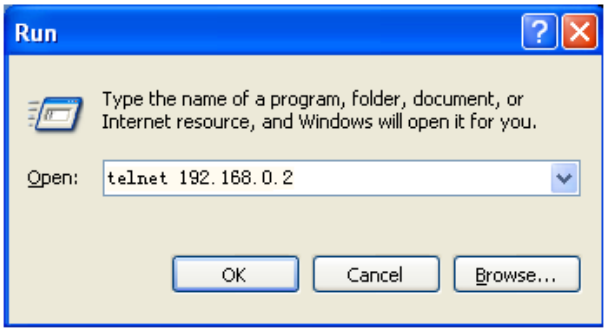



Рисунок 7 – Доступ через Telnet

При подтверждении IP-адреса, пожалуйста, обратитесь к разделу 6.2.1 «IP-адрес коммутатора» настоящего руководства для получения информации о IP адресе.

3. В интерфейсе Telnet введите имя пользователя «admin» и пароль «123» для входа в коммутатор. В дальнейшем Вы также можете ввести имя пользователя и пароль, созданные самостоятельно.

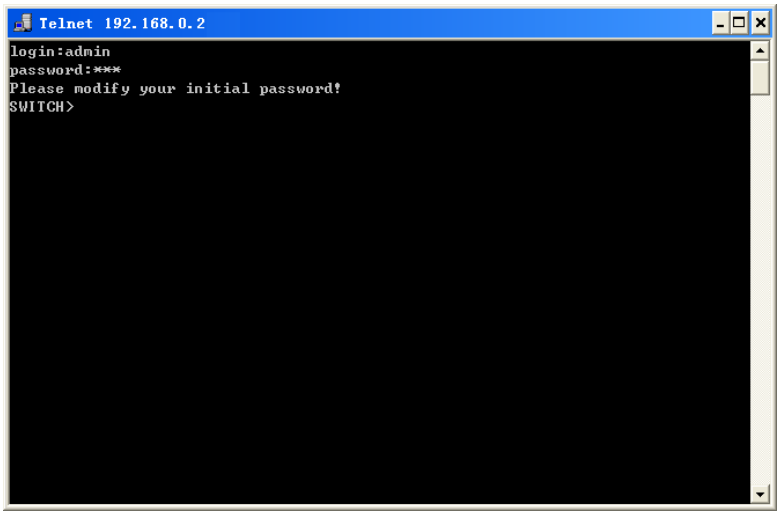



Рисунок 8 – Интерфейс терминала Telnet

## 2.4 Доступ через WEB-интерфейс

Предварительным условием для доступа к коммутатору через WEB-интерфейс является устойчивая связь между портами Ethernet ПК и коммутатора.

1. Подключите любой RJ45 порт коммутатора к Ethernet порту ПК.

2. Введите IP адрес коммутатора в web-браузере (IP адрес по умолчанию – 192.168.0.2). Появится диалоговое окно авторизации, показанное ниже. Введите:
- логин – «admin»;
- пароль – «123»;
- код верификации;
- нажмите кнопку <Login> (вход).

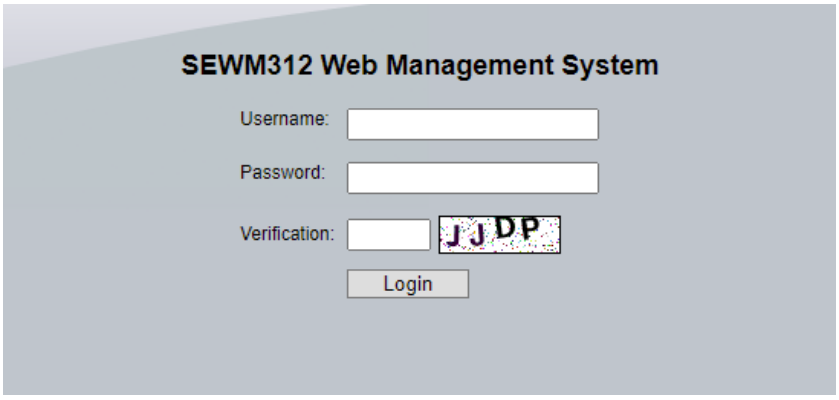



Рисунок 9 – Авторизация через WEB-интерфейс

3. После подключения к Web-интерфейсу коммутатора вы увидите навигационное дерево (меню) в левой части экрана:


Рисунок 10 – Страница WEB-интерфейса

# 3. Информация об устройстве

## 3.1 Основная информация о коммутаторе

Основная информация о коммутаторе включает имя устройства, MAC-адрес, версии аппаратного и программного обеспечения, версию BootROM, дату компиляции и время работы. Нажмите [Device Information] → [Switch basic information] для отображения основной информации о коммутаторе.

Switch basic information

```
Prompt:             SWITCH
Device MAC Address: 48-BE-2D-00-4A-28
Hardware version:   V1.0
Software version:   R0005.P01
BootRom version:    168
Device type:        SEWM312
Compiled Time:      Aug 26 2020 03:22:44
Uptime:             0 weeks, 0 days, 2 hours, 35 minutes
```

Рисунок 11 – Основная информация о коммутаторе

# 4. Управление настройками

В дереве навигации нажмите [Save current running-config], чтобы сохранить текущую конфигурацию, или [Reboot with the default configuration], чтобы перейти на страницу,

показанную на рисунке 12. Затем вы можете нажать <Yes>, чтобы восстановить конфигурацию по умолчанию.


Рисунок 12 – Восстановление конфигурации по умолчанию

## 4.1 Перезагрузка

Чтобы перезагрузить устройство, нажмите [Switch maintenance] → [Reboot] в дереве навигации. Интерфейс перезагрузки показан на рисунке 13.


Рисунок 13 – Перезагрузка

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

## 4.2 Обновление прошивки

Обновление программного обеспечения может повысить производительность коммутатора. Для этого достаточно обновить один файл прошивки. Он содержит не только версию системного ПО, но и версию ПО загрузчика (BootROM). Для обновления требуется сервер FTP/TFTP.

### 4.2.1 Обновление прошивки через FTP

Установите FTP-сервер. Ниже в качестве примера используется программное обеспечение WFTPD для обновления программного обеспечения.

1. Нажмите [Security] → [Users/Rights]. Откроется диалоговое окно «Users/Rights Security Dialog». Нажмите <New User>, чтобы создать нового пользователя FTP, как показано на рисунке 14. Создайте имя пользователя и пароль. Например, имя пользователя «admin» и пароль «123». Нажмите <OK>.

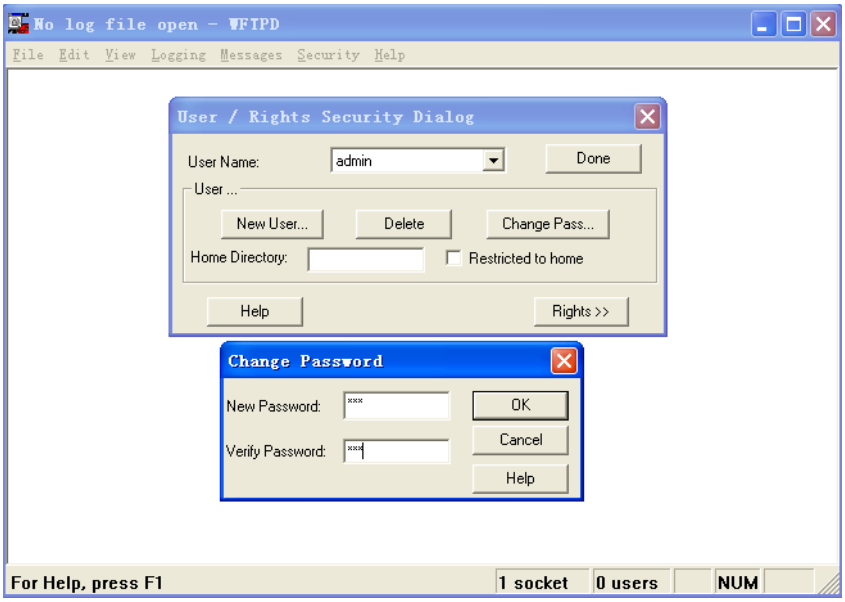



Рисунок 14 – Создание нового пользователя FTP

2. Укажите путь хранения файла с обновлением в «Home Directory», как показано на рисунке 15. Нажмите <Done>.

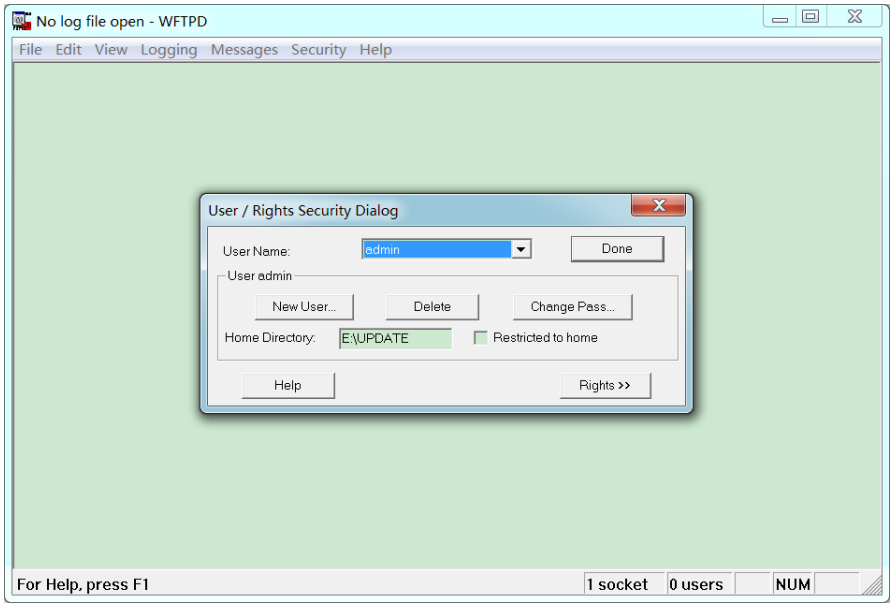



Рисунок 15 – Путь расположения файла

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

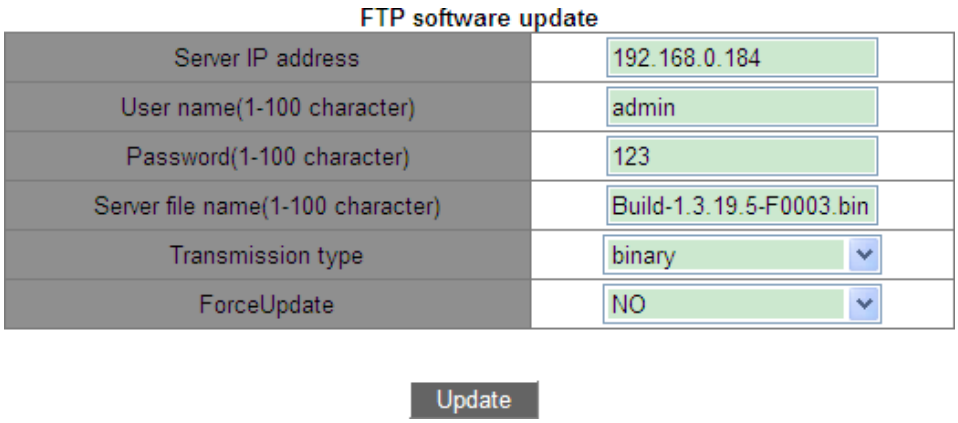



Рисунок 16 – Обновление прошивки через FTP

**Transmission type (тип передачи)**
Опции: binary/ascii.
Значение по умолчанию: binary.
Функция: выбор стандарта передачи файла.
Описание: «ascii» означает использование кодировки ASCII для передачи файла; «binary» означает использование для передачи файла двоичного кода.

**Force Update (принудительное обновление)**
Опции: Yes/No (да/нет).
Значение по умолчанию: No (нет).
Функция: выбор действия в случае, если версия программного обеспечения не соответствует аппаратному обеспечению коммутатора.
Пояснение: «No» означает отмену обновления программного обеспечения, если программное и аппаратное обеспечение не совпадают. «Yes» означает продолжение обновления программного обеспечения, даже если программное и аппаратное обеспечение не совпадают. Однако такое действие может привести к к некорректной работе системы, вплоть до невозможности запуска устройства.

---

- Имя файла должно содержать расширение. В противном случае обновление может завершиться неудачно.
- Файл версии программного обеспечения не является текстовым файлом.
- Чтобы гарантировать нормальную работу, выберите «No» для принудительного обновления. То есть, не обновляйте прошивку при несовпадении версий программного и аппаратного обеспечения.

---

4. Убедитесь, что между FTP-сервером и коммутатором установлена нормальная связь, как показано ниже.

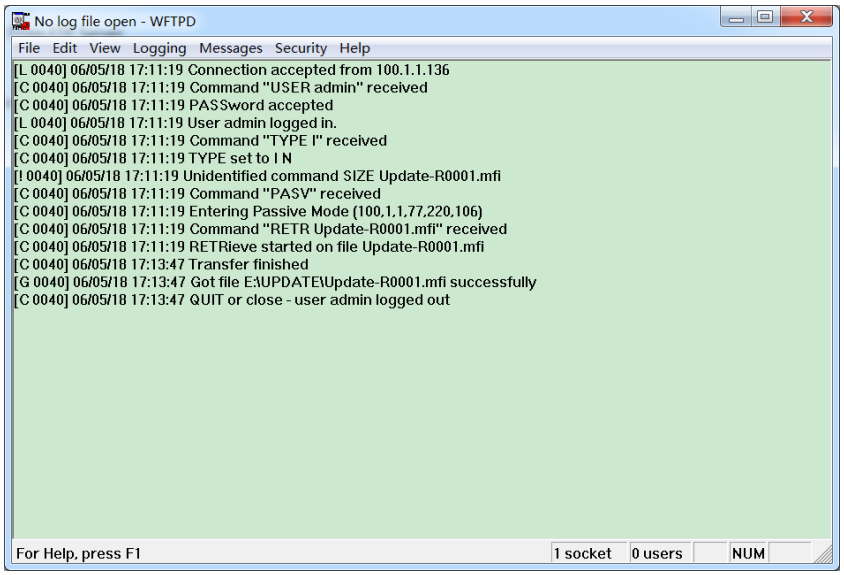



Рисунок 17 – Проверка связи с сервером FTP

---

Чтобы отобразить информацию журнала обновлений, как показано на рисунке 17, нужно нажать [Logging] → [Log Options] в WFTPD и выбрать «Enable Logging».

---

5. Когда обновление будет завершено, перезагрузите устройство и откройте страницу «Switch Basic Information», чтобы проверить, прошло ли обновление успешно и активна ли новая версия.

---

- В процессе обновления прошивки не отключайте сервер FTP.
- После завершения обновления перезагрузите устройство, чтобы активировать новую версию.
- В случае сбоя обновления не перезагружайте устройство во избежание потери файла прошивки и некорректного запуска устройства.

---

### 4.2.2 Обновление прошивки через TFTP

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

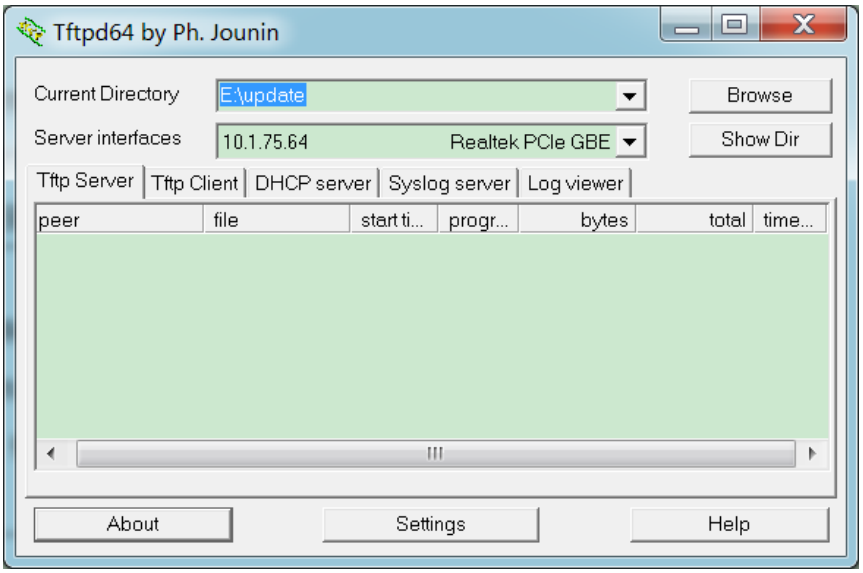



Рисунок 18 – Настройка сервера TFTP

1. В разделе «Current Directory» укажите путь хранения файла с обновлением. Введите IP-адрес сервера в разделе «Server interfaces».

2. Нажмите [Switch maintenance] → [TFTP software update] в дереве навигации, чтобы перейти на страницу обновления программного обеспечения, как показано на рисунке 19. Введите IP-адрес TFTP-сервера и имя файла на сервере. Нажмите <Update> и дождитесь завершения обновления.

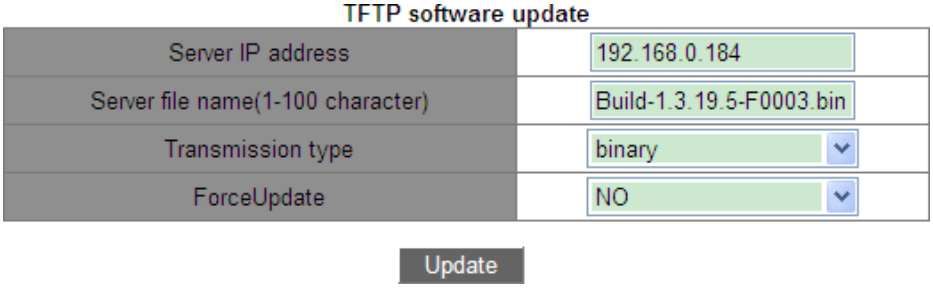



Рисунок 19 – Обновление ПО через TFTP

**Transmission type (тип передачи)**
Опции: binary/ascii.
Значение по умолчанию: binary
Функция: выбор стандарта передачи файла.
Описание: «ascii» означает использование кодировки ASCII для передачи файла; «binary» означает использование для передачи файла двоичного кода.

**Force Update (принудительное обновление)**

Опции: Yes/No (да/нет).
Значение по умолчанию: No (нет).
Функция: выбор действия в случае, если версия программного обеспечения не соответствует аппаратному обеспечению коммутатора.
Объяснение: «No» означает отмену обновления программного обеспечения, если программное и аппаратное обеспечение не совпадают. «Yes» означает продолжение обновления программного обеспечения, даже если программное и аппаратное обеспечение не совпадают. Однако такое действие может привести к системной аномалии или сбою загрузки.

---

- Имя файла должно содержать расширение. В противном случае обновление может завершиться неудачно.
- Файл версии программного обеспечения не является текстовым файлом.
- Чтобы гарантировать нормальную работу, выберите «No» для принудительного обновления. То есть, не обновляйте прошивку при несовпадении версий программного и аппаратного обеспечения.

---

3. Убедитесь, что между TFTP-сервером и коммутатором установлена нормальная связь, как показано ниже.

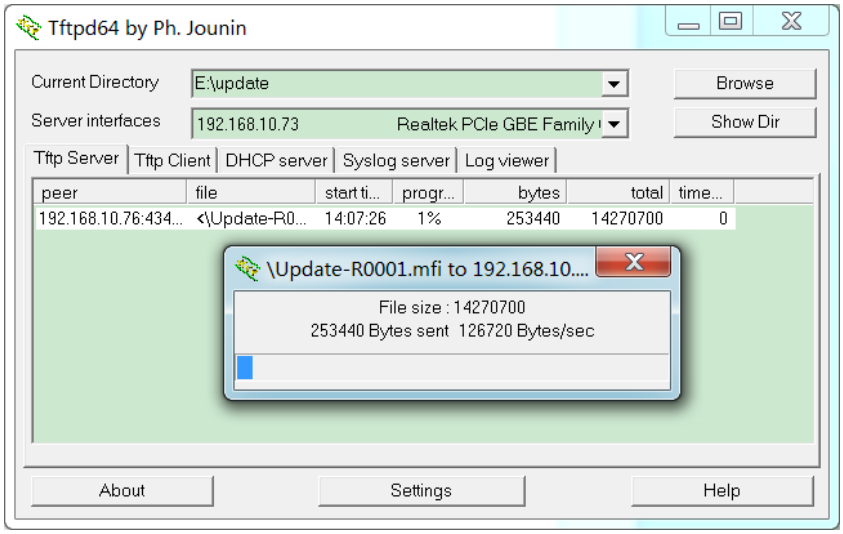



Рисунок 20 – Проверка связи с сервером TFTP

4. Когда обновление будет завершено, перезагрузите устройство и откройте страницу «Switch Basic Information», чтобы проверить, прошло ли обновление успешно и активна ли новая версия.

---

- В процессе обновления прошивки не отключайте сервер TFTP.
- После завершения обновления перезагрузите устройство, чтобы

активировать новую версию.

- В случае сбоя обновления не перезагружайте устройство, чтобы избежать потери файла ПО и ошибок загрузки.

---

# 5. Базовые настройки устройства

## 5.1 Базовые настройки коммутатора

Базовая настройки коммутатора включают имя хоста, сопоставление между именем хоста и IP-адресом, а также настройку даты и времени.

### 5.1.1 Базовые настройки

1. Настройка имени хоста.
Нажмите [Device Basic Configuration] → [Switch Basic Configuration] → [Basic Config], чтобы открыть страницу базовой конфигурации коммутатора, как показано на рисунке 21.

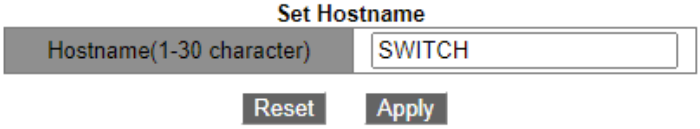



Рисунок 21 – Настройка имени хоста

**Hostname (имя хоста)**
Настраиваемый диапазон: 1~30 символов.
Значение по умолчанию: SWITCH.
Функция: настройка быстрого ввода имени хоста в интерфейсе командной строки коммутатора (CLI).

2. Настройка сопоставления между именем хоста и IP-адресом (см. рисунок 22).

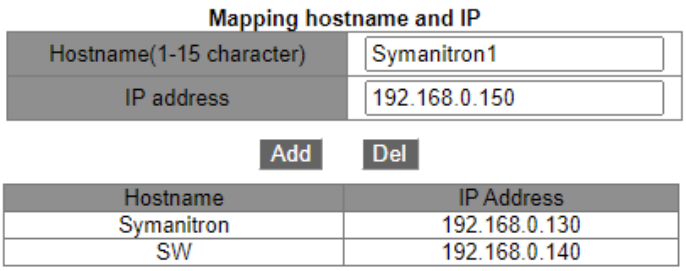



Рисунок 22 – Настройка согласования имени хоста и IP-адреса

**{Host name, IP address} – {Имя хоста, IP адрес}**
Формат: {1~15 символов, A.B.C.D}.
Значение по умолчанию: SWITCH.

Функция: в соответствии с сопоставлением используйте имя хоста для доступа к соответствующему устройству. Введите правильное имя хоста и IP-адрес. Затем нажмите <Add>, чтобы добавить запись сопоставления имени хоста и IP-адреса, или <Del>, чтобы удалить запись сопоставления.
Пример: после успешной настройки сопоставления между именем хоста «SW» и IP-адресом «192.168.0.140» вы можете пропинговать коммутатор с помощью команды «ping host SW» вместо «ping 192.168.0.140».

## 5.1.2 Настройка часов

Вы можете установить системную дату и время. Коммутаторы этой серии поддерживают часы реального времени (Real-Time Clock, RTC). Даже если устройство выключено, часы продолжают работать.
Коммутатор поддерживает функцию «Летнее время» (Daylight Saving Time, DST). В России данная функция не используется.
Нажмите [Device Basic Configuration] → [Switch Basic Configuration] → [Clock configuration], чтобы открыть страницу настройки даты и времени (см. рисунок 23).

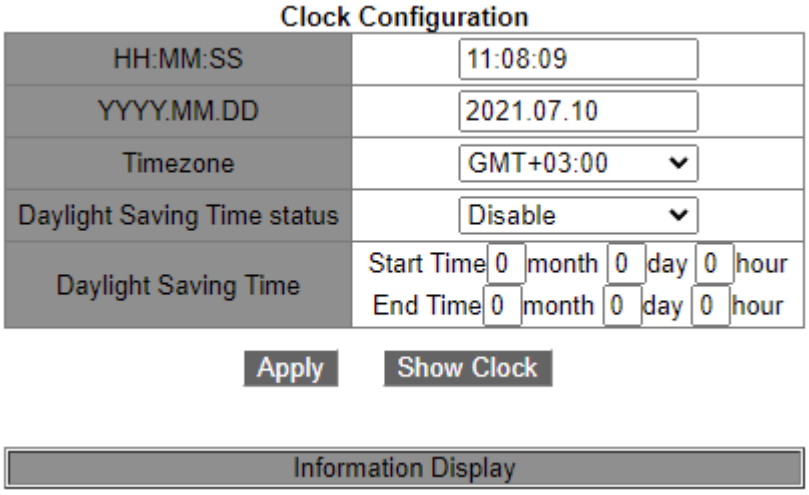



Рисунок 23 – Настройка даты и времени

**HH:MM:SS (ЧЧ:ММ:СС)**
Настраиваемый диапазон: значение HH находится в диапазоне от 0 до 23, а значение MM и SS — в диапазоне от 0 до 59.

**YYYY.MM.DD (ГГГГ:ММ:ДД)**
Настраиваемый диапазон: значение YYYY находится в диапазоне от 1970 до 2099, значение MM — от 1 до 12, а значение DD — от 1 до 31.
Описание: диапазон DD меняется в зависимости от месяца. Например, диапазон DD для марта — от 1 до 31, а для апреля — от 1 до 30. Вы можете настроить его в соответствии с реальной ситуацией.

**Timezone (часовой пояс)**
Функция: выбор часового пояса.

**Daylight Saving Time status (статус летнего времени)**
Функция: Для региона «Россия» всегда устанавливается как «Disable».

**Летнее время (Daylight Saving Time)**
Настроить временные рамки использования DST.

---

- Время начала использования DST должно отличаться от времени завершения.
- Время начала использования DST не является временем, когда DST активен (то есть, часы ещё не переведены на час вперёд). Время завершения является временем DST (то есть, часы переведены на час вперёд).

---

Например, использовать DST с 10:00:00 первого апреля до 9:00:00 первого октября.
Не-DST время будет использовано до 10:00:00 первого апреля. Затем, часы будут переведены на 11:00:00 в соответствии с Летним временем. DST будет активен до 9:00:00 первого октября. После этого, часы будут переведены на час назад, на 8:00:00, снова задействовав тем самым не-DST время.

## 5.2 Управление пользователями

Чтобы решить проблему безопасности, вызванную подключением к коммутатору незарегистрированных пользователей, ПО коммутатора обеспечивает функцию иерархического управления пользователями, основанную на различных идентификаторах пользователей и позволяет установить разные разрешения для разного типа пользователей.

Таблица 2

| **Пользователь** | **Описание** |
|---|---|
| Гость (Guest) | Самый низкий уровень. Гостевые пользователи могут только просматривать конфигурацию коммутатора, но не могут выполнять настройку или модификацию.<br>Гостевые пользователи не могут получить доступ к следующим функциям: обновление программного обеспечения, управление пользователями, передача файлов, перезагрузка, сохранение текущей конфигурации и загрузка настроек по умолчанию. |
| Супервизор (System) | Средний уровень. Пользователи уровня Супервизор имеют определенные права для доступа и настройки.<br>Пользователи уровня Супервизор не могут получить доступ к следующим функциям: обновление программного обеспечения, управление пользователями, передача файлов, перезагрузка и загрузка настроек по умолчанию.<br>Примечание: Супервизор может изменить собственный пароль. |

| | |
|---|---|
| Администратор (Admin) | Самый высокий уровень. Пользователи с правами администратора имеют права на выполнение всех функций. |

## 5.2.1 Настройка с помощью WEB-интерфейса

1. Создание пользователей.
Нажмите [Device Basic Configuration] → [User Configuration] → [User Configuration], чтобы открыть страницу настроек пользователей (см. рисунок 24).

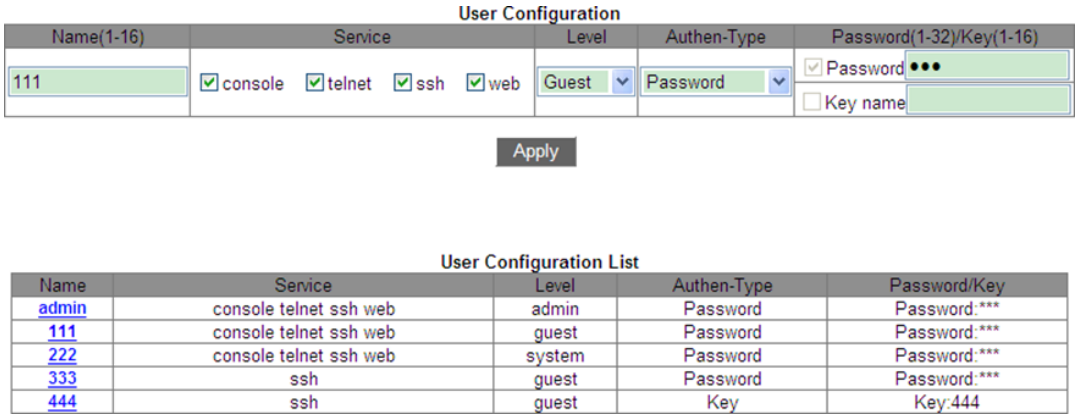



Рисунок 24 – Создание пользователей

**Name (имя)**
Настраиваемый диапазон: 1~16 символов.
Функция: настройка имени пользователя.

**Service (режим доступа)**
Опции: 1 ~ 16 символов.
Функция: выбор режима доступа к коммутатору для текущего пользователя. Можно выбрать один или несколько режимов доступа.

**Level (уровень пользователя)**
Опции: Guest/System/Admin.
Значение по умолчанию: Guest.
Функция: настройка уровня разрешений для пользователя. Пользователи с разными уровнями разрешений имеют разные права доступа.

**Authen-Type (тип аутентификации)**
Опции: Password/Key/Password or Key (Пароль/Ключ/Пароль или Ключ).
Значение по умолчанию: Password
Функция: выбор типа аутентификации, который будет использоваться при доступе текущего пользователя к коммутатору. При выборе значения «Password» необходимо

настроить параметр «Password». При выборе значения «Key» необходимо настроить параметр имени «Key name».

**Password (пароль)**
Настраиваемый диапазон: 0~32 символов.
Функция: настройка пароля, который будет использовать пользователь для подключения к коммутатору.

**Key name (имя ключа)**
Функция: выбор имени ключа, которое будет использоваться при доступе текущего пользователя к коммутатору в режиме «SSH».

---

- В настоящее время режимы подключений console/telnet/web не поддерживают режим аутентификации на основе ключа. Поэтому, когда выбраны службы console/telnet/web, проверка подлинности на основе ключа не доступна.
- SSH поддерживает два режима аутентификации: аутентификацию на основе пароля и аутентификацию на основе ключа.
- Для доступа к коммутатору можно настроить максимум 9 пользователей.
- Пользователь по умолчанию «admin» не может быть удален. Службы по умолчанию (консоль, telnet, ssh, web) и уровень (уровень администратора) этого пользователя нельзя изменить, но пароль по умолчанию (123) изменить можно.
- Информацию о режиме доступа к коммутатору SSH см. в разделе 5.11 «Настройка сервера SSH».

---

2. Изменение настроек пользователя.
Нажмите имя пользователя в списке конфигураций пользователей (см. рисунок 24). Вы можете изменить и удалить конфигурацию пользователя (см. рисунок 25).

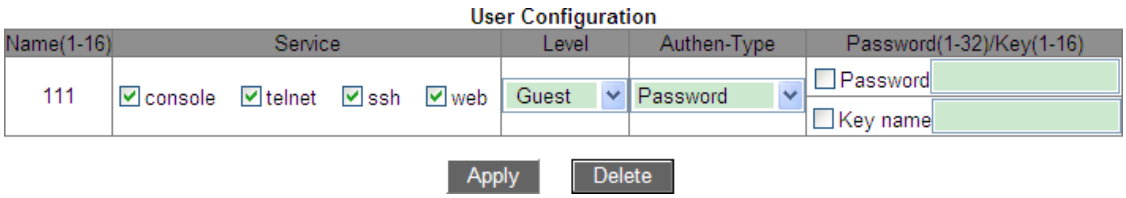



Рисунок 25 – Изменение настроек пользователя

3. Настройка ключа SSH.
Нажмите [Device Basic Configuration] → [User Configuration] → [SSH Key Configuration], чтобы открыть страницу настроек ключа SSH (см. рисунок 26).

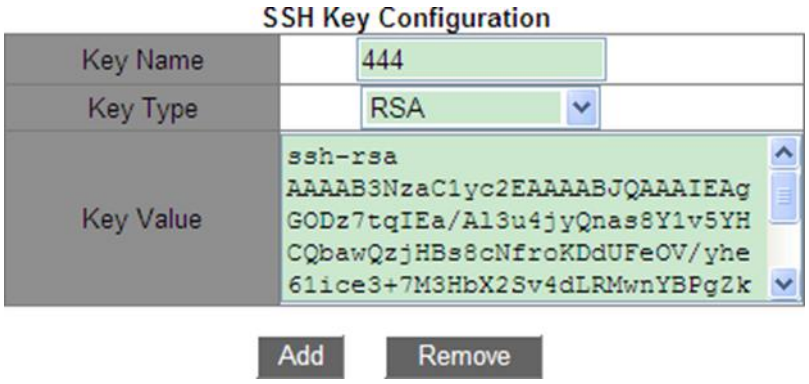



Рисунок 26 – Уровень привилегий

**Group Name (имя группы)**
Настраиваемый диапазон: 1~16 символов.

**Key Type (тип ключа)**
Опции: RSA.
Коммутаторы этой серии поддерживают только алгоритм ключа RSA.

**Key Value (значение ключа)**
Формат: {algorithm name, public key, key info} (Имя алгоритма, открытый ключ, информация о ключе).
Имя алгоритма: ssh-rsa | ssh-dsa.
Открытый ключ: основан на 64-битных кодах и имеет длину менее 2048 байт.
Информация о ключе: дополнительная информация о ключе.
Функция: настройка открытого ключа, соответствующего пользователю. Как правило, открытый ключ генерируется программным обеспечением Puttygen и копируется в значение ключа сервера, скрытый ключ (private key) обычно хранится у пользователя.

4. Изменение пароль текущего пользователя.
Нажмите [Device Basic Configuration] → [User Configuration] → [Modify Password], чтобы открыть страницу изменения пароля (см. рисунок 27).

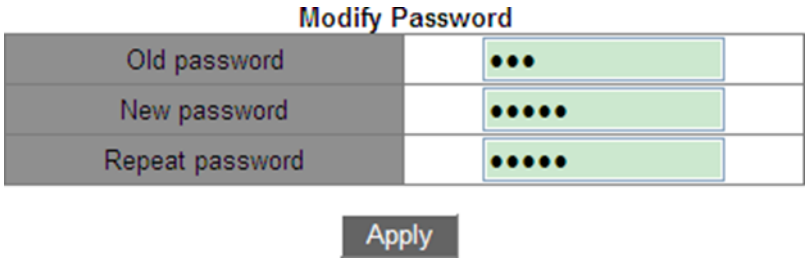



Рисунок 27 – Изменение пароля

Максимальное значение пароля – 32 символа.

5. Настройка значения тайм-аута для режимов подключения к коммутатору.
Нажмите [Device Basic Configuration] → [User Configuration] → [Timeouts Configuration], чтобы открыть страницу настройки времени ожидания (см. рисунок 28).

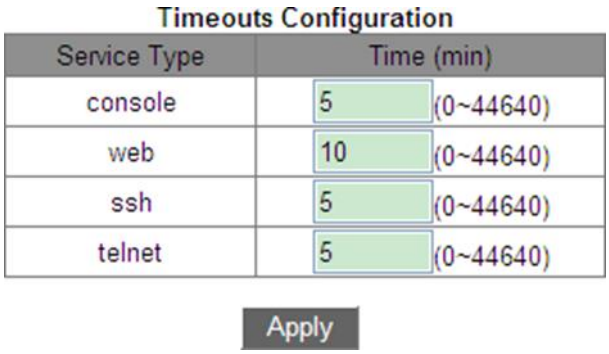



Рисунок 28 – Настройка времени ожидания

**Time (время)**
Настраиваемый диапазон: 0~44640 минут.
Значение по умолчанию: 5 минут для console/ssh/telnet и 10 минут для web.
Функция: настроить время ожидания входа пользователя и время отключения службы. Отсчет времени начинается, когда пользователь завершит все настройки. По истечении заданного времени, система автоматически выйдет из режима доступа. Если значение времени установлено на 0, пользовательская функция тайм-аута отключена. В этом случае сервер не будет определять, истекло ли время входа пользователя в систему, поэтому автоматического выхода не произойдёт.

# 5.3 Настройка портов

## 5.3.1 Настройка портов Ethernet

### 5.3.1.1 Введение

В настройках физических портов вы можете указывать тип кабеля, возможность управления, скорость/режим и другую информацию.

### 5.3.1.2 Настройка с помощью WEB-интерфейса

Чтобы открыть страницу конфигурации порта (рисунок 29), нажмите [Device Basic Configuration] → [Port configuration] → [Ethernet port configuration] → [Physical port configuration].

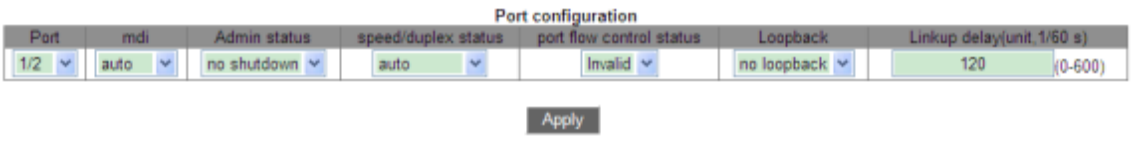



Рисунок 29 – Настройка физического порта

**Port (порт)**
Варианты: все порты коммутатора.

Описание: X/Y — формат имени порта; X — это 1 для данного коммутатора, а Y — это номер порта на панели.

**mdi (зависимость от передающей среды)**
Варианты: auto/normal/across.
Значение по умолчанию: auto – автоматический режим.
Функция: назначение типа кабеля Ethernet порта.
Описание: auto означает автоматическое определение типа кабеля; across означает, что порт поддерживает только кабели типа cross-over (или «перекрещенные»); normal означает, что порт поддерживает только кабели типа straight-through (или «прямые»).

---

Рекомендуется использовать режим auto.

---

**Статус порта (Admin status)**
Варианты: shutdown/no shutdown (закрыть/не закрывать).
Значение по умолчанию: no shutdown (не закрывать).
Функция: запрещение и разрешение передачи данных через порт.
Описание: no shutdown означает, что порт включён и через него можно передавать данные; shutdown означает, что порт выключен, и передача любых данных запрещена. Эта настройка непосредственно влияет на аппаратное состояние порта и включает тревожные оповещения о его изменении.

**Скорость/дуплексность (Speed/duplex status)**
Варианты: auto, 10M/Half, 10M/Full, 100M/Half, 100M/Full, 1000M/Half, 1000M/Full
По умолчанию: auto – автоматический режим.
Функция: настройка режима скорости и дуплекса.
Описание: скорость и режим передачи данных для порта поддерживают как автоматическое определение, так и ручную настройку. Если установлен режим «auto», скорость и режим передачи данных будут автоматически определены в соответствии с типом подключения. Если duplex-режим устанавливается вручную в full duplex или half duplex, скоростной режим также будет установлен в один из ручных режимов. Рекомендуется устанавливать этот параметр в auto во избежание проблем, возникающих при несовпадении настроек портов с двух сторон соединения. Если вы устанавливаете скорость или duplex-режим на одном из портов соединения вручную, убедитесь, что на другом конце соединения порт имеет те же настройки.

---

- Порты 10/100Base-TX могут быть установлены в режимы: auto, 10M/Half, 10M/Full, 100M/Half или 100M/Full.
- Порты 10/100/1000Base-TX могут быть установлены в режимы: auto, 10M/Half,

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

---

**port flow control status (статус управления потоком)**
Варианты: Invalid/Valid (недействительно/действительно).
Значение по умолчанию: Invalid (недействительно).
Функция: включить или отключить управление потоком через назначенный порт.
Описание: после того, как функция управления потоком будет включена, порт сообщит отправителю о замедлении скорости передачи, чтобы избежать потери пакетов в соответствии с каким-либо алгоритмом или протоколом, в том случае, если поток, полученный портом больше, чем размер кэша порта. Настройка режимов управления потоком для устройств, работающих по разным типам способа связи (дуплекс/полудуплекс) выполняется разными способами. Для устройств, работающих в полнодуплексном режиме, принимающая сторона должна отправить специальный кадр (Pause frame), чтобы сообщить отправителю о прекращении отправки сообщений. Когда отправитель получит Pause frame, он должен прекратить отправку сообщений на период «времени ожидания» (wait time), указанного в Pause frame и продолжить отправку сообщений после окончания «времени ожидания». Для устройств, работающих в полудуплексном режиме, обеспечивается поддержка режима управления потоком методом обратного давления. Дело в том, что принимающая сторона намеренно создает конфликт или выдает сигнал несущей. Соответственно, когда отправитель обнаруживает конфликт или сигнал несущей (Backoff), необходима задержка передачи данных.

**Linkup delay (задержка подключения)**
Диапазон: 0~600 (единица измерения: 1/60 с).
Значение по умолчанию: 0 с.
Функция: настройка времени задержки подключения к порту. На обеих сторонах соединения должно быть установлено одинаковое значение задержки.

Вы можете просмотреть список всех портов, содержащий информацию об их настройках и текущем состоянии (рисунок 30).

Port list

| Port | Type | mdi | Status | Admin status | Speed | Mode | Flow control | Loopback | Linkup delay(unit:1/60 s) |
|---|---|---|---|---|---|---|---|---|---|
| 1/1 | FE | auto | down | no shutdown | auto | auto | Invalid | no loopback | 0 |
| 1/2 | FE | auto | down | no shutdown | auto | auto | Invalid | no loopback | 120 |
| 1/3 | FE | auto | up | no shutdown | auto | auto | Invalid | no loopback | 0 |
| 1/4 | FE | auto | down | no shutdown | auto | auto | Invalid | no loopback | 0 |
| 1/5 | FE | auto | down | no shutdown | auto | auto | Invalid | no loopback | 0 |
| 1/6 | FE | auto | down | no shutdown | auto | auto | Invalid | no loopback | 0 |
| 1/7 | FE | auto | down | no shutdown | auto | auto | Invalid | no loopback | 0 |
| 1/8 | FE | auto | down | no shutdown | auto | auto | Invalid | no loopback | 0 |
| 1/9 | GE | auto | down | no shutdown | auto | auto | Invalid | no loopback | 0 |
| 1/10 | GE | auto | down | no shutdown | auto | auto | Invalid | no loopback | 0 |
| 1/11 | GE | auto | down | no shutdown | auto | auto | Invalid | no loopback | 0 |
| 1/12 | GE | auto | down | no shutdown | auto | auto | Invalid | no loopback | 0 |

Рисунок 30 – Список портов

### 5.3.2 Информация о портах

Нажмите [Device Basic Configuration] → [Port configuration] → [Port debug and maintenance] → [Show port information], чтобы открыть страницу информации о портах. Она содержит статус подключения порта, тип порта, статистику входящих/исходящих пакетов и другую информацию, как показано на рисунке 31.


Information Display

```
Ethernet1/8 is up, line protocol is up
Ethernet1/8 is layer 2 port, alias name is (null), index is 8
Hardware is Fast-Ethernet,  address is 00-1E-CD-0F-01-0A
PVID is 1
MTU 10240 bytes, BW 100000 Kbit
Encapsulation ARPA, Loopback  not set
Auto-duplex:  Negotiation  full-duplex,   Auto-speed:  Negotiation
100M bits
FlowControl is off,  MDI type is auto

Input and output rate statistics:
5 minute input rate 2576 bytes/sec, 29 packets/sec
5 minute output rate 1238 bytes/sec, 1 packets/sec
The last 5 second input rate 7450 bytes/sec, 78 packets/sec
The last 5 second output rate 71659 bytes/sec, 86 packets/sec

Input packets statistics:
177281 input packets, 19390123 bytes, 0 no buffer
8590 unicast packets, 7791 multicast packets, 160900 broadcast packets
0 input errors, 0 CRC, 0 frame alignment, 0 overrun, 0 ignored,
0 abort, 0 length error , 0 pause frame

Output packets statistics:
15501 output packets, 14575608 bytes, 0 underruns
14684 unicast packets, 815 multicast packets, 2 broadcast packets
0 output errors, 0 collisions , 0 pause frame

Input and output packets by length:
(64)          bytes:      91383, (65~127)      bytes:      75519,
(128~255)     bytes:       4359,  (256~511)     bytes:       1502,
(512~1023)    bytes:       7828, (1024~10240) bytes:      12191
```

Рисунок 31 – Информация о порте

## 5.4 Настройка VLAN

### 5.4.1 Введение

Любая локальная сеть (LAN) может быть разделена на несколько логических виртуальных локальных сетей (VLAN). Устройство при этом может обмениваться данными только с устройствами, находящимися с ним в одной VLAN. В результате, широковещательные

пакеты ограничиваются своей VLAN, а также оптимизируется безопасность локальной сети.
Разделение на VLAN не ограничено физическим расположением устройств. 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 коммутатор 3-го уровня.

## 5.4.2 Принцип работы

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

Таблица 3 – Структура кадра 802.1Q

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

В обычный Ethernet кадр добавляется 4-х байтный заголовок 802.1Q, который служит тегом VLAN. Заголовок 802.1Q включает следующие поля:

**Type:** 16 бит. Используется для обозначения части кадра, несущего тег VLAN. Значение: 0x8100.

**PRI:** 3 бита. Обозначает приоритет кадра в соответствии с 802.1p.

**CFI:** 1 бит. «0» обозначает Ethernet, а «1» – Token Ring.

**VID:** 12 бит. Обозначает номер VLAN. Диапазон значений: от 1 до 4093. 0, 4094 и 4095 – зарезервированные значения.

---

- VLAN 1 – это VLAN по умолчанию, его нельзя создать или удалить.
- Зарезервированные номера VLAN нужны для системных функций и также не могут быть созданы или удалены.

---

Кадр, несущий заголовок 802.1Q является тегированным; не несущий заголовок 802.1Q – соответственно, нетегированным. Внутри коммутатора все кадры являются тегированными.

## 5.4.3 VLAN на основе портов

Разделение на сети VLAN может быть либо по портам, либо по MAC адресам. Данная серия коммутаторов поддерживает разделение по портам. Устройства, принадлежащие

определённым VLAN, распознаются в соответствии с портами коммутатора. После добавления порта в указанную, он может передавать в сеть тегированные пакеты.

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

- Нетегированный порт (untag port): пересылаемые им пакеты не имеют тегов VLAN. Нетегированные порты обычно используются для подключения к терминалам, которые не поддерживают 802.1Q. По умолчанию все порты коммутатора являются нетегированными и принадлежат VLAN1.
- Тегированный порт (tag port): все пакеты, пересылаемые через тегированный порт, содержат тег VLAN. Эти порты обычно используются для соединения коммутирующих сетевых устройств.

2. Режим порта.

- Access: в режиме доступа порт должен быть нетегированным, его нельзя добавить в какую-либо VLAN.
- Trunk: когда PVID (Port VLAN ID) порта совпадает с VLAN ID кадра, пакет передаётся без тега; в противном случае, пакет передаётся с тегом. Транковые порты обычно используются для соединения коммутирующих сетевых устройств.

3. PVID (идентификатор порта VLAN).
Каждый порт имеет PVID. При получении нетегированного пакета порт добавляет к пакету тег в соответствии с PVID. По умолчанию для всех портов PVID равен 1.
PVID порта доступа — это идентификатор VLAN, к которой принадлежит порт, и его нельзя настроить.
PVID транкового порта может быть настроен как один из идентификаторов VLAN, разрешенных через порт.
В таблице 4 показано, как коммутатор обрабатывает полученные и пересылаемые пакеты в зависимости от режима порта, типа порта и PVID.

Таблица 4 – Различные режимы обработки пакетов

<table>
<tr><th colspan="2">Обработка входящих пакетов</th><th colspan="2">Обработка исходящих пакетов</th></tr>
<tr><th>Нетегированные пакеты</th><th>Тегированные пакеты</th><th>Тип порта</th><th>Обработка пакетов</th></tr>
<tr><td rowspan="2">Добавление тегов PVID к пакетам</td><td rowspan="2">➢ Если VLAN ID пакета есть в списке разрешенных VLAN, пакет принимается.<br>➢ Если VLAN ID пакета отсутствует в списке разрешенных VLAN, пакет отклоняется.</td><td>Нетегированный</td><td>Отправление пакета после удаления тега</td></tr>
<tr><td>Тегированный</td><td>Сохранение тега и отправление пакета</td></tr>
</table>

## 5.4.4 Настройка с помощью WEB-интерфейса

1. Создание и удаление VLAN.
чтобы открыть страницу конфигурации VLAN, нажмите [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Create/Remove VLAN] → [VLAN ID allocation], как показано на рисунке 32.

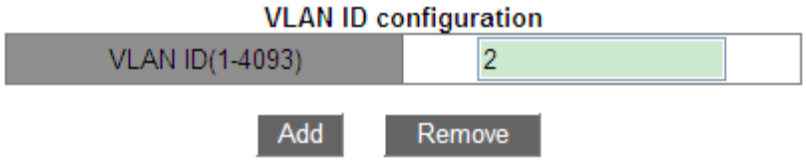



Рисунок 32 – Создание/удаление VLAN

**VLAN ID (идентификатор VLAN)**
Диапазон: 2~4093.
Функция: использование разных VLAN ID для разграничения сетей VLAN.
Описание: данные коммутаторы поддерживают до 4093 VLAN.
Действие: нажмите <Add> для создания VLAN; нажмите <Remove> для удаления выбранной VLAN.

2. Настройка имени VLAN.
чтобы открыть страницу настройки имени VLAN, нажмите [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Create/Remove VLAN] → [VLAN ID attribution configuration], как показано на рисунке 33.

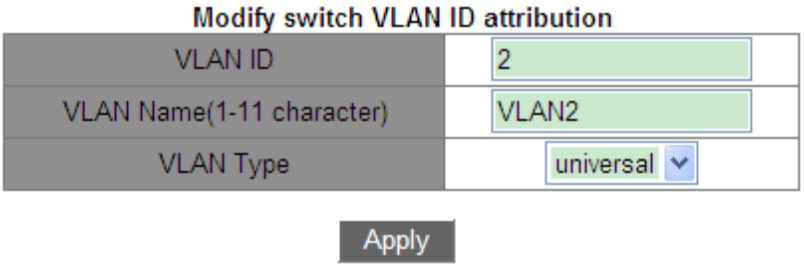



Рисунок 33 – Настройка VLAN

**VLAN ID (идентификатор VLAN)**
Диапазон: все созданные VLAN.
Функция: ввод идентификатора VLAN, имя которой необходимо изменить.

**VLAN Name (имя VLAN)**
Диапазон: 1~11 символов.
Функция: ввод имени VLAN с указанным идентификатором.

**VLAN Type (тип VLAN)**
Варианты: universal.

Значение по умолчанию: universal.

После завершения настройки на странице информации об идентификаторе VLAN отображается информация об атрибутах всех созданных сетей VLAN, как показано на рисунке 34.

**VLAN ID information**

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

Рисунок 34 – Список VLAN

3. Настройка режима порта.
Нажмите [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Port type configuration] → [Set port mode (Trunk/Access)], чтобы открыть страницу конфигурации типа порта, как показано на рисунке 35.

**Port mode configuration**

| Port | Type |
|---|---|
| 1/1 | access |

Apply

Рисунок 35 – Настройка режима порта

**Port (порт)**
Варианты: все порты коммутатора.

**Type (тип)**
Варианты: access/trunk
Значение по умолчанию: access.
Функция: выбрать режим для указанного порта. Каждый порт поддерживает только один режим.

После завершения настройки на странице конфигурации перечислены все типы портов, как показано на рисунке 36.

**Port mode configuration**

| Port | Type |
|---|---|
| 1/1 | access |
| 1/2 | access |
| 1/3 | access |
| 1/4 | access |
| 1/5 | access |
| 1/6 | access |
| 1/7 | trunk |
| 1/8 | access |
| 1/9 | access |
| 1/10 | access |
| 1/11 | access |
| 1/12 | access |

Рисунок 36 – Информация о типах портов

4. Назначение портов созданным сетям VLAN.
Нажмите [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Allocate ports for VLAN], чтобы открыть страницу конфигурации портов доступа VLAN, как показано на рисунке 37.

**Allocate ports for VLAN**

| | |
|---|---|
| VLAN ID | 2 |
| Ethernet port | 1/1 |
| Tag Type | Untag |

Add Port  Delete Port

*Note:TR : Trunk mode, TG : Tag, S-CH : Serial Card, H-CH : HSR/PRP Card, T-CH : TMS Card*

| VLAN ID | Name | Type | Media | Port ID |
|---|---|---|---|---|
| 1 | default | Static | ENET | 1/7(TR)<br>1/8<br>1/9<br>1/10<br>1/11<br>1/12 |
| 2 | VLAN2 | Static | ENET | 1/1<br>1/2<br>1/7(TR\|TG) |
| 100 | VLAN100 | Static | ENET | 1/3<br>1/4<br>1/7(TR\|TG) |
| 200 | VLAN200 | Static | ENET | 1/5<br>1/6<br>1/7(TR\|TG) |

Рисунок 37 – Назначение портов доступа сетям VLAN

**Tag Type (тип тегирования)**
Варианты: Tag/Untag (тегированный/нетегированный).
Функция: выбор типа порта для добавления в VLAN.

---

- В режиме доступа порт должен быть нетегированным и назначается в одну VLAN.
- В транковом режиме нетегированный порт добавлен в Native VLAN. Порт может быть настроен как тегированный/нетегированный и добавлен в любую другую VLAN.

---

5. Настройка PVID для транкового порта.
Нажмите [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Trunk port configuration] → [VLAN setting for trunk port], чтобы перейти на страницу конфигурации VLAN транкового порта, как показано на рисунке 38.

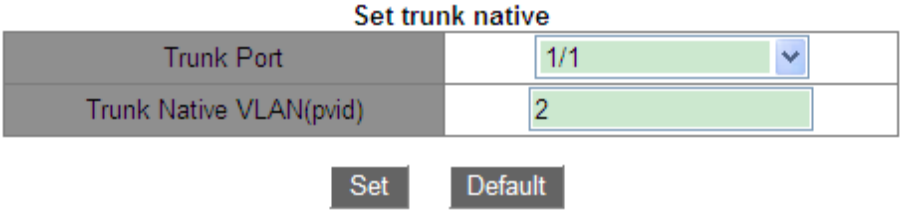



Рисунок 38 – Настройка PVID транкового порта

**Trunk Port (магистральный порт)**
Варианты: все транковые порты.

**Trunk Native VLAN (pvid) – собственная VLAN**
Варианты: все созданные VLAN.
Значение по умолчанию: 1.
Функция: настройка PVID для транкового порта.
Описание: это настройка которая определяет, какая VLAN должна быть использована по умолчанию для трафика, который не отмечен тегом VLAN в транк-соединении с другим коммутатором. По умолчанию это VLAN 1, но можно изменить её на любую другую существующую VLAN на коммутаторе. Независимо от того, является ли порт участником VLAN, находится в режиме Untag/tag, после указания PVID этот порт будет добавлен в VLAN в виде Untag.
Действие: нажмите <Default>, для возвращения PVID выбранного транкового порта к значению 1.
6. Настройка VLAN для транкового порта, как показано на рисунке 39.

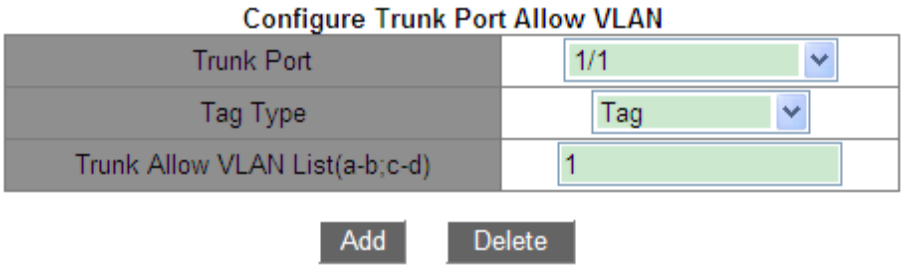



Рисунок 39 – Настройка сетей VLAN для транкового порта

**Trunk Port (транковый порт)**
Варианты: все транковые порты.

**Tag Type (тип тегирования)**
Варианты: Tag/Untag (тегированный/нетегированный).
Функция: выберите тип транкового порта, который необходимо добавить в VLAN.

**Trunk Allow VLAN List (список разрешённых VLAN)**
Варианты: все созданные VLAN.
По умолчанию: все созданные VLAN.
Функция: настроить VLAN для выбранного транкового порта.
После завершения настройки отобразится информация о VLAN всех транковых портов, как показано на рисунке 40.

| Trunk Port | Native VLAN | Allow VLAN List(Tag) | Allow VLAN List(Untag) |
|---|---|---|---|
| 1/7 | 1 | 2;100;200 | 1 |
| 1/9 | 2 | 1 | 2;100 |

Рисунок 40 – Настройка VLAN транковых портов

7. Настройка правил обработки входящего трафика VLAN для порта.
Нажмите [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [Enable/Disable VLAN ingress rule] → [Enable/Disable VLAN ingress rule] чтобы зайти на страницу настройки обработки входящих данных, как показано на рисунке 41.

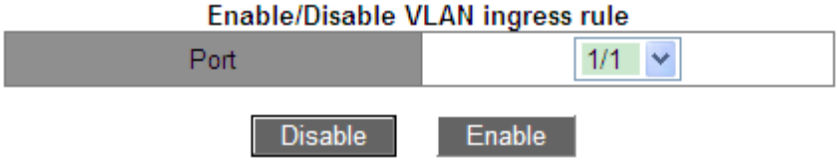



Рисунок 41 – Настройка правил обработки входящих данных VLAN

Варианты: Enable/Disable (включить/отключить).
Значение по умолчанию: Enable (включить).
Функция: включить или отключить правило входящего трафика VLAN для порта.
Описание: если эта функция включена, при получении входящих данных порт сверяет идентификатор VLAN пакета со своим разрешенным списком VLAN. Если совпадение

найдено, порт пересылает пакет; в противном случае пакет отбрасывается. Если эта функция отключена, порт пересылает все пакеты без проверки их идентификаторов VLAN. После внесения изменений, информация о правилах обработки входящих данных VLAN для всех портов будет отображена в соответствующей таблице (рисунок 42).

| Port | Type | Ingress Rule |
|---|---|---|
| 1/1 | FE | Disable |
| 1/2 | FE | Enable |
| 1/3 | FE | Enable |
| 1/4 | FE | Enable |
| 1/5 | FE | Enable |
| 1/6 | FE | Enable |
| 1/7 | FE | Enable |
| 1/8 | FE | Disable |
| 1/9 | FE | Enable |
| 1/10 | FE | Enable |
| 1/11 | FE | Enable |
| 1/12 | FE | Enable |

Рисунок 42 – Информация о правилах обработки входящих данных VLAN

8. Настройка поддержки VLAN 802.1Q (VLAN-aware).
Нажмите [Device Basic Configuration] → [VLAN configuration] → [VLAN configuration] → [VLAN-aware] → [VLAN-aware], чтобы открыть страницу настройки поддержки VLAN 802.1Q, как показано на рисунке 43.

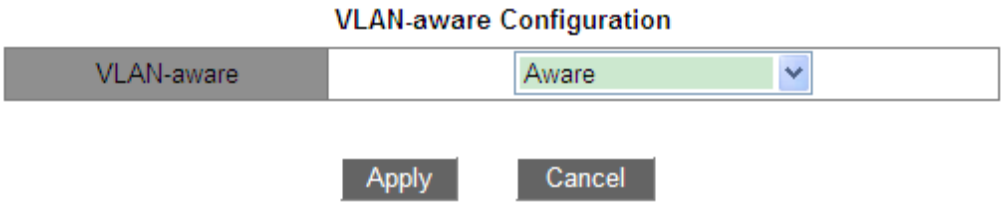



Рисунок 43 – Настройка поддержки VLAN 802.1Q

Варианты: Aware/Unaware (известно/неизвестно).
Значение по умолчанию: Aware (известно).
Функция: если выбрано значение «Aware», устройство идентифицирует и оценивает VLAN в соответствии с протоколом IEEE802.1Q и правильно пересылает пакеты. Если выбран параметр «Unaware», устройство не оценивает VLAN ID неизвестного одноадресного пакета и пересылает пакет на любой порт (в широковещательном режиме). Для известного одноадресного пакета устройство также не оценивает VLAN ID и пересылает пакет на соответствующий порт в соответствии с таблицей MAC-адресов.

9. Просмотр информации обо всех созданных VLAN.
Нажмите [Device Basic Configuration] → [VLAN configuration] → [VLAN debug and maintenance] → [Show VLAN], чтобы перейти на страницу информации о VLAN, как показано на рисунке 44.

| VLAN ID | Name | Type | Media | Portid |
|---|---|---|---|---|
| 1 | default | Static | ENET | 1/7(TR)<br>1/8<br>1/9(TR\|TG)<br>1/10<br>1/11<br>1/12 |
| 2 | VLAN2 | Static | ENET | 1/1<br>1/2<br>1/7(TR\|TG)<br>1/9(TR) |
| 100 | VLAN100 | Static | ENET | 1/3<br>1/4<br>1/7(TR\|TG)<br>1/9(TR) |
| 200 | VLAN200 | Static | ENET | 1/5<br>1/6<br>1/7(TR\|TG) |

Рисунок 44. Информация о VLAN.

### 5.4.5 Пример типовой настройки

Как показано на рисунке 45, вся локальная сеть разделена на 3 VLAN: VLAN2, VLAN100 и VLAN200. Требуется, чтобы устройства в одной VLAN могли взаимодействовать друг с другом, но разные VLAN были изолированы. Конечные ПК не могут различать тегированные пакеты, поэтому порты, соединяющие коммутатор A и коммутатор B с ПК, настроены в режиме «access». Пакеты VLAN2, VLAN100 и VLAN200 должны передаваться между коммутатором A и коммутатором B, поэтому порты, соединяющие коммутаторы, должны быть настроены режиме «trunk», что позволит пропускать пакеты VLAN 2, VLAN 100 и VLAN 200. В таблице 5 показана соответствующая конфигурация.

Таблица 5 – Настройка VLAN

| **VLAN** | **Настройка** |
|---|---|
| VLAN2 | Порты 1/1 и 1/2 коммутаторов A и B в режиме Untag, а порт 1/7 в режиме Tag. |
| VLAN100 | Порты 1/3 и 1/4 коммутаторов A и B в режиме Untag, а порт 1/7 в режиме Tag. |
| VLAN200 | Порты 1/5 и 1/6 коммутаторов A и B в режиме Untag, а порт 1/7 в режиме Tag. |

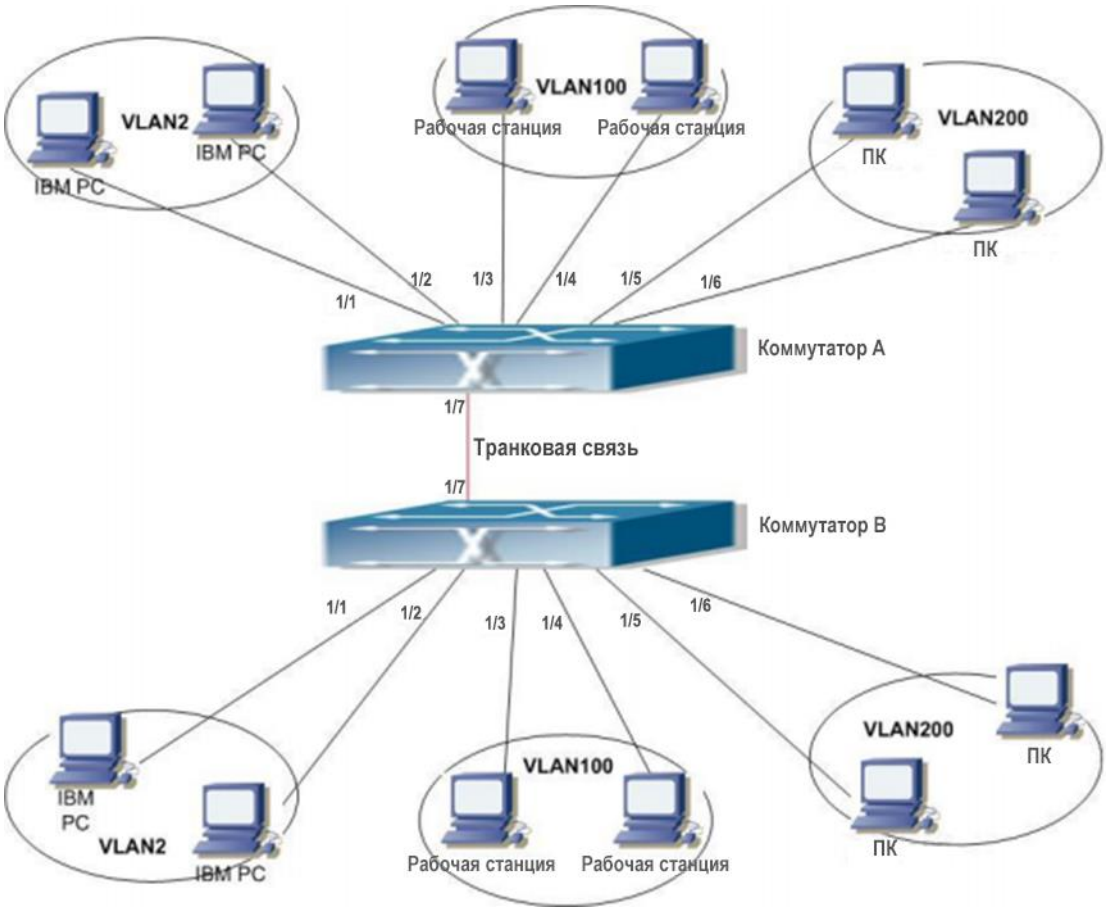



Рисунок 53 – Схема VLAN

**Настройки на коммутаторах A и B:**
1. Создайте VLAN2, VLAN100 и VLAN200 (см. рисунок 32).

2. Настройте порты 1/1, 1/2, 1/3, 1/4, 1/5, 1/6 в качестве портов доступа и порт 1/7 в качестве транкового порта (см. рисунок 35).

3. Добавьте порты 1/1 и 1/2 в VLAN2 как нетегированные порты; порты 1/3 и 1/4 в VLAN100 как нетегированные порты; порты 1/5 и 1/6 в VLAN200 как нетегированные порты; порт 1/7 в VLAN2, VLAN100, VLAN200 как тегированный порт (см. рисунок 37).

## 5.5 Настройка PVLAN

### 5.1.1 Введение

Для реализации комплексной функции изоляции трафика порта, обеспечения безопасности сети и изоляции широковещательного домена PVLAN (изолированная или частная VLAN) использует два уровня технологии изоляции. Верхняя (upper) VLAN – это VLAN с общим доменом, в которой порты являются магистральными (Uplink). Нижняя

(lower) VLAN – это VLAN с изолированными доменами, в которых порты являются оконечными (Downlink). Оконечные порты могут быть назначены в различных изолированных доменах, и они могут одновременно устанавливать соединение с магистральным портом. Изолированные домены не могут устанавливать соединение друг с другом.

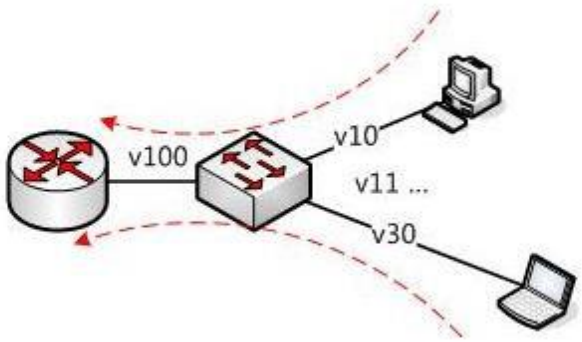



Рисунок 46 – Схема PVLAN

Как показано на рисунке 46, общим доменом является VLAN 100, а изолированными доменами являются VLAN 10 и VLAN 30; устройства в изолированных доменах могут устанавливать соединение с устройством в общем домене, например, VLAN 10 может связываться с VLAN 100; VLAN 30 также может взаимодействовать с VLAN100, но устройства в изолированных доменах не могут устанавливать соединение друг с другом, например, VLAN 10 не может связываться с VLAN 30.

## 5.5.2 Описание

Функция PVLAN может быть реализована посредством специальной настройки портов.

- PVID магистральных портов совпадает с идентификатором VLAN общего домена; PVID оконечных портов совпадает с их собственным идентификатором VLAN изолированного домена.
- Магистральные порты устанавливаются в режим Untag и назначаются в общий домен VLAN и во все изолированные домены; оконечные порты устанавливаются в режим Untag и назначаются VLAN в общий домен VLAN и в собственный изолированный домен.

## 5.5.3 Пример типовой настройки

На рисунке 47 показано пример конфигурации PVLAN. VLAN 300 является общим доменом, а порт 1 и порт 2 – магистральными портами; VLAN 100 и VLAN 200 являются изолированными доменами, а порты 3, 4, 5 и 6 являются оконечными портами.

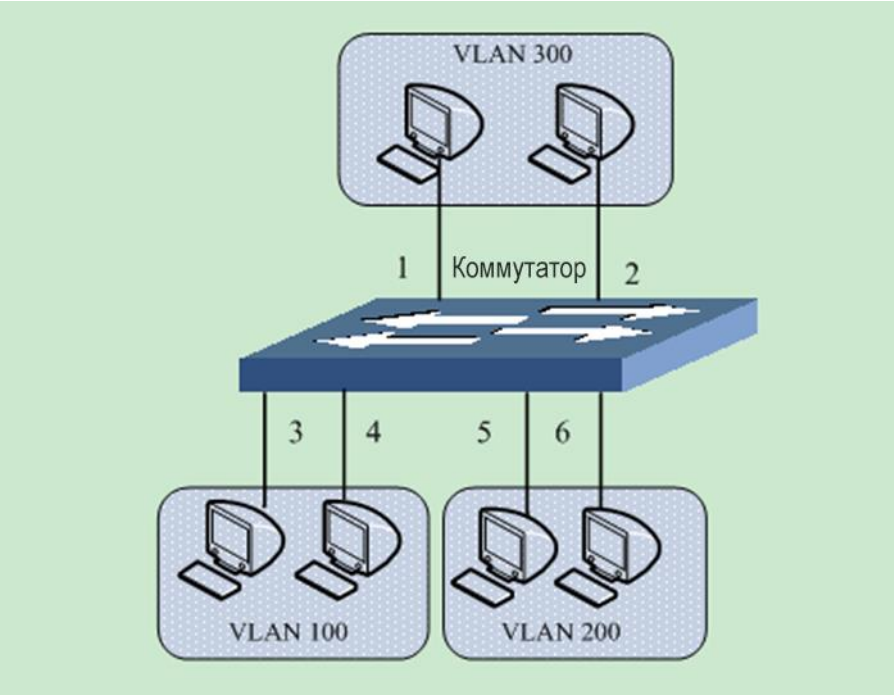



Рисунок 47 – Пример настройки PVLAN

Настройка коммутатора:
1. Создайте VLAN300, VLAN 100, VLAN 200 (см. рисунок 32).
2. Настройте порты 1, 2, 3, 4, 5, 6 как магистральные (транковые) порты (см. рисунок 35).
3. Добавьте порты 1~6 в сеть VLAN300 в режиме Untag; порты 1~4 в VLAN100 в режиме Untag; порты 1, 2, 5, 6 в VLAN200 в режиме Untag (см. рисунок 37).
4. В окне «Trunk Native VLAN (pvid)» введите следующие значения: PVID портов 1 и 2 – 300; PVID портов 3 и 4 – 100; PVID портов 5 и 6 (см. рисунок 38).

## 5.6 Зеркалирование портов

### 5.6.1 Введение

При помощи функции зеркалирования портов «Port Mirroring» коммутатор копирует все полученные или переданные кадры данных на одном порту (исходный порт зеркалирования) на другой порт (порт назначения зеркалирования). Порт назначения зеркалирования подключается к анализатору протокола или RMON-монитору для отслеживания сети, управления и диагностики неисправностей.

### 5.6.2 Описание

Коммутатор поддерживает только один порт назначения для зеркалирования, но несколько портов-источников.
Порты, данные которых зеркалируются, могут быть в одной сети VLAN или в разных. При этом, порты источника и назначения зеркалирования также могут быть в одной или в разных VLAN.
Исходный порт и порт назначения не могут являться одним и тем же портом.

- Порт назначения зеркалирования и логический интерфейс Port channel являются взаимоисключающими. Порт назначения зеркалирования не может быть добавлен к Port channel, и ни один физический порт интерфейса Port channel не может быть выбран в качестве порта назначения зеркалирования.
- Порт назначения зеркалирования и резервный порт являются взаимоисключающими. Порт назначения зеркалирования не может быть настроен в качестве резервного порта, а резервный порт не может быть настроен в качестве порта назначения зеркалирования.
- Резервный порт в этом документе относится к кольцевому порту Sy2-Ring, резервному порту Sy2-Ring, кольцевому порту Sy2-RP, резервному порту Sy2-RP, порту RSTP или MSTP.

## 5.6.3 Настройка с помощью WEB-интерфейса

1. Выберите порт источника зеркалирования и режим зеркалирования.
Нажмите [Device Basic Configuration] → [Port mirroring configuration] → [Mirror configuration], чтобы открыть страницу конфигурации исходного порта, как показано на рисунке 48.

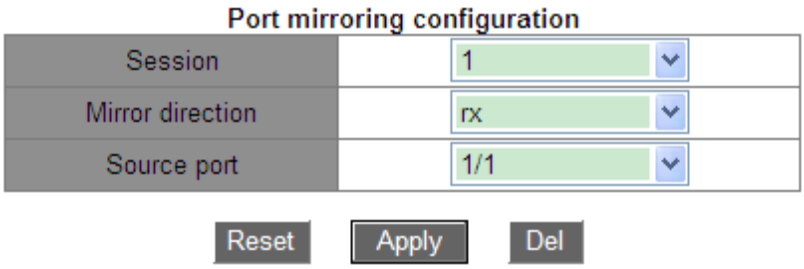



Рисунок 48 – Настройка порта-источника

**Session (сессия)**
Варианты: 1~7.
Значение по умолчанию: 1.
Функция: выбрать группу зеркалирования.

**Mirror direction (направление зеркалирования)**
Варианты: rx/tx/both (приём/передача/оба).
Значение по умолчанию: rx (приём).
Функция: выбрать на исходном порту данные для зеркалирования.
Описание: «rx» обозначает, что зеркалироваться будут только получаемые данные.
«tx» обозначает, что зеркалироваться будут только передаваемые данные.
«both» обозначает, что зеркалироваться будут все данные.

**Source port (порт-источник)**
Варианты: все порты коммутатора.
Функция: выбор порта-источника зеркалирования. Можно выбрать несколько портов.

2. Выберите порт назначения зеркалирования, как показано на рисунке 49.

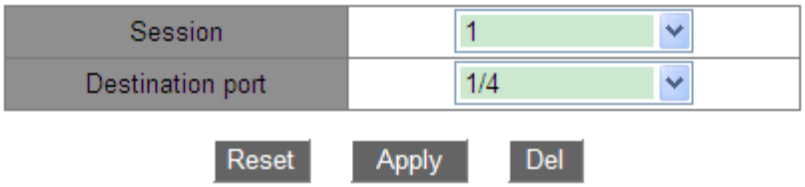



Рисунок 49 – Настройка порта назначения

**Session (сессия)**
Варианты: 1~7.
Значение по умолчанию: 1.
Функция: выбрать группу зеркалирования.

**Destination port (порт назначения)**
Варианты: все порты, кроме порта-источника.
Функция: выбор порта назначения зеркалирования.
Описание: выберите порт, куда будут отправляться зеркалируемые данные. Можно выбрать только один порт назначения. Порт назначения зеркалирования не может быть участником группы Port channel. Желательно, чтобы пропускная способность порта назначения была больше или равна суммарной пропускной способности портов-источников.

## 5.6.4 Пример типовой настройки

Как показано на рисунке 50, порт назначения зеркалирования — это порт 2, а порт источника — порт 1. Как передаваемые, так и принимаемые пакеты на порту 1 зеркалируются на порт 2.

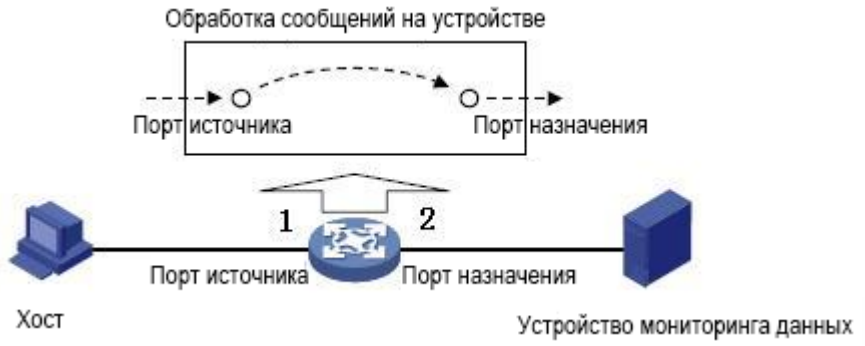



Рисунок 50 – Пример зеркалирования портов

Процесс настройки:
1. Установите порт 2 в качестве порта назначения зеркалирования, как показано на рисунке 49.
2. Установите порт 1 в качестве исходного порта. Выберите значение «both» в окне «Mirror direction», как показано на рисунке 48.

## 5.7 Подавление штормов

### 5.7.1 Введение

**Port Storm Control** (контроль штормов на порту) – механизм, предназначенный для ограничения широковещательных/многоадресных/неопознанных одноадресных пакетов данных, принимаемых портом.
Когда количество входящих широковещательных/многоадресных/неопознанных одноадресных пакетов превышает указанный порог, система начнёт отбрасывать весь входящий широковещательный/многоадресный/неопознанный одноадресный трафик для обеспечения нормальной работы сети.

### 5.7.2 Настройка с помощью WEB-интерфейса

1. Настройка порогового значения для подавления штормов.
Нажмите [Device Basic Configuration] → [Port Storm Suppression configuration] → [Port Storm Suppression configuration], чтобы открыть страницу настройки, как показано на рисунке 51.

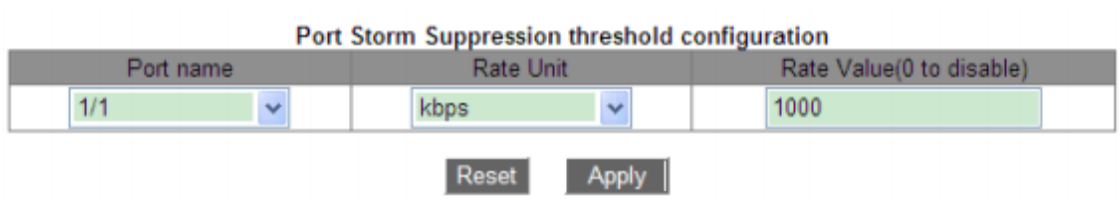



Рисунок 51 – Настройка порога подавления штормов для порта.

**Port name (имя порта)**
Варианты: все порты коммутатора.
Действие: выбрать порты, которым нужно установить режим ограничения.

**Rate Unit (единица измерения)**
Параметры: bps/kbps/percent (бит/с; Кбит/с; процент).
Функция: выбрать единицу измерения порога.

**Rate Value (пороговое значение скорости)**
Диапазон: 1~1000000 Кбит/с; 1~1000000000 бит/с; 1~100 процентов.
Значение по умолчанию: 0. Когда значение равно 0, подавление штормов на порту отключено.

Функция: настроить пороговое значение трафика на порту. Пакеты, превышающие пороговое значение, будут отброшены. Диапазон значений зависит от фактической пропускной способности порта (см. табл. 6).
Описание: порог порта Fast Ethernet находится в диапазоне 1~100000 Кбит/с или 1~100000000 бит/с; порог порта Gigabit Ethernet находится в диапазоне 1~1000000 Кбит/с или 1~1000000000 бит/с. Процент соответствует пропускной способности порта, например, если значение порога ограничения трафика на порту 100 Мбит составляет 60%, порт начинает отбрасывать пакеты после получения 60 Мбит данных.

Таблица 6 – Диапазон значений порога скорости порта

| **Пропускная способность порта** | **Единица измерения** | **Шаг** | **Диапазон значений** |
|---|---|---|---|
| 10Mb | bps | 512 | 512~10000000 |
| | kbps | Не рекомендуется | Не рекомендуется |
| 100Mb | bps | 5120 | 5120~100000000 |
| | kbps | 5 | 5~100000 |
| 1000Mb | bps | 51200 | 51200~1000000000 |
| | kbps | 50 | 50~1000000 |

2. Выберите тип контролируемых пакетов, как показано на рисунке 52.

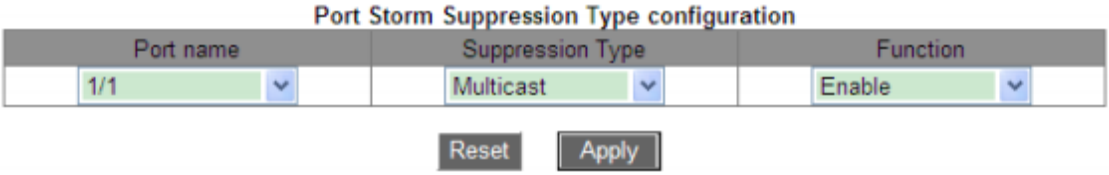



Рисунок 52 – Настройка типа контролируемых пакетов

**Port name (имя порта)**
Варианты: все порты, на которых включена функция Storm control.

**Suppression Type (тип подавления)**
Варианты: Multicast/Broadcast/dlf (многоадресные/широковещательные/неопознанные).
Функция: выбрать тип пакетов для контроля.

**Function (функция)**
Опции: Enable/Disable (включить/отключить).
По умолчанию: Disable (отключить).
Функция: включение или выключение контроля за выбранным типом трафика.

На каждом порту может быть настроено только одно пороговое значение, применяемое к выбранному типу данных.

### 5.7.3 Пример типовой настройки

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

Процесс настройки:
1. Выберите порт 1/1 и задайте единицу измерения скорости в kbps а пороговое значение скорости – 1000, как показано на рисунке 51.
2. Установите режим «Multicast» в меню «Suppression Type», как показано на рисунке 52.

## 5.8 Изоляция портов

### 5.8.1 Введение

Чтобы реализовать изоляцию пакетов на 2-м уровне, можно добавить порты в разные VLAN. Однако этот метод приведет нерациональному расходованию ограниченных ресурсов VLAN. Функция изоляции портов предоставляет пользователям более безопасное и гибкое сетевое решение, позволяя изолировать порты в одной и той же VLAN друг от друга. Достаточно добавить порт в группу изоляции, и порты, находящиеся в этой группе, не смогут обмениваться пакетами. В то же время порты из различных групп изоляции или неизолированные могут пересылать данные друг другу обычным образом.

- Порты группы изоляции могут быть только портами одного и того же коммутатора.
- Одно устройство поддерживает максимум 14 групп изоляции, и количество портов Ethernet в каждой группе не ограничено.
- После настройки группы изоляции только пакеты между портами группы изоляции не могут обмениваться друг с другом, связь между портами в группе изоляции и портами вне группы не затрагивается.
- Изолированный порт и логический интерфейс Port channel являются взаимоисключающими. Порт группы изоляции нельзя добавить в Port channel, так же, как и порт из группы Port channel нельзя изолировать.
- Не рекомендуется, чтобы порты в группе изоляции одновременно настраивались как резервные порты, а резервные порты не могут быть добавлены в группу изоляции.

### 5.8.2 Настройка с помощью WEB-интерфейса

Разрешите изоляцию портов, как показано на рисунке 53.

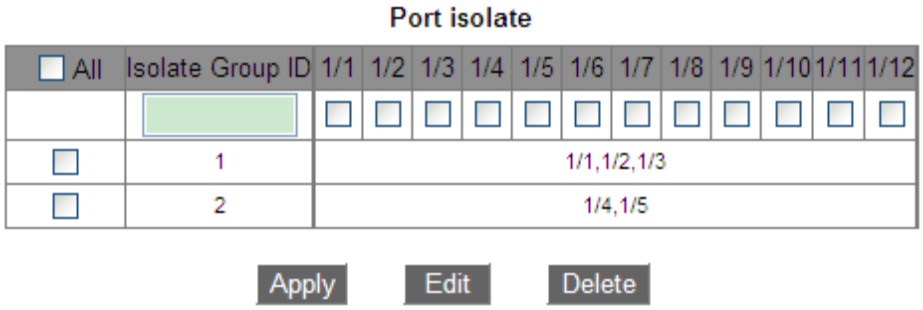



Рисунок 53 – Настройка изоляции портов

**Port isolate (изоляция порта)**
Варианты: включить/отключить.
Значение по умолчанию: отключить.
Функция: включить или отключить изоляцию порта.

---

Один порт может быть добавлен только в одну группу изоляции.

---

## 5.8.3 Пример типовой настройки

Подключите ПК1, ПК2 и ПК3 к портам Ethernet 1, 2 и 3 коммутатора, а порт 4 подключите к внешней сети. Порты 1, 2, 3 и 4 входят в сеть VLAN 1. ПК1, ПК2 и ПК3 не могут обмениваться данными друг с другом, но имеют доступ к внешней сети, как показано на рисунке 54.

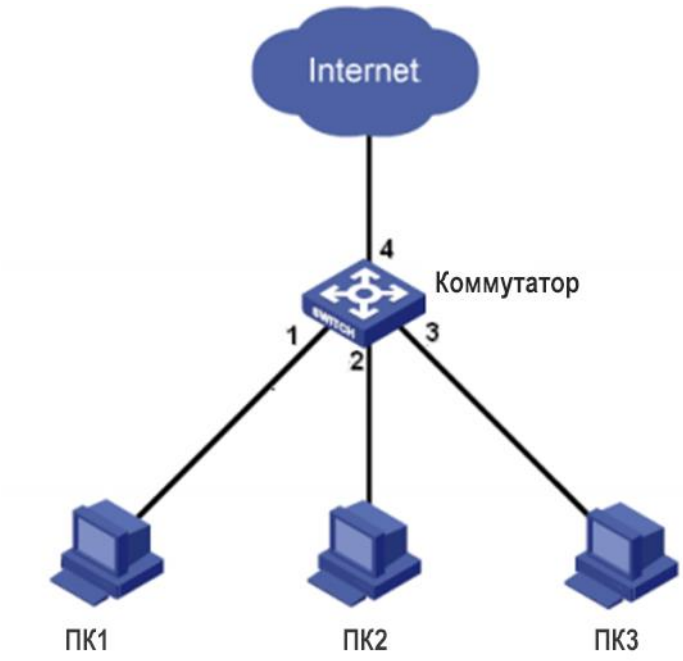



Рисунок 54 – Схема подключения изолированных портов

Добавьте порты 1, 2 и 3 в группу изоляции, чтобы изолировать ПК1, ПК2 и ПК3, как показано на рисунке 53.

## 5.9 Агрегирование портов

### 5.9.1 Введение

Технология **Port channel** предназначена для объединения группы физических портов с одинаковой конфигурацией в один логический порт для увеличения пропускной способности и повышения скорости передачи. Порты-участники одной группы совместно используют трафик и служат друг для друга динамическими резервными копиями, повышая надежность соединения.
Для управления группами агрегации используется протокол LACP (Link Aggregation Control Protocol). Объединение физических портов происходит на уровне настроек. Только порты, соответствующие определённым условиям и объединённые в группу, могут быть агрегированными и становиться независимым логическим портом Port channel, тем самым увеличивая пропускную способность сети и обеспечивая резервирование канала.

### 5.9.2 Реализация

Как показано на рисунке 55, три порта на коммутаторах A и B объединяются, образуя один агрегированный канал Port channel. Пропускная способность такого канала — это общая пропускная способность входящих в него трёх портов.

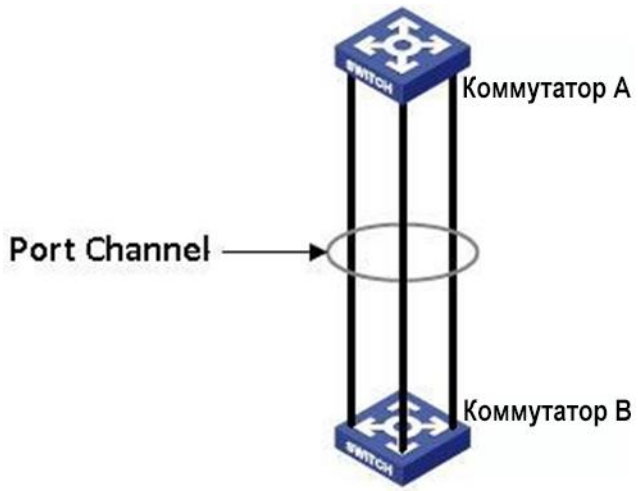



Рисунок 55 – Агрегированный канал Port channel

Если коммутатор A отправляет данные на коммутатор B через Port channel, то коммутатор A использует порты группы в соответствии с алгоритмом балансировки нагрузки. Если один из портов группы выходит из строя, данные отправляются через оставшиеся порты, также в соответствии с алгоритмом балансировки.

### 5.9.3 Пояснение

Коммутаторы серии поддерживают не более 8 групп портов; каждая группа содержит не более 8 агрегированных портов-участников.

- Порт можно добавить только в одну группу портов.
- Агрегированный и изолированный порты являются взаимоисключающими. Порт из группы Port channel нельзя добавить в группу изоляции; порт группы изоляции не может быть добавлен в агрегированный канал.
- Агрегированный порт и порт назначения зеркалирования являются взаимоисключающими. Порт из группы Port channel нельзя настроить как порт назначения зеркалирования; порт назначения зеркалирования не может быть добавлен в агрегированный канал.
- Агрегированный порт и резервный порт являются взаимоисключающими. Порт из группы Port channel не может быть настроен как резервный порт, а резервный порт не может быть добавлен в агрегированный канал.

## 5.9.4 Настройка с помощью WEB-интерфейса

1. Настройте режим распределения нагрузки канала Port channel.
Нажмите [Device Basic Configuration] → [Port channel configuration] → [LACP port group configuration], чтобы открыть страницу конфигурации, как показано на рисунке 56.

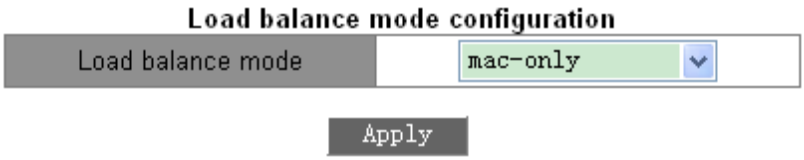



Рисунок 56 – Настройка режима распределения нагрузки

**Load balance mode (режим балансировки нагрузки)**
Варианты: mac-only/ip-only/mac-ip/ip-l4/mac-ip-l4
Значение по умолчанию: mac-only (только MAC-адреса).
Функция: назначение режима распределения нагрузки для агрегированной группы.
Описание: «mac-only» обозначает балансировку, основанную на MAC адресах устройств. «ip-only» обозначает балансировку, основанную на IP адресах устройств. «mac-ip» обозначает балансировку, основанную и на MAC, и на IP адресах устройств. «ip-l4» обозначает балансировку, основанную на IP адресах устройств и номерах портов TCP/UDP. «mac-ip-l4» обозначает балансировку, основанную на IP и MAC адресах устройств, а также на номерах портов TCP/UDP.
Пояснение: если режим балансировки нагрузки необходимо изменить после создания агрегированной группы, изменения вступят в силу после следующей агрегации.

2. Создание или удалите группы портов (см. рисунок 57).


Рисунок 57 – Настройка группы Port channel

**LACP group number (номер группы)**
Диапазон: 1~8.
Функция: задать номер группы портов (максимум 8 групп).

**Operation type (тип операции)**
Варианты: add port group/remove port group (добавить группу/удалить группу).
Значение по умолчанию: add port group (добавить группу портов).
Функция: Добавление или удаление группы портов.
После завершения настройки в соответствующей таблице будут представлены все созданные группы портов и режимы распределения нагрузки, как показано на рисунке 58.

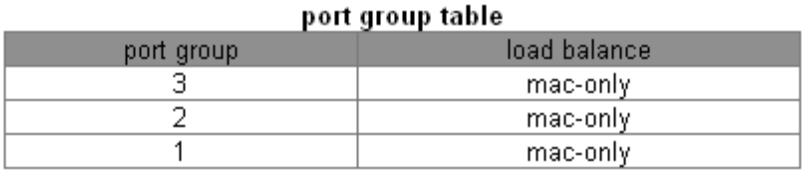



Рисунок 58 – Таблица групп портов

3. Настройка порта-участника группы.
Нажмите [Device Basic Configuration] → [Port channel configuration] → [port configuration], чтобы открыть страницу настройки, как показано на рисунке 59.

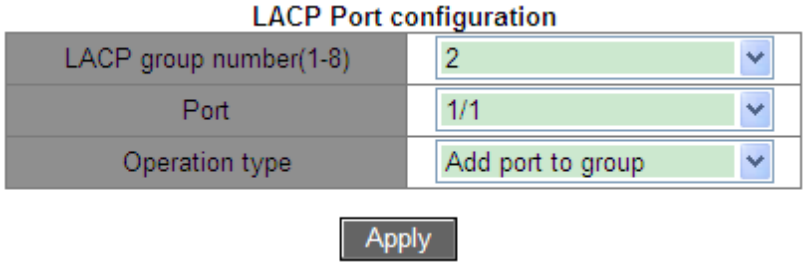



Рисунок 59 – Настройка порта-участника группы

**LACP group number (номер группы)**
Варианты: номера всех созданных групп портов.

**Port (порт)**
Варианты: все порты коммутатора.

Функция: выберите порт, который необходимо добавить или удалить из группы портов.
Описание: порты-участники группы имеют одинаковые свойства.

**Operation type (тип операции)**
Варианты: Add port to group/Remove port from group (добавить порт в группу/удалить порт из группы).
Значение по умолчанию: Add port to group.
Функция: добавить или удалить порт из группы портов.

### 5.9.5 Пример типовой настройки

Как показано на рисунке 55, добавьте три порта (порт 1, 2 и 3) коммутатора A в группу портов 1 и три порта (порт 1, 2 и 3) коммутатора B в группу портов 2. Соединив эти порты при помощи сетевых кабелей, мы получим агрегированный канал Port channel, реализующий механизм распределения нагрузки между портами. Подразумевается, что порты-участники канала на коммутаторах A и B имеют одинаковые настройки.

**Настройки на коммутаторах:**
1. Добавьте группу портов 1 на коммутатор A, как показано на рисунке 57;
2. Добавьте порты 1, 2 и 3 в группу портов 1, как показано на рисунке 58;
3. Добавьте группу портов 2 на коммутатор B, как показано на рисунке 57;
4. Добавьте порты 1, 2 и 3 в группу портов 2, как показано на рисунке 58.

## 5.10 Настройка сервера Telnet

### 5.10.1 Введение

Telnet – это протокол доступа к удалённым терминалам. При помощи Telnet вы можете войти на удалённое устройство, используя его IP-адрес или имя. Telnet передаёт команды на удалённый узел и возвращает информацию о результате на ваш монитор посредством TCP.
Telnet использует архитектуру «клиент-сервер». Локальная машина является клиентом, а удалённый узел – сервером. Данные коммутаторы могут быть как серверами, так и клиентами.
Когда коммутатор выступает в роли Telnet сервера, вы можете зайти на устройство при помощи Telnet-клиента, встроенного в Windows или другую операционную систему. При этом, соединение может быть установлено с пятью Telnet клиентами.
Когда коммутатор выступает в роли Telnet-клиента, вы можете использовать Telnet команды для управления другими устройствами. При этом, соединение может быть установлено только с одним сервером. Если необходимо подключиться к другому серверу, сначала отключитесь от текущего.

### 5.10.2 Настройка с помощью WEB-интерфейса

1. Включение функции сервера Telnet.

Нажмите [Device Basic Configuration] → [Telnet server configuration] → [Telnet server user configuration], чтобы открыть страницу настройки сервера Telnet, как показано на рисунке 60.


Рисунок 60 – Настройка сервера Telnet

**Telnet server state (состояние Telnet-сервера)**
Варианты: Open/Close (открыто/закрыто).
Значение по умолчанию: Open (открыто).
Функция: включение или выключение функции Telnet-сервера.
Описание: «Open» значит, что Telnet-клиенты могут авторизоваться на коммутаторе. «Close» означает, что Telnet-клиенты авторизоваться на устройстве не могут.

---

Коммутатор может быть Telnet-клиентом и авторизоваться на посторонних серверах вне зависимости, включена ли эта функция или нет.

---

2. Настройка доверенного IP-адреса для авторизации Telnet-клиентов.
Нажмите [Device Basic Configuration] → [Telnet server configuration] → [Telnet security IP], чтобы открыть страницу настройки доверенного IP-адреса, как показано на рисунке 61.

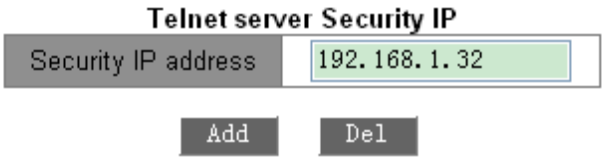



Рисунок 61 – Доверенный IP-адрес Telnet

**Security IP address (доверенный IP-адрес)**
Формат: A.B.C.D.
Функция: настройка доверенного IP-адреса для авторизации Telnet-клиентов, когда коммутатор выступает в роли Telnet сервера.
Описание: если доверенный IP-адрес не указан, то подключиться может клиент с любым IP. Если доверенный IP адрес указан, то авторизоваться на коммутаторе может только клиент с соответствующим IP.
Коммутатор позволяет настраивать до 32 IP-адресов. По умолчанию доверенные IP-адреса не указаны.
После завершения настройки в соответствующей таблице отображаются IP-адреса клиентов, которые могут авторизоваться на коммутаторе, как показано на рисунке 62.

| Telnet server Security IP list |
|---|
| 192.168.1.30 |
| 192.168.1.31 |
| 192.168.1.32 |
| 192.168.1.33 |
| 192.168.1.34 |
| 192.168.1.35 |

Рисунок 62 – Список доверенных IP-адресов

## 5.11 Настройка сервера SSH

### 5.11.1 Введение

SSH (Secure Shell) – это сетевой протокол для безопасного удаленного входа в систему. Он шифрует все передаваемые данные, чтобы предотвратить несанкционированный доступ и раскрытие информации. Когда данные зашифрованы посредством SSH, пользователи могут использовать для настройки коммутаторов только командную строку (CLI).
Коммутатор поддерживает функцию сервера SSH и позволяет работать нескольким пользователям SSH, которые подключаются к коммутатору удаленно через SSH. Одновременно к коммутатору могут подключаться не более двух пользователей.

### 5.11.2 Секретный ключ (Secret Key)

Незашифрованное сообщение называется открытым текстом (plain text), а зашифрованное сообщение зашифрованным текстом (cipher text). Шифрование или дешифрование обеспечивается секретным ключом. Секретный ключ – это специфический набор символов, который является основным и единственным параметром для управления преобразованием между обычным текстом и зашифрованным текстом, т.е. он работает как ключ доступа. Шифрование может преобразовать простой текст в зашифрованный, а дешифрование может преобразовать зашифрованный текст в открытый.
Для безопасной аутентификации на основе ключей необходимо наличие секретных ключей. Для клиента и сервера всегда есть пара секретных ключей: персональный ключ (private key) и открытый ключ (public key). Открытый ключ используется для шифрования данных, персональный – для дешифрования. Законный владелец персонального ключа может использовать его для расшифровки данных, чтобы гарантировать их безопасность.

### 5.11.3 Реализация

Для реализации безопасного соединения по протоколу SSH в процессе коммуникации, серверу и клиенту необходимо пройти следующие пять этапов:

- Этап согласования версии: в настоящее время SSH состоит из двух версий, SSH1 и SSH2. Обе стороны согласовывают необходимую версию для использования.
- Этап согласования ключей и алгоритмов: SSH поддерживает несколько типов алгоритмов шифрования. Обе стороны согласовывают соответствующий алгоритм.

- Этап аутентификации: клиент SSH отправляет запрос аутентификации на сервер, который выполняет аутентификацию клиента.
- Этап запроса сеанса: клиент отправляет запрос сеанса на сервер после прохождения аутентификации.
- Этап сеанса: клиент и сервер начинают связь после передачи запроса на сеанс.

## 5.11.4 Настройка с помощью WEB-интерфейса

- Настройка SSH-сервера по шагам:

Чтобы перейти на страницу конфигурации сервера SSH, нажмите [Device Basic Configuration] → [SSH Server Configuration] → [SSH server configuration].

1. Статус SSH установите в состояние «Отключено» (Close).
2. Нажмите <Destroy>, чтобы удалить старую пару ключей, как показано на рисунке 63.

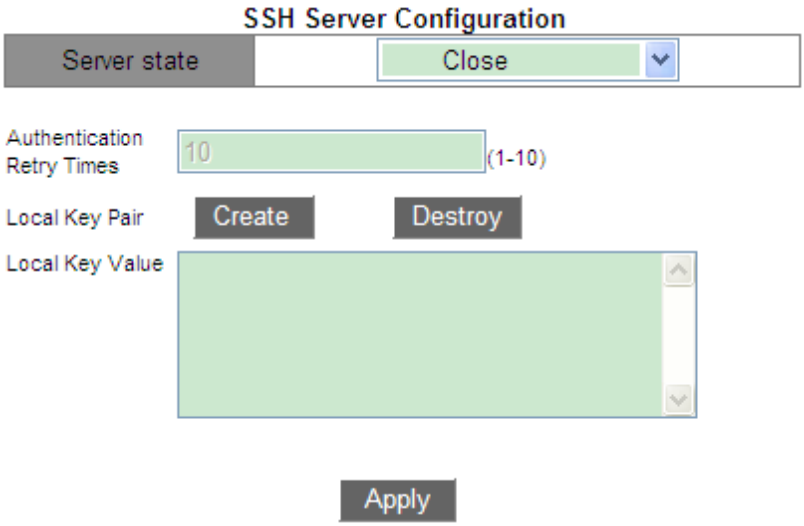



Рисунок 63 – Удаление старой пары ключей

3. Нажмите <Create>, чтобы создать новую пару ключей.
4. Включите протокол SSH и настройте сервер SSH, как показано на рисунке 64.

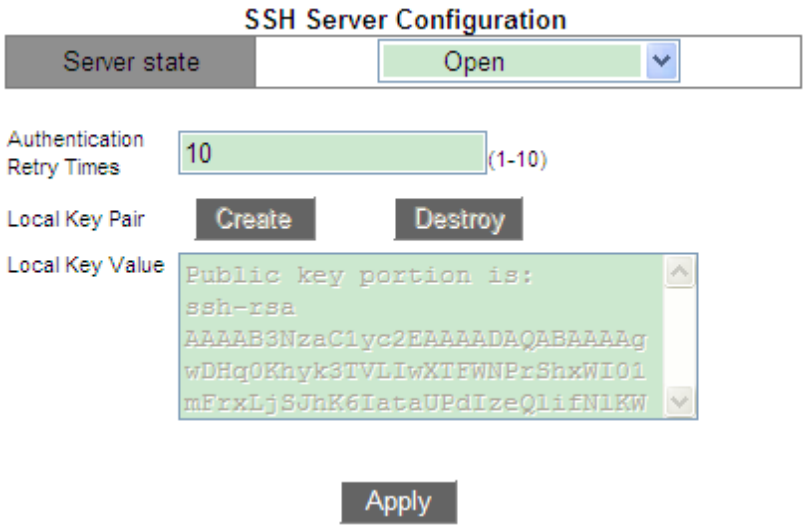



Рисунок 64 – Настройка сервера SSH

**Server state (состояние сервера)**
Варианты: Open/Close (включен/выключен).
Значение по умолчанию: Close (выключен).
Функция: включить/отключить протокол SSH. Если режим включен, коммутатор работает как SSH-сервер.

**Authentication Retry Times (количество повторов аутентификации)**
Диапазон: 1~10.
Значение по умолчанию: 10.
Функция: настройка количества попыток входа на SSH-сервер.

**Local Key Pair (пара локальных ключей)**
Варианты: Create/Destroy (создать/удалить).
Функция: создать или удалить пару локальных ключей SSH-сервера. Пожалуйста, создайте пару локальных ключей перед включением SSH-сервера; удалите старую пару ключей перед созданием новой пары ключей.

**Local Key Value (значение локального ключа)**
Функция: показать значение локального ключа. Нажмите <Create>, чтобы автоматически сгенерировать значение ключа.

- Настройка довереного IP-адреса для входа клиента SSH.

Чтобы перейти на страницу настройки доверенного IP-адреса, нажмите [Device Basic Configuration] → [SSH Server Configuration] → [SSH security IP], как показано на рисунке 65.

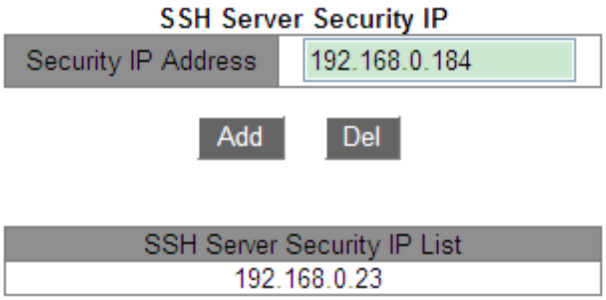



Рисунок 65 – Настройка доверенного IP-адреса сервера SSH

**Security IP Address (доверенный IP-адрес)**
Формат: A.B.C.D.
Функция: настройка доверенного IP-адреса для входа клиента SSH в том случае, когда коммутатор работает как сервер SSH. Если значения доверенного IP-адреса не задано, идентифицируется любой IP-адрес клиента SSH. После того, как доверенные IP-адреса установлены, войти в систему и настроить коммутатор с помощью SSH может только клиент с определенным IP-адресом.
Пояснение: коммутатор позволяет использовать до шести безопасных IP-адресов. По умолчанию безопасный IP-адрес не установлен.

## 5.11.5 Пример типовой настройки

Хост работает как клиент SSH для установки локального соединения с коммутатором, как показано на рисунке 66.

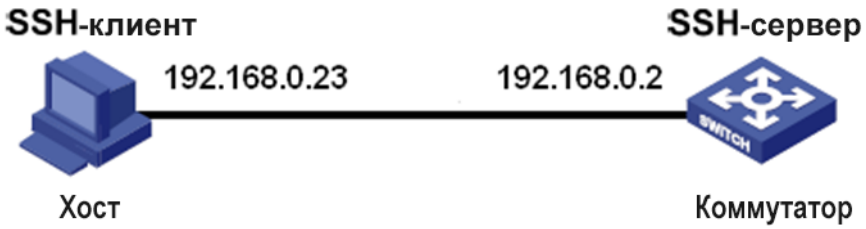



Рисунок 66 – Пример настройки SSH

➢ Если пользователь SSH выбирает тип аутентификации «Password» (пароль):
1. Удалите старую пару ключей сервера. Создайте новую пару ключей и запустите сервер SSH (см. рисунки 63 и 64).
2. Установите имя пользователя SSH как «333», тип сессии SSH, тип аутентификации «Password». Настройте пароль как «333» (см. рисунок 24).
3. Установите соединение с SSH-сервером. Сначала запустите программу PuTTY.exe, как показано на рисунке 67; введите IP-адрес SSH-сервера «192.168.0.2» в поле «Host Name (or IP address)».

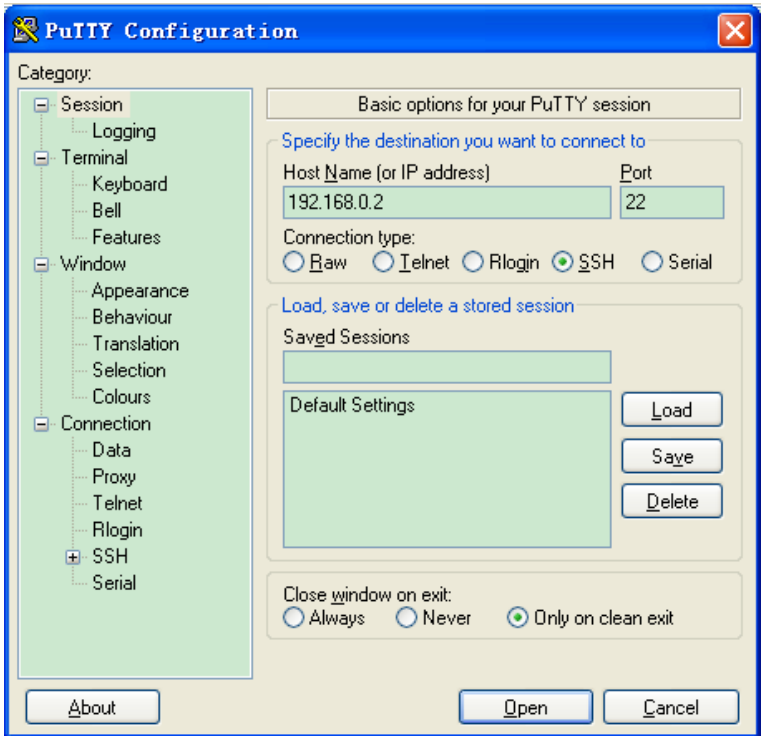



Рисунок 67 – Настройка клиента SSH

4. Нажмите кнопку <Open>. Появится следующее предупреждающее сообщение, показанное на рисунке 68. Нажмите кнопку <Да>.

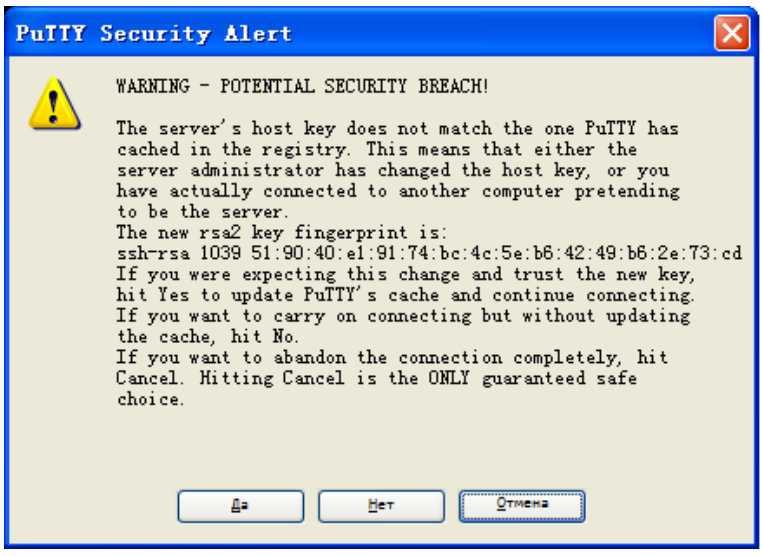



Рисунок 68 – Предупреждающее сообщение

5. Введите имя пользователя «333» и пароль «333», чтобы войти в интерфейс настройки коммутатора, как показано на рисунке 69.


Рисунок 69 – Интерфейс входа для аутентификации SSH по паролю

➢ Если пользователь SSH выбирает тип аутентификации «Key» (ключ):

1. Удалите старую пару ключей сервера. Создайте новую пару ключей и запустите SSH-сервер (см. рисунки 63 и 64).

2. Выполните настройки клиента SSH, см. рисунок 26. Запустите у клиента программу PuTTYGen.exe. Нажмите кнопку <Generate>, чтобы сгенерировать пару клиентских ключей, как показано на рисунке 70.


Рисунок 70 – Генерация клиентского ключа

3. В процессе генерации перемещайте указатель мыши по экрану. В противном случае индикатор выполнения задачи не будет перемещаться, и генерация остановится (см. рисунок 71).

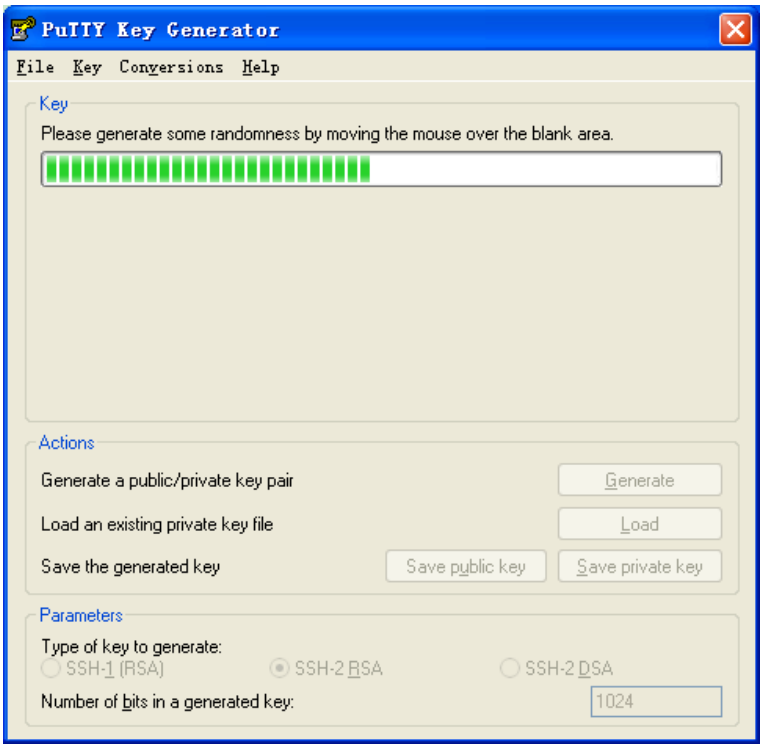



Рисунок 71 – Генерация ключей

4. Нажмите кнопку <Save private key>, чтобы сохранить закрытый ключ как 444.ppk (см. рисунок 72). Скопируйте открытый ключ в область значения ключа в интерфейсе конфигурации ключа SSH и введите имя ключа «444», как показано на рисунке 26.

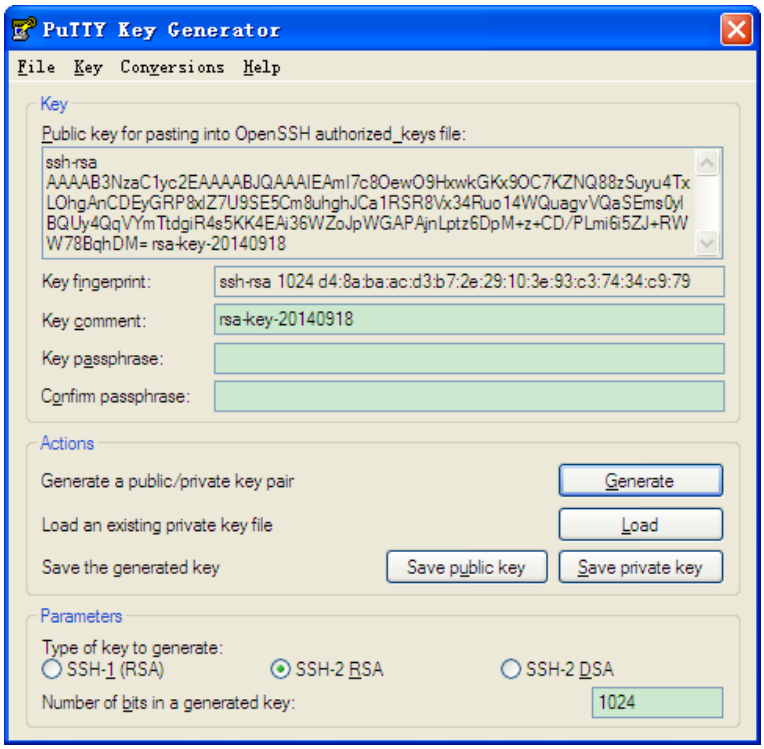



Рисунок 72 – Генерация значения ключей

5. Установите имя пользователя SSH как «444», имя ключа как «444», тип аутентификации «Key», включите службу SSH, (см. рисунок 24).

6. Установите соединение с SSH-сервером. Сначала запустите программу PuTTY.exe, как показано на рисунке 73; введите IP-адрес SSH-сервера «192.168.0.2» в поле «Host Name (or IP address)».

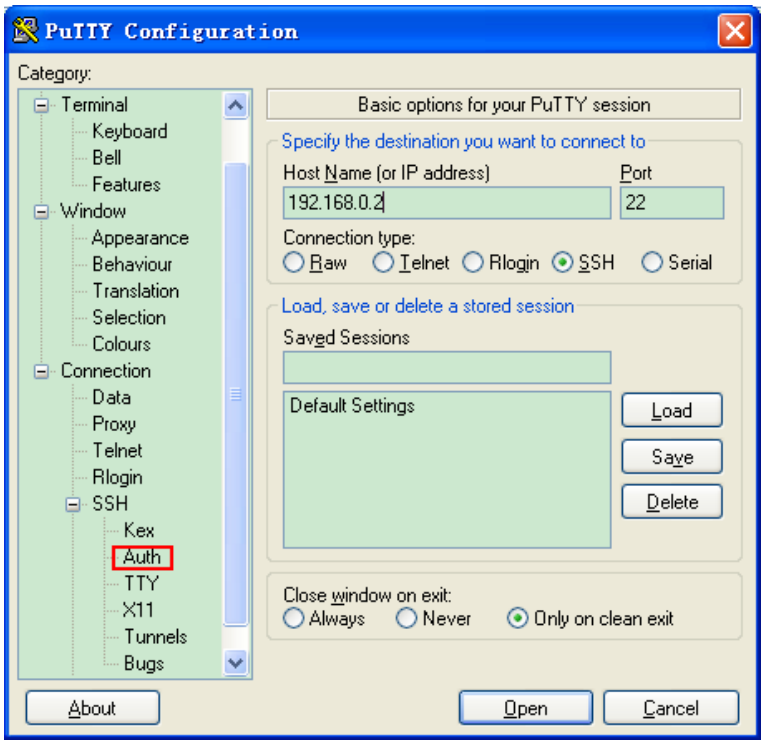



Рисунок 73 – Конфигурация клиента SSH для аутентификации «по ключам»

7. Нажмите [SSH] → [Auth] в окне «Category» (см. рисунок 73). После чего появится экран, показанный на рисунке 74. Нажмите кнопку <Browse> и выберите файл, сохраненный на шаге 4.

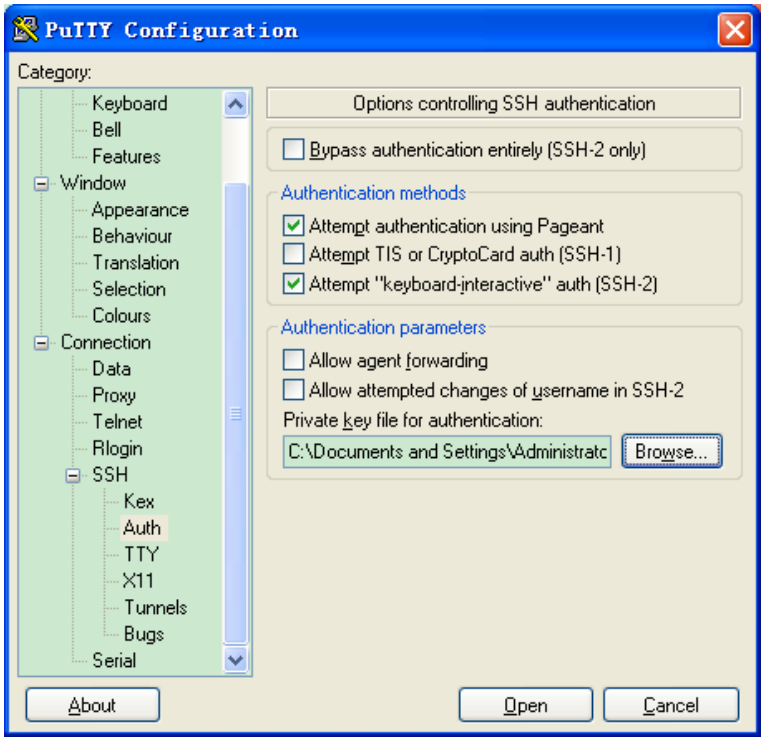



Рисунок 74 – Выбор сохраненного файла с ключами

8. Нажмите кнопку <Open>; введите имя пользователя, чтобы войти в интерфейс настройки коммутатора, как показано на рисунке 75.


Рисунок 75 – Интерфейс входа при аутентификации с открытым ключом SSH

## 5.12 Настройка SSL

### 5.12.1 Введение

SSL (Secure Socket Layer) — это протокол безопасности, обеспечивающий безопасный канал для протокола прикладного уровня на основе TCP, такого как HTTPS. SSL шифрует сетевое соединение на транспортном уровне и использует алгоритм симметричного шифрования для обеспечения безопасности данных, а также использует код аутентификации с секретным ключом для обеспечения надежности информации. Этот протокол широко используется в веб-браузерах, для получения и отправки электронной почты, сетевого факса, связи в реальном времени и т. д., обеспечивая криптографическую защиту для безопасной передачи в сети. Когда коммутатор включает SSL, пользователи должны использовать безопасную ссылку https, например, https://192.168.0.2, для доступа к коммутатору.

### 5.12.2 Настройка с помощью WEB-интерфейса

1. Включение протокола HTTPS.
Нажмите [Device Basic Configuration] → [SSL Server configuration] → [SSL server configuration], чтобы открыть страницу конфигурации SSL, как показано на рисунке 76.

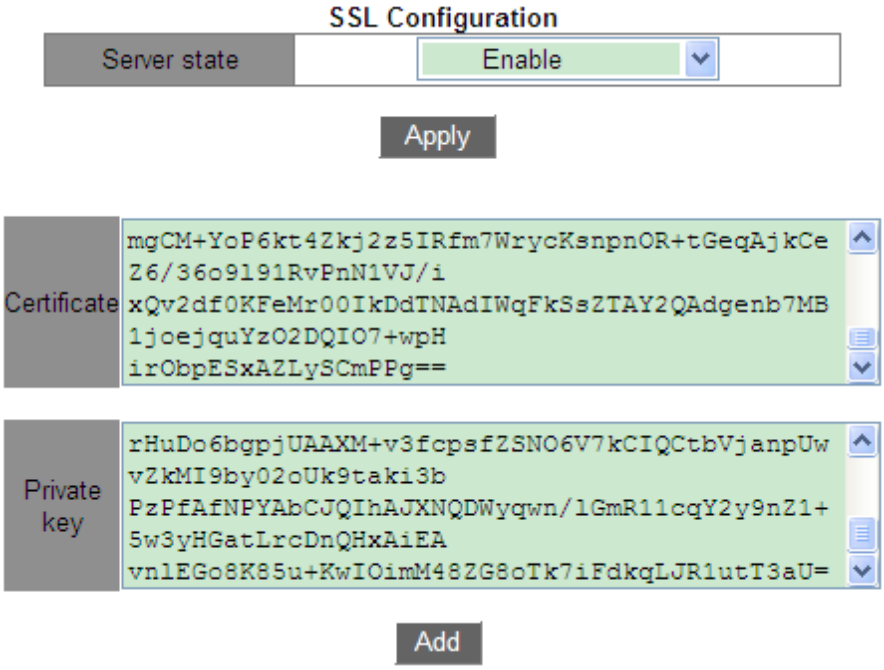



Рисунок 76 – Включение протокола HTTPS

**Server state (состояние сервера)**
Варианты: Enable/Disable (включить/отключить)
Значение по умолчанию: Disable (отключить)
Функция: включить или отключить протокол SSL.
Пояснение: После включения SSL пользователи должны использовать безопасную ссылку https://*ip-адрес* для доступа к коммутатору.

**Certificate/Private key (сертификат/закрытый ключ)**
Функция: введите правильный сертификат и закрытый ключ, затем нажмите кнопку <Add>, чтобы импортировать их в коммутатор.

---

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

---

2. Введите имя пользователя и пароль для успешной аутентификации на коммутаторе через HTTPS.

## 5.13 Служба передачи файлов

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

Коммутатор может служить клиентом или сервером для загрузки и выгрузки файлов при помощи FTP или TFTP.

## 5.13.1 TFTP

1. Коммутатор выступает в роли TFTP-клиента.

➢ Сначала необходимо установить TFTP-сервер на ПК, указать путь к хранилищу файлов и IP-адрес сервера (см. рисунок 77).

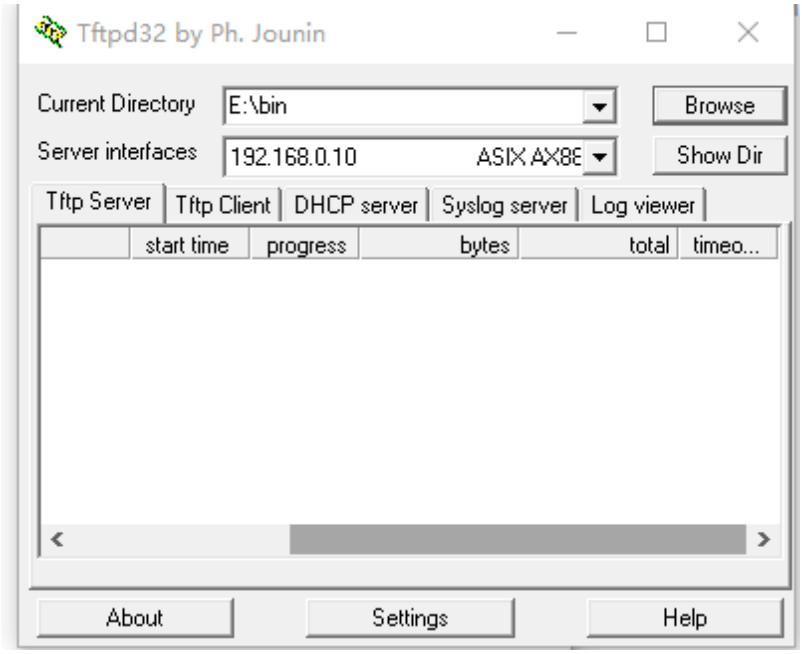



Рисунок 77 – Настройка TFTP-сервера

➢ Нажмите [Device Basic Configuration] → [File transmit] → [TFTP Service] → [TFTP client service], чтобы зайти на страницу настройки TFTP-клиента, как показано на рисунке 78.

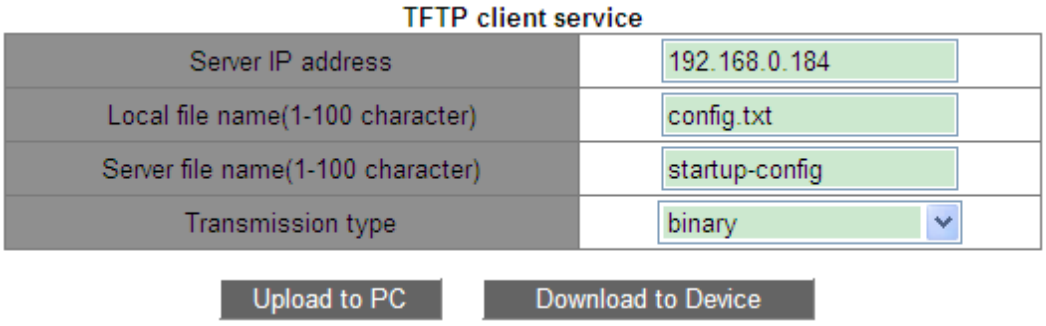



Рисунок 78 – Служба TFTP-клиента

**Server IP address (IP-адрес сервера)**
Формат: A.B.C.D.
Описание: введите IP-адрес сервера.

**Local file name (имя локального файла)**
Диапазон: 1~100 символов.
Описание: введите имя файла на коммутаторе.

**Server file name (имя файла на сервере)**
Диапазон: 1~100 символов.
Описание: введите имя файла на сервере.

**Transmission type (тип передачи)**
Варианты: binary/ascii.
Значение по умолчанию: binary.
Функция: выбор стандарта передачи файлов.
Пояснение: «ascii» означает использование стандарта ASCII для передачи файла; «binary» означает использование двоичного стандарта для передачи файла.
Действие: нажмите <Upload to PC>, чтобы загрузить файл с коммутатора на сервер, или <Download to Device>, чтобы скачать файл с сервера на коммутатор.

➢ При успешной передаче файла в веб-интерфейсе появляется информация, показанная на рисунках 79 и 80.

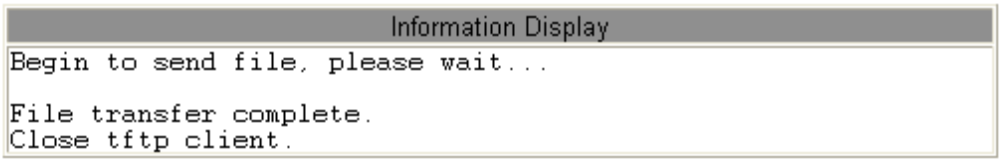



Рисунок 79 – Успешная загрузка файла на сервер через TFTP

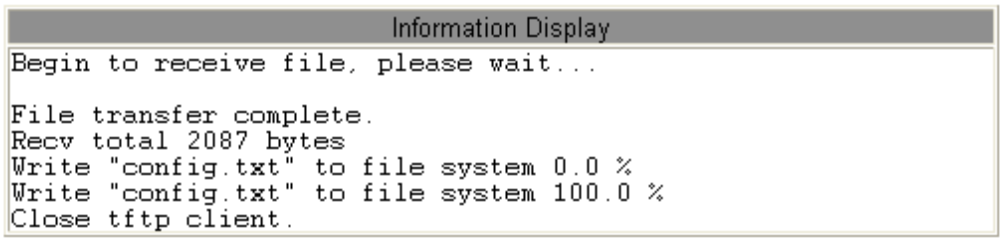



Рисунок 80 – Успешная загрузка файла на коммутатор через TFTP

---

➢ В процессе передачи файлов нельзя выключать TFTP-сервер.
➢ Файл версии программного обеспечения не является текстовым файлом и должен поддерживать двоичный стандарт для передачи.

---

2. Коммутатор выступает в роли TFTP-сервера.
➢ Нажмите [Device Basic Configuration] → [File transmit] → [TFTP Service] → [TFTP server service], чтобы зайти на страницу настройки TFTP-сервера, как показано на рисунке 81.

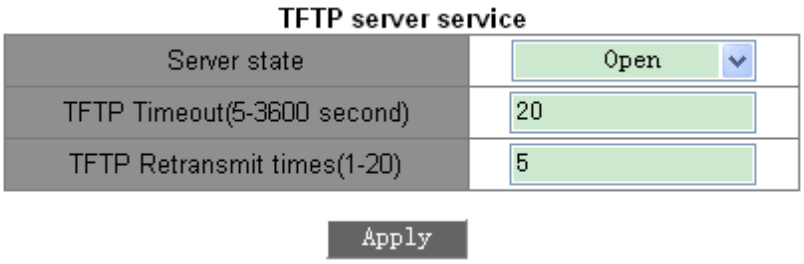



Рисунок 81 – Служба TFTP-сервера

**Server state (состояние сервера)**
Варианты: Close/Open (выключено/включено).
Значение по умолчанию: Close (выключено).
Функция: включение/выключение TFTP сервера.

**TFTP Timeout (время ожидания TFTP)**
Диапазон: 5~3600 с.
Значение по умолчанию: 20.
Функция: установка времени ожидания для TFTP соединения.

**TFTP Retransmit times (количество попыток повторной передачи данных по TFTP)**
Диапазон: 1~20.
Значение по умолчанию: 5.
Функция: установить количество попыток передачи данных по TFTP в заданное время.

➢ Установите на ПК клиентское программное обеспечение TFTP, как показано на рисунке 82. Введите IP-адрес коммутатора в окне «Host»; выберите путь к хранилищу файлов клиента в окне «Local File»; введите имя файла, находящегося на коммутаторе; нажмите <Get>, чтобы загрузить файл с коммутатора на ПК; нажмите <Put>, чтобы передать файл с клиента на коммутатор.

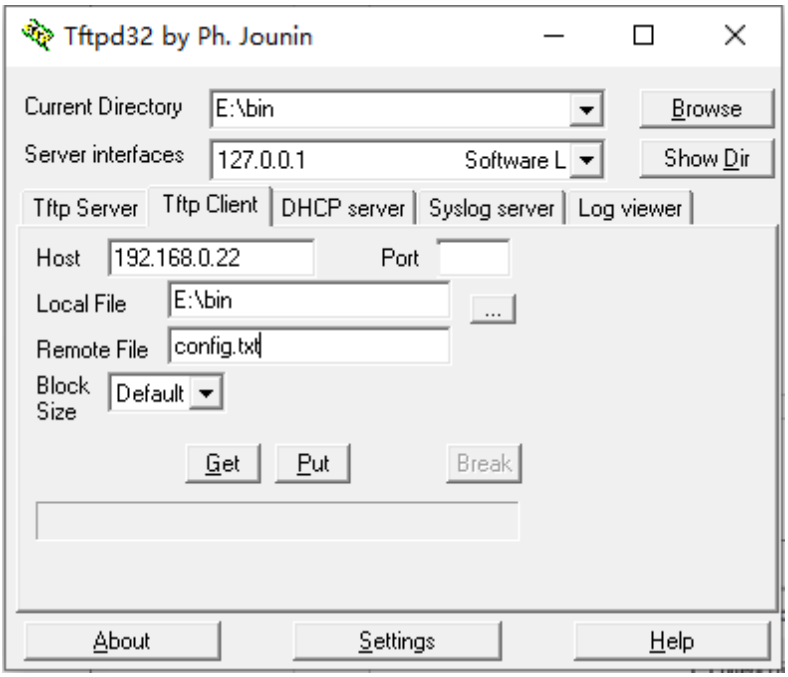



Рисунок 82 – Настройка TFTP-клиента

В процессе передачи файлов нельзя выключать клиентское программное обеспечение TFTP.

## 5.13.2 FTP

1. Коммутатор выступает в роли FTP-клиента.

➢ Сначала необходимо установить FTP-сервер на ПК. Нажмите [Security] → [users/rights], чтобы открыть диалоговое окно. Нажмите <new user>, чтобы создать нового пользователя FTP, как показано на рисунке 83. Введите имя пользователя и пароль. Например, имя пользователя: admin; пароль: 123. Нажмите <OK>.

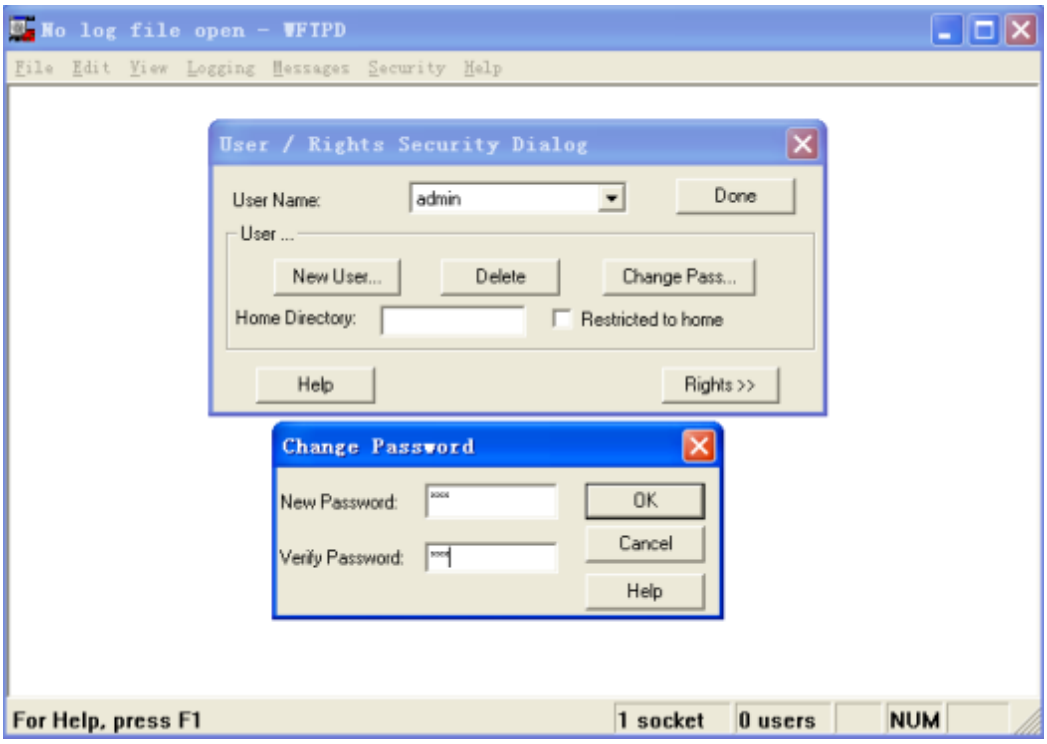



Рисунок 83 – Создание нового пользователя FTP

➢ Введите путь к хранилищу файлов на сервере в домашнем каталоге, как показано на рисунке 84. Нажмите <Done>.

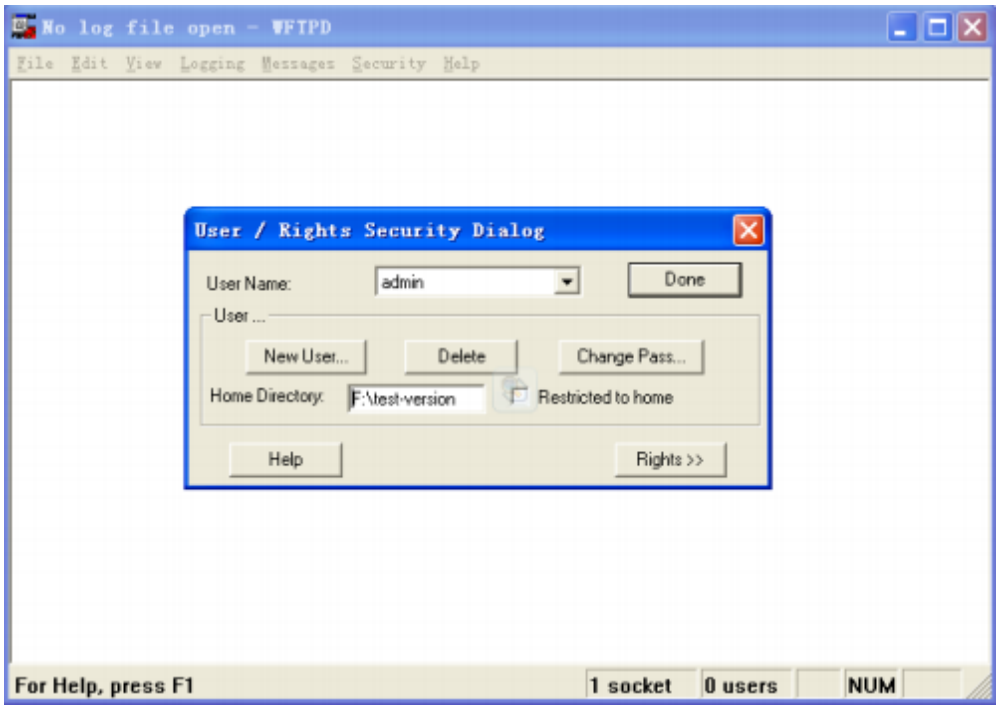



Рисунок 84 – Путь к хранилищу файлов

➢ Нажмите [Device Basic Configuration] → [File transmit] → [FTP Service] → [FTP client service], чтобы открыть страницу конфигурации клиента FTP, как показано на рисунке 85.

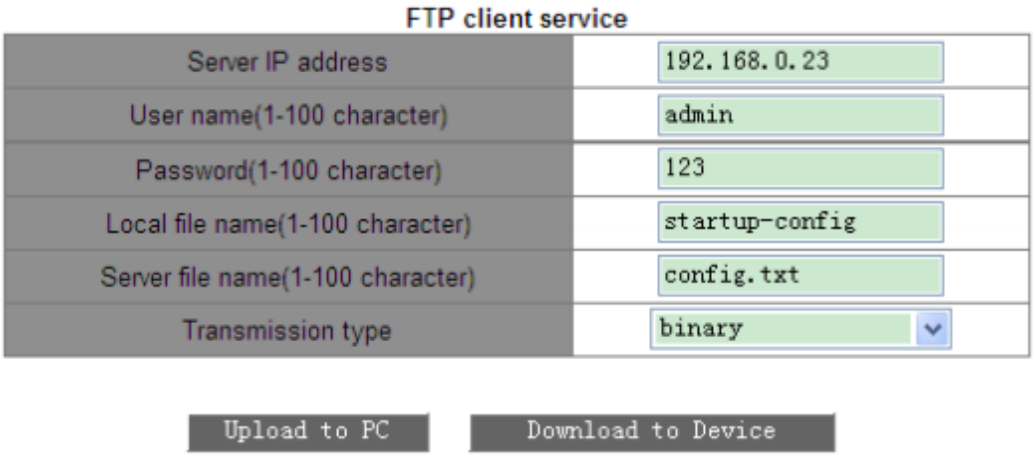



Рисунок 85 – Служба FTP-клиента

**Server IP address (IP-адрес сервера)**
Формат: A.B.C.D.
Описание: указывает IP-адрес сервера.

**{User name, Password} – {имя пользователя, пароль}**
Диапазон: {1~100 символов, 1~100 символов}.
Описание: пароль и имя пользователя, созданного на FTP сервере.

**Local file name (имя локального файла)**
Диапазон: 1~100 символов.
Описание: имя файла на коммутаторе.

**Server file name (имя файла на сервере)**
Диапазон: 1~100 символов.
Описание: имя файла на сервере.

**Transmission type (тип передачи)**
Варианты: binary/ascii.
Значение по умолчанию: binary.
Функция: выбор стандарта передачи файлов.
Пояснение: «ascii» означает использование стандарта ASCII для передачи файла; «binary» означает использование двоичного стандарта для передачи файла.
Действие: нажмите <Upload to PC>, чтобы загрузить файл с коммутатора на сервер. Нажмите <Download to Device>, чтобы скачать файл с сервера на коммутатор.

После успешной передачи файла в веб-интерфейсе появляется информация, показанная на рисунках 86 и 87.

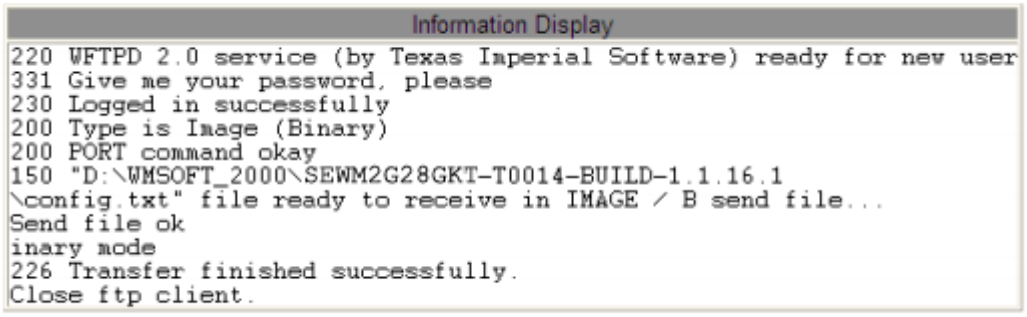



Рисунок 86 – Успешная загрузка файла на сервер через FTP

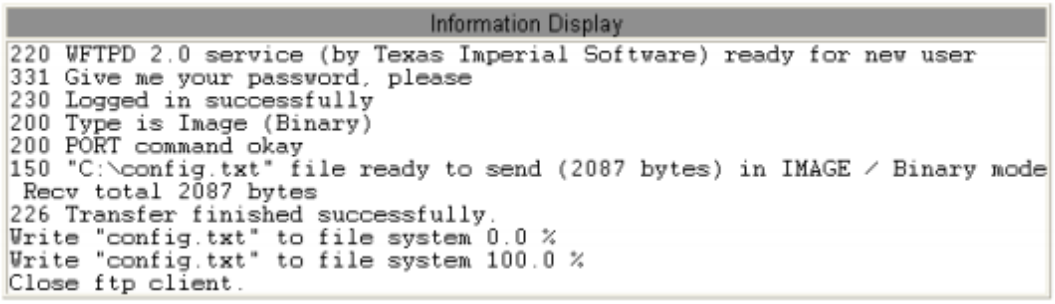



Рисунок 87 – Успешная загрузка файла на коммутатор через FTP

---

- В процессе передачи файлов нельзя выключать FTP-сервер.
- Файл версии программного обеспечения не является текстовым файлом и должен поддерживать двоичный стандарт для передачи.

---

2. Коммутатор выступает в роли FTP-сервера.

➢ Нажмите [Device Basic Configuration] → [File transmit] → [FTP Service] → [FTP server service], чтобы зайти на страницу настройки FTP-сервера, как показано на рисунке 88.

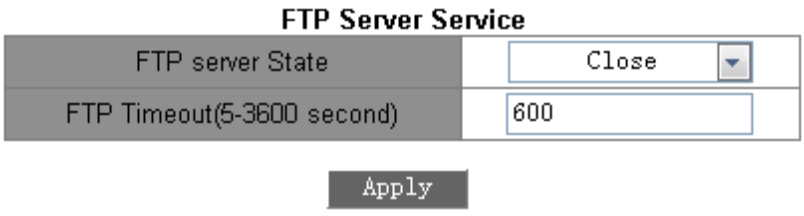



Рисунок 88 – Служба FTP-сервера

**Server state (состояние сервера)**
Варианты: Close/Open (выключено/включено).
Значение по умолчанию: Close (выключено).
Функция: включение/выключение FTP сервера.

**FTP Timeout (время ожидания FTP)**
Диапазон: 5~3600 с.
Значение по умолчанию: 600.
Функция: установка времени ожидания для FTP соединения.
Описание: если в течение времени ожидания данные между FTP-сервером и клиентом не передаются, соединение между ними разрывается.

➢ Настройте имя пользователя и пароль, используемые для входа на FTP-сервер, как показано на рисунке 89.

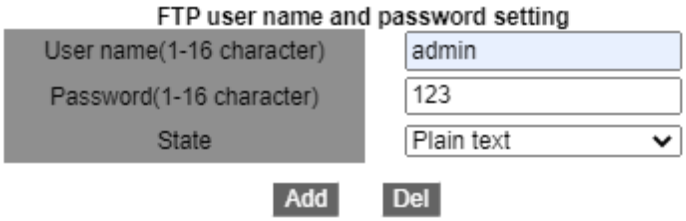



Рисунок 89 – Настройка имени пользователя и пароля на FTP-сервере

**{Username, Password} – {Имя пользователя Пароль}**
Диапазон: {1~16 символов, 1~16 символов}.
Функция: настройка имени пользователя и пароля для входа на FTP-сервер.
Описание: когда коммутатор работает как FTP-сервер, он может одновременно подключаться к нескольким FTP-клиентам.

**State (индикация)**
Варианты: Plain text/Encrypted text (простой текст/зашифрованный текст).
Значение по умолчанию: Plain text (простой текст).
Функция: выбрать режим отображения пароля.

➢ На удалённом ПК в диалоговом окне Выполнить ОС Windows введите «cmd» и нажмите Enter. Отобразится интерфейс командной строки (CLI).

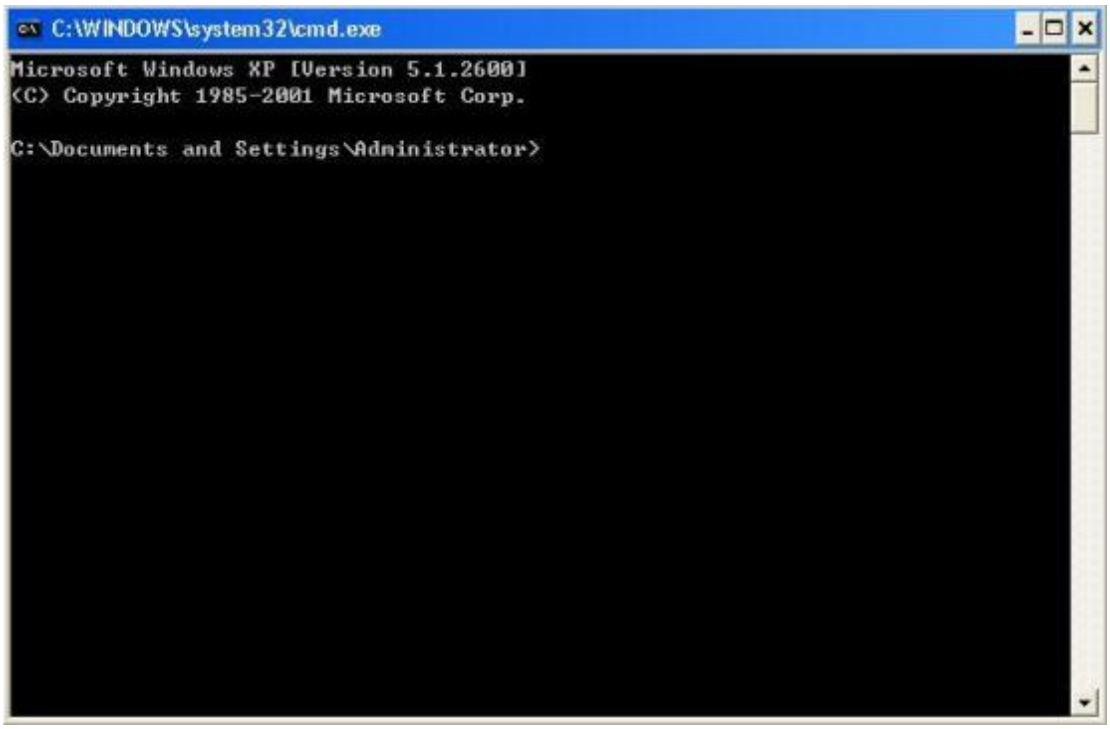



Рисунок 90 – Интерфейс командной строки

➢ Путь передачи файла может быть изменен. Войдите на FTP-сервер, как показано на рисунке 91.

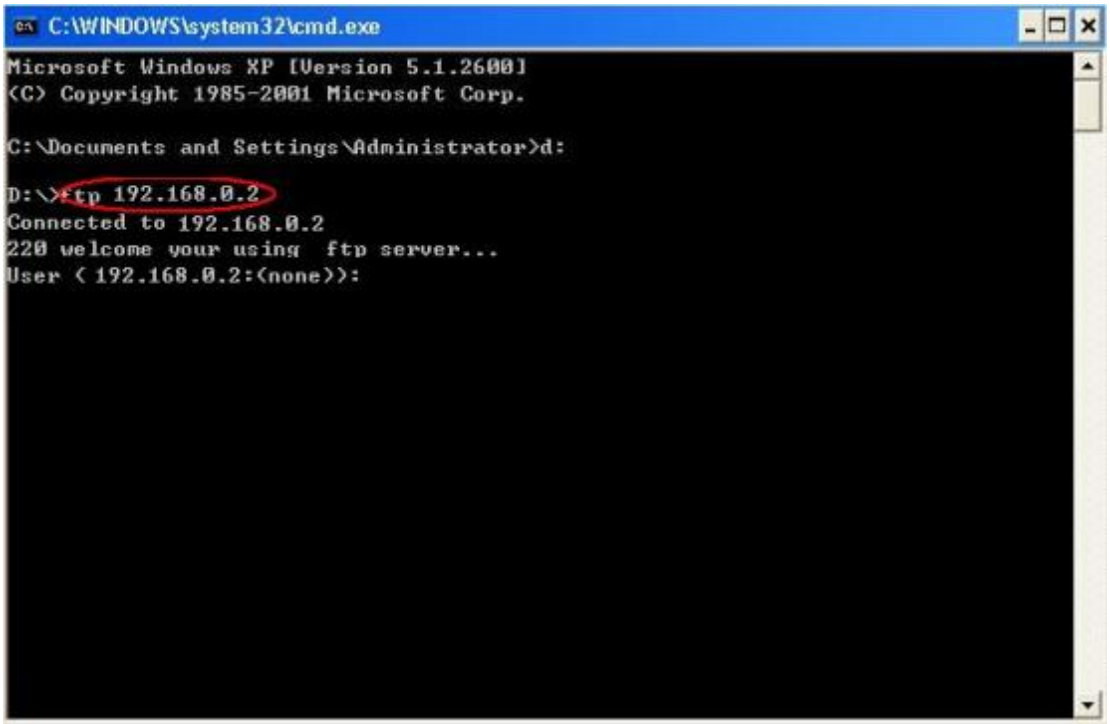



Рисунок 91 – Подключение к FTP-серверу.

➢ Используйте настроенное ранее имя пользователя «admin» и пароль «123» для входа на FTP-сервер, как показано на рисунке 92.

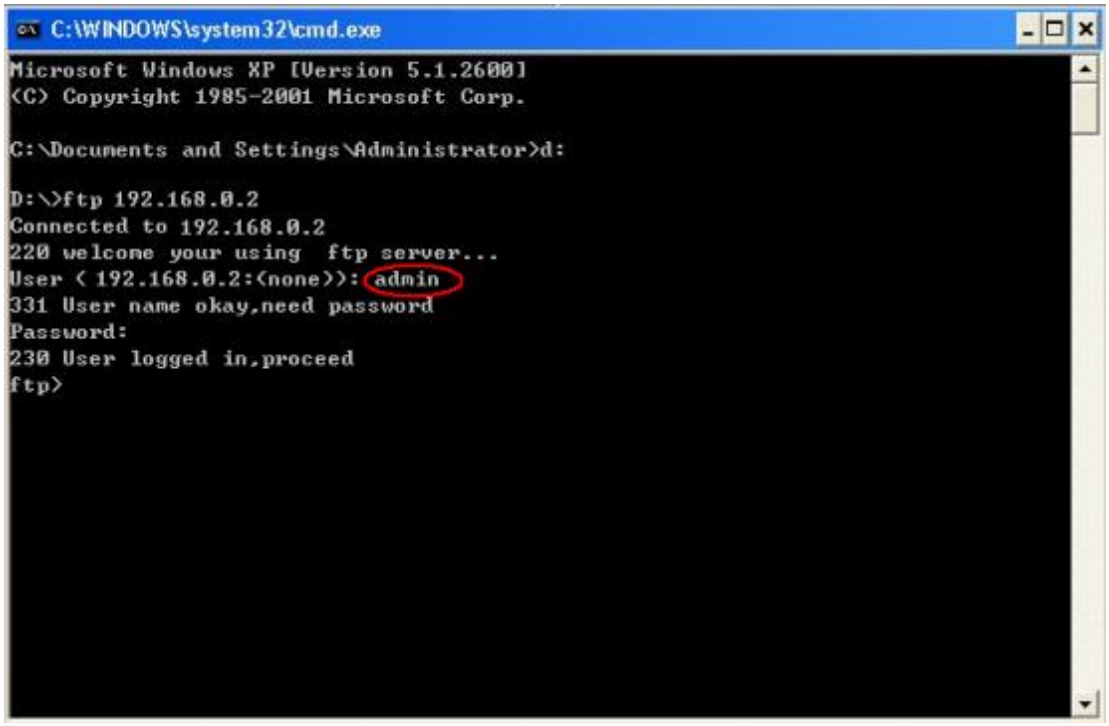



Рисунок 92 – Вход на FTP-сервер

➢ Используйте команду «get», чтобы загрузить файл по указанному пути на клиенте, как показано на рисунке 93. Введите команду «get» и нажмите Enter. В строке «Remote file» введите имя скачиваемого файла на коммутаторе. В строке «Local file» введите имя файла на ПК.

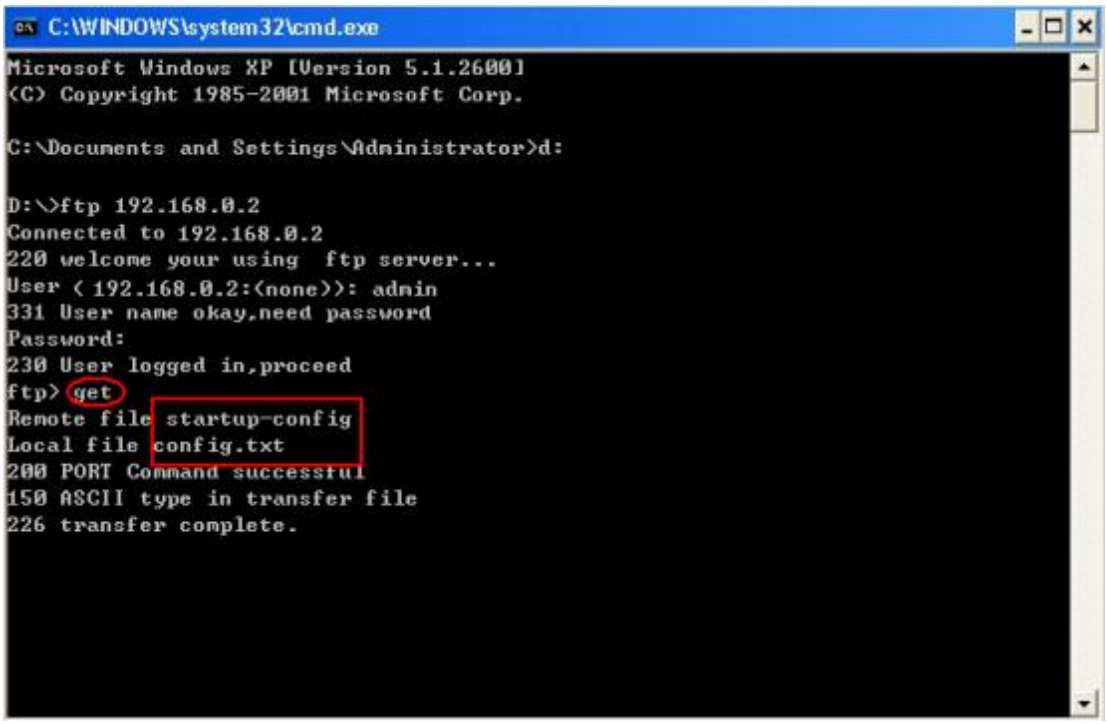



Рисунок 93 – Загрузка файла с коммутатора на клиент

➢ Используйте команду «put», чтобы загрузить файл из указанной директории клиента на сервер (см. рисунок 94). Запустите команду «put» и нажмите Enter. В строке «Remote file» введите имя файла на коммутаторе. В строке «Local file» введите имя файла, который будет загружен с ПК на коммутатор.

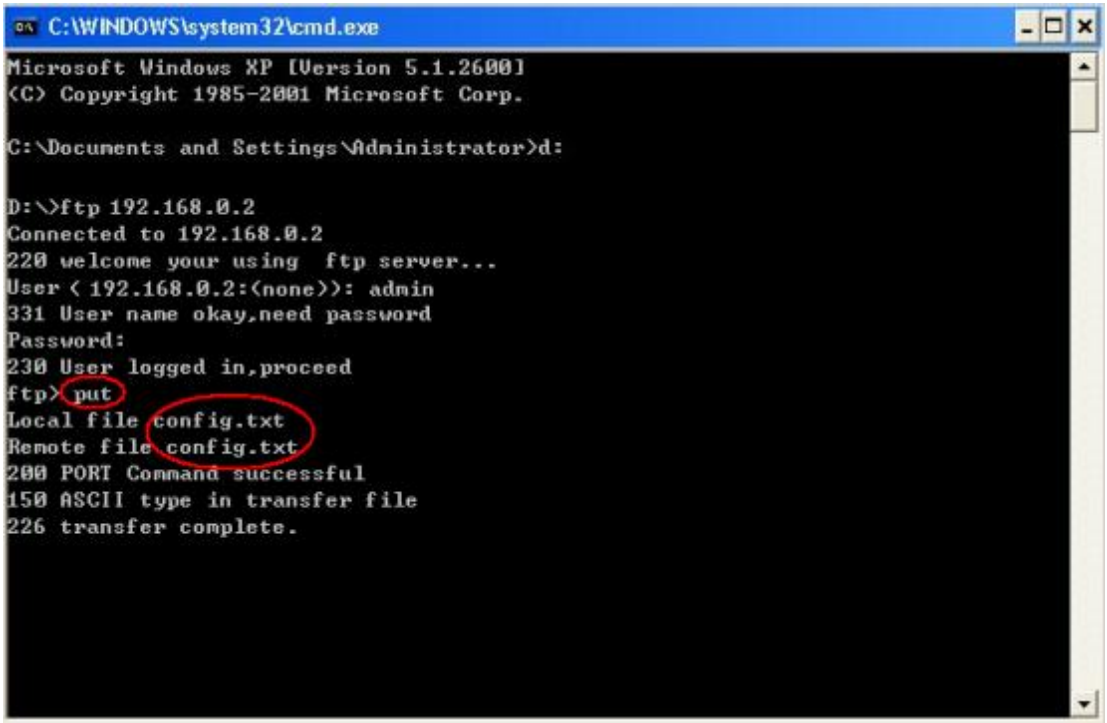



Рисунок 94 – Загрузка файла с клиента на коммутатор

# 5.14 Таблица MAC-адресов

## 5.14.1 Введение

При передаче данных, коммутатор определяет порт, с которого необходимо передавать кадры, при помощи таблицы MAC-адресов, исходя из MAC-адреса назначения.
MAC-адреса могут быть статическими и динамическими.
Статические MAC-адреса настраиваются пользователями. У таких адресов максимальный приоритет (выше, чем у динамических) и они априори достоверные.
Динамические MAC-адреса появляются в таблице во время проверки передаваемых данных. Они считаются достоверными только в течении определённого периода времени. Коммутатор периодически обновляет свою таблицу MAC-адресов. При получении кадра коммутатор записывает в свою таблицу MAC-адрес отправителя, содержащийся в этом кадре, наряду с портом, на который кадр был получен, а затем проверяет в своей таблице наличие MAC-адреса порта назначения, также содержащегося в кадре. Если этот адрес присутствует в таблице, коммутатор передаёт данные на соответствующий порт. Если совпадения не найдено, коммутатор рассылает этот кадр на все порты.
Период устаревания (Aging time) отсчитывается с момента, когда динамический MAC-адрес добавляется в таблицу. Если коммутатор не получит ни одного кадра данных с соответствующим MAC-адресом до истечения периода устаревания, этот MAC-адрес удаляется из таблицы динамических адресов. Статические MAC-адреса никак не связаны с периодом устаревания.
Коммутатор поддерживает не более 1024 записей статических MAC-адресов.

## 5.14.2 Настройка с помощью WEB-интерфейса

1. Настройка привязки по MAC-адресу.
Нажмите [Device Basic Configuration] → [MAC address table configuration] → [MAC bind Configuration], чтобы открыть страницу настройки привязки MAC-адресов, как показано на рисунке 95.

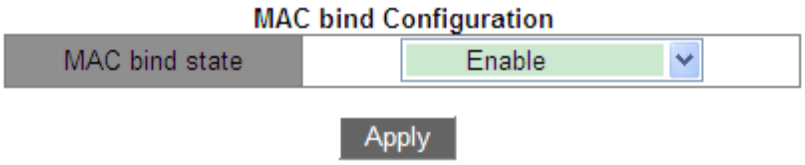



Рисунок 95 – Настройка привязки по MAC-адресу

**MAC bind state (состояние привязки MAC)**
Варианты: Enable/Disable (включить/отключить).
Значение по умолчанию: Disable (отключить).
Функция: включение или отключение функции привязки MAC-адресов. Если выбрано значение «Enable», для пакета, исходный MAC-адрес и VLAN ID которого соответствуют записи статического индивидуального MAC-адреса, коммутатор проверяет, соответствует ли входной порт порту, указанному в записи этого MAC-адреса. Если да, коммутатор

принимает и пересылает пакет. Если нет, то пакет отбрасывается. При выборе значения «Disable» данная проверка не выполняется.
2. Добавление статического индивидуального MAC-адреса (Unicast MAC operation).
Нажмите [Device Basic Configuration] → [MAC address configuration] → [Unicast address configuration], чтобы открыть страницу настройки индивидуального MAC-адреса, как показано на рисунке 96.

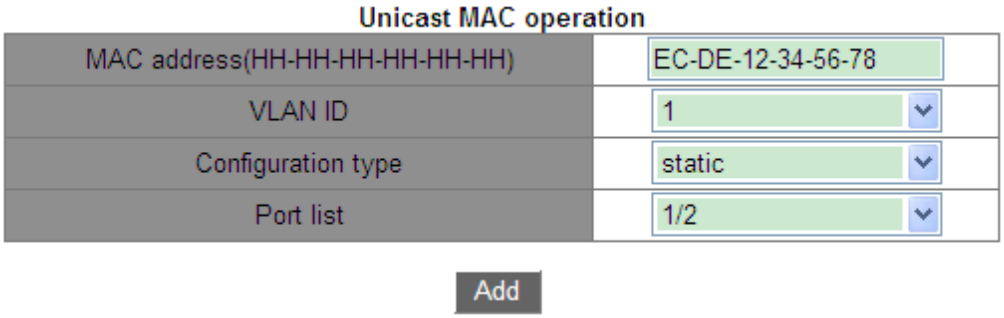



Рисунок 96 – Добавление статической записи в таблицу коммутации

**MAC address (MAC адрес)**
Формат: FF-FF-FF-FF-FF-FF (F – шестнадцатеричное число).
Функция: назначение индивидуального MAC-адреса. Младший бит старшего байта равен нулю.

**VLAN ID (идентификатор VLAN)**
Варианты: – все созданные ID VLAN.
Значение по умолчанию: 1.

**Configuration type (тип)**
Варианты: static/blackhole.
Значение по умолчанию: static.
Функция: выбор типа записи MAC-адреса.
Описание: «static» означает статическую запись, связывающую выбранный MAC адрес и номер порта, либо номер VLAN.
«blackhole» означает запись, в соответствии с которой все кадры, имеющие указанный MAC, будь это адрес отправителя или назначения, будут отброшены.

**Port list (список портов)**
Варианты: – все порты коммутатора.
Функция: выбор портов, куда будут отправляться данные с указанным MAC-адресом назначения. Выбранные порты должны принадлежать к указанной VLAN.

3. Удаление индивидуального адреса.
Нажмите [Device Basic Configuration] → [MAC address configuration] → [Delete unicast address], чтобы открыть страницу конфигурации, как показано на рисунке 97.

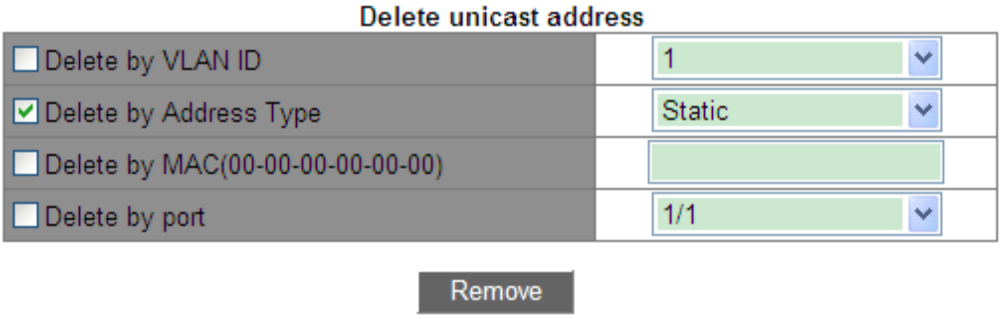



Рисунок 97 – Удаление индивидуального MAC-адреса

Выберите критерий удаления индивидуального адреса. Если выбрано несколько критериев, то их отношение описывается логическим «И».

4. Настройка времени устаревания MAC-адреса.
Нажмите [Device Basic Configuration] → [MAC address configuration] → [MAC address aging time setting], чтобы открыть страницу настройки времени устаревания, как показано на рисунке 98.

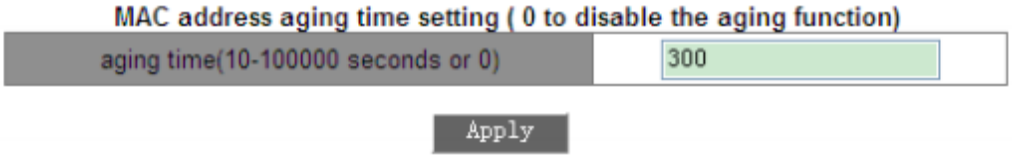



Рисунок 98 – Настройка времени устаревания MAC-адреса

**aging time (период устаревания)**
Диапазон: 10~100000 с
Значение по умолчанию: 300
Функция: установка периода устаревания для динамических записей MAC-адресов.
Описание: Если период устаревания установлен в 0, устаревание адресов запрещено. В этом случае, все динамические записи не устаревают со временем.

5. Выборка индивидуальных MAC-адресов.
Нажмите [Device Basic Configuration] → [MAC address configuration] → [MAC address query], чтобы запросить выборку индивидуальных MAC-адресов, как показано на рисунке 99.

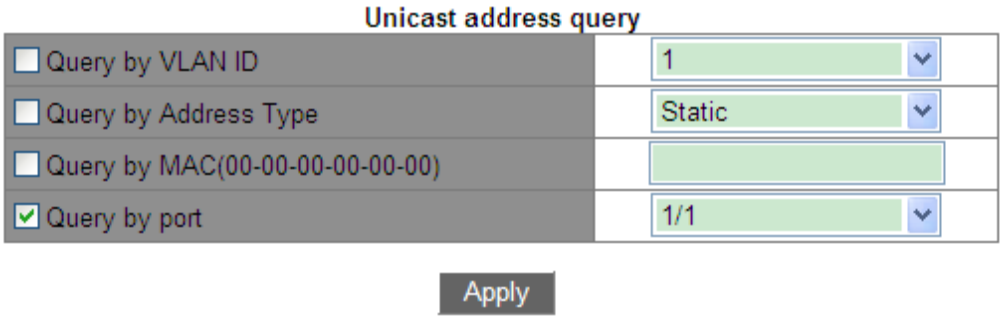



Рисунок 99 – Запрос на выборку индивидуальных MAC-адресов

Выберите критерии выборки для индивидуальных MAC-адресов. Если выбрано несколько критериев, их отношение описываются логическим "И". Например, если вы запрашиваете индивидуальный адрес порта Ethernet 1/1, отображается следующая страница:

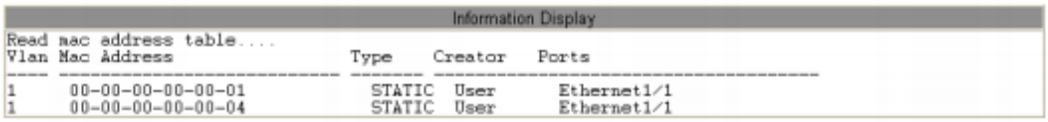



Рисунок 100 – Список индивидуальных MAC-адресов

6. Просмотр записей индивидуальных MAC-адресов в таблице.
Нажмите [Device Basic Configuration] → [MAC address configuration] → [Show mac-address table], чтобы открыть таблицу коммутации. Отображаются все динамические и статические записи, как показано на рисунке 101.

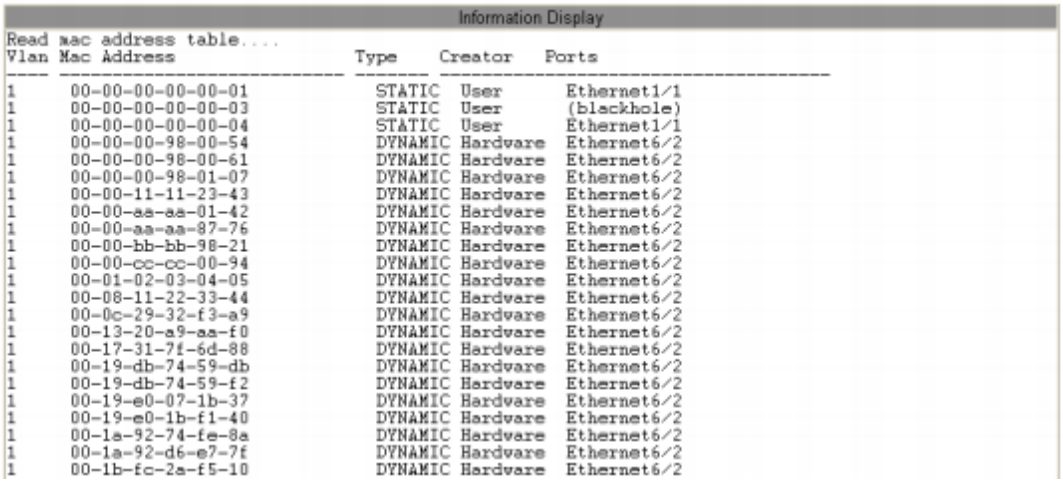



Рисунок 101 – Таблица индивидуальных MAC-адресов

## 5.15 Сопровождение и отладка

При настройке коммутатора и возникновении неполадок вам может потребоваться проверить корректность различных настроек и определить причину неисправности. В этих случаях вы можете выполнить следующие операции для просмотра системных настроек и состояния работы устройства:

1. Ping.
Нажмите [Device Basic Configuration] → [Basic configuration debug] → [Ping and Traceroute], чтобы перейти на страницу операции ping, как показано на рисунке 102.

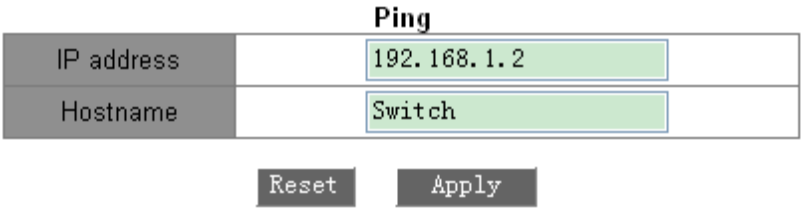



Рисунок 102 – Ping

**IP address (IP-адрес)**
Формат: A.B.C.D.
Описание: ввод IP адреса удалённого устройства.

**Hostname (имя устройства)**
Диапазон: 1~30 символов
Функция: если соответствие между именем данного устройства и его IP-адресом установлено, достаточно ввести это имя и нажать кнопку <Apply>.
Описание: коммутатор отправляет ICMP-запросы на удалённое устройство для индикации соединения между устройствами.

2. Traceroute.

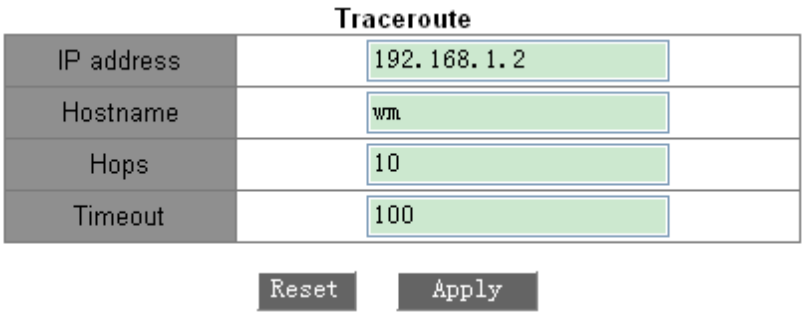



Рисунок 103 – Traceroute

**IP address (IP адрес)**
Формат: A.B.C.D

Описание: введите IP адрес удалённого устройства.

**Hostname (имя устройства)**
Диапазон: 1~30 символов.
Функция: если соответствие между именем данного устройства и его IP адресом установлено, достаточно ввести это имя и нажать кнопку <Apply>.
**Hops (количество транзитных участков сети)**
Варианты: 1~255.
Функция: проверка количества шлюзов на пути данных между отправляющим и принимающим запрос устройствами.
**Timeout (время ожидания)**
Варианты: 100~10000 мс.
Функция: назначение времени ожидания. Если отправляющее запрос устройство не получит ответ за данное время, считается, что соединения между устройствами нет.

3. Системные часы и дата.
Данные коммутаторы поддерживают RTC: время продолжит отсчитываться даже при отключении питания устройства.
Чтобы открыть страницу информации о часах, нажмите [Device Basic Configuration] → [Basic configuration debug] → [show clock] (см. рисунок 104).

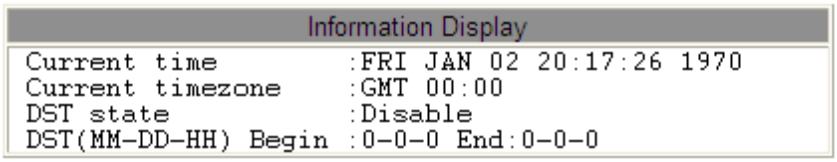



Рисунок 104 – Системные часы

4. Информация о файлах, сохранённых на флеш-памяти.
Нажмите [Device Basic Configuration] → [Basic configuration debug] → [show flash], чтобы открыть страницу информации о флеш-памяти, как показано на рисунке 105.

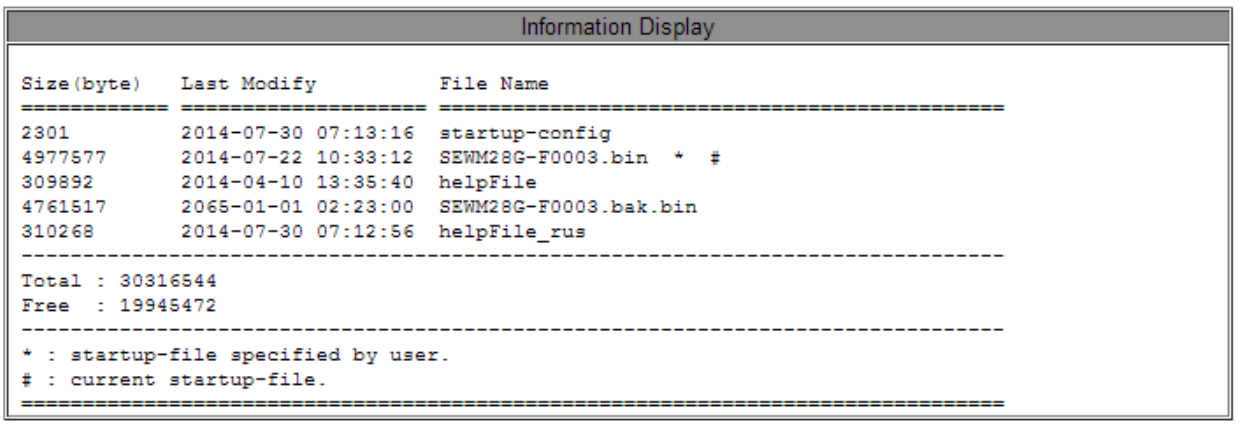



Рисунок 105 – Информация флеш-памяти

5. Чтобы показать текущие настройки со всеми внесёнными изменениями, нажмите [Device Basic Configuration] → [Basic configuration debug] → [show running-config] (см. рисунок 106).

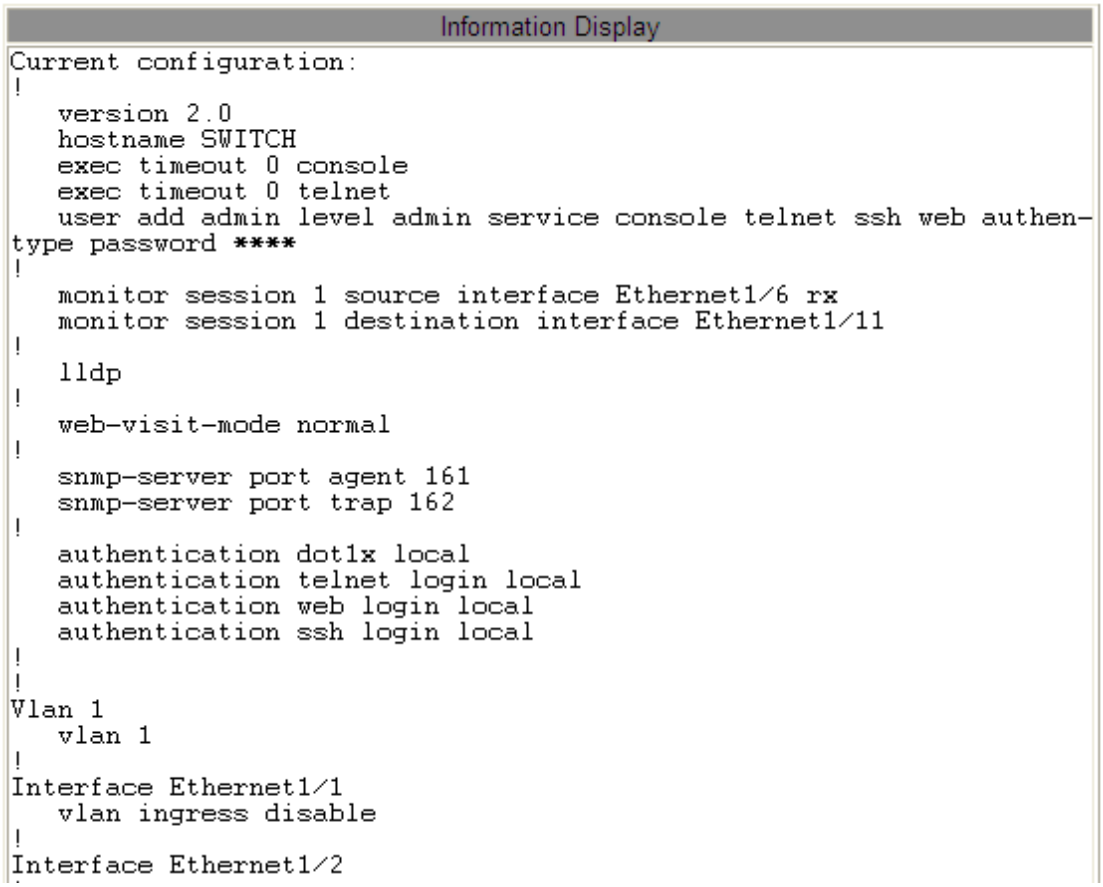



Рисунок 106. Информация о настройках.

6. Просмотр информации о порте.
Нажмите [Device Basic Configuration] → [Basic configuration debug] → [show switchport interface], чтобы перейти на страницу информации о порте, как показано на рисунке 107.

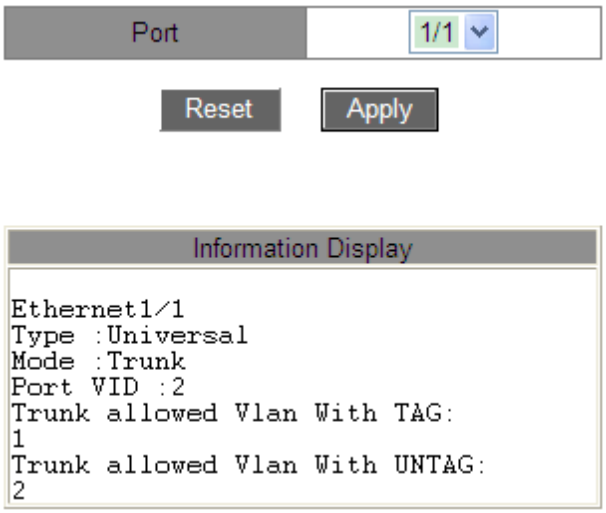



Рисунок 107 – Информация о порте

**Type (тип)**
Описание: тип порта.

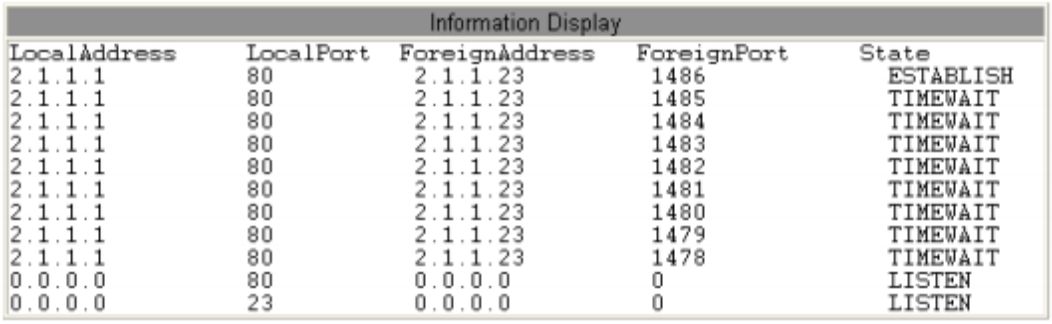
**Mode (режим)**
Описание: режим VLAN на порту.

**Port VID (идентификатор VLAN порта)**
Описание: PVID порта.

**Trunk allowed Vlan With TAG (пропустить разрешённую VLAN с тегом)**
Описание: отображение VLAN, чьи тегированные данные могут быть переданы через транковый порт.

**Trunk allowed Vlan With UNTAG (пропустить разрешённую VLAN без тега)**
Описание: отображение VLAN, чьи нетегированные данные могут быть переданы через транковый порт.

7. Просмотр состояния TCP-соединения.
Нажмите [Device Basic Configuration] → [Basic configuration debug] → [show tcp], чтобы открыть страницу с информацией о TCP-соединении, как показано на рисунке 108.



Information Display

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

Рисунок 108 – TCP-соединение

**Local Address (локальный адрес)**
Описание: отображает локальный адрес TCP-соединения.

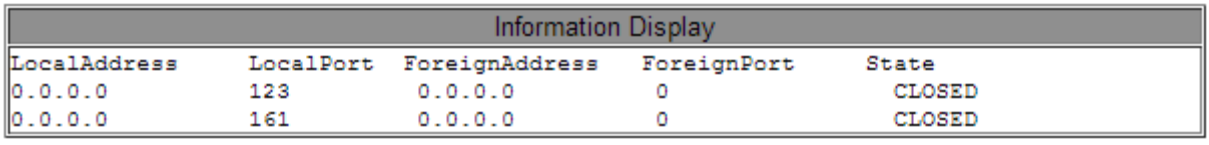
**Local Port (локальный порт)**
Описание: отображает номер локального порта TCP-соединения.

**Foreign Address (запрашиваемый адрес)**
Описание: отображает запрашиваемый адрес TCP-соединения.

**Foreign Port (запрашиваемый порт)**
Описание: отображает номер запрашиваемого порта TCP-соединения.

**State (статус)**
Описание: отображает текущий статус TCP-соединения.

8. Просмотр статуса соединения UDP.
Нажмите [Device Basic Configuration] → [Basic configuration debug] → [show udp], чтобы перейти на страницу информации о соединении UDP, как показано на рисунке 109.



Information Display

| LocalAddress | LocalPort | ForeignAddress | ForeignPort | State |
|---|---|---|---|---|
| 0.0.0.0 | 123 | 0.0.0.0 | 0 | CLOSED |
| 0.0.0.0 | 161 | 0.0.0.0 | 0 | CLOSED |

Рисунок 109 – UDP-соединение

**Local Address (локальный адрес)**
Описание: отображает локальный адрес UDP-соединения.

**Local Port (локальный порт)**
Описание: отображает номер локального порта UDP-соединения.

**Foreign Address (запрашиваемый адрес)**
Описание: отображает запрашиваемый адрес UDP-соединения.

**Foreign Port (запрашиваемый порт)**
Описание: отображает номер запрашиваемого порта UDP-соединения.

**State (статус)**
Описание: отображает текущий статус UDP соединения.

9. Просмотр информации о пользователях, вошедших в систему.
Нажмите [Device Basic Configuration] → [Basic configuration debug] → [show login], чтобы открыть страницу с информацией о пользователях, подключенных к коммутатору, как показано на рисунке 110.

Information Display

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

Рисунок 110 – Подключенные пользователи

# 6. Расширенная конфигурация устройства

## 6.1 Конфигурация ARP

### 6.1.1 Введение

Address Resolution Protocol (ARP) – протокол разрешения адресов, определяющий соответствие между IP-адресом и MAC-адресом через механизм запросов и ответов. Коммутатор может запоминать соответствие между IP-адресом и MAC-адресом устройств в сети. Также коммутаторы поддерживают статические ARP-записи, связывающие IP-адреса и MAC-адреса. Динамические ARP-записи периодически устаревают, что обеспечивает обновление информации.
Данные коммутаторы поддерживают не только коммутацию второго уровня, но и ARP-разрешение адресов, обеспечивая взаимодействие между NMS и управляемыми устройствами.

### 6.1.2 Пояснение

ARP-записи делятся на статические и динамические.
Динамические записи генерируются и поддерживаются на основании полученных коммутатором ARP-запросов. Динамические записи могут устаревать, обновляться новыми ARP запросами и перезаписываться статическими записями.
Статические записи вводятся вручную, и также вручную поддерживаются. Они не устаревают и не перезаписываются динамическими записями.

Коммутаторы поддерживают до 512 ARP-записей (до 256 статических) Если число ARP-записей превышает 512, новые записи автоматически начинают перезаписывать старые динамические.

### 6.1.3 Прокси-ARP

Если запрос ARP отправляется с хоста на другой хост, который находится в том же сетевом сегменте, но в другой физической сети, шлюз, находящийся в прямом соединении с хостом-источником и имеющий функцию «прокси-ARP», может ответить на этот запрос. Такой процесс называется прокси-ARP.
Процесс прокси-ARP выглядит следующим образом:
1. Хост-источник отправляет запрос ARP другому хосту в другой физической сети.
2. Функция прокси-ARP на этом интерфейсе VLAN была включена на шлюзе, находящемся в прямом соединении с хостом-источником. Если нормальный маршрут к целевому хосту существует, шлюз предлагает свой собственный MAC-адрес в качестве (якобы конечного) места назначения
3. IP-пакеты, отправленные с исходного узла на узел назначения, отправляются на устройство с включенным прокси-ARP.
4. Шлюз выполняет обычную IP-маршрутизацию и пересылку пакетов.
5. IP-пакеты, которые должны быть отправлены на узел назначения, наконец достигают узла назначения по сети.

---

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

---

### 6.1.4 Настройка с помощью WEB-интерфейса

1. Добавление или удаление статической записи ARP.
Нажмите [Device Advanced Configuration] → [ARP configuration] → [ARP configuration], чтобы открыть страницу конфигурации ARP, как показано на рисунке 111.

**ARP configuration**

| | |
|---|---|
| IP address(0.0.0.0) | 192.168.0.23 |
| MAC address(HH-HH-HH-HH-HH-HH) | 00-00-00-00-00-01 |
| Operation type | Add |
| L3 interface | Vlan1 |
| Ethernet port | 1/8 |

Apply

Рисунок 111 – Настройка статической ARP-записи

**IP address (IP-адрес)**
Формат: A.B.C.D.

Функция: назначение IP-адреса статической записи ARP.

**MAC-address (MAC-адрес)**
Формат: FF-FF-FF-FF-FF-FF (F – это шестнадцатеричное число).
Функция: назначение MAC-адреса статической записи ARP.

**Operation type (тип действия)**
Варианты: Add/Del (добавить/удалить).
Значение по умолчанию: Add (добавить).
Функция: ДОБАВИТЬ или удалить ARP запись.

**L3 interface (интерфейс L3)**
Варианты: все созданные VLAN интерфейсы L3.
Значение по умолчанию: VLAN1.
Функция: выбор VLAN интерфейса L3 для текущей записи ARP.

**Ethernet port (порт Ethernet)**
Варианты: все порты выбранной VLAN.
Функция: выбор порта, соответствующего текущей записи ARP.

---

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

---

2. Просмотр записей адресов ARP.
Нажмите [Device Advanced Configuration] → [ARP configuration] → [Show ARP], чтобы открыть страницу конфигурации ARP, как показано на рисунке 112.

ARP list

| IP address | MAC address | L3 interface | Ethernet port | Type |
|---|---|---|---|---|
| 192.168.0.21 | 12-2a-bd-c3-44-55 | Vlan1 | 1/8 | dynamic |
| 192.168.0.120 | 78-2b-cb-60-3c-e3 | Vlan1 | 1/8 | dynamic |
| 192.168.0.23 | 00-00-00-00-00-01 | Vlan1 | 1/8 | static |
| 192.168.0.18 | 00-72-75-78-88-5b | Vlan1 | 1/8 | dynamic |
| 192.168.0.19 | d0-67-e5-2d-95-a5 | Vlan1 | 1/8 | dynamic |
| 192.168.0.199 | 70-71-bc-95-cc-22 | Vlan1 | 1/8 | dynamic |
| 192.168.0.86 | 80-c1-6e-e0-5b-9a | Vlan1 | 1/8 | dynamic |
| 192.168.0.192 | 78-2b-cb-2c-6b-87 | Vlan1 | 1/8 | dynamic |
| 192.168.0.2 | 00-1e-cd-00-e6-5f | Vlan1 | 1/8 | dynamic |
| 192.168.0.212 | 00-71-bc-95-cc-4d | Vlan1 | 1/8 | dynamic |
| 192.168.0.99 | c8-9c-dc-a8-c4-ac | Vlan1 | 1/8 | dynamic |
| 192.168.0.184 | 44-37-e6-88-6e-90 | Vlan1 | 1/8 | dynamic |
| 192.168.0.44 | 08-00-3e-32-53-29 | Vlan1 | 1/8 | dynamic |

Refresh

Рисунок 112 – Таблица ARP

**ARP list (таблица ARP)**
Заголовок таблицы: {IP-адрес, MAC-адрес, интерфейс L3, порт Ethernet, тип}
Функция: просмотр записей ARP.
Описание: таблица ARP показывает все ARP-записи, соответствующие активным портам, включая статические и динамические записи.

3. Очистка кэша ARP.
Нажмите [Device Advanced Configuration] → [ARP configuration] → [Clear ARP cache], чтобы очистить кэш ARP, как показано на рисунке 113.

Clear ARP cache

Apply

Рисунок 113 – Очистка кэша ARP

Нажмите <Apply> для очистки всех динамических ARP записей из кэша.

4. Включение прокси-ARP.
Нажмите [Device Advanced Configuration] → [ARP configuration] → [Proxy ARP configuration], чтобы настроить прокси-ARP, как показано на рисунке 114.

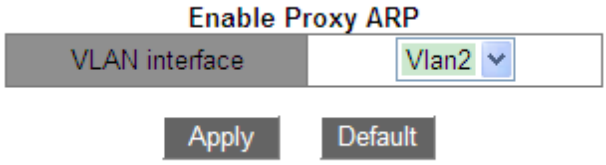



Рисунок 114 – Настройка прокси-ARP

**VLAN interface (интерфейс VLAN)**
Функция: выбор интерфейса VLAN 3-го уровня для включения прокси-ARP.

## 6.1.5 Пример типовой настройки

Как показано на рисунке 115, ПК1, ПК2 и ПК3 — это узлы в одном сегменте сети, принадлежащие к разным подсетям VLAN1, VLAN2 и VLAN4 соответственно.

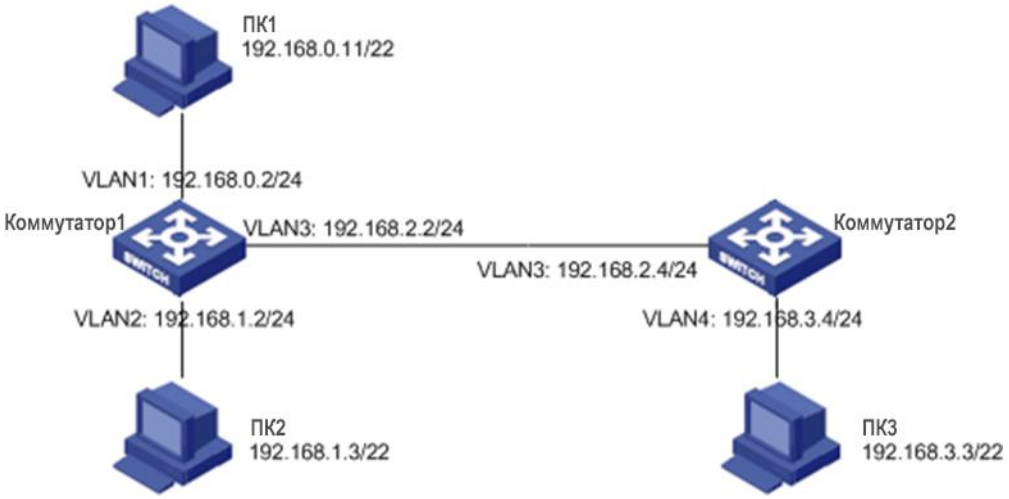



Рисунок 115 – Пример конфигурации прокси-ARP

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

## 6.2 Настройка интерфейсов третьего уровня

### 6.2.1 IP-адрес коммутатора

Войдите в интерфейс командной строки коммутатора через консольный порт. Запустите команду **enable** в общем режиме, чтобы войти в привилегированный режим. Запустите команду **show interface vlan 1**, чтобы просмотреть IP-адрес коммутатора, как показано в красном круге на рисунке 116.

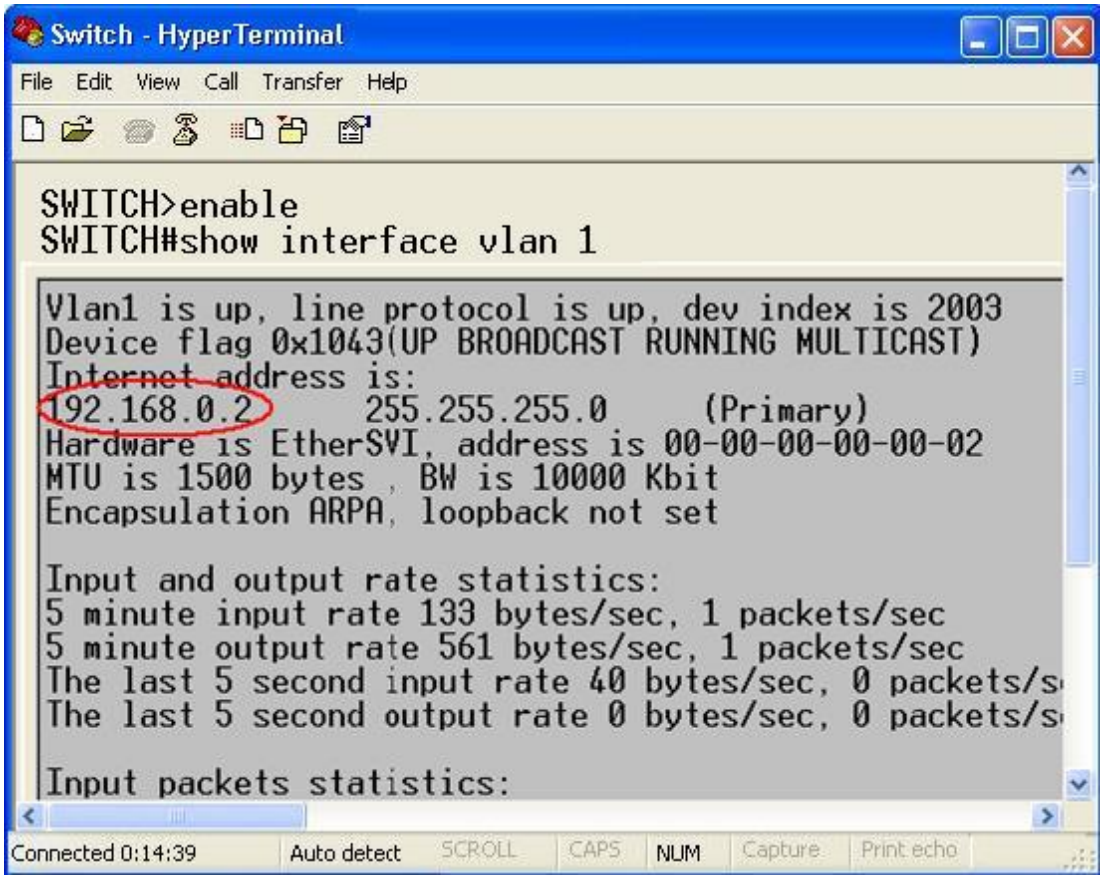



Рисунок 116 – Отображение IP-адреса коммутатора

### 6.2.2 Настройка IP-адреса

1. Создание интерфейса VLAN 3-го уровня.

Узлы, находящиеся в различных VLAN, не могут взаимодействовать между собой. Данные, передаваемые между ними, должны быть переданы на маршрутизатор или коммутатор третьего уровня через VLAN-интерфейс.

Данные коммутаторы поддерживают виртуальные VLAN-интерфейсы третьего уровня, которые можно использовать для коммуникации между различными VLAN. Вы можете создать один VLAN-интерфейс для каждой VLAN. Этот интерфейс используется для передачи пакетов третьего уровня портов VLAN.

Нажмите [Device Advanced Configuration] → [L3 interface configuration] → [Add interface VLAN], чтобы открыть страницу конфигурации, как показано на рисунке 117.

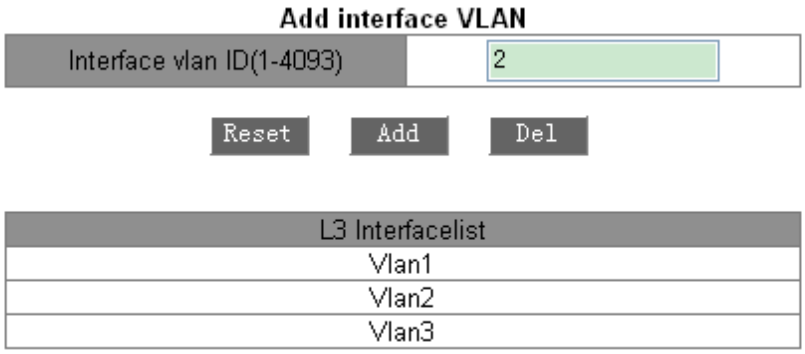



Рисунок 117 – Создание интерфейса VLAN

**Interface VLAN ID (идентификатор интерфейса VLAN)**
Опции: все созданные номера VLAN.
Функция: создание интерфейса VLAN L3.

---

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

---

2. Получение IP-адреса
IP-адрес коммутатора можно настроить вручную или получить автоматически.
Нажмите [Device Advanced Configuration] → [L3 interface configuration] → [L3 interface IP address mode configuration], чтобы открыть страницу конфигурации IP-адреса интерфейса L3, как показано на рисунке 118.

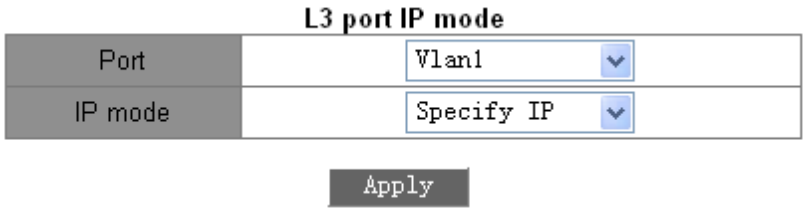



Рисунок 118 – Получение IP-адреса

**Port (интерфейс)**
Параметры: все созданные интерфейсы VLAN L3.
Значение по умолчанию: VLAN1.

**IP Mode (IP-режим)**
Варианты: bootp-client/dhcp-client/Specify IP.
По умолчанию: Specify IP (указать IP).
Функция: выбор режима получения IP-адреса.
Описание: указать IP-адрес — настроить IP-адрес вручную; bootp-client/dhcp-client заключается в том, что коммутатор автоматически получает IP-адрес через DHCP/BOOTP. В сети должен быть сервер DHCP/BOOTP для назначения IP-адресов клиентам. О конфигурации сервера DHCP/BootP см. раздел 6.14 «Настройка DHCP».

3. Задать IP-адрес вручную.
Нажмите [Device Advanced Configuration] → [L3 interface configuration] → [Allocate IP address for L3 port], чтобы назначить IP-адрес, как показано на рисунке 119.

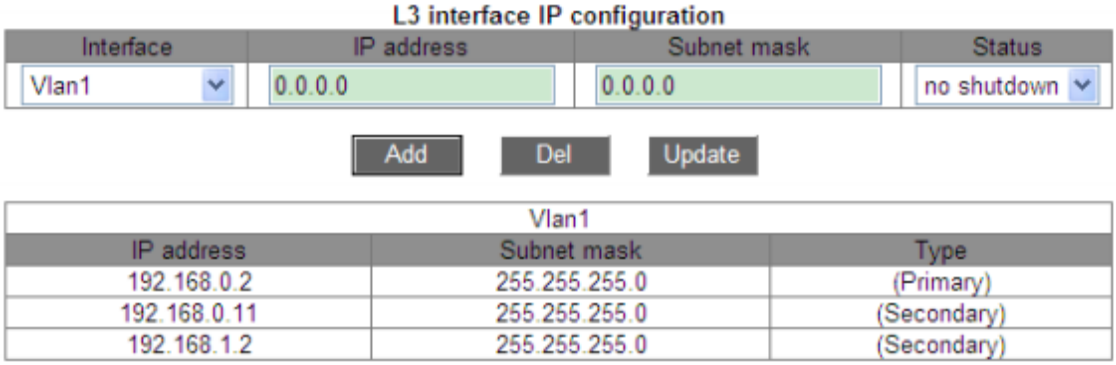



Рисунок 119 – Ручная настройка IP-адреса

**IP Address (IP-адрес)**
Формат: A.B.C.D.
Функция: назначение IP адреса для выбранного интерфейса L3 VLAN.

**Subnet mask (Маска подсети)**
Маска подсети – это число с длиной в 32 бита, состоящая из последовательности единиц и нулей. «1» определяют часть адреса, содержащую номер сети или подсети, а «0» обозначают адрес конкретного узла. Обычно равно 255.255.255.0.

**Status (состояние)**
Варианты: no shutdown/shutdown (не закрывать/закрыть).
По умолчанию: no shutdown (не закрывать).
Функция: настройка статуса IP адреса интерфейса L3.
Описание: режим «no shutdown» открывает интерфейс VLAN L3; режим «shutdown» – закрывает.

**Type (тип)**
Варианты: secondary/primary (вторичный/основной).
Значение по умолчанию: primary (основной).

Функция: на одном и том же порту можно установить более двух IP-адресов разных сетевых сегментов для реализации связи между ними в одной локальной сети. Как правило, поскольку одного сегмента сети пользователю недостаточно, можно использовать этот метод.
Описание: вторичный IP-адрес может решить проблему агрегации маршрутизации в RIP v1. Его можно использовать для NAT, после преобразования он не является адресом прямого подключения маршрутизатора. Нажмите <Add>, чтобы настроить IP-адрес для интерфейса VLAN; нажмите <Del>, чтобы удалить текущий IP-адрес. Вы должны сначала удалить вторичный IP-адрес, прежде чем удалять основной; нажмите <Update>, чтобы изменить основной IP-адрес интерфейса VLAN.

---

- Каждый интерфейс VLAN L3 поддерживает до 32 IP адресов.
- Для каждого VLAN интерфейса могут быть указаны IP адреса в одном или в разных сегментах сети.
- IP адреса разных сетевых сегментов должны принадлежать разным интерфейсам VLAN.

---

## 6.3 SNMPv2c

### 6.3.1 Введение

Simple Network Management Protocol (SNMP) – протокол управления сетевыми устройствами через TCP/IP. Благодаря функции SNMP, администратор может запрашивать информацию об устройстве, менять настройки, следить за состоянием устройства и обнаруживать неполадки сети.

### 6.3.2 Реализация

Для управления устройствами, SNMP использует архитектуру «station/agent». Таким образом, по функциональности разделяется на два типа: NMS и агент.

- Network Management Station (NMS) – клиент, имеющий программное обеспечение, использующее SNMP. Он является ядром сетевого управления и архитектуры SNMP.
- Агент – это процесс, находящийся в памяти сетевого устройства. Он получает и обрабатывает запросы от NMS. Если возникает неполадка, агент самостоятельно оповещает о ней NMS.

NMS является средством управления SNMP сетью, а агент – частью управляемого устройства. NMS и агенты обмениваются управленческими данными через SNMP. SNMP включает следующие основные команды:

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

NMS отправляет команды Get-Request, Get-Next-Request и Set-Request для запроса данных, настройки и управления устройством. После получения этих запросов, агенты отвечают командами Get-Response. При возникновении неполадки, агент самостоятельно оповещает о них NMS с помощью Trap-команды.

### 6.3.3 Пояснение

Коммутаторы данной серии поддерживают SNMPv2. SNMPv2 обратно совместима с SNMPv1.

Для аутентификации SNMPv1 использует «community name». «Community name» играет роль пароля, ограничивая доступ NMS к агентам. Если «community name» в SNMP запросе неизвестно коммутатору, запрос отклоняется.

SNMPv2 также использует «community name» для аутентификации. Протокол обратно совместим с SNMPv1, при этом расширяя его возможности.

Для поддержки соединения между NMS и агентом, их версии SNMP должны совпадать. На агенте может быть настроена своя версия SNMP, для возможности работы с разными NMS.

### 6.3.4 MIB. Введение

Любой настраиваемый ресурс называется объектом управления. MIB (Management Information Base) хранит в себе все объекты управления. Она определяет иерархию объектов управления и их атрибуты, такие как имя, доступ, тип данных. Каждый агент имеет свою MIB. NMS может считывать и записывать данные в MIB, в зависимости от разрешений. На рисунке 120 показаны взаимосвязи между NMS, агентом и MIB.

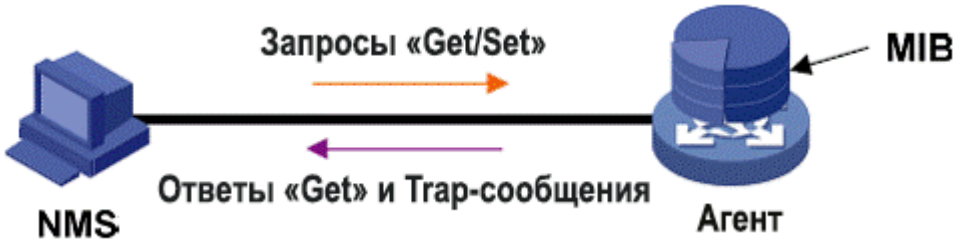



Рисунок 120 – Взаимосвязи между NMS, агентом и MIB

MIB представляет из себя древовидную структуру. Узлы дерева являются объектами управления. Каждый узел имеет уникальный идентификатор (Object Identifier – OID), который определяет положение узла в структуре MIB. Как показано на рисунке 121, OID объекта A равен 1.2.1.1.

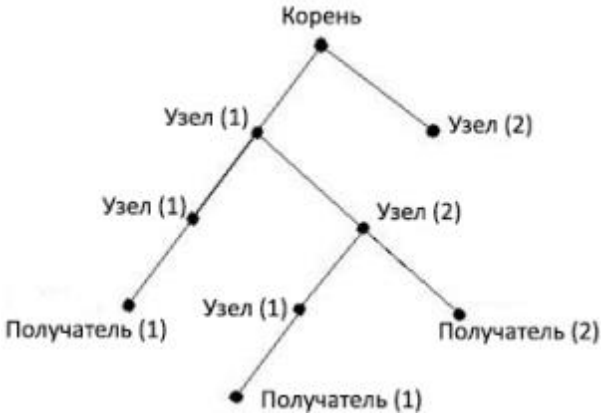



Рисунок 121 – Структура дерева MIB

## 6.3.5 Настройка с помощью WEB-интерфейса

1. Настройка SNMPv2c

Нажмите [Device Advanced Configuration] → [SNMP Configuration] → [SNMP Base Configuration], чтобы настроить SNMPv2c, как показано на рисунке 122.

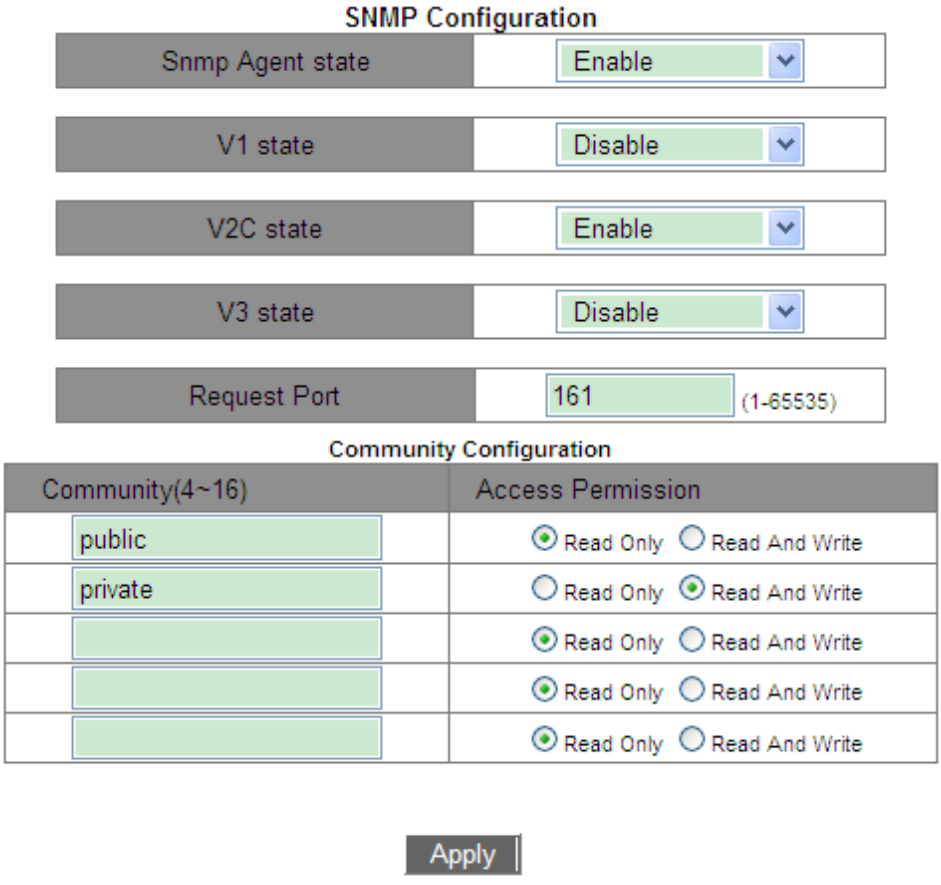



Рисунок 122 – Настройка SNMPv2c

**Snmp Agent state (состояние агента SNMP)**
Варианты: Enable/Disable (включить/отключить).
По умолчанию: Disable (отключить).
Функция: включить/отключить SNMP.

**V1/V2C/V3 state (состояние V1/V2C/V3)**
Варианты: Enable/Disable (включить/отключить).
Функция: выбор версии SNMP.

**Request Port (порт запроса)**
Диапазон: 1~65535.
Значение по умолчанию: 161.
Функция: настройка номера порта для приема SNMP-запросов.

**Community (сообщество)**
Диапазон: 4~16 символов.
Функция: настройка community коммутатора.
Описание: пакет может получить доступ к MIB коммутатора только в том случае, если имя сообщества, передаваемое в SNMP-пакете, совпадает с именем, настроенном на коммутаторе.
Пояснение: можно задать не более 5 строк «community».

**Access Permission (права доступа)**
Варианты: Read Only/Read And Write (только чтение/чтение и запись).
Значение по умолчанию: Read Only (только чтение).
Функция: настройка режима доступа к MIB.
Описание: Read Only: можно только считывать MIB-информацию. Read And Write: MIB-информацию можно и считывать, и записывать.

2. Настройка доверенных IP-адресов.
Нажмите [Device Advanced Configuration] → [SNMP Configuration] → [IP Address of SNMP Manager], чтобы открыть страницу конфигурации доверенного IP-адреса, как показано на рисунке 123.

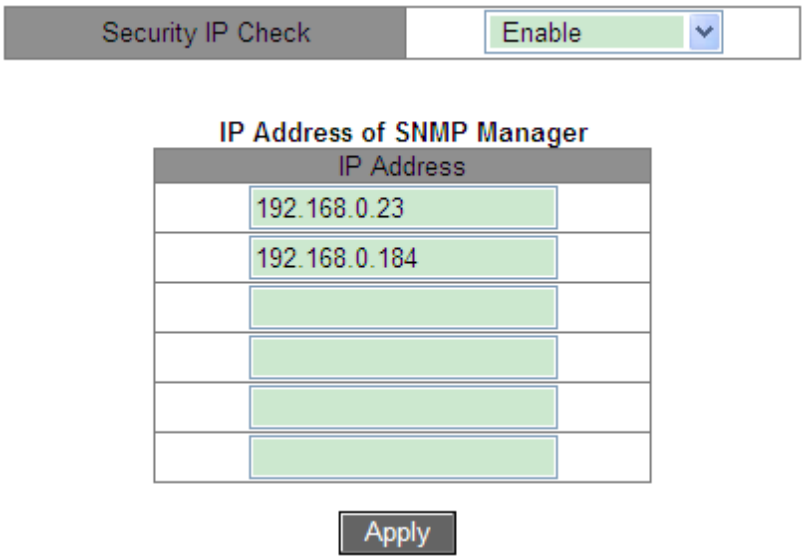



Рисунок 123 – Настройка доверенного IP-адреса

**Security IP Check (проверка доверенного IP)**
Варианты: Enable/Disable (включить/отключить).
По умолчанию: Disable (отключить).
Функция: включить или отключить проверку доверенного IP. Если проверка отключена, нет ограничений на IP-адрес NMS, любая NMS, подключенная к коммутатору, может получить доступ к информации MIB коммутатора. После того, как проверка включена, необходимо назначить доверенный IP-адрес, и доступ к информации MIB коммутатора сможет получить только NMS с доверенным адресом.

**IP Address (IP-адрес)**
Формат: A.B.C.D.
Функция: настройка доверенного IP-адреса NMS.
Описание: только NMS, чей IP-адрес соответствует доверенному IP-адресу, может получить доступ к информации MIB коммутатора. Коммутатор позволяет использовать до шести таких адресов.

3. Настройка параметров SNMP Trap.
Нажмите [Device Advanced Configuration] → [SNMP Configuration] → [TRAP Configuration], чтобы настроить SNMP Trap, как показано на рисунке 124.

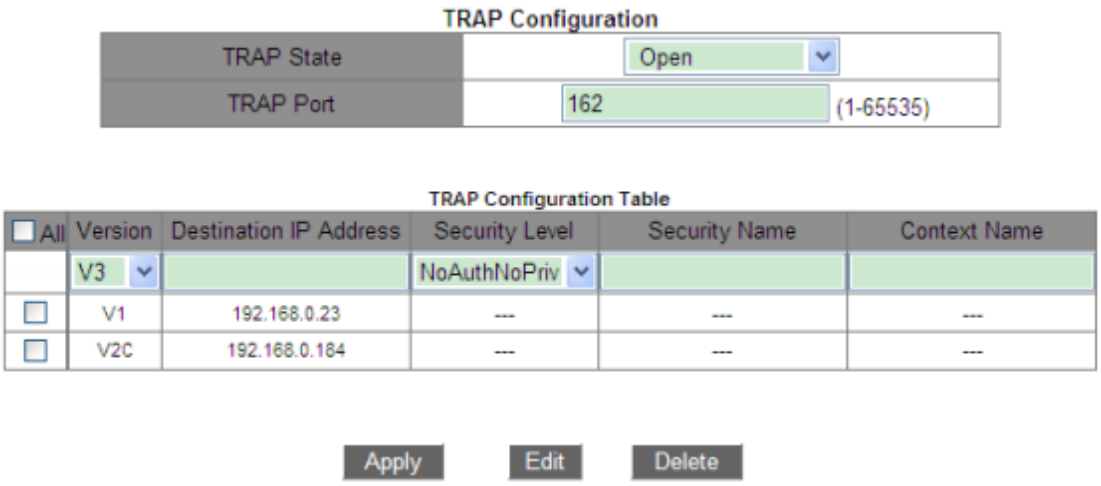



Рисунок 124 – Включение Trap

**TRAP State (статус Trap)**
Варианты: Open/Close (открыть/закрыть).
По умолчанию: Close (закрыть).
Функция: разрешить коммутатору отправлять Trap-сообщения, или нет.

**TRAP Port**
Варианты: 1~65535
Значение по умолчанию: 162
Функция: назначение номера порта для отправки Trap-сообщений.

**Version (версия)**
Варианты: V1/V2C/V3.
Функция: указывает, что коммутатор отправляет на сервер Trap-сообщения соответствующей версии. Если вы выберете V1/V2C, необходимо настроить только IP-адрес назначения.

**Destination IP Address (IP-адрес получателя)**
Формат: A.B.C.D.
Функция: настройка адреса сервера для получения Trap-сообщений. Можно настроить до восьми серверов, то есть восемь записей в таблице.

4. Просмотр статистики SNMP.
Нажмите [Device Advanced Configuration] → [SNMP Configuration] → [SNMP Statistics], чтобы открыть страницу статистики SNMP, как показано на рисунке 125.

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

Show

Рисунок 125 – Статистика SNMP

## 6.3.6 Пример типовой настройки

Сервер управления SNMP подключен к коммутатору через Ethernet. IP-адрес сервера управления — 192.168.0.23, а коммутатора — 192.168.0.2. NMS отслеживает и управляет агентом через SNMPv2c, а также считывает и записывает информацию об узле MIB агента. Когда агент неисправен, он активно отправляет Trap-пакеты в NMS, как показано на рисунке 126.

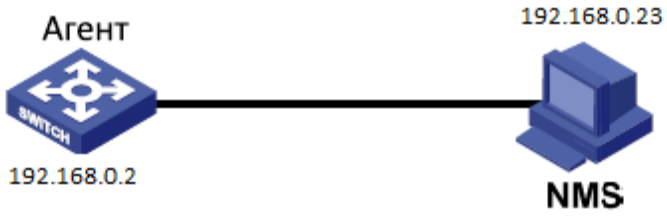



Рисунок 126 – Пример настройки SNMPv2c

Настройка агента:

1. Включите SNMP в режиме V2C. Установите права доступа «Read Only» для public community и «Read And Write» для private community, как показано на рисунке 122.
2. Установите доверенный IP-адрес 192.168.0.23, как показано на рисунке 123.
3. Включите SNMP Trap; выберите версию V2C, IP-адрес получателя – 192.168.0.23, как показано на рисунке 124.

Если вы хотите отслеживать агентские устройства и управлять ими, запустите соответствующее программное обеспечение управления в NMS.

## 6.4 SNMPv3

### 6.4.1 Введение

SNMPv3 обеспечивает механизм аутентификации User-Based Security Model (USM). Он позволяет настроить функции аутентификации и шифрования. Аутентификация используется для проверки подлинности отправителя пакета, предотвращая доступ незаконных пользователей. Шифрование служит для защиты передаваемых между NMS и агентом пакетов от перехвата. Это повышает безопасность связи между NMS и агентом.

### 6.4.2 Реализация

SNMPv3 предоставляет пять таблиц конфигурации. Каждая таблица может содержать 16 записей. Эти таблицы определяют, могут ли определенные пользователи получать доступ к информации MIB.
В таблице пользователей вы можете создать нескольких пользователей с разными политиками безопасности для аутентификации и шифрования.
Групповая таблица — это совокупность нескольких пользователей. В групповой таблице права доступа определяются на основе групп пользователей. Все пользователи группы имеют права группы.
Контекстная таблица идентифицирует строки, которые могут быть прочитаны пользователями, независимо от их моделей безопасности.
Таблица представления указывает информацию MIB, к которой могут получить доступ пользователи. Представление MIB может содержать все узлы определенного поддерева (то есть, пользователям разрешен доступ ко всем узлам поддерева MIB) или не содержать ни одного из узлов определенного поддерева (то есть, пользователям не разрешен доступ ни к одному узлу поддерева MIB).
В таблице доступа вы можете определить права доступа MIB по имени группы, контекстному имени, модели безопасности и уровню безопасности.

### 6.4.3 Настройка с помощью WEB-интерфейса

1. Настройка таблицы пользователей.
Нажмите [Device Advanced Configuration] → [SNMP Configuration] → [V3 User Table], чтобы открыть страницу конфигурации таблицы пользователей V3, как показано на рисунке 127.

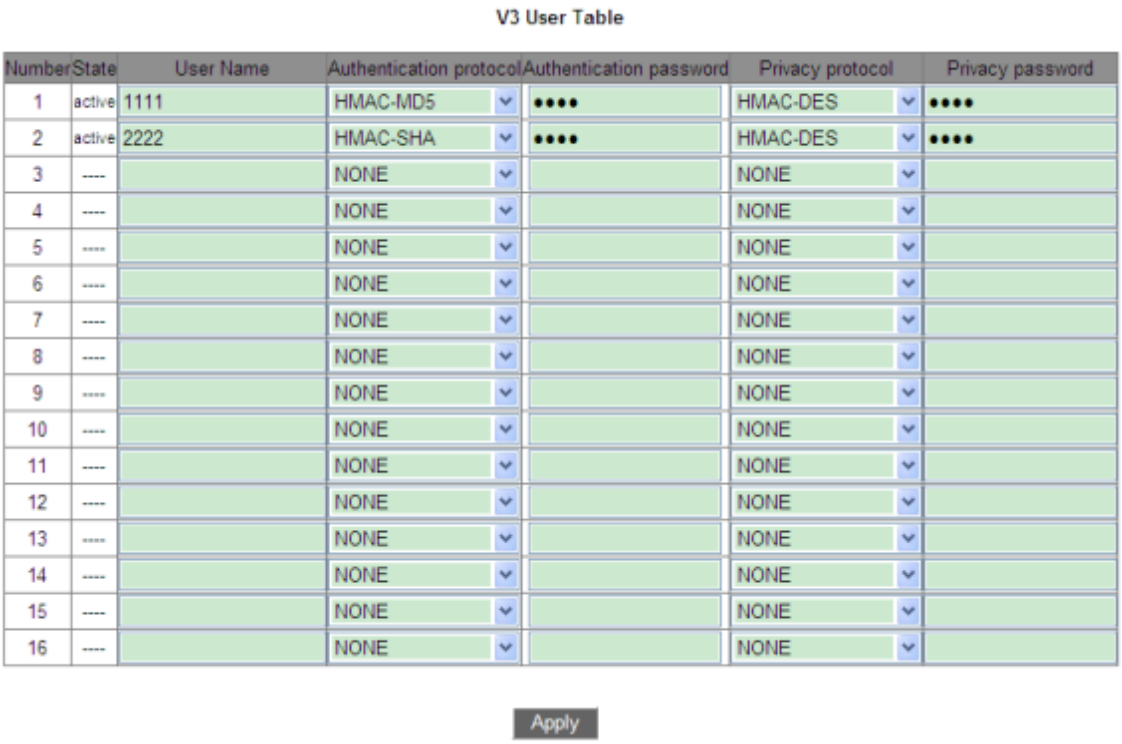



Рисунок 127 – Настройка таблицы пользователей SNMPv3

**User Name (имя пользователя)**
Диапазон: 4~16 символов.
Функция: создание имени пользователя.

**Authentication protocol (протокол аутентификации)**
Варианты: NONE/HMAC-MD5/HMAC-SHA
Значение по умолчанию: NONE (нет).
Функция: выбор алгоритма аутентификации.

**Authentication password (пароль аутентификации)**
Диапазон: 4~16 символов.
Функция: создание пароля аутентификации.

**Privacy protocol (протокол конфиденциальности)**
Варианты: NONE/CBC-DES
Значение по умолчанию: NONE (нет).
Функция: выбор протокола шифрования пакетов.

**Privacy password (пароль конфиденциальности)**
Диапазон: 4~16 символов.
Функция: создание пароля для шифрования пакетов.

2. Настройка групповой таблицы.

Нажмите [Device Advanced Configuration] → [SNMP Configuration] → [V3 Group Table], чтобы перейти на страницу настройки групповой таблицы V3, как показано на рисунке 128.

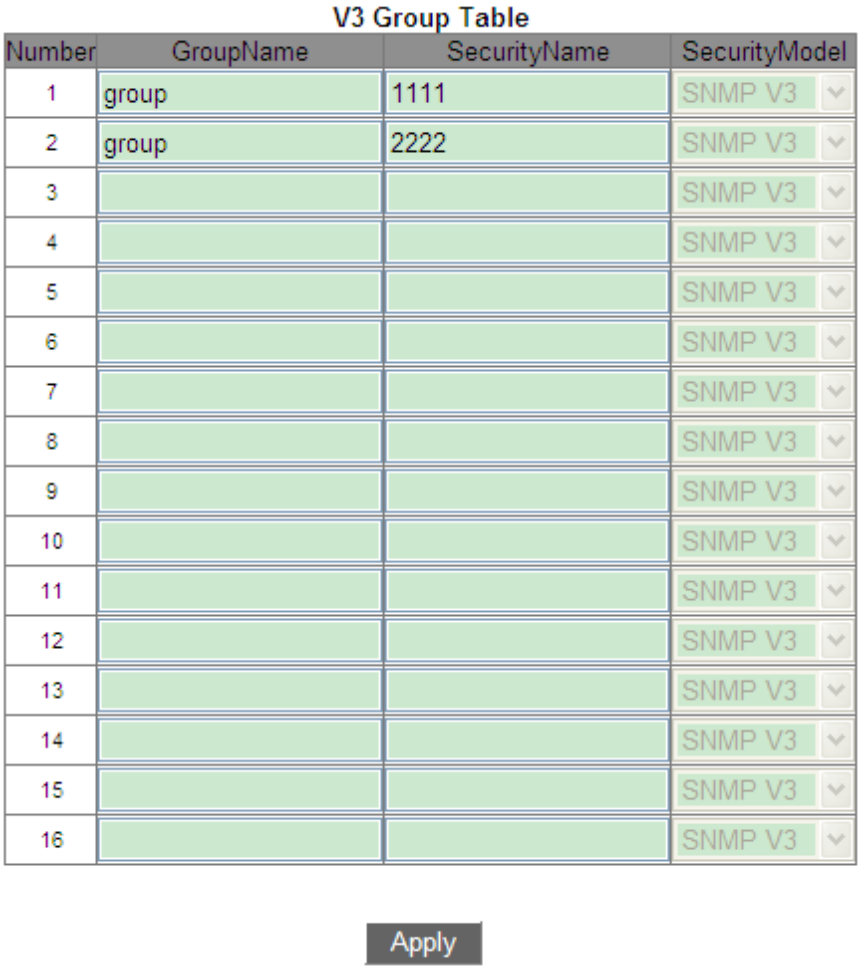



Рисунок 128 – Настройка групповой таблицы SNMPv3

**Group Name (имя группы)**
Диапазон: 4~16 символов.
Функция: Настройка имени групповой таблицы.

**Security Name (доверенное имя)**
Диапазон: все существующие имена пользователей, 4~16 символов.
Функция: настройка доверенного имени. Это имя должно совпадать с именем пользователя в пользовательской таблице. Пользователи с одинаковым именем группы принадлежат к одной группе.

**Security Model (модель безопасности)**
Значение по умолчанию: SNMPv3.
Описание: SNMPv3 указывает, что применяется модель безопасности на основе пользователей (USM). На текущий момент значение должно быть SNMPv3.

3. Настройка контекстной таблицы.
Нажмите [Device Advanced Configuration] → [SNMP Configuration] → [V3 Context Table], чтобы открыть страницу настройки контекстной таблицы V3, как показано на рисунке 129.


Рисунок 129 – Настройка контекстной таблицы SNMPv3

**Context Name (контекстное имя)**
Диапазон: 4~16 символов.
Функция: настроить контекстное имя.
Описание: первое контекстное имя должно быть пустым.

4. Настройка таблицы представлений.
Нажмите [Device Advanced Configuration] → [SNMP Configuration] → [V3 View Table], чтобы перейти на страницу настройки таблицы представлений V3, как показано на рисунке 130.

V3 View Table

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

Apply

Рисунок 130 – Настройка таблицы представлений SNMPv3

**View Name (имя представления)**
Диапазон: 4~16 символов.
Функция: настройка имени представления.

**Type (тип)**
Опции: included/excluded (включено/исключено).
Значение по умолчанию: included (включено).
Функция: «included» указывает, что данное представление включает все узлы дерева MIB. «excluded» указывает, что данное представление не включает узлы дерева MIB.

**oid-tree (дерево MIB)**
Функция: MIB-дерево, обозначенное идентификатором OID корневого узла дерева.

**Mask (маска)**
Функция: маска дерева MIB. «Oid-tree» и «Mask» вместе определяют информацию об узле MIB текущего представления.

Например, на рисунке 147 представление с именем «view1» может иметь доступ только к информации узла 1.3.6.1.2.1.1.1, 1.3.6.1.2.1.2.1, 1.3.6.1.2.1.3.1 и 1.3.6.1.2.1.4.1… 1.3.6.1.2.1.n.1.

5. Настройка таблицы доступа.
Нажмите [Device Advanced Configuration] → [SNMP Configuration] → [V3 Access Table], чтобы открыть страницу настройки таблицы доступа V3, как показано на рисунке 131.


Рисунок 131 – Настройка таблицы доступа SNMPv3

**Group Name (имя группы)**
Диапазон: все существующие имена групп, 4~16 символов.
Функция: пользователи в группе имеют одинаковые права доступа.

**Context Prefix (префикс контекста)**
Диапазон: все существующие имена контекстов, 4~16 символов
Функция: настроить имя контекста. Имя группы и имя контекста вместе определяют права доступа группы. Поскольку первое имя контекста в контекстной таблице должно быть пустым, префикс контекста может быть пустым.

**Context Match (соответствие контексту)**
Варианты: exact/prefix (строгое/префикс).
Значение по умолчанию: exact (строгое).
Функция: выберите режим соответствия имени контекста. «Exact» указывает, что значение префикса контекста должно строго совпадать с контекстным именем. «Prefix» указывает, что значение префикса контекста должно совпадать с первыми 4–16 символами контекстного имени. В этом случае имена контекстов с одинаковым префиксом имеют одинаковые права доступа.

**Security Model (модель безопасности)**
Значение по умолчанию: SNMP V3.
Описание: SNMPv3 указывает, что применяется модель безопасности на основе пользователей (USM). На текущий момент значение должно быть SNMPv3.

**Security Level (уровень безопасности)**
Варианты: NoAuthNoPriv/AuthNoPriv/AuthPriv.
Значение по умолчанию: NoAuthNoPriv.
Функция: выбрать права доступа к информации MIB.
Описание: NoAuthNoPriv указывает, что не требуется ни аутентификация, ни шифрование пакетов. AuthNoPriv указывает, что требуется только аутентификация. AuthPriv указывает, что требуется как аутентификация, так и шифрование пакетов. Когда требуется шифрование, пользователь может получить доступ к указанной информации MIB только в том случае, если алгоритм шифрования и пароль идентичны настроенным в пользовательской таблице.

**read View (представление с правом чтения)**
Параметры: все существующие имена представлений.
Функция: выбрать имя представления с правом на чтение.

**write View (представление с правом записи)**
Параметры: все существующие имена представлений.
Функция: выбрать имя представления с правом на запись.

**notify View (представление с правом уведомления)**
Параметры: все существующие имена представлений.
Функция: выбрать имя представления, которое может отправлять trap-сообщение.

6. Настройка доверенных IP-адресов.
Нажмите [Device Advanced Configuration] → [SNMP Configuration] → [IP Address of SNMP Manager], чтобы перейти на страницу настройки доверенного IP-адреса, как показано на рисунке 132.

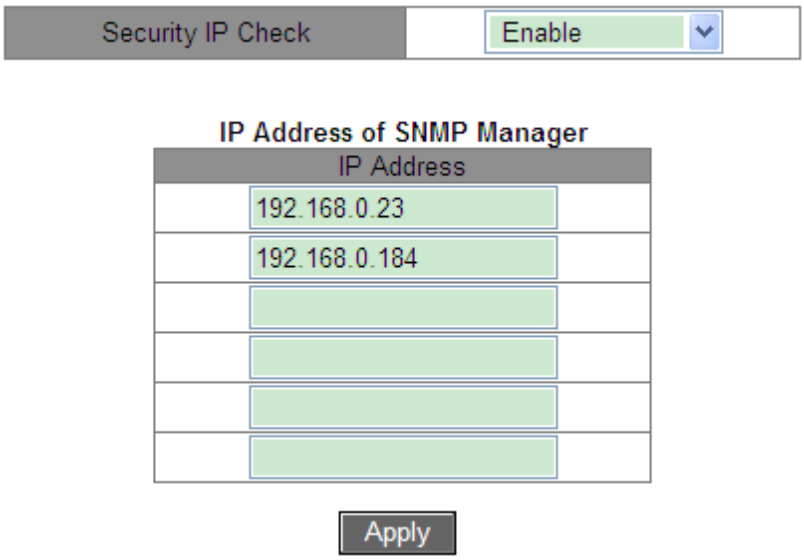



Рисунок 132 – Настройка доверенного IP-адреса

**Security IP Check (проверка доверенного IP)**
Варианты: Enable/Disable (включить/отключить).
Значение по умолчанию: Disable (отключить).
Функция: включить или отключить проверку безопасности IP. Если проверка безопасности IP отключена, нет ограничений на IP-адрес NMS, любая NMS, подключенная к коммутатору, может получить доступ к информации MIB коммутатора. После включения проверки необходимо внести доверенные IP-адреса, и только NMS с этими адресами смогут получить доступ к информации MIB коммутатора.

**IP Address (IP-адрес)**
Формат: A.B.C.D.
Функция: настроить доверенный IP-адрес NMS.
Описание: только NMS, чей IP-адрес соответствует доверенному, может получить доступ к информации MIB коммутатора. Коммутатор позволяет настроить шесть доверенных IP-адресов NMS.

7. Настройка Trap.
Нажмите [Device Advanced Configuration] → [SNMP Configuration] → [TRAP Configuration], чтобы настроить Trap SNMPv3, как показано на рисунке 133.

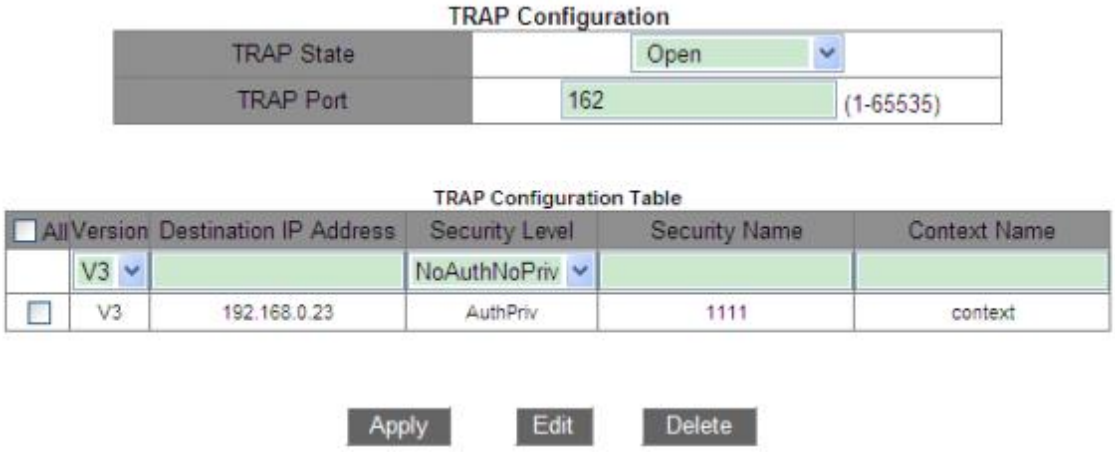



Рисунок 133 – Настройка Trap SNMPv3

**TRAP State (статус)**
Варианты: Open/Close (открыть/закрыть).
По умолчанию: Close (закрыть).
Функция: разрешить коммутатору отправлять Trap-сообщения, или нет.

**TRAP Port**
Варианты: 1~65535
Значение по умолчанию: 162
Функция: назначение номера порта для отправки Trap-сообщений.

**Version (версия)**
Варианты: V1/V2C/V3.
Функция: указывает, что коммутатор отправляет на сервер Trap-сообщения соответствующей версии. V3 указывает на то, что коммутатор отправляет на сервер trap-сообщения версии 3.

**Destination IP Address (IP-адрес получателя)**
Формат: A.B.C.D.
Функция: настройка адреса сервера для получения Trap-сообщений. Можно настроить до восьми серверов, то есть восемь записей в таблице.

**{Security Level, Security Name, Context Name} {уровень безопасности, доверенное имя, контекстное имя}**
Варианты: {NoAuthNoPriv/AuthNoPriv/AuthPriv, 4~16 символов, 4~16 символов}
Функция: эти три параметра необходимо настраивать только при выборе V3. Данные настройки должны соответствовать настройкам в таблице доступа. Уровень безопасности может быть равен или выше, чем в таблице доступа. Например, когда право доступа пользователя 1111 установлено на AuthNoPriv, коммутатор может отправлять trap-сообщения на сервер только в том случае, если уровень безопасности доверенного имени 1111 — AuthNoPriv или AuthPriv. Контекстное имя должно совпадать с префиксом контекста в таблице доступа.

### 6.4.4 Пример типовой настройки

Сервер управления SNMP подключен к коммутатору через Ethernet. IP-адрес сервера управления — 192.168.0.23, а коммутатора — 192.168.0.2. Пользователь 1111 и пользователь 2222 управляют агентом через SNMPv3. Уровень безопасности установлен на AuthNoPriv, и коммутатор может выполнять только операцию чтения информации узла Агента. При возникновении неисправности агент заранее отправляет сообщения trap v3 в NMS, как показано на рисунке 134.

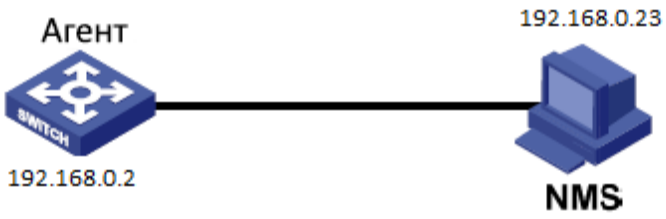



Рисунок 134 – Пример конфигурации SNMPv3

Настройка агента.

1. Настройте таблицу пользователей SNMPv3. Выберите имя пользователя 1111, протокол аутентификации HMAC-MD5, пароль аутентификации «аааа», протокол конфиденциальности HMAC-DES и пароль конфиденциальности «хххх». Выберите другое имя пользователя 2222, протокол аутентификации HMAC-SHA, пароль аутентификации «bbbb», протокол конфиденциальности HMAC-DES и пароль конфиденциальности «уууу», как показано на рисунке 127.

2. Создайте группу и добавьте в нее пользователя 1111 и пользователя 2222, как показано на рисунке 128.

3. Создайте контекстное имя, то есть контекст, как показано на рисунке 129.

4. Создайте таблицу представлений. «view-all» включает все узлы дерева MIB 1, «view-no» не включает ни один узел дерева MIB 1, как показано на рисунке 130.

5. Настройте таблицу доступа SNMPv3 (см. рисунок 131). Установите следующие параметры:

- group name – group;
- context name – context;
- context match – exact;
- security level – AuthNoPriv;
- readView – view-all;
- writeView – view-no;
- notifyView – view-all.

6. Включите функцию Trap и настройте номер порта 162. Настройте запись параметров в таблице. Установите для Trap версию V3, IP-адрес назначения — 192.168.0.23, уровень безопасности — AuthPriv, доверенное имя — 1111, контекстное имя — context, как показано на рисунке 133. Если необходимо отслеживать и управлять устройствами агента, запустите соответствующее программное обеспечение управления в NMS.

## 6.5 Sy2-Ring

### 6.5.1 Введение

Sy2-Ring и Sy2-Ring+ – проприетарные протоколы резервирования компании Symanitron. Они позволяют сети восстанавливаться менее чем за 50 мс при обрыве связи, обеспечивая надёжную работу.
Sy2-Ring бывают двух типов: кольцо, основанное на портах (Sy2-Ring-Port), и кольцо, основанное на VLAN (Sy2-Ring-VLAN).
Sy2-Ring-Port: определяет порт, через который необходимо передавать или блокировать данные.
Sy2-Ring-VLAN: определяет порт определённой VLAN, через который необходимо передавать или блокировать данные. Это позволяет настраивать несколько колец, относящихся к разным VLAN, на одном порту.
Sy2-Ring-Port и Sy2-Ring-VLAN нельзя использовать одновременно.

### 6.5.2 Концепция

**Мастер-узел** (Master station): кольцо может иметь только один мастер-узел. Мастер-узел отправляет пакеты Sy2-Ring и следит за текущим статусом кольца.
**Мастер-порт** (Master port): первый порт, чьё состояние на мастер-узле меняется на рабочее, называется мастер-порт. Он переходит в режим перенаправления пакетов.
**Ведомый-порт** (Slave port): порт на мастер-узле, чьё состояние меняется на рабочее позже мастер-порта, называется ведомый порт. Когда кольцо замкнуто, ведомый порт находится в режиме отбрасывания пакетов. Если кольцо разомкнуто, например, из-за обрыва связи или выхода из строя порта, статус ведомого порта меняется на продвижение пакетов.
**Ведомый-узел** (Slave station): кольцо может иметь множество ведомых узлов. Ведомые узлы ждут Sy2-Ring пакетов и оповещают мастер-узел о неисправностях.
**Резервный порт** (Backup port): порт для связи между Sy2-кольцами называется резервным.
**Резервный мастер-порт** (Master Backup Port): Если в кольце множество резервных портов, резервным мастер-портом является резервный порт, подключённый к устройству с бóльшим MAC-адресом, находящийся при этом в состоянии пересылки данных.
**Резервный ведомый порт** (Slave Backup Port): если в кольце множество резервных портов, все порты, кроме резервного мастер-порта, станут резервными мастер-портами и перейдут в режим отбрасывания пакетов.
**Состояние пересылки данных**: порт может получать и передавать данные.
**Состояние блокировки**: порт может получать и передавать только Sy2-Ring пакеты, но не может получать и передавать любые другие данные.

## 6.5.3 Sy2-Ring. Реализация

**Реализация Sy2-Ring-Port**

Мастер-порт на мастер-узле периодически отправляет Sy2-Ring пакеты для определения состояния кольца. Если резервный порт мастер-узла получает пакеты, кольцо замкнуто, если нет, то разомкнуто.

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

1. Коммутатор A настроен как ведущий (master), а остальные коммутаторы — как ведомые (slave).

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

3. Канал связи CD неисправен, как показано на рисунке 135.

а) Когда канал связи CD неисправен, порты 6 и 7 ведомого устройства находятся в состоянии блокировки. Порт 2 на ведущем устройстве переходит в состояние пересылки данных, обеспечивая нормальную связь по каналу.
б) Когда неисправность устранена, порты 6 и 7 ведомого устройства находятся в состоянии пересылки. Порт 2 на ведущем устройстве переходит в состояние блокировки. Происходит переключение каналов, и каналы восстанавливаются до состояния, предшествующего отказу канала CD.

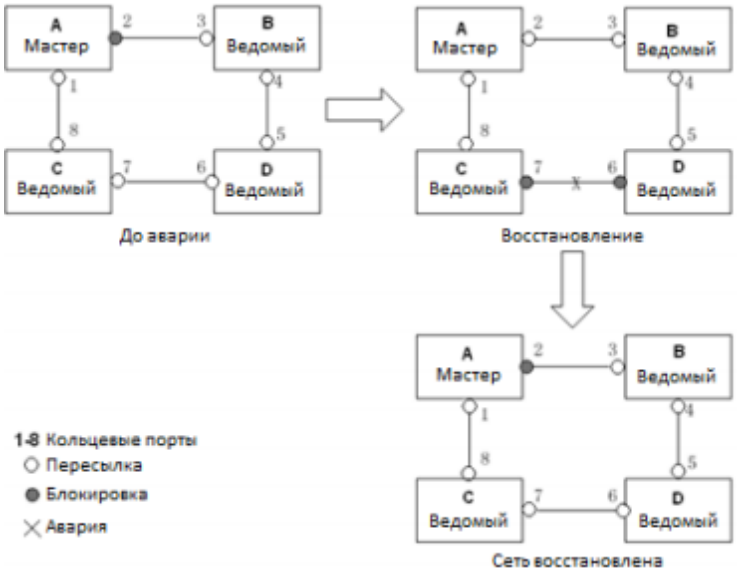



Рисунок 135 – Неисправность канала связи CD

4. Канал связи AC неисправен, как показано на рисунке 136.

а) Когда канал AC неисправен, порт 1 находится в состоянии блокировки, а порт 2 переходит в состояние пересылки, обеспечивая нормальную связь по каналу.
б) После устранения неисправности порт 1 все еще находится в состоянии блокировки, а порт 8 — в состоянии пересылки. Переключения не происходит.

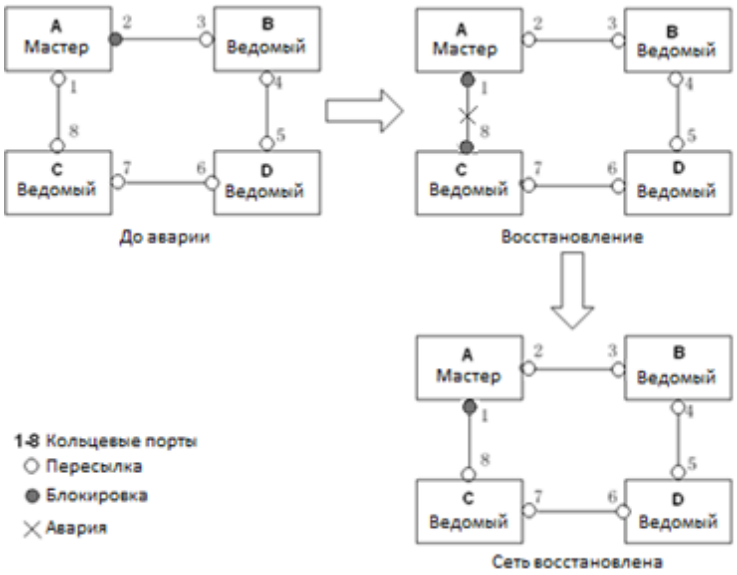



Рисунок 136 – Неисправность канала связи AC

Изменение состояния соединения влияет на состояние портов кольца.

**Реализация Sy2-Ring-VLAN**

Sy2-Ring-VLAN позволяет пересылать пакеты из разных VLAN по разным путям.
Каждый путь пересылки для VLAN образует Sy2-Ring-VLAN. У разных колец Sy2-Ring-VLAN могут быть разные мастер-узлы. Как показано на рисунке 137, настроены две Sy2-Ring-VLAN:

- VLAN 10: AB-BC-CD-DE-EA.
- VLAN 20: FB-BC-CD-DE-EF.

Два кольца могут объединяться на определённых участках. В данном примере это связи BC, CD и DE. Коммутатор C и коммутатор D используют в двух кольцах одни и те же порты, но разные логические каналы на основе VLAN.

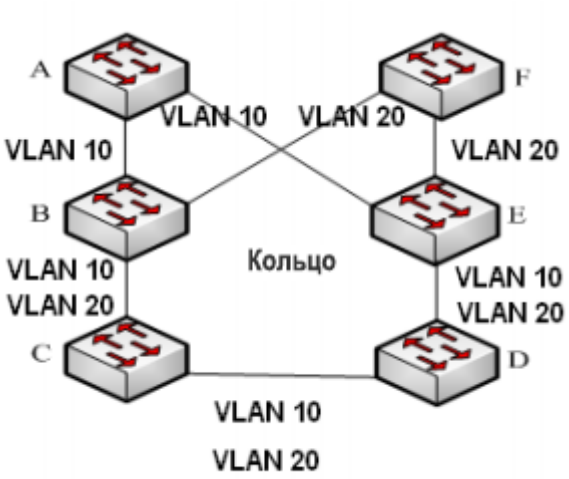



Рисунок 137 – Sy2-Ring-VLAN

---

В каждом логическом кольце Sy2-Ring-VLAN реализация идентична реализации Sy2-Ring-Port.

---

**Реализация Sy2-Ring+**

Sy2-Ring+ может обеспечивать резервирование для двух колец SY2, как показано на рисунке 138. Один резервный порт настроен соответственно на коммутаторе C и коммутаторе D. Какой порт является резервным мастер-портом, зависит от MAC-адресов двух портов. Если главный резервный порт или его канал выходят из строя, ведомый резервный порт будет пересылать пакеты, предотвращая образование петель и обеспечивая нормальную связь между резервными кольцами.

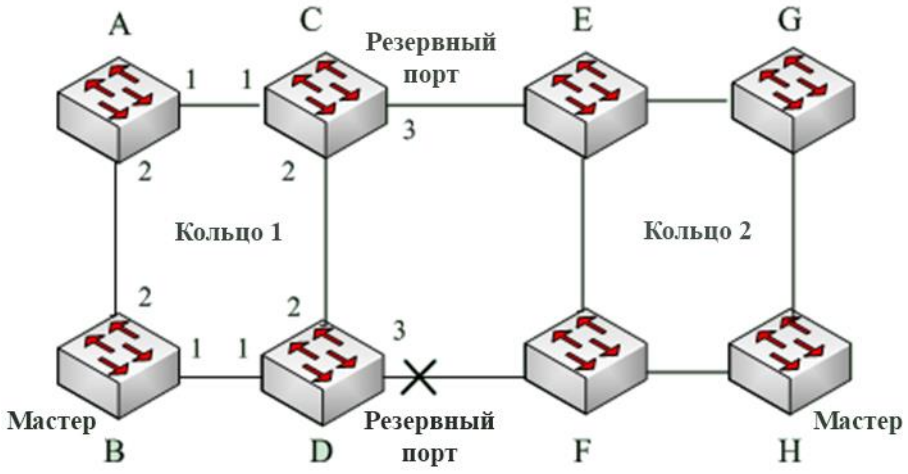



Рисунок 138 – Топология Sy2-Ring+

Изменение состояния соединения влияет на состояние резервных портов.

## 6.5.4 Пояснение

Конфигурации Sy2-Ring должны соответствовать следующим условиям:

- Все коммутаторы в одном кольце должны иметь одинаковый номер домена.
- В каждом кольце может быть только один мастер-узел и несколько ведомых узлов.
- На каждом коммутаторе можно настроить только два порта для кольца.
- Для двух соединенных колец резервные порты можно настроить только в одном кольце.
- Для одного кольца можно настроить не более двух резервных портов.
- На коммутаторе для одного кольца можно настроить только один резервный порт.
- Sy2-Ring-Port и Sy2-Ring-VLAN нельзя настроить на одном коммутаторе одновременно.

## 6.5.5 Настройка с помощью WEB-интерфейса

1. Настройка режима резервируемого кольца.
Нажмите [Device Advanced Configuration] → [Sy2-Ring Configuration] → [Sy2-Ring Mode], чтобы открыть страницу настройки, как показано на рисунке 139.


Рисунок 139 – Настройка режима резервируемого кольца

**Настройка режима резервирования**
Варианты: Sy2-PORT/Sy2-VLAN.
По умолчанию: Sy2-PORT.
Функция: выбор режима кольцевого резервирования.

- Кольцевые протоколы на основе портов включают RSTP, Sy2-Ring-Port и Sy2-RP-Port, а кольцевые протоколы на основе VLAN включают MSTP, Sy2-Ring - VLAN и Sy2-RP-VLAN.
- Кольцевые протоколы на основе VLAN являются взаимоисключающими, и для одного устройства можно настроить только один тип кольцевого протокола на основе VLAN.
- Кольцевой протокол на основе портов и кольцевой протокол на основе VLAN являются взаимоисключающими, и для одного устройства можно выбрать только один режим кольцевого резервирования.

2. Создание Sy2-Ring.
Нажмите Click [Device Advanced Configuration] → [Sy2-Ring Configuration] → [Sy2-Ring Configuration], чтобы создать Sy2-Ring, как показано на рисунке 140.

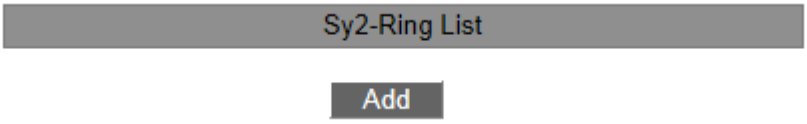



Рисунок 140 – Создание Sy2-Ring

Нажмите <Add> для создания Sy2-Ring.

3. Настройка Sy2-Ring и Sy2-Ring-VLAN как показано на рисунках 141 и 142.

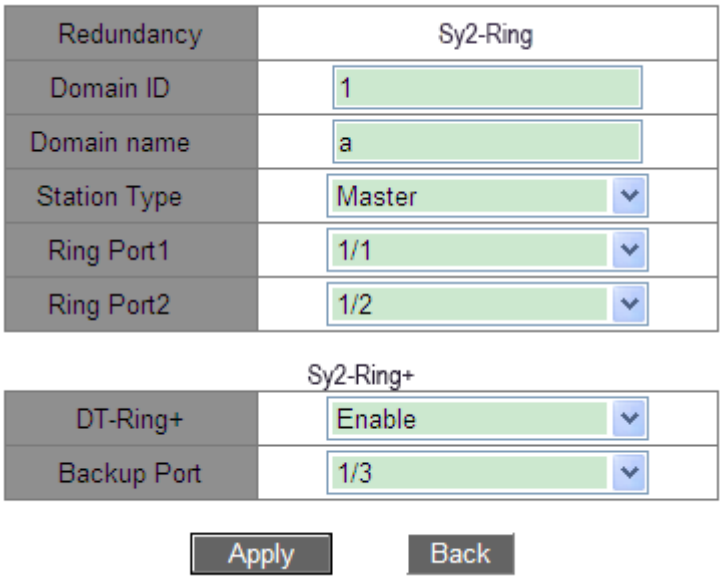



Рисунок 141 – Настройка Sy2-Ring

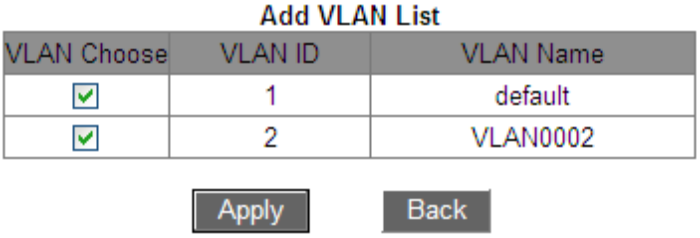



Рисунок 142 – Настройка Sy2-Ring-VLAN

**Redundancy (резервирование)**

По умолчанию: Sy2-Ring.

**Domain ID (идентификатор домена)**
Диапазон значений: 1~32.
Функция: идентификатор домена используется для разграничения колец. Один коммутатор поддерживает до 16 колец, определяемых по портам и до 8 колец, определяемых по VLAN.

**Domain name (доменное имя)**
Диапазон: 1~31 символов.
Функция: назначение доменного имени.

**Station Type (тип узла)**
Варианты: Master/Slave (мастер/ведомый).
По умолчанию: Master (мастер).
Функция: выбор роли устройства в кольце.

**Ring port 1/Ring port 2 (кольцевой порт 1/кольцевой порт 2)**
Варианты: все порты коммутатора.
Функция: выбор двух кольцевых портов.

---

- Порт кольца Sy2-Ring, а также резервные порты не могут быть добавлены в группу агрегации «port channel». Порт, добавленный в группу агрегации не может быть портом кольца Sy2-Ring или резервным портом.
- Порт кольца Sy2-Ring, а также резервные порты не могут быть портом назначения зеркалирования. Порт назначения зеркалирования не может быть портом кольца Sy2-Ring или резервным-портом.
- STP не может быть включен на кольцевом порту или на резервном-порту. STP-порт не может быть портом кольца Sy2-Ring или резервным-портом. Протоколы Sy2-Ring и Sy2-RP – взаимоисключающие. Коммутатор не может быть одновременно в кольце Sy2-Ring и в кольце Sy2-RP.
- Не рекомендуется настраивать порты в группе изоляции одновременно как порты Sy2-Ring и резервные порты, а порты Sy2-Ring и резервные порты нельзя добавлять в группу изоляции.

---

**Sy2-Ring+**
Варианты: Enable/Disable (включить/выключить).
По умолчанию: Disable (выключен).
Функция: включение/выключение Sy2-Ring+.

**Backup port (резервный порт)**
Варианты: все порты коммутатора.
Функция: сделать порт резервным.
Примечание: до назначения резервного порта включите Sy2-Ring+.

**Add VLAN list (добавить список VLAN)**
Варианты: все созданные VLAN.
Функция: выбор VLAN для кольцевого порта.

После завершения настройки в списке Sy2-Ring List отображаются все созданные кольца, как показано на рисунке 143.

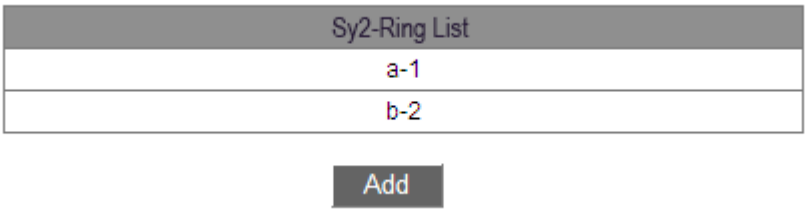



Рисунок 143 – Отображение всех созданных колец

4.Просмотр и изменение конфигурации Sy2-Ring
Выберите запись в таблице Sy2-Ring для отображения и изменения её настроек, как показано на рисунке 144.

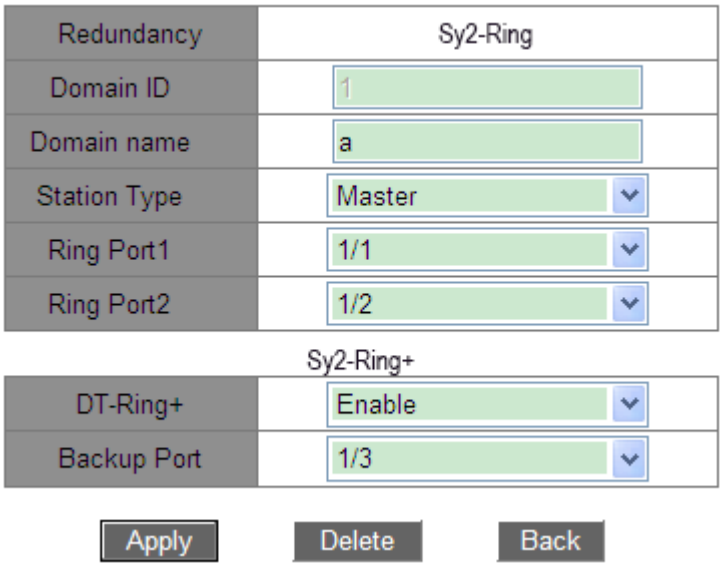



Рисунок 144 – Конфигурация Sy2-Ring

Нажмите <Apply> для сохранения изменений. Нажмите <Delete> для удаления записи настроек Sy2-Ring.

5. Просмотр статуса Sy2-Ring и портов (рисунок 145).

**Sy2-Ring State List**

| Redundancy | Sy2-Ring |
|---|---|
| Ring Port1 | blocking |
| Ring Port2 | blocking |
| Ring State | RING-OPEN |

| Redundancy | Sy2-Ring+ |
|---|---|
| Equipment IP | 192.168.0.3 |
| Equipment MAC | 48-be-2d-00-01-60 |
| BackupPort Status | blocking |

Рисунок 145 – Статус Sy2-Ring

## 6.5.6 Пример типовой настройки

Как показано на рисунке 138, коммутаторы A, B, C и D образуют кольцо 1; коммутаторы E, F, G и H образуют кольцо 2. Каналы CE и DF являются резервными соединениями между кольцом 1 и кольцом 2. Далее описан пример настройки данных коммутаторов при помощи веб-интерфейса (см. рисунок 141).

**Конфигурация коммутатора A:**

1. Идентификатор домена: 1; доменное имя: Ring; кольцевой порт: port 1, port 2; тип узла: Slave; Sy2-Ring+: Disable. Резервные порты не назначены.

**Конфигурация коммутатора B:**

2. Идентификатор домена: 1; доменное имя: Ring; кольцевой порт: port 1, port 2; тип узла: Master; Sy2-Ring+: Disable. Резервные порты не назначены.

**Конфигурация коммутаторов C и D:**

3. Идентификатор домена: 1; доменное имя: Ring; кольцевой порт: port 1, port2; тип узла: Slave; Sy2-Ring+: Enable; резервный порт: port 3.

**Конфигурация коммутаторов E, F и G:**

4. Идентификатор домена: 2; доменное имя: Ring; кольцевой порт: port 1, port2; тип узла: Slave; Sy2-Ring+: Disable. Резервные порты не назначены.

**Конфигурация коммутатора H:**

5. Идентификатор домена: 2; доменное имя: Ring; кольцевой порт: port 1, port2; тип узла: Master; Sy2-Ring+: Disable.  Резервные порты не назначены.

# 6.6 STP/RSTP

## 6.6.1 Введение

Протокол STP (Spanning Tree Protocol) основан на стандарте IEEE802.1D и разработан для предотвращения широковещательных штормов, вызванных циклическими соединениями, а также используется для резервирования связей. Устройства, поддерживающие STP, обмениваются служебными пакетами и блокируют определённые порты для разрыва «петель» и создания «деревьев», предотвращая бесконечную передачу данных по кругу. Недостатком STP является то, что он не поддерживает быстрый переход порта в рабочее состояние и существует необходимость выдерживать техническую паузу перед переходом в режим пересылки.

Для решения проблемы с протоколом STP, IEEE разработал стандарт 802.1w в качестве дополнения стандарта 802.1D. Стандарт IEEE802.1w даёт определение протоколу Rapid Spanning Tree Protocol (RSTP). По сравнению с STP, RSTP работает быстрее за счёт добавления альтернативных и резервных портов для корневых и назначенных портов соответственно. Когда корневой/назначенный порт выходит из строя, его альтернативный/резервный порт немедленно переходит в состояние пересылки.

## 6.6.2 Концепция

**Корневой мост** (Root bridge): является «корнем дерева». Сеть может иметь только один корневой мост. Какой из коммутаторов будет корневым, зависит от сетевой топологии. Корневой мост меняется вместе с топологией сети. Он периодически отправляет BPDU другим устройствам, которые пересылают BPDU для обеспечения стабильности топологии.

**Корневой порт** (Root port): порт некорневого коммутатора, расстояние от которого до корневого коммутатора наименьшее. Под наименьшим расстоянием понимается расстояние до корневого коммутатора с наименьшей стоимостью пути. Все коммутаторы сети связываются с корневым коммутатором через корневые порты. При этом у всех некорневых устройств может быть только один корневой порт. На корневом коммутаторе

**Назначенный порт** (Designated port): порт, который отвечает за пересылку конфигурации BPDU другому устройству или локальной сети. Все порты в корневом мосту являются назначенными портами.

**Альтернативный порт** (Alternate port): резервный порт корневого порта. Если корневой порт выходит из строя, альтернативный порт становится новым корневым.

**Резервный порт** (Backup port): резервный для назначенного порта. Когда назначенный порт выходит из строя, резервный порт становится новым назначенным портом и передаёт данные вместо него.

## 6.6.3 BPDU

Для предотвращения петель все устройства в сети совместно вычисляют структуру логического дерева (ST). Они подтверждают топологию сети путем доставки сообщений BPDU между собой. В таблице 8 показана структура данных BPDU.

Таблица 7 – BPDU

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

Структура данных BPDU включает:
**Идентификатор корневого моста** (Root bridge ID): приоритет корневого коммутатора (2 байта) + MAC-адрес корневого коммутатора (6 байт).
**Стоимость пути** (Root path cost): стоимость кратчайшего пути до корневого моста
**Идентификатор назначенного моста** (Designated bridge ID): приоритет назначенного коммутатора (2 байт) + MAC-адрес назначенного моста (6 байт).
**Идентификатор назначенного порта** (Designated port ID): приоритет порта + номер порта.
**Возраст сообщения** (Message age): время, в течение которого BPDU может распространяться по сети.
**Максимальный возраст или время старения** (Max age): максимальное время хранения BPDU на устройстве. Когда возраст сообщения больше, чем время старения, BPDU отбрасывается.
**Время приветствия** (Hello time): интервал времени для отправки BPDU.
**Задержка отправки** (Forward delay): задержка изменения статуса (отбрасывание – обучение – пересылка).

### 6.6.4 Реализация

Процесс вычисления логического дерева для всех устройств следующий:

1. Начальная стадия.
Все устройства на всех своих портах генерируют BPDU, считая себя корневым мостом; и идентификатор корневого моста, и идентификатор назначенного моста являются идентификатором локального устройства; стоимость корневого пути равна 0; назначенный порт является локальным портом.

2. Выбор оптимальной конфигурации BPDU.
Все устройства отсылают свои BPDU и получают BPDU от других устройств. При получении BPDU, каждый порт сравнивает полученный BPDU со своим.

- Если приоритет конфигурации BPDU, сгенерированного локальным портом выше, чем принятые настройки BPDU, устройство не выполняет никакой обработки.
- Если приоритет полученного BPDU выше, то порт заменяет локальный BPDU полученным.

Устройство выбирает оптимальную конфигурацию BPDU после сравнения конфигураций BPDU всех портов. Принципы сравнения BPDU:

- Конфигурация BPDU с наименьшим идентификатором корневого моста имеет наивысший приоритет.
- Если ID корневого коммутатора двух BPDU одинаковы, сравнивается стоимость пути до корневого коммутатора. Если стоимость пути до корневого коммутатора плюс стоимость пути до локального порта меньше, приоритет BPDU выше.

- Если стоимость пути до корневого коммутатора также одинаковы, по порядку сравниваются ID назначенных коммутаторов, ID назначенных портов и ID портов, получивших BPDU. BPDU с наименьшим ID будет иметь наивысший приоритет.
-

3. Выбор корневого моста.
Корневым мостом связующего дерева (spanning tree) является устройство с наименьшим идентификатором (ID) устройства.

4. Выбор корневых портов.
Некорневые коммутаторы сделают свои порты, получающие наилучшую конфигурацию BPDU, корневыми.

5. Вычисление конфигурации BPDU назначенного порта.
В соответствии с конфигурацией BPDU и стоимостью пути корневого порта, конфигурация BPDU назначенного порта рассчитывается для каждого порта следующим образом:

- Идентификатор корневого моста заменяется идентификатором корневого моста, взятым из конфигурации BPDU корневого порта.
- Стоимость корневого пути заменяется на стоимость из конфигурации BPDU корневого порта плюс соответствующая стоимость пути корневого порта.
- ID назначенного моста заменяется ID устройства.
- ID назначенного порта заменяется на ID данного локального порта.

6. Выбор назначенного порта.
Если вычисленное значение BPDU лучше, устройство делает этот порт назначенным, заменяет BPDU порта вычисленным и отправляет новый BPDU. Если текущее значение BPDU лучше, устройство не обновляет его и блокирует порт. Заблокированные порты могут принимать и отправлять только техническую информацию RSTP, но не данные.

## 6.6.5 Настройка с помощью WEB-интерфейса

1. Включение RSTP.
Нажмите [Device Advanced Configuration] → [RSTP configuration] → [RSTP configuration], чтобы открыть страницу конфигурации RSTP, как показано на рисунке 146.


Рисунок 146 – Включение RSTP/STP

**Protocol Status (статус протокола)**
Варианты: Enable/Disable (включить/отключить).
По умолчанию: Disable (отключить).
Функция: включение/выключение RSTP или STP.

- Кольцевые протоколы на основе портов включают RSTP, Sy2-Ring-Port и Sy2-RP-Port, а кольцевые протоколы на основе VLAN включают MSTP, Sy2-Ring-VLAN и Sy2-RP-VLAN.
- Кольцевой протокол на основе портов и кольцевой протокол на основе VLAN являются взаимоисключающими, и для одного устройства можно выбрать только один тип кольцевого протокола.

2. Установка временных параметров сетевого моста, как показано на рисунке 147.

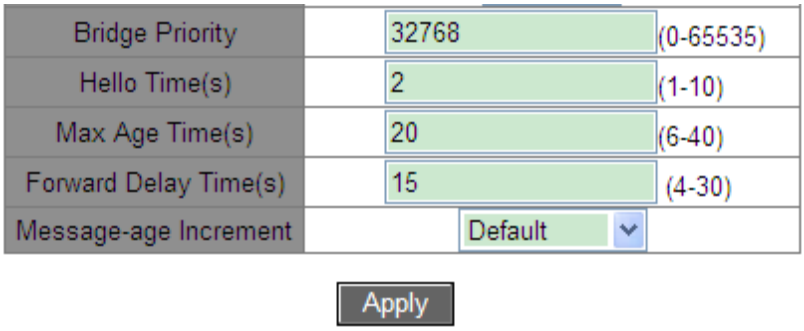



Рисунок 147 – Настройка временных параметров сетевого моста

**Bridge Priority (приоритет моста)**
Диапазон: 0~65535. Шаг 4096.
Значение по умолчанию: 32768.
Функция: настройка приоритета сетевого моста.
Описание: приоритет используется для выбора корневого моста. Чем меньше значение, тем выше приоритет.

**Hello Time (время приветствия)**
Диапазон: 1~10 с.
Значение по умолчанию: 2 с.
Функция: настройка интервала отправки BPDU.

**Max Age Time (максимальный возраст)**
Диапазон: 6~40 с.
Значение по умолчанию: 20 с.
Описание: если значение возраста сообщения в BPDU превышает указанное, то BPDU отбрасывается.

**Forward Delay Time (время задержки отправки)**
Диапазон: 4~30 с.
По умолчанию: 15 с.
Функция: настройка времени изменения статуса с отбрасывания на обучение или с обучения на пересылку.

**Message-age Increment (увеличение возраста сообщения)**
Варианты: Compulsion/Default (принудительно/по умолчанию).
Значение по умолчанию: Default.
Функция: настройка значения, которое будет добавляться к возрасту сообщения, когда BPDU проходит через сетевой мост.
Описание: в принудительном режиме значение равно 1.
В режиме по умолчанию значение равно max (max age time/16, 1).
Forward Delay Time, Max Age Time, Hello Time должны соответствовать следующим требованиям:
2 x (Forward Delay Time – 1.0 c) ≥ Max Age Time;
Max Age Time ≥ 2 x (Hello Time + 1.0 c).

3. Включение RSTP на портах, как показано на рисунке 148.

Port Configuration

| Port | Type | Protocol Status | Port Priority(0~255) | Auto Cost Count | Path Cost(1~200000000) |
|---|---|---|---|---|---|
| 1/1 | FE | ☑ | 128 | ☑ | 2000000 |
| 1/2 | FE | ☑ | 128 | ☐ | 2000000 |
| 1/3 | FE | ☑ | 128 | ☑ | 2000000 |
| 1/4 | FE | ☑ | 128 | ☐ | 2000000 |
| 1/5 | FE | ☐ | 128 | ☑ | 2000000 |
| 1/6 | FE | ☐ | 128 | ☑ | 2000000 |
| 1/7 | FE | ☐ | 128 | ☑ | 2000000 |
| 1/8 | FE | ☐ | 128 | ☑ | 2000000 |
| 1/9 | FE | ☐ | 128 | ☑ | 2000000 |
| 1/10 | FE | ☐ | 128 | ☑ | 2000000 |
| 1/11 | FE | ☐ | 128 | ☑ | 2000000 |
| 1/12 | FE | ☐ | 128 | ☑ | 2000000 |

Apply

Рисунок 148 – Настройка портов

**Protocol Status (состояние протокола)**
Варианты: Enable/Disable (включить/отключить).
По умолчанию: Disable (отключить).
Функция: включить или отключить STP/RSTP на портах.

---

- RSTP-порт и порты группы агрегации «port channel» являются взаимоисключающими. Порт RSTP нельзя добавить в группу агрегации; порт из группы агрегации не может быть настроен как порт RSTP.

- Порт RSTP и порт назначения зеркалирования являются взаимоисключающими. Порт RSTP нельзя настроить как порт назначения зеркалирования; порт назначения зеркалирования не может быть настроен как порт RSTP.
- Порт RSTP нельзя настроить как кольцевой порт Sy2-Ring и Sy2-RP, а порты Sy2-Ring и Sy2-RP нельзя настроить как RSTP.
- Не рекомендуется настраивать порты в группе изоляции одновременно как порты RSTP, а порты RSTP нельзя добавлять в группу изоляции.

---

**Port Priority (приоритет портов)**
Диапазон: 0~255. Шаг – 16.
Значение по умолчанию: 128.
Функция: настройка приоритета, который определяет роли портов.

**Path Cost (стоимость пути)**
Диапазон: 1~200000000.
Значение по умолчанию: 2000000 (порт 10M), 200000 (порт 100M), 20000 (порт 1000M).
Описание: стоимость пути порта используется для расчета наилучшего пути. Значение параметра зависит от пропускной способности. Чем больше значение, тем ниже стоимость. Вы можете изменить роль порта, изменив значение параметра стоимости пути. Чтобы настроить значение вручную, выберите «No» для автоматического счетчика.

**Auto Cost Count (автоматический подсчет стоимости)**
Диапазон: Yes/No (да/нет).
По умолчанию: Yes (да).
Описание: «Yes» указывает, что стоимость пути порта принимает значение по умолчанию. «No» означает, что вы можете настроить стоимость пути вручную.

4. Просмотр статуса RSTP, как показано на рисунке 149.

**Root Info**

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

**Bridge Info**

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

**Port Info**

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

Рисунок 149 – Информация о состоянии RSTP

### 6.6.6 Пример типовой настройки

Приоритеты коммутаторов A, B и C — 0, 4096 и 8192. Стоимость пути для каналов — 4, 5 и 10, как показано на рисунке 150.

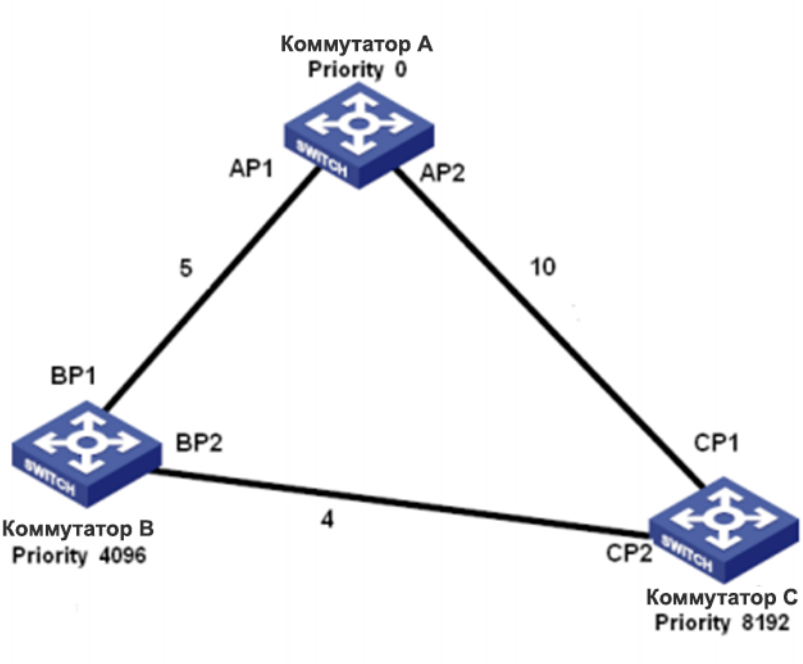



Рисунок 150 – Пример конфигурации RSTP

Настройки коммутатора A:
1. Установите приоритет на «0» и временные параметры на значения по умолчанию, как показано на рисунке 147.
2. Установите стоимость пути для порта 1 на «5», а для порта 2 на «10», как показано на рисунке 148.

Настройки коммутатора B:
1. Установите приоритет на «4096» и временные параметры на значения по умолчанию, как показано на рисунке 147.
2. Установите стоимость пути для порта 1 на «5», а для порта 2 на «4», как показано на рисунке 148.

Настройки коммутатора C:
1. Установите приоритет на «8192» и временные параметры на значения по умолчанию, как показано на рисунке 147.
2. Установите стоимость пути для порта 1 на «10», а для порта 2 на «4», как показано на рисунке 148.

- Приоритет коммутатора A равен 0, а его корневой идентификатор является наименьшим. Таким образом, коммутатор A является корневым мостом.
- Стоимость пути от AP1 к BP1 равна 5, а от AP2 к BP2 — 14. Таким образом, BP1 является корневым портом.
- Стоимость пути от AP1 к CP2 равна 9, а от AP2 к CP1 — 10. Следовательно, CP2 — это корневой порт, а BP2 — назначенный порт.

# 6.7 Sy2-RP

## 6.7.1 Обзор

Symanitron разработал Sy2-RP (Symanitron Redundancy Protocol) для передачи данных в кольцевых сетях. Протокол может предотвращать широковещательные штормы в кольцевых топологиях. Если канал или узел выходят из строя, вместо них задействуется резервная связь, обеспечивающая бесперебойную передачу данных.
Совместимый со стандартом IEC 62439-6, протокол Sy2-RP использует механизм определения мастера без привязки. Sy2-RP предоставляет следующие возможности:

- **Время восстановление сети, не зависящее от размеров сети.**

Sy2-RP обеспечивает время восстановления, не зависящее от размера сети, за счет оптимизации механизма определения передачи данных по кольцу. Sy2-RP позволяет сетям восстанавливаться менее, чем за 20 мс, благодаря функции оповещения реального времени, обеспечивающей надёжную передачу данных реального времени. Эта функция позволяет коммутаторам достигать максимальной надёжности в таких отраслях, как энергетика, железные дороги и множестве других.

- **Функция диверсифицированного определения сбоя соединения.**

Для увеличения сетевой стабильности Sy2-RP предоставляет функцию диверсифицированного определения сбоя соединения для типичных сетевых проблем, включая быстрое определение отсутствия соединения, определение однонаправленной оптической передачи данных, исследование качества связи и проверку состояния оборудования.

- **Применимость к различным сетевым топологиям.**

Кроме быстрого восстановления для простых кольцевых топологий, Sy2-RP также поддерживает топологии сложных колец, например, пересекающиеся кольца и кольца с общими участками. Также Sy2-RP поддерживает множественные кольца, основанные на VLAN и таким образом подходит для использования в различных сетях.

- **Функции диагностики и поддержки**

Sy2-RP имеет функции запроса статуса и механизм создания тревог, использующиеся для сетевой диагностики и поддержки, а также механизм предотвращения непреднамеренных воздействий на сеть и создания настроек, которые могут привести к широковещательным штормам.

## 6.7.2 Концепция

1. Режимы Sy2-RP
Sy2-RP имеет два режима: Sy2-RP-Port-Based и Sy2-RP-VLAN-Based.
**Sy2-RP-Port-Based**: определяет порты, через которые необходимо передавать или блокировать данные.
**Sy2-RP-VLAN-Based**: передаёт или блокирует данные, в зависимости от VLAN. Если порт находится в состоянии отбрасывания, отбрасываются только пакеты указанной VLAN.

Таким образом, на одних физических портах могут быть настроены различные VLAN. Порт может принадлежать к разным Sy2-RP кольцам, в зависимости от настроек.

2. Статус Sy2-RP порта

**Состояние пересылки данных:** если порт в режиме пересылки, он может принимать и отправлять данные.

**Состояние блокировки:** если порт в режиме блокировки, он может принимать и отправлять Sy2-RP пакеты, но не другие данные.

---

- Если на корневом устройстве не настроен первичный порт, первый порт, на котором активизируется связь при закрытии кольца, переходит в состоянии пересылки. Другой кольцевой порт находится в состоянии блокировки.
- Порт на корневом устройстве, находящийся в состоянии блокировки, может активно отправлять пакеты Sy2-RP.

---

3. Роли Sy2-RP.

Sy2-RP определяет роли коммутаторов путём передачи пакетов Announce, предотвращая создание петель в кольцах резервирования.

**INIT**: обозначает устройство, на котором Sy2-RP включен и оба его кольцевых порта выключены.

**Корневой**: обозначает устройство, на котором Sy2-RP включен и как минимум один его порт активен. В кольце Корневой коммутатор выбирается согласно векторам пакетов Announce. Это может измениться при изменении топологии. Корневой коммутатор периодически отправляет свои собственные Announce-пакеты. Статус кольцевых портов: один кольцевой порт в состоянии пересылки, а второй – в состоянии блокировки. После получения пакета Announce от другого устройства, Корневой коммутатор сравнивает вектор полученного пакета со своим собственным пакетом Announce. Если полученный вектор больше, Корневой коммутатор меняет свою роль на «Обычный» или «B-Root», в зависимости от состояния соединения и CRC-деградации порта.

**B-Root**: обозначает устройство, на котором Sy2-RP включен, один порт активен, а второй – неактивен или в режиме деградации CRC. B-Root сравнивает и передаёт пакеты Announce. Если вектор полученного пакета Announce меньше, чем собственный пакет Announce, B-Root меняет свою роль на «Корневой», в противном случае он передаёт полученный пакет и не меняет собственной роли. Статусы кольцевых портов: один кольцевой порт в состоянии пересылки.

**Обычный**: обозначает устройство, на котором Sy2-RP включен и оба порта активны без CRC-деградации. Обычные коммутаторы только передают пакеты Announce, без проверки содержимого. Статус кольцевых портов: оба порта в состоянии пересылки.

---

Деградация CRC: указывает, что число пакетов CRC превышает пороговое значение за 15 минут.

---

### 6.7.3 Реализация

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

Таблица 8 – Вектор пакета Announce

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

**Link status (статус соединения)**: значение устанавливается равным 1, если один кольцевой порт находится в состоянии Link down, и устанавливается в 0, если оба кольцевых порта находятся в состоянии Link up;

**CRC degradation status (статус CRC-деградации)**: Если на одном из портов присутствует CRC деградация, значение равно 1. Если CRC деградации ни на одном порту нет, значение равно 0;

**CRC degradation rate (скорость деградации CRC)**: отношение количества пакетов CRC к порогу за 15 минут;

**Role priority (приоритет роли):** значение можно установить через веб-интерфейс;

**IP address of the device (IP-адрес устройства);**

**MAC address of the device (MAC-адрес устройства).**

Параметры вектора из таблицы 8 сравниваются следующим образом:

1. Сначала проверяется статус соединения. Устройство с бóльшим значением этого поля считается устройством с бóльшим вектором.

2. Если два сравниваемых устройства имеют одинаковое значение поля статуса соединения, сравниваются значения поля деградации CRC. Устройство с бóльшим значением CRC деградации считается устройством с бóльшим вектором. Если значение статуса деградации CRC всех сравниваемых устройства равно 1, считается, что устройство с бóльшим значением скорости деградации CRC имеет больший вектор.

3. Если два сравниваемых устройства имеют одинаковый статус соединения и значение CRC деградации, последовательно сравниваются приоритет роли, IP-адрес и MAC-адрес. Устройство с бóльшим значением считается устройством с бóльшим вектором.

4. Устройство с бóльшим вектором выбирается Корневым.

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

- **Реализация режима Sy2-RP-Port-Based.**

Роль коммутатора определяется следующим образом:

1. Во время запуска, все коммутаторы находятся в режиме INIT. Когда статус одного порта меняется на активный, коммутатор становится Корневым и начинает отсылать пакеты Announce другим коммутаторам в кольце.

2. Коммутатор с наибольшим вектором Announce выбирается Корневым. Его кольцевой порт, перешедший в активное состояние первым переходит в режим пересылки данных, второй порт переходит в режим блокировки. Один из остальных коммутаторов, один из портов которого в неактивном состоянии или в режиме CRC-деградации, переходит в режим B-Root. Коммутаторы с двумя активными кольцевыми портами, не имеющие CRC деградации получают статус Обычный.

Процедура устранения неисправности следующая (см. рис.168):

1. В исходной топологии A является Корневым (Root); порт 1 находится в состоянии пересылки, а порт 2 в состоянии блокировки. B, C и D являются Обычными, и их кольцевые порты находятся в состоянии пересылки.

2. Когда канал CD неисправен, Sy2-RP изменяет статусы портов 6 и 7 на блокировку. В результате C и D становятся Корневыми. Поскольку A, C и D в данный момент являются Корневыми, все они отправляют пакеты Announce. Векторы C и D больше, чем векторы A, потому что порты 7 и 6 находятся в состоянии Link down. В этом случае, если вектор D больше, чем вектор C, D выбирается в качестве Корневого, 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 Обычным (Normal) и изменяет статус порта 2 на пересылку данных.

3. Когда связь CD восстанавливается, D все еще является Корневым, потому что его вектор больше, чем вектор C.

- Если на D не настроен основной порт, порт 7 по-прежнему находится в состоянии блокировки, а порт 8 — в состоянии пересылки.
- Если порт 7 на D настроен как основной порт, порт 7 переходит в состояние пересылки, а порт 8 — в состояние блокировки.

Sy2-RP изменяет статус порта 6 на состояние пересылки. В результате C становится Обычным. Следовательно, роли коммутаторов не меняются при восстановлении канала связи.


Рисунок 151 – Восстановление сети с Sy2-RP

---

В кольцевой сети Sy2-RP роли коммутаторов меняются при сбое линии связи, но не меняются при её восстановлении. Этот механизм повышает безопасность сети и надежность передачи данных.

---

➢ **Реализация режима Sy2-RP-VLAN-Based.**

Режим Sy2-RP-VLAN-Based определяет соответствия между VLAN и экземплярами STG. Одна или несколько сетей VLAN могут быть сопоставлены с одним экземпляром STG.

STG-экземпляр: каждый STG-экземпляр связан с одним кольцом Sy2-RP-Port-Based. Благодаря Sy2-RP, STG-экземпляр определяет роли и статусы портов. После получения пакета с VLAN атрибутом, коммутатор определяет по нему соответствующий STG-экземпляр. Далее, коммутатор обрабатывает пакет в соответствии со своей ролью и статусом портов в экземпляре.

Благодаря конфигурации Sy2-RP-VLAN-Based колец, данные разных VLAN могут передаваться разными путями. Как показано на рисунке 152, сопоставление экземпляров STG и VLAN одинаково для всех устройств.

**Кольцевой канал на основе STG1**: AB-BC-CD-DE-EA. По каналу пересылаются пакеты VLAN10 и VLAN20. A — корневой коммутатор (Root).

**Кольцевой канал на основе STG2**: FB-BC-CD-DE-EF. По каналу пересылаются пакеты VLAN30. F — корневой коммутатор (Root).

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

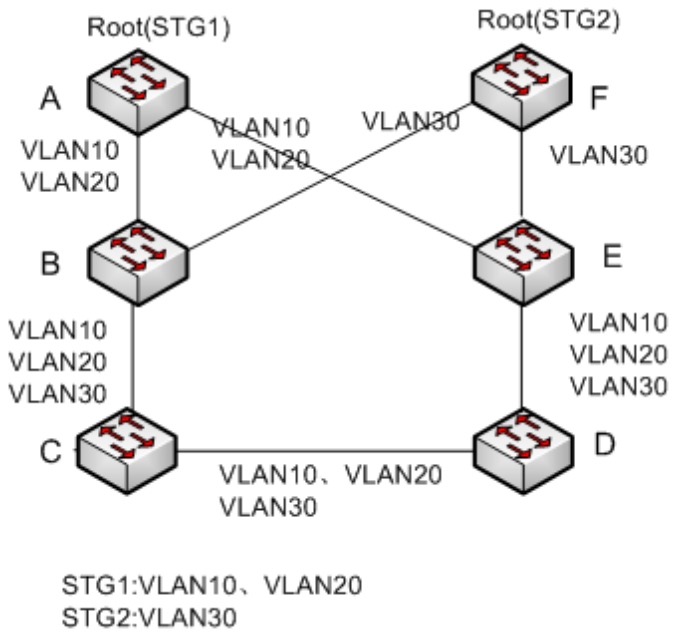



Рисунок 152 – Sy2-RP-VLAN-Based

---

Статусы и роли режима Sy2-RP-VLAN-Based не отличаются от соответствующих в режиме Sy2-RP-Port-Based.

---

➢ **Sy2-RP Backup**

Sy2-RP также может обеспечивать резервируемое соединение между двумя кольцами Sy2-RP, предотвращая появление петель и обеспечивая надёжную связь между кольцами.

Резервный порт: обозначает порт связи между Sy2-RP кольцами. Можно назначать множество резервных портов, однако все они должны быть в одном кольце. Первый активный порт становится главным (мастером-резервным-портом) и переходит в режим пересылки данных. Все остальные резервные порты становятся ведомыми и переходят в режим блокировки.

Как показано на следующем рисунке, на каждом коммутаторе можно настроить один резервный порт. Главный резервный порт находится в состоянии пересылки, а ведомые — в состоянии блокировки. Если мастер-резервный-порт выходит из строя, один из ведомых резервных портов займёт его место.

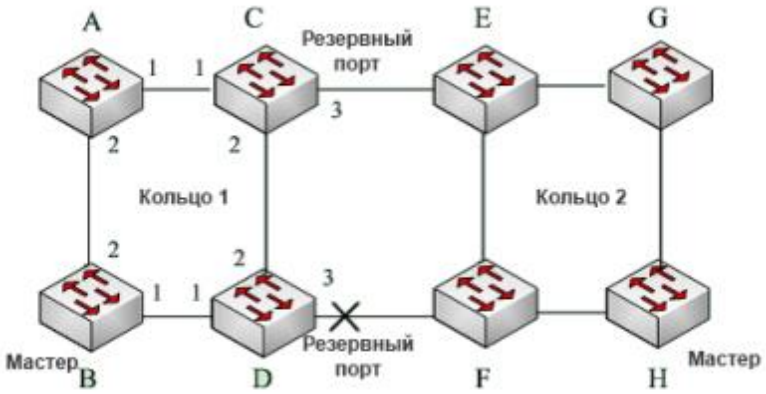



Рисунок 153 – Резервирование Sy2-RP.

Изменение статуса соединения влияет на статус резервных портов.

## 6.8 DHP

### 6.8.1 Обзор

Как показано на рисунке 154, коммутаторы A, B, C и D подключены к кольцу. Протокол Dual Homing (DHP) выполняет следующие функции, если он включен на коммутаторах A, B, C и D:

- Коммутаторы A, B, C и D могут связываться друг с другом, не влияя на корректную работу устройств в кольце.
- Если связь между коммутаторами A и B неисправна, коммутатор A все еще может связываться с коммутаторами B, C и D через устройства 1 и 2.

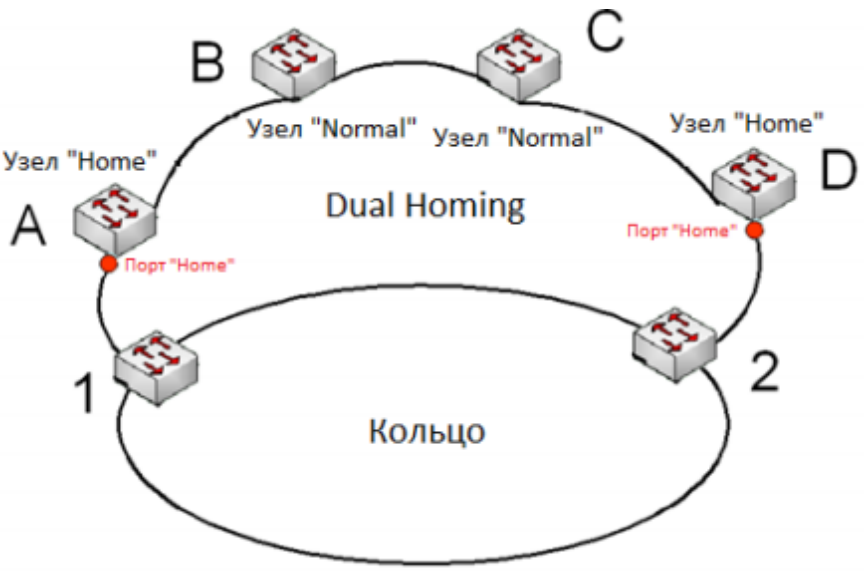



Рисунок 154 – Реализация протокола Dual Homing

## 6.8.2 Концепция

Реализация Dual Homing основана на Sy2-RP. Механизм выбора и назначения ролей в Dual Homing такой же, как и в Sy2-RP. Dual Homing обеспечивает резервирование канала связи через настройки узлов «Home», «Normal» и порта «Home». Узел «Home» означает устройства, находящиеся на обоих концах канала Dual Homing и принимающих пакеты Sy2-RP. Порт «Home» означает порт, соединяющий узел «Home» с внешней сетью. Порт «Home» обеспечивает следующие функции:

- Отправку ответных пакетов корневому коммутатору при получении от него пакетов Announce. Если корневой коммутатор получает ответные пакеты, он определяет статус кольца как замкнутый. Если корневой коммутатор не получает ответных пакетов, он определяет статус кольца как открытый.
- Блокировку пакетов Sy2-RP внешних сетей и изоляцию канала Dual Homing от внешних сетей.
- Отправку пакетов очистки записей подключенным устройствам во внешних сетях при изменении топологии канала Dual Homing.

Узел «Normal»: означает все устройства в канале Dual Homing, за исключением крайних устройств, т.е. узлов «Home». Узлы «Normal» передают ответные пакеты узлов «Home».

## 6.8.3 Реализация

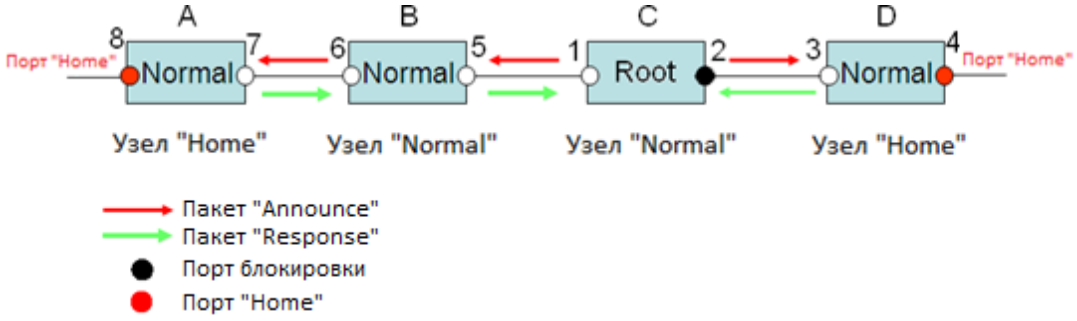



Рисунок 155 – Конфигурация Dual Homing

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

- Конфигурация Sy2-RP: C – корневой коммутатор; порт 2 находится в состоянии блокировки; коммутаторы A, B и D – обычные («Normal»); все остальные порты кольца находятся в состоянии пересылки.
- Конфигурация Dual Homing: коммутаторы A и D – узлы «Home»; порты 8 и 4 являются портами «Home»; коммутаторы B и C – обычные («Normal»).

Реализация.

Корневой коммутатор C отправляет пакеты Announce через два своих кольцевых порта. Порты «Home» 8 и 4 получают пакеты Announce и отправляют ответные пакеты коммутатору C. Коммутатор C соответственно идентифицирует состояние кольца как закрытое. Порт 2 находится в состоянии блокировки.

Если линия связи между коммутаторами A и B заблокирована, в топологии остаются два канала: A и B-C-D.

- Коммутатор A назначается корневым. Порт 7 находится в состоянии блокировки.

- В канале B-C-D коммутатор B выбирается в качестве корневого. Порт 6 находится в состоянии блокировки. Коммутатор C становится обычным («Normal»). Порт 2 находится в состоянии пересылки. Коммутатор A может связываться с коммутаторами B, C и D через устройства 1 и 2, как показано на рисунке 173.

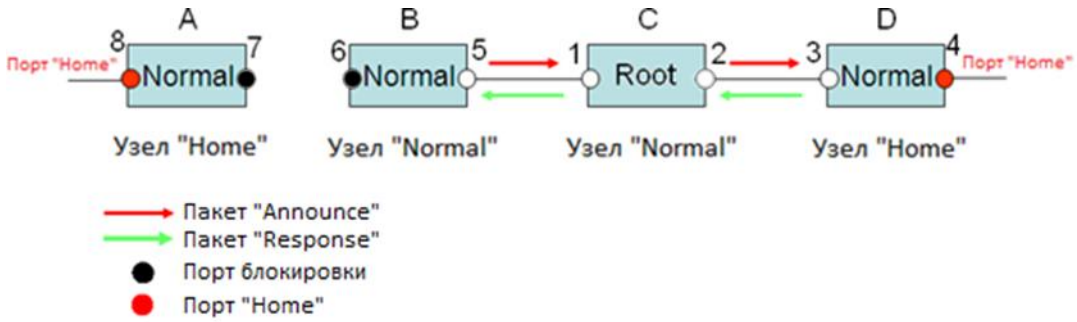



Рисунок 156 – Восстановление связи Dual Homing

## 6.8.4. Описание

Конфигурации Sy2-RP должны соответствовать следующим требованиям:

- Все коммутаторы в одном кольце должны иметь одинаковый номер домена.
- Одно кольцо включает только один корневой коммутатор, но при этом может включать несколько коммутаторов B-Root или «Normal».
- На каждом коммутаторе для кольца можно настроить только два порта.
- Для двух объединенных колец резервные порты можно настроить только в одном кольце.
- В одном кольце можно настроить несколько резервных портов.
- На коммутаторе только один резервный порт может быть настроен для одного кольца.

## 6.8.5 Настройка с помощью WEB-интерфейса

1. Настройка режима Sy2-RP.

Нажмите [Device Advanced Configuration] → [Sy2-RP configuration] → [Sy2-RP Mode], чтобы открыть страницу конфигурации режима Sy2-RP, как показано на следующем рисунке.


Рисунок 157 – Режим Sy2-RP

**Sy2-RP Mode (режим Sy2-RP)**

Варианты: Port Based/VLAN Based (на основе порта/на основе VLAN).

По умолчанию: Port Based (на основе порта).

Функция: Настройка режима Sy2-RP.

- Кольцевые протоколы на основе портов включают RSTP, Sy2-Ring-Port и Sy2-RP-Port, а кольцевые протоколы на основе VLAN включают MSTP, Sy2-Ring-VLAN и Sy2-RP-VLAN.
- Кольцевые протоколы на основе VLAN являются взаимоисключающими, и для одного устройства можно настроить только тип кольцевого протокола на основе VLAN.
- Кольцевой протокол на основе портов и кольцевой протокол на основе VLAN являются взаимоисключающими, и для одного устройства можно выбрать только один режим кольцевого протокола.

2. Создание записи Sy2-RP-Port-Based.
Нажмите [Device Advanced Configuration] → [Sy2-RP configuration] → [Port-Based Sy2-RP Configuration], чтобы открыть страницу создания записи Sy2-RP, как показано на следующем рисунке.


Рисунок 158 – Создание записи Sy2-RP-Port-Based

Нажмите <Add>, чтобы создать запись Sy2-RP.
- Установите параметры для записи Sy2-RP-Port-Based, как показано на рисунке 159.

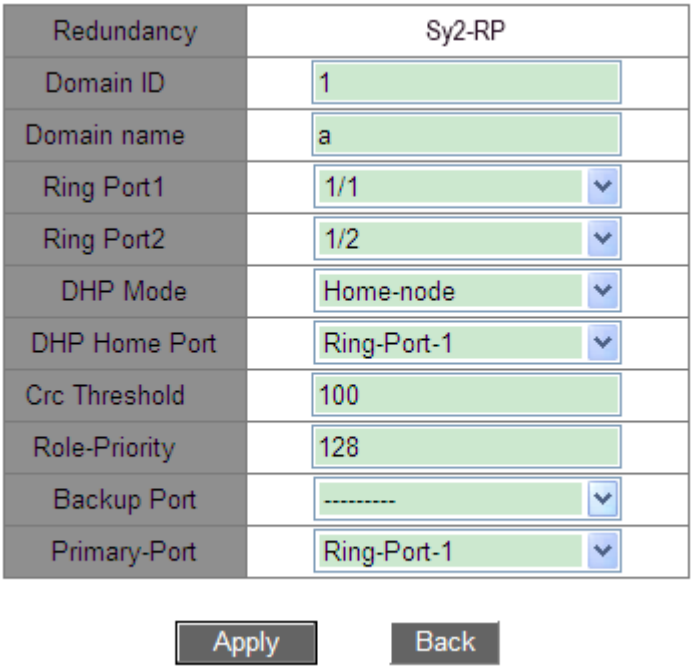



Рисунок 159 – Настройка записи Sy2-RP-Port-Based

**Redundancy (резервирование)**
Обязательная настройка: Sy2-RP.

**Domain ID (идентификатор домена)**
Диапазон: 1~32.
Описание: идентификатор домена используется для разграничения колец. Один коммутатор поддерживает до 16 колец.

**Domain name (доменное имя)**
Диапазон: 1~31 символов.
Действие: указать доменное имя.

**Ring Port 1/ Ring Port 2 (кольцевой порт 1/кольцевой порт 2)**
Варианты: все порты коммутатора.
Функция: выбор двух кольцевых портов.

**DHP Mode (режим DHP)**
Варианты: Disable/Normal-node/Home-node.
По умолчанию: Disable (выключено).
Функция: выключение DHP или настройка его режима.

**DHP Home Port (домашний порт DHP)**
Варианты: Ring-Port-1/Ring-Port-2/Ring-Port-1-2.
Функция: выбор Home-port для DHP Home-node.
Описание: если в сегменте DHP только одно устройство, оба кольцевых порта должны быть установлены как Home-port.

**Crc Threshold (порог CRC)**
Диапазон: 25~65535
Значение по умолчанию: 100.
Функция: выбор порогового значения для CRC.
Описание: этот параметр используется для определения Корневого коммутатора. Система считает количество полученных CRC. Если количество CRC на каком-либо кольцевом порту превысит пороговое значение, система посчитает, что порт находится в режиме CRC деградации. В результате, значение CRC деградации будет установлено в 1 в векторе пакета Announce на данном порту.

**Role-Priority (ролевой приоритет)**
Диапазон: 0~255
Значение по умолчанию: 128
Функция: настройка приоритета коммутатора.

**Backup Port (резервный порт)**
Варианты: все порты коммутатора.
Функция: выбор резервного порта.

Не указывайте кольцевой порт в качестве резервного порта.

**Primary-Port (основной порт)**
Варианты: --/Ring-Port-1/Ring-Port-2
По умолчанию: --
Функция: настройка основного порта. Когда кольцо замкнуто, основной порт Корневого устройства находится в состоянии пересылки.
После завершения настройки параметров созданная запись будет отображаться в списке Sy2-RP, как показано на рисунке 160.

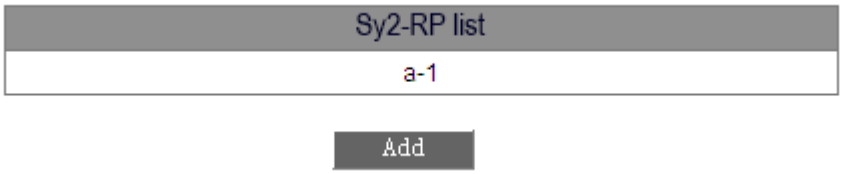



Рисунок 160 – Список Sy2-RP-Port-Based

- Кольцевой порт Sy2-RP или резервный порт и порты группы агрегации «port channel» являются взаимоисключающими. Порт Sy2-RP или резервный порт нельзя добавить в группу агрегации; порт из группы агрегации не может быть настроен как порт Sy2-RP или резервный порт.
- Кольцевой порт Sy2-RP или резервный порт и порт назначения зеркалирования являются взаимоисключающими. Порт Sy2-RP или резервный порт нельзя настроить как порт назначения зеркалирования; порт назначения зеркалирования не может быть настроен как порт Sy2-RP или резервный порт.
- Порт RSTP нельзя настроить как кольцевой или резервный порт, а кольцевые или резервные порты нельзя настроить как RSTP.
- Не рекомендуется настраивать порты в группе изоляции одновременно как порты Sy2-RP или резервные порты, а порты Sy2-RP или резервные порты нельзя добавлять в группу изоляции.

- Просмотр настроек параметров записи Sy2-RP-Port-Based.

Выберите запись Sy2-RP (см. рисунок 160). Вы можете просматривать и изменять настройки параметров записи, как показано на следующем рисунке.

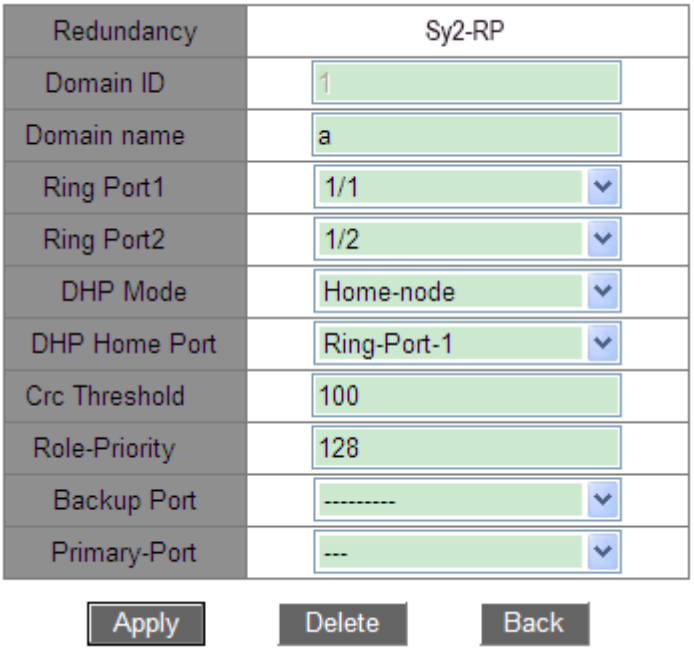



Рисунок 161 – Запрос и изменение записи Sy2-RP-Port-Based

После завершения изменения нажмите <Apply>, чтобы изменение вступило в силу. Вы можете удалить запись Sy2-RP, нажав <Delete>.

➢ Просмотрите роли и состояние портов кольца Sy2-RP, как показано на рисунке 162.

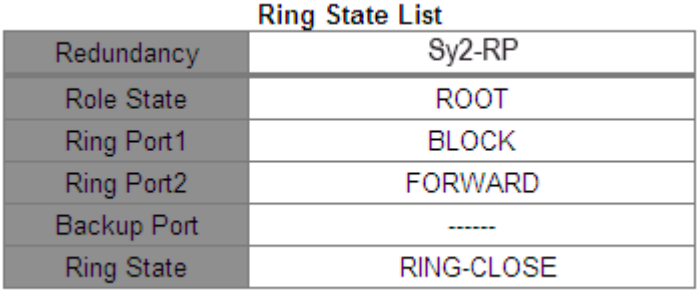



Рисунок 162 – Запрос статуса Sy2-RP-Port-Based

3. Настройка записи на основе Sy2-RP-VLAN.

Нажмите [Device Advanced Configuration] → [Sy2-RP configuration] → [Sy2-RP Mode], чтобы открыть страницу конфигурации режима Sy2-RP. Выберите «VLAN Based».

➢ Конфигурация экземпляра Sy2-RP.

Нажмите [Device Advanced Configuration] → [Sy2-RP configuration] → [VLAN-Based Sy2-RP Configuration] → [STG Instance Configuration], чтобы открыть страницу настройки экземпляра Sy2-RP STG, как показано на рисунке 163.

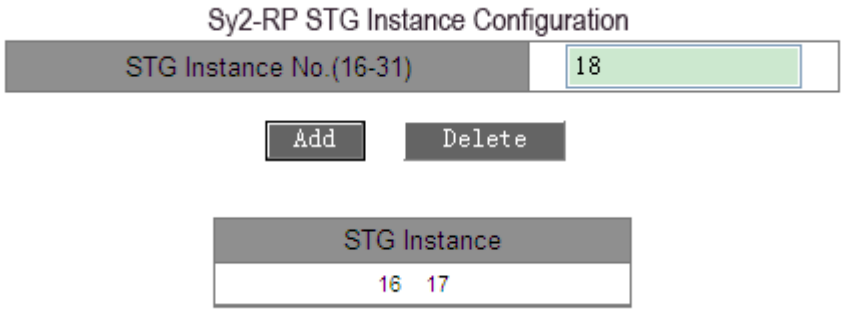



Рисунок 163 – Настройка экземпляра Sy2-RP STG

**STG Instance No. (16-31) – номер экземпляра STG**
Диапазон: 16~31
Функция: настройка ID экземпляра Sy2-RP.

➢ Конфигурация VLAN в экземпляре Sy2-RP.
Нажмите [Device Advanced Configuration] → [Sy2-RP configuration] → [VLAN-Based Sy2-RP Configuration] → [STG Instance Protocol VLAN Configuration], чтобы открыть страницу конфигурации VLAN экземпляра Sy2-RP, как показано на рисунке 164.

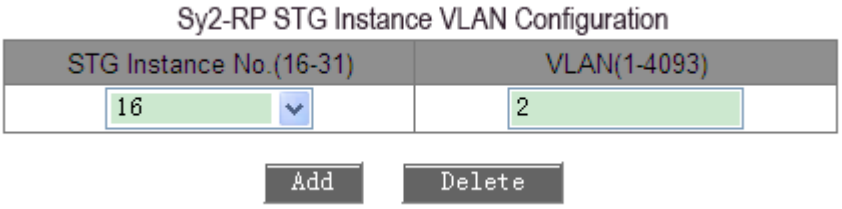



Рисунок 164 – Настройка VLAN для экземпляра Sy2-RP

**Sy2-RP STG Instance VLAN Configuration (конфигурация экземпляра Sy2-RP STG VLAN)**
Опции: {STG instance ID, VLAN ID}
Диапазон: {16~31, 1~4093}
Функция: настройка идентификаторов для VLAN и экземпляра Sy2-RP.
Описание: один экземпляр Sy2-RP может соответствовать нескольким идентификаторам VLAN, но один идентификатор VLAN может соответствовать только одному экземпляру Sy2-RP.

➢ Просмотр информации об экземплярах Sy2-RP.
Нажмите [Device Advanced Configuration] → [Sy2-RP configuration] → [VLAN-Based Sy2-RP Configuration] → [STG Instance Information], чтобы открыть страницу информации об экземпляре Sy2-RP, как показано на рисунке 165.

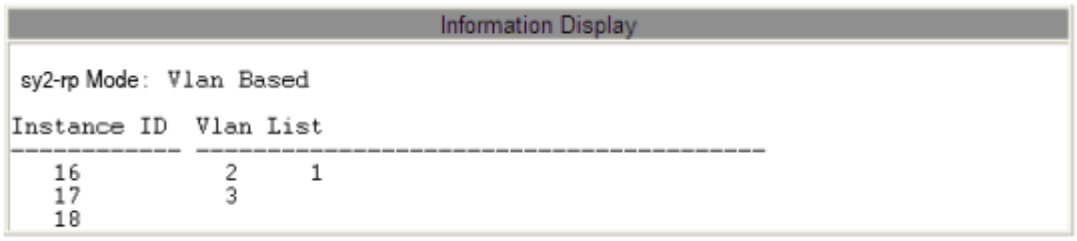



Рисунок 165 – Информация экземпляра Sy2-RP

➢ Настройка Sy2-RP-VLAN-Based.

Нажмите [Device Advanced Configuration] → [Sy2-RP configuration] → [VLAN-Based Sy2-RP Configuration], чтобы открыть страницу создания Sy2-RP-VLAN-Based, как показано на следующем рисунке.


Рисунок 166 – Создание записи Sy2-RP-VLAN-Based

Нажмите <Add>, чтобы создать запись Sy2-RP. Задайте параметры записи, как показано на рисунке 167.

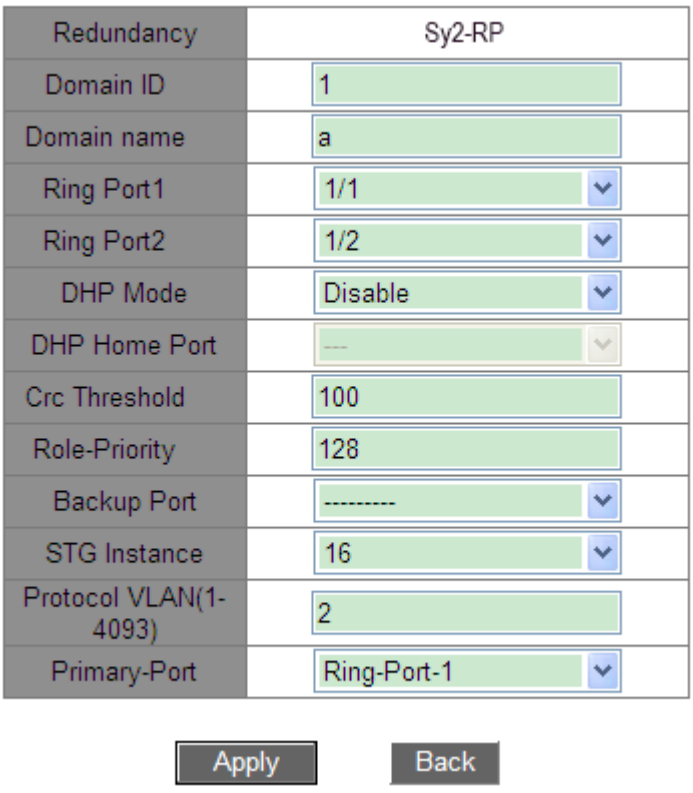



Рисунок 167 – Настройка записи Sy2-RP-VLAN-Based

**Redundancy (резервирование)**
Обязательная настройка: Sy2-RP.

**Domain ID (идентификатор домена)**
Диапазон: 1~32.
Описание: каждое кольцо имеет свой уникальный идентификатор домена. Коммутатор поддерживает до восьми Sy2-RP-колец.

**Domain name (доменное имя)**
Диапазон: 1~31 символов.
Действие: указать доменное имя.

**Ring Port 1/ Ring Port 2 (кольцевой порт 1/кольцевой порт 2)**
Варианты: все порты коммутатора.
Функция: выбор двух кольцевых портов.

**DHP Mode (режим DHP)**
Варианты: Disable/Normal-node/Home-node
По умолчанию: Disable (выключено).
Функция: выключение DHP или настройка его режима.

**DHP Home Port («домашний» порт DHP)**
Варианты: Ring-Port-1/Ring-Port-2/Ring-Port-1-2.
Функция: выбор Home-port для DHP Home-node.
Описание: если в сегменте DHP только одно устройство, оба кольцевых порта должны быть установлены как Home-port.

**Crc Threshold (порог CRC)**
Диапазон: 25~65535.
Значение по умолчанию: 100.
Функция: выбор порогового значения для CRC.
Описание: этот параметр используется для определения Корневого коммутатора. Система считает количество полученных CRC. Если количество CRC на каком-либо кольцевом порту превысит пороговое значение, система посчитает, что порт находится в режиме CRC деградации. В результате, значение CRC деградации будет установлено как 1 в векторе пакета Announce на данном порту.

**Role-Priority (ролевой приоритет)**
Диапазон: 0~255
Значение по умолчанию: 128
Функция: настройка приоритета коммутатора.

---

- Кольцевой порт Sy2-RP или резервный порт и порты группы агрегации «port channel» являются взаимоисключающими. Порт Sy2-RP или резервный порт

нельзя добавить в группу агрегации; порт из группы агрегации не может быть настроен как порт Sy2-RP или резервный порт.

- Кольцевой порт Sy2-RP или резервный порт и порт назначения зеркалирования являются взаимоисключающими. Порт Sy2-RP или резервный порт нельзя настроить как порт назначения зеркалирования; порт назначения зеркалирования не может быть настроен как порт Sy2-RP или резервный порт.
- Порт RSTP нельзя настроить как кольцевой или резервный порт, а кольцевые или резервные порты нельзя настроить как RSTP.
- Не рекомендуется настраивать порты в группе изоляции одновременно как порты Sy2-RP или резервные порты, а порты Sy2-RP или резервные порты нельзя добавлять в группу изоляции.

---

**Backup Port (резервный порт)**
Варианты: все порты коммутатора.
Функция: выбор резервного порта.

---

Не указывайте кольцевой порт в качестве резервного порта.

---

**STG Instance (экземпляр STG)**
Варианты: созданные экземпляры Sy2-RP.
Функция: настроить экземпляр для кольца.
Описание: блокирующий порт в кольце будет блокировать пакеты данных всех VLAN, соответствующих экземпляру.

**Protocol VLAN (1~4093)**
Диапазон: 1~4093.
Описание: идентификатор VLAN должен быть одним из тех, которые соответствуют экземпляру STG.
Функция: пакеты Sy2-RP с идентификатором VLAN служат основой для диагностики и обслуживания кольца Sy2-RP-VLAN-Based.

**Primary-Port (основной порт)**
Варианты: --/Ring-Port-1/Ring-Port-2
По умолчанию: --
Функция: настройка основного порта. Когда кольцо замкнуто, основной порт Корневого устройства находится в состоянии пересылки.
После завершения настройки параметров созданная запись будет отображаться в списке Sy2-RP, как показано на рисунке 168.

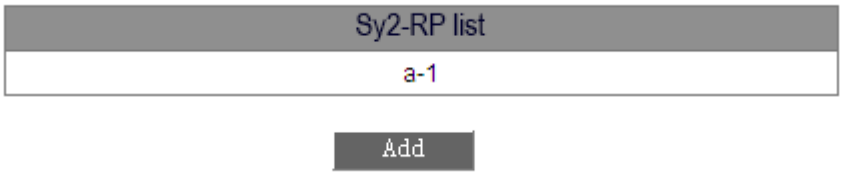



Рисунок 168 – Список Sy2-RP-VLAN-Based

Выберите запись Sy2-RP. Вы можете просматривать и изменять настройки параметров записи, как показано на рисунке 169.

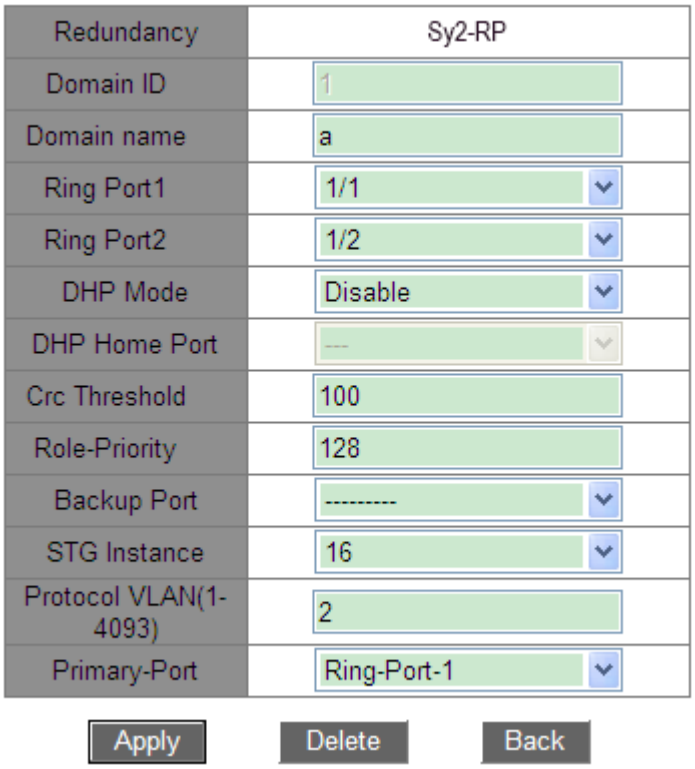



Рисунок 169 – Запрос и изменение записи Sy2-RP-VLAN-Based

После завершения изменения нажмите <Apply>, чтобы изменение вступило в силу. Вы можете удалить запись Sy2-RP, нажав <Delete>.

Просмотрите роли и состояние портов кольца Sy2-RP, как показано на рисунке 170.

Ring State List

| | |
|---|---|
| Redundancy | Sy2-RP |
| Role State | ROOT |
| Ring Port1 | BLOCK |
| Ring Port2 | FORWARD |
| Backup Port | ------ |
| Ring State | RING-CLOSE |

Рисунок 170 – Запрос статуса Sy2-RP-VLAN-Based

### 6.8.6 Пример типовой настройки

Как показано на рисунке 153, A, B, C и D образуют кольцо 1; E, F, G и H образуют кольцо 2; CE и DF являются резервными каналами кольца 1 и кольца 2.

Конфигурация на коммутаторе A и коммутаторе B:
1. Установите для идентификатора домена значение 1, а для имени домена — значение Ring. Выберите кольцевой порт 1 и кольцевой порт 2. Оставьте значения по умолчанию для ролевого приоритета и резервного порта, как показано на рисунке 159.

Конфигурация на коммутаторе C и коммутаторе D:
2. Установите для идентификатора домена значение 1, для имени домена — значение Ring, а для резервного порта — значение 3. Выберите кольцевой порт 1 и кольцевой порт 2. Оставьте значение по умолчанию для ролевого приоритета, как показано на рисунке 159.
Конфигурация на коммутаторах E, F, G и H:
3. Установите для идентификатора домена значение 2, для имени домена — значение Ring. Выберите кольцевой порт 1 и кольцевой порт 2. Оставьте значения по умолчанию для ролевого приоритета и резервного порта, как показано на рисунке 159.

## 6.9 Настройка MSTP

### 6.9.1 Введение

Хотя протокол RSTP обеспечивает достаточно быструю сходимость, он имеет такой же недостаток, как и STP: все мосты в локальной сети используют одно связующее дерево, и пакеты всех VLAN пересылаются по связующему дереву. Как показано на рисунке 171, определенные конфигурации могут блокировать связь между коммутатором A и коммутатором C. Поскольку коммутатор B и коммутатор D не входят в VLAN 1, они не могут пересылать пакеты VLAN 1. В результате порт VLAN 1 коммутатора A не может связываться с соответствующим портом коммутатора C.

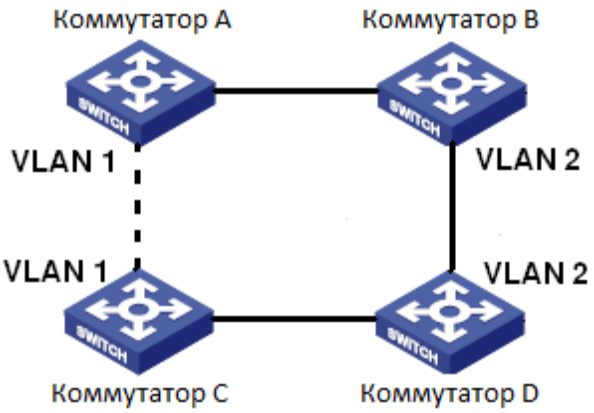



Рисунок 171 – Недостаток RSTP

Чтобы решить эту проблему, появился протокол MSTP. Он предоставляет как быструю конвергенцию, так и отдельные пути пересылки трафика разных VLAN для обеспечения лучшего механизма распределения нагрузки для каналов резервирования. MSTP группирует одну или несколько VLAN в один инстанс (экземпляр). Коммутаторы с одинаковой конфигурацией образуют так называемый «Регион». Каждый Регион содержит несколько взаимно независимых связующих деревьев. Регион служит коммутационным узлом. Он участвует в вычислениях с другими Регионами на основе алгоритма связующего дерева, вычисляя общее связующее дерево. На основе этого алгоритма сеть на рисунке 171 образует топологию, показанную на рисунке 172. Коммутаторы A и C находятся в Регионе 1. Ни один канал связи не заблокирован, потому что в регионе отсутствуют петли. Ситуация аналогична и для Региона 2. Регион 1 и Регион 2 аналогичны коммутационным узлам. Эти два «коммутатора» образуют петлю. Следовательно, линия связи должна быть заблокирована.

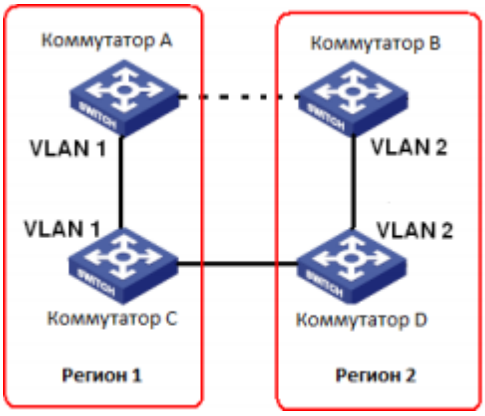



Рисунок 172 – Топология MSTP

## 6.9.2 Основные понятия

Концепция работы MSTP отображена на рисунках 173 – 176.

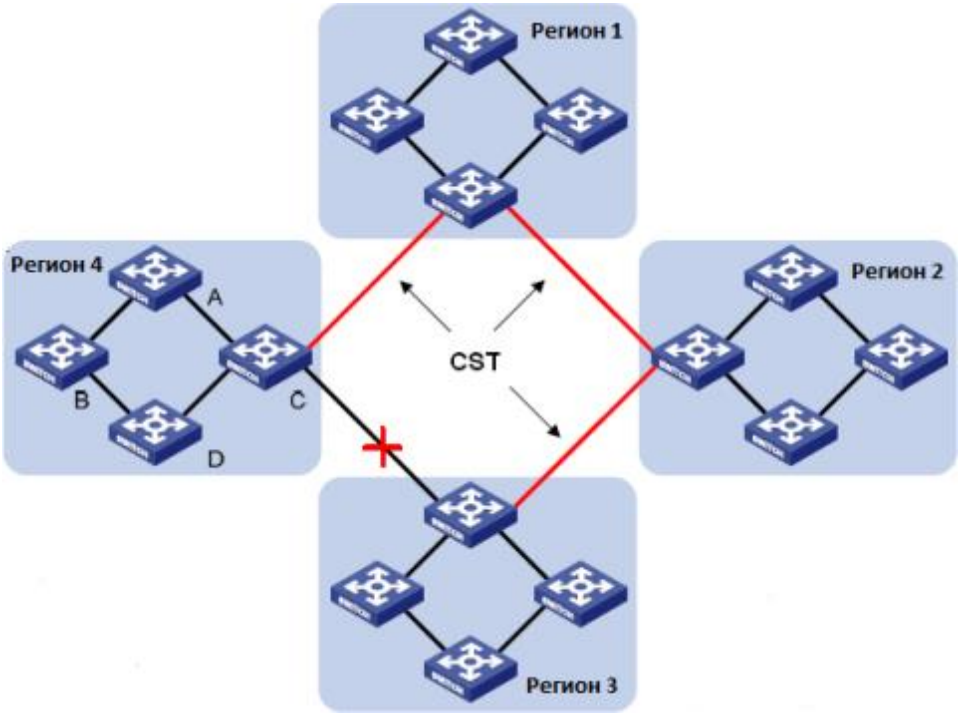



Рисунок 173 – Концепция MSTP


Рисунок 174 – Сопоставление VLAN 1 к Инстансу 1


Рисунок 175 – Сопоставление VLAN 2 к Инстансу 2


Рисунок 176 – Сопоставление других VLAN к Инстансу 0

**Инстанс (экземпляр)**: набор из нескольких VLAN. Одна VLAN (см. рисунки 174 и 175) или несколько VLAN с одинаковой топологией (см. рисунок 176) могут быть сопоставлены с одним инстансом; то есть одна VLAN может сформировать связующее дерево, а несколько VLAN могут совместно использовать одно связующее дерево. Разные инстансы сопоставляются с разными связующими деревьями. Инстанс 0 – это связующее дерево для устройств всех регионов, а другие инстансы – это связующие деревья для устройств определенного региона.

**Регион MST** (Multiple Spanning Tree Region): коммутаторы с одинаковым именем региона MSTP, уровнем версии и сопоставлением VLAN-инстанс находятся в одном регионе MST. Как показано на рисунке 173, Регион 1, Регион 2, Регион 3 и Регион 4 – это четыре разных региона MST.

**Таблица сопоставления VLAN**: состоит из сопоставления между VLAN и связующими деревьями. На рисунке 173 таблица сопоставления VLAN региона 2 – это сопоставление

между VLAN 1 и инстансом 1, как показано на рисунке 174; VLAN 2 сопоставлена с инстансом 2, как показано на рисунке 175. Другие VLAN сопоставлены с инстансом 0, как показано на рисунке 176.

**Связующее дерево (CIST)** (Common and Internal Spanning Tree / Общее и внутреннее связующее дерево): означает инстанс 0, то есть связующее дерево, охватывающее все устройства в сети. Как показано на рисунке 173, CIST состоит из IST и CST.

**Внутреннее связующее дерево (IST)**: означает сегмент CIST в области MST, то есть инстанс 0 для каждого региона, как показано на рисунке 176.

**Общее связующее дерево (CST)**: означает связующее дерево, соединяющее все регионы MST в сети. Если каждый регион MST является узлом, CST – это связующее дерево, вычисленное этими узлами на основе STP/RSTP. Красные линии обозначают связующее дерево (см. рисунок 173).

**MSTI** (Multiple Spanning Tree Instance / Несколько экземпляров связующего дерева): один регион MST может образовывать несколько связующих деревьев, и они не зависят друг от друга. Каждое связующее дерево является MSTI (см. рисунки 174 и 175). IST также является специальным MSTI.

**Common root**: означает корневой мост CIST. Коммутатор с наименьшим идентификатором корневого моста в сети является общим корневым коммутатором. В регионе MST связующие деревья имеют разную топологию и их корневые мосты также могут быть разными. Как показано на рисунках 174, 175 и 176, у этих трех инстансов разные региональные корневые мосты. Корневой мост MSTI рассчитывается на основе STP/RSTP в текущем регионе MST. Корневой мост IST – это устройство, которое подключено к другому региону MST и выбирается на основе полученной информации о приоритете.

**Граничный порт** (Boundary port): означает порт, который соединяет регион MST с другим регионом MST, регионом работы STP или регионом работы RSTP.

**Состояние порта** (Port state): порт может находиться в одном из следующих состояний в зависимости от того, изучает ли он MAC-адреса и пересылает ли трафик:

- **статус пересылки** (Forwarding state): означает, что порт изучает MAC-адреса и выполняет пересылку пакетов;
- **статус обучения** (Learning state): означает, что порт изучает MAC-адреса, но не осуществляет пересылку пакетов;
- **статус отбрасывания** (Discarding state): означает, что порт не изучает MAC-адреса и не осуществляет пересылку пакетов.

**Корневой порт** (Root port): это наилучший порт подключения некорневого моста к корневому мосту, то есть порт с наименьшими затратами для корневого моста. Некорневой мост взаимодействует с корневым мостом именно через корневой порт. Некорневой мост имеет только один корневой порт, при этом у корневого моста нет

корневого порта. Корневой порт может находиться в состоянии пересылки, обучения или отбрасывания.

**Назначенный порт** (Designated port): порт для пересылки пакетов BPDU на другие устройства или локальные сети. Все порты корневого моста являются назначенными. Такой порт может находиться в состоянии пересылки, обучения или отбрасывания.

**Главный (основной) порт** (Master port): порт, который соединяет регион MST с общим корневым мостом и имеет к нему кратчайший путь. Исходя из CST, главный порт – это корневой порт региона (как узел). Главный порт – это специальный граничный порт. Это корневой порт для CIST и главный порт для других инстансов. Главный порт может находиться в состоянии пересылки, обучения или отбрасывания.

**Альтернативный порт** (Alternate port): это резервный порт для корневого порта или главного порта. При выходе из строя корневого порта или главного порта альтернативный порт становится новым корневым портом или главным портом. Альтернативный порт может находиться только в состоянии отбрасывания.

**Резервный порт** (Backup port): это резервный порт для назначенного порта. Если назначенный порт выходит из строя, резервный порт берёт на себя его роль и пересылает данные без каких-либо задержек. Резервный порт может находиться только в состоянии отбрасывания.

### 6.9.3. Реализация MSTP

MSTP делит сеть на несколько регионов MST. CST рассчитывается между регионами. В регионе вычисляется несколько связующих деревьев. Каждое связующее дерево – это MSTI. Инстанс 0 – это IST, а другие инстансы - это MSTI.

1. Расчет CIST.

- Устройство отправляет и принимает пакеты BPDU. На основе сравнения пакетов с конфигурацией MSTP, устройство с наивысшим приоритетом выбирается в качестве корневого моста CIST.
- IST рассчитывается в каждом регионе MST.
- Каждый регион MST рассматривается как одно устройство, и CST рассчитывается между регионами.
- CST и IST составляют CIST всей сети.

2. Расчет MSTI.

MSTP в регионе MST генерирует различные связующие деревья для VLAN на основе сопоставления VLAN и связующих деревьев. Каждое связующее дерево рассчитывается независимо. Процесс расчета аналогичен STP.

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

### 6.9.4 Настройка с помощью WEB-интерфейса

1. Включение протокола MSTP.

Нажмите [Device Advanced Configuration] → [MSTP configuration] → [Enable MSTP], чтобы открыть страницу конфигурации протокола MSTP, как показано на рисунке 177.


Рисунок 177 – Включение протокола MSTP

**Mstp status (состояние MSTP)**
Варианты: Enable/Disable (включить/отключить).
По умолчанию: Disable (отключить)
Функция: включить/отключить MSTP.

---

- Кольцевые протоколы на основе портов включают RSTP, Sy2-Ring-Port и Sy2-RP-Port, а кольцевые протоколы на основе VLAN включают MSTP, Sy2-RingVLAN и Sy2-RP-VLAN.
- Кольцевые протоколы на основе VLAN являются взаимоисключающими, и для одного устройства можно настроить только один режим кольцевого протокола на основе VLAN.
- Кольцевые протоколы на основе портов и на основе VLAN являются взаимоисключающими, и для одного устройства можно настроить только один режим кольцевого протокола.

---

Принудительный перевод порта в режим MSTP.

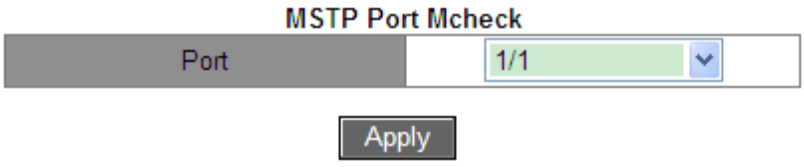



Рисунок 178 – Перевод в режим MSTP

**Port (порт)**
Варианты: все порты коммутатора
Функция: когда порт с поддержкой MSTP подключен к устройству с поддержкой STP, он автоматически изменит конфигурацию для работы в режиме STP. Если устройство с поддержкой STP будет удалено, порт не вернется автоматически к работе в режиме MSTP. Если требуется работа в режиме MSTP, эту функцию следует включить принудительно. Как только порт снова получит STP-сообщение, он автоматически переключится на работу в режиме STP.

Эта настройка вступит в силу, только если коммутатор изначально работает в режиме MSTP; в противном случае она бесполезна.

3. Настройка статуса MSTP порта.
Нажмите [Device Advanced Configuration] → [MSTP configuration] → [Enable Port MSTP], чтобы открыть страницу конфигурации протокола MSTP, как показано на рисунке 179.

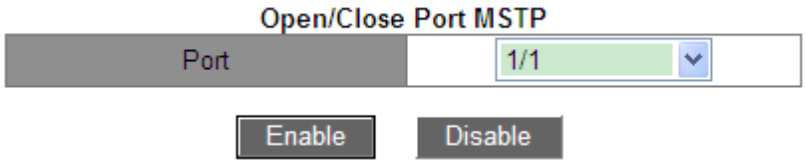



Рисунок 179 – Настройка MSTP для порта

**Port (порт)**
Варианты: все порты коммутатора.
По умолчанию: если на устройстве включен протокол MSTP, функция MSTP на всех портах открыта.
Функция: включение/выключение MSTP на порту.

4. Настройка параметров региона MST.
Нажмите [Device Advanced Configuration] → [MSTP configuration] → [MSTP Region Config], чтобы открыть страницу конфигурации параметров региона MST, как показано на рисунке 180.

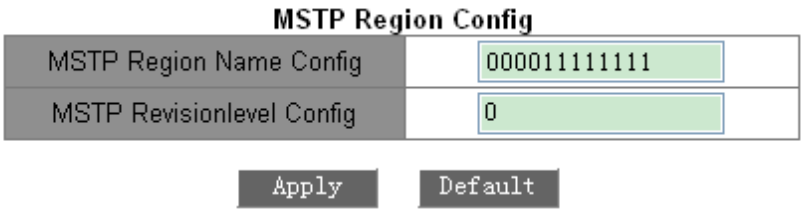



Рисунок 180 – Настройка параметров региона MST

**MSTP Region Name config (настройка имени MSTP-зоны)**
Диапазон: 1-32 символов.
По умолчанию: MAC-адрес устройства.
Функция: Настройка имени региона MST.

**MSTP Revision level config (настройка уровня MSTP Revision)**
Варианты: 0~65535.
Значение по умолчанию: 0.

Функция: Настройка параметра Revision MSTP зоны.
Описание: параметр Revision, имя MST зоны и таблица соответствия VLAN определяют MST зону, к которой принадлежит устройство. Когда все настройки одинаковы, устройства принадлежат к одной MST зоне.

5. Настройка таблицы сопоставления VLAN (см. рисунок 181).


Рисунок 181 – Таблица сопоставления VLAN

**{ID MSTP Instance ID, Vlanlist}**
Диапазон: {0~16, 1~4094}
По умолчанию: {0, 1~4094}
Функция: Настройка таблицы соответствия VLAN в MST-зоне.
Описание: по умолчанию все сети VLAN соответствуют инстансу 0. Одна VLAN может соответствовать только одному инстансу логического дерева. Если сети VLAN с уже указанным соответствием присваивается новый инстанс, предыдущее соответствие стирается. Если соответствие между выбранной VLAN и инстансом удаляется, VLAN будет соответствовать инстансу 0.

---

С помощью <Del> нельзя удалить соответствие между VLAN и инстансом 0.

---

После завершения настройки список экземпляров Instance List покажет сопоставление между VLAN и инстансом.

6. Настройка приоритета моста коммутатора в назначенном экземпляре.
Нажмите [Device Advanced Configuration] → [MSTP configuration] → [MSTP Instance Config], чтобы перейти на страницу конфигурации параметров экземпляра MSTP, как показано на рисунке 182.

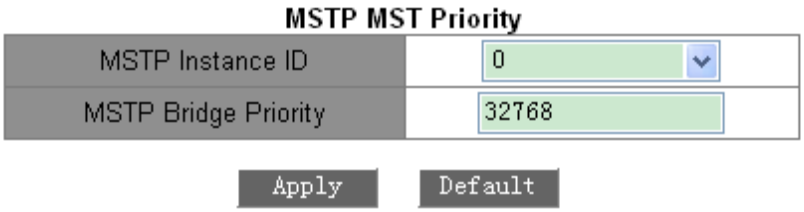



Рисунок 182 – Настройка приоритета моста в назначенном экземпляре.

**MSTP Instance ID (идентификатор экземпляра MSTP)**
Варианты: все созданные экземпляры.

**MSTP Bridge Priority (приоритет моста MSTP)**
Диапазон: 0~61440 с шагом 4096.
По умолчанию: 32768.
Функция: настроить приоритет моста коммутатора в назначенном экземпляре.
Описание: приоритет моста определяет, может ли коммутатор быть выбран в качестве регионального корня экземпляра связующего дерева. Чем меньше значение, тем выше приоритет. Установив более низкий приоритет, определенное устройство может быть назначено корневым мостом связующего дерева. Устройство с поддержкой MSTP можно настроить с разными приоритетами в разных экземплярах связующего дерева.

7. Настройка приоритета порта и стоимости пути в назначенном инстансе (см. рисунок 183).

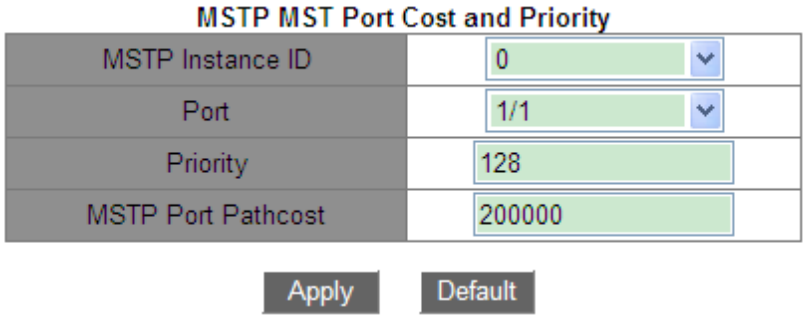



Рисунок 183 – Приоритет порта и стоимость пути в назначенном инстансе

**MSTP Instance ID (идентификатор экземпляра MSTP)**
Варианты: все созданные экземпляры.

**Port (порт)**
Варианты: все порты коммутатора.

**Priority (приоритет)**
Диапазон: 0~240 с шагом 16.
По умолчанию: 128.
Функция: настройка приоритета порта в выбранном экземпляре.

Описание: приоритет порта определяет возможность порта стать корневым. В одинаковых условиях, порт с меньшим приоритетом будет выбран корневым. Порты MSTP могут иметь разные приоритеты и играть разные роли в разных экземплярах логических деревьев.

**MSTP Port Path cost (стоимость пути для порта MSTP)**
Диапазон: 1~200000000.
Значение по умолчанию: значения указаны в таблицах 9 и 10.

Таблица. 9 – Стоимость пути по умолчанию для обычного порта

| Тип порта | Стоимость пути по умолчанию | Рекомендованное значение |
|---|---|---|
| 10 Мбит/с | 2000000 | 2000000~20000000 |
| 100 Мбит/с | 200000 | 200000~2000000 |
| 1 Гбит/с | 20000 | 20000~200000 |

Таблица 10 – Стоимость пути по умолчанию для порта агрегации

| Тип порта | Количество портов агрегации (в допустимом диапазоне агрегации) | Рекомендованное значение |
|---|---|---|
| 10 Мбит/с | N | 2000000/N |
| 100 Мбит/с | N | 200000/N |
| 1 Гбит/с | N | 20000/N |

Функция: настройка стоимости пути порта в выбранном инстансе.
Описание: стоимость пути порта используется для вычисления оптимального пути. Этот параметр зависит от пропускной способности. Чем больше пропускная способность, тем ниже стоимость пути. Изменение стоимости пути может изменить путь передачи данных от данного устройства до корневого, таким образом изменив роль порта. MSTP-порту могут быть присвоены разные стоимости пути в разных экземплярах логических деревьев.

8. Настройка временных параметров MSTP.
Нажмите [Device Advanced Configuration] → [MSTP configuration] → [MSTP Time Config], чтобы открыть страницу конфигурации параметров времени MSTP, как показано на рисунке 184.

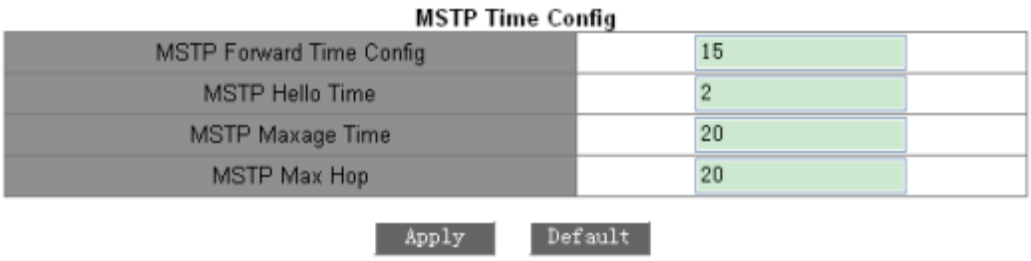



Рисунок 184 – Настройка временных параметров MSTP.

**MSTP Forward Time Config (настройка максимального времени передачи MSTP)**
Варианты: 4~30 с.
По умолчанию: 15 с.
Функция: настройка временного интервала для смены состояния порта (отбрасывание — обучение или обучение — передача).

**MSTP Hello Time (время приветствия MSTP)**
Диапазон: 1~10 с.
По умолчанию: 2 с.
Функция: настройка временного интервала для отправки BPDU.

**MSTP Max Age Time (максимальный возраст MSTP)**
Диапазон: 6~40 с.
По умолчанию: 20 с.
Функция: выбор времени старения пакетов BPDU.

---

- Значения времени передачи, Hello-интервал и Max Age-интервал должны соответствовать следующим критериям: 2 x (Время передачи – 1 секунда) >= Max Age Time; Max Age Time >= 2 x (Hello-интервал + 1 секунда).
- Рекомендуется использовать настройки по умолчанию.

---

**MSTP Max Hop (максимальное количество транзитных участков сети для MSTP)**
Диапазон: 1~40.
По умолчанию: 20.
Функция: настройка максимального количества переходов (хопов) для MST-региона. Максимальное количество хопов ограничивают размер MST-зоны; максимальное количество хопов от регионального корня равно максимальному числу хопов в MST-регионе.
Описание: начиная с корневого коммутатора логического дерева MST-зоны, количество хопов уменьшается на 1 при прохождении BPDU какого-либо устройства зоны. Устройство отбросит BPDU с количеством переходов, равным 0.

---

- Настройка максимального количества переходов MST-зоны имеет смысл только на корневом коммутаторе. Все остальные устройства используют настройку корневого коммутатора.
- Рекомендуется использовать настройки по умолчанию.

---

9. Настройка функции быстрого переключения состояний MSTP.
Нажмите [Device Advanced Configuration] → [MSTP configuration] → [MSTP Fast Transfer Config], чтобы открыть страницу настройки, как показано на рисунке 185.

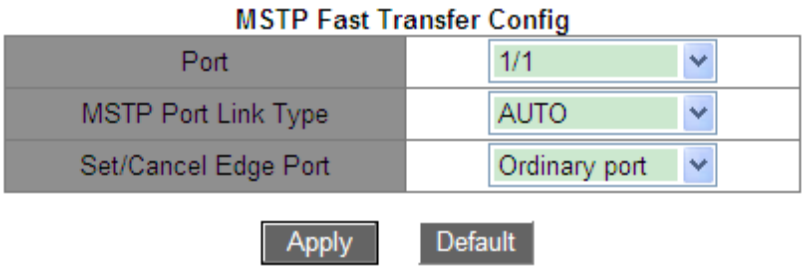



Рисунок 185 – Настройка функции быстрого переключения состояний

**MSTP Port Link Type (тип подключения порта MSTP)**
Варианты: AUTO/Force True/Force False
По умолчанию: AUTO
Функция: выбор типа порта. Если порт подключён в режиме точка-точка, состояния порта могут быть изменены быстро
Описание: «AUTO» означает, что коммутатор автоматически будет определять тип соединения, в соответствии с дуплексным режимом. Если порт работает в дуплексном режиме, протокол MSTP автоматически примет, что этот порт подключен в режиме «точка-точка». Если порт работает в режиме полудуплекса, MSTP автоматически определит, что порт подключён к разделяемой среде.
«Force True» означает, что порт подключён в режиме «точка-точка».
«Force False» означает, что порт подключён к разделяемой среде.

**Set/Cancel Edge Port (установить/отменить граничный порт)**
Варианты: Edge port/Ordinary port (граничный порт/обычный порт).
По умолчанию: Ordinary port (обычный порт).
Функция: настройка порта как edge-порт или обычный порт.
Описание: когда порт подключён к конечному устройству, а не к другому коммутатору или разделяемой среде, этот порт является граничным (edge-портом). Edge-порт может быстро переходить из стадии отбрасывания в стадию продвижения без задержки. Если граничный порт получает BPDU сообщение, он снова становится обычным.

10. Просмотр информации о настройках MSTP.
Нажмите [Device Advanced Configuration] → [MSTP configuration] → [MSTP Information], чтобы отобразить конфигурацию MSTP, как показано на рисунке 186.

```
Information Display

                -- MSTP Bridge Config Info --

Bridge MAC    :  00:00:11:11:11:11
Bridge Times  :  Max Age 20, Hello Time 2, Forward Delay 15
Force Version:  3

############################ Instance 0 ############################
Self Bridge Id    : 32768 -  00:00:11:11:11:11
Root Id           : this switch
Ext.RootPathCost  : 0
Region Root Id    : this switch
Int.RootPathCost  : 0
Root Port ID      : 0
Current port list in Instance 0:
Ethernet3/4 (Total 1)

   PortName      ID      ExtRPC   IntRPC  State Role     DsgBridge      DsgPort
-------------- ------- --------- --------- --- ---- ----------------- -------
   Ethernet3/4 128.012        &
```

Рисунок 186 – Конфигурация MSTP

## 6.9.5 Пример типовой настройки

Как показано на рисунке 187, коммутаторы A, B, C и D принадлежат одному и тому же региону MST. VLAN, отмеченные красным, означают, что пакеты VLAN могут быть переданы по каналам связи. После завершения настройки пакеты VLAN можно пересылать по разным инстансам связующего дерева. Пакеты VLAN 10 пересылаются по инстансу 1, а корневым мостом инстанса 1 является коммутатор A. Пакеты VLAN 30 пересылаются по инстансу 3, а корневой мост инстанса 3 – это коммутатор B. Пакеты VLAN 40 пересылаются по инстансу 4, а корневой мост инстанса 4 – это коммутатор C. Пакеты VLAN 20 пересылаются по инстансу 0, а корневым мостом инстанса 0 является коммутатор B.

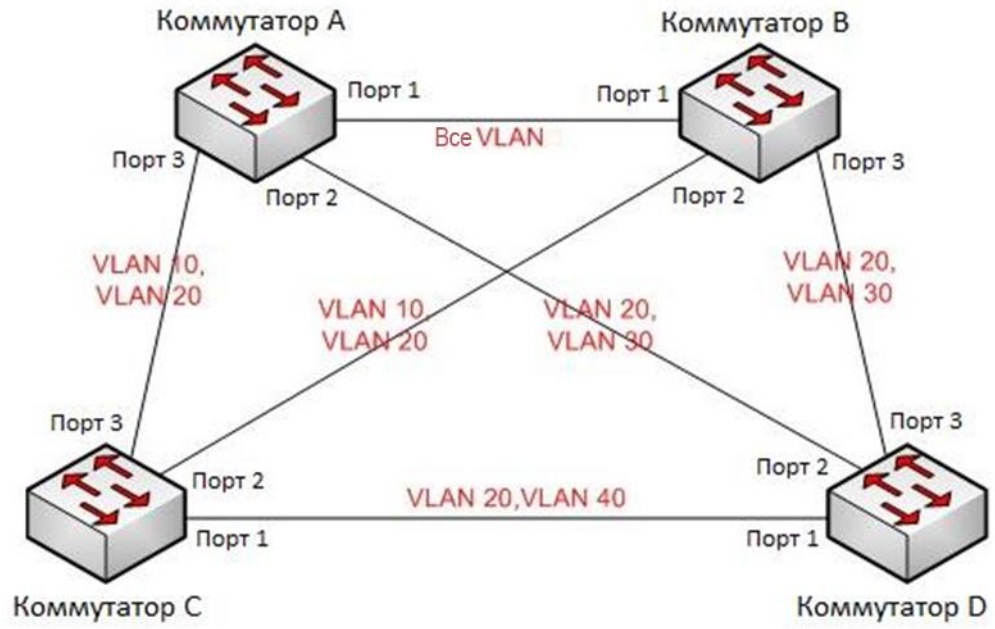



Рисунок 187 – Пример типовой настройки MSTP

**Настройка коммутатора A:**
1. Создайте VLAN 10, 20 и 30 на коммутаторе A; на портах установите разрешение на прохождение пакетов, соответствующих VLAN.
2. Включите глобальный протокол MSTP (см. рисунок 177).
3. Задайте для имени региона MST значение «Region», а для параметра «Revision» – 0 (см. рисунок 180).
4. Создайте MSTI 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с инстансами 1, 3 и 4 соответственно (см. рисунок 180).
5. Установите приоритет моста коммутатора в MSTI 1 на 4096 и сохраните приоритет по умолчанию в других инстансах (см. рисунок 182).

**Настройка коммутатора B:**
1. Создайте VLAN 10, 20 и 30 на коммутаторе B; на портах установите разрешение на прохождение пакетов, соответствующих VLAN.
2. Включите глобальный протокол MSTP (см. рисунок 177).
3. Задайте для имени региона MST значение «Region», а для параметра «Revision» – 0 (см. рисунок 180).
4. Создайте MSTI 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с инстансами 1, 3 и 4 соответственно (см. рисунок 180).
5. Установите приоритет моста коммутатора в MSTI 3 и MSTI 0 на 4096 и сохраните приоритет по умолчанию в других инстансах (см. рисунок 182).

**Настройка коммутатора C:**
1. Создайте VLAN 10, 20 и 40 на коммутаторе C; на портах установите разрешение на прохождение пакетов, соответствующих VLAN.
2. Включите глобальный протокол MSTP (см. рисунок 177).
3. Задайте для имени региона MST значение «Region», а для параметра «Revision» – 0 (см. рисунок 180).
4. Создайте MSTI 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с инстансами 1, 3 и 4 соответственно (см. рисунок 180).
5. Установите приоритет моста коммутатора в MSTI 4 на 4096 и сохраните приоритет по умолчанию в других инстансах (см. рисунок 182).

**Настройка коммутатора D:**
1. Создайте VLAN 20, 30 и 40 на коммутаторе D; на портах установите разрешение на прохождение пакетов, соответствующих VLAN.
2. Включите глобальный протокол MSTP (см. рисунок 177).
3. Задайте для имени региона MST значение «Region», а для параметра «Revision» – 0 (см. рисунок 180).
4. Создайте MSTI 1, 3 и 4 и сопоставьте VLAN 10, 30 и 40 с инстансами 1, 3 и 4 соответственно (см. рисунок 180).

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

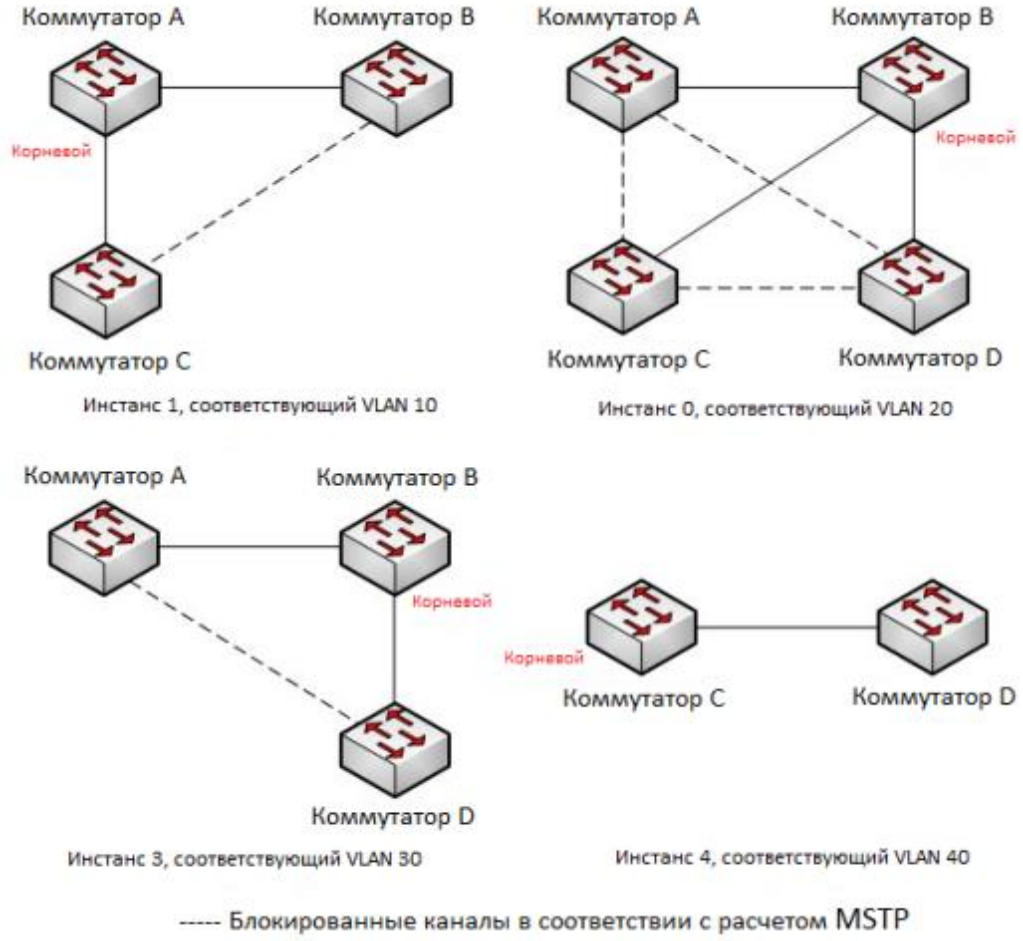



Рисунок 188 – Экземпляры связующего дерева для каждой VLAN

## 6.10 Аварийная сигнализация (Alarm)

### 6.10.1 Введение

Данная серия коммутаторов поддерживает следующие типы аварийной сигнализации:

- **Port alarm.** Аварийная сигнализация порта: если включена данная функция, аварийная сигнализация будет срабатывать в случае получении информации об отключении соответствующего порта (состояние Link Down).
- **Power alarm.** Аварийная сигнализация электропитания: доступно для устройств с двумя источниками питания. Если включена данная функция, аварийная сигнализация будет срабатывать в случае проблем с одним из источников электропитания;
- **Ring alarm.** Аварийная сигнализация кольца: если включена данная функция, аварийная сигнализация будет срабатывать в случае нарушения кольцевой топологии, т.е. при размыкании кольца.
- **High-temperature alarm.** Аварийная сигнализация высокой температуры: если эта функция включена, аварийная сигнализация срабатывает, когда температура коммутатора превышает пороговое значение высокой температуры.

Диапазон основного порога высокой температуры (T-high) составляет от 85℃ до 94℃ с настройкой по умолчанию 85℃.
Диапазон опасного порога высокой температуры (T-Max) составляет от 95℃ до 100℃ с настройкой по умолчанию 95℃.
Основной аварийный сигнал высокой температуры срабатывает, когда температура коммутатора (T-cur) выше порога T-high и ниже порога T-Max (T-high<T-cur<T-max).
Аварийный сигнал опасной высокой температуры срабатывает, когда температура переключателя равна или превышает пороговое значение T-Max (T-cur>=T-max).

- **Low-temperature alarm.** Аварийная сигнализация низкой температуры: если эта функция включена, аварийная сигнализация срабатывает, когда температура коммутатора опускается ниже порогового значения низкой температуры.
  Диапазон порога низкой температуры (T-low) составляет от -40 ℃ до 10 ℃ с настройкой по умолчанию -40 ℃.
  Аварийный сигнал низкой температуры срабатывает, когда температура переключателя (T-cur) ниже порогового значения T-low (T-cur<T-low).

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

---

Функцию аварийной сигнализации кольца (Ring alarm) поддерживают только Мастер кольца Sy2-Ring и корневой коммутатор Sy2-RP.

---

## 6.10.2 Настройка с помощью WEB-интерфейса

1. Настройка и отображение аварийной сигнализации порта.
Нажмите [Device Advanced Configuration] → [Alarm] → [Alarm Configuration] для входа на страницу настройки сигнализации порта, как показано на рисунке 189.

**Set Port Alarm**

| | |
|---|---|
| Port | 1/1 |
| Alarm Administrative State | Disable |

Apply Cancel

| Port | Alarm Administrative State | Port | Alarm Administrative State |
|---|---|---|---|
| 1/1 | Enable | 1/2 | Disable |
| 1/3 | Disable | 1/4 | Disable |
| 1/5 | Disable | 1/6 | Disable |
| 1/7 | Disable | 1/8 | Enable |
| 1/9 | Disable | 1/10 | Disable |
| 1/11 | Disable | 1/12 | Disable |

Рисунок 189 – Настройка аварийной сигнализации порта

**Port (порт)**
Варианты: все порты коммутатора.

**Alarm Administrative State (статус сигнализации)**
Варианты: Disable/Enable (отключить/включить).
По умолчанию: Disable (отключить).
Функция: включить/выключить аварийную сигнализацию порта.

Нажмите [Device Advanced Configuration] → [Alarm] → [Alarm Show], чтобы отобразить сигнализацию порта, как показано на рисунке 190.

**Port Alarm Status**

| Port | Alarm Administrative State | Port | Alarm Administrative State |
|---|---|---|---|
| 1/1 | LinkDown | 1/8 | LinkUp |

Рисунок 190 – Аварийная сигнализация порта

**Alarm Administrative State (статус сигнализации)**
Варианты: LinkDown/LinkUp (нет связи/есть связь).
Функция: просмотр состояния подключения порта, для которого включена функция сигнализации.

Описание: «LinkUp» означает, что порт находится в состоянии подключения и поддерживает нормальную связь. «LinkDown» означает, что порт отключен или соединение неустойчиво и происходит сбой связи.

2. Настройка и отображение аварийной сигнализации Sy2-Ring.
Нажмите [Device Advanced Configuration] → [Alarm] → [Alarm Configuration], чтобы перейти на страницу настройки аварийной сигнализации Sy2-Ring, как показано на рисунке 191.

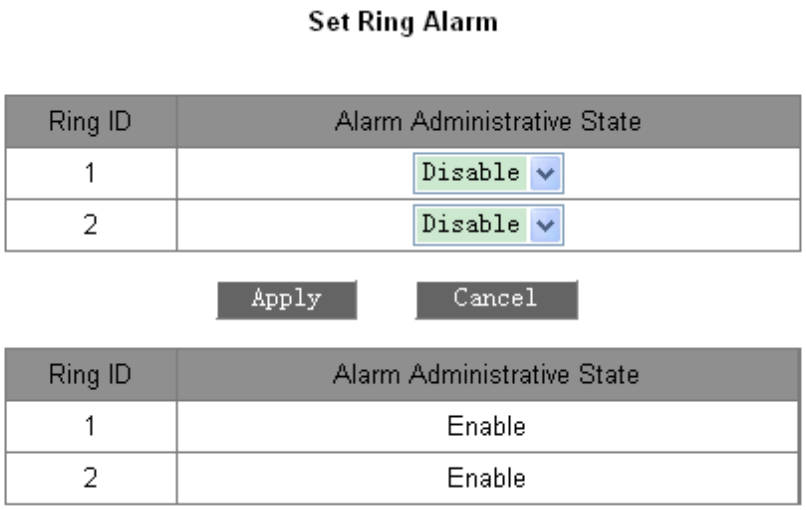



Рисунок 191 – Настройка сигнализации Sy2-Ring

**Alarm Administrative State (статус сигнализации)**
Варианты: Disable/Enable (отключить/включить).
По умолчанию: Disable (отключить).
Функция: включить/выключить аварийную сигнализацию Sy2-Ring.

Нажмите [Device Advanced Configuration] → [Alarm] → [Alarm Show], чтобы отобразить сигнализацию Sy2-Ring, как показано на рисунке 192.

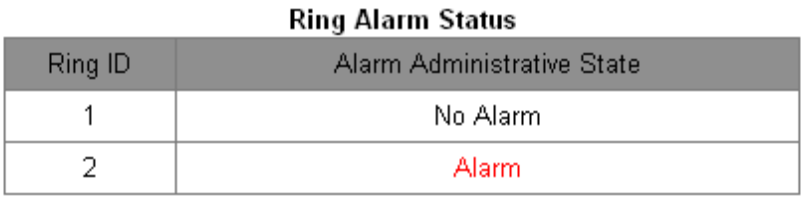



Рисунок 192 – Аварийная сигнализация Sy2-Ring

**Alarm Administrative State (статус сигнализации)**
Варианты: Alarm/No alarm (тревога/нет тревоги).
Функция: просмотр состояния колец, на которых включена функция тревоги Sy2-Ring.
Описание: отсутствие сигнала тревоги означает, что кольцо замкнуто. Аварийный сигнал означает, что кольцо разомкнуто или работает в нештатном режиме.

3. Настройка и отображение аварийной сигнализации Sy2-RP.
Нажмите [Device Advanced Configuration] → [Alarm] → [Alarm about DRP], чтобы перейти на страницу настройки аварийной сигнализации Sy2-RP, как показано на рисунке 193.

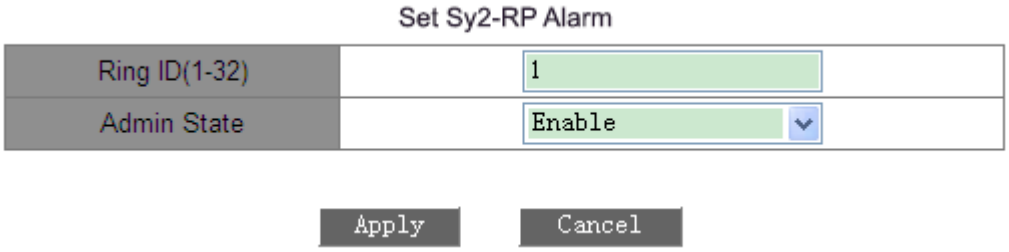



Рисунок 193 – Настройка сигнализации Sy2-RP

**Ring ID (идентификатор кольца)**
Варианты: все созданные идентификаторы Sy2-RP.

**Admin State (статус сигнализации)**
Варианты: Disable/Enable (отключить/включить).
По умолчанию: Disable (отключить).
Функция: включить/выключить тревогу Sy2-RP.

Отображение сигнализации Sy2-RP, как показано (см. рисунок 194).

| Ring ID | Admin State | Current State |
|---|---|---|
| 1 | Enable | Normal |
| 2 | Enable | Alarm |

Рисунок 194 – Аварийная сигнализация Sy2-RP

**Current State (текущее состояние)**
Варианты: Alarm/Normal (тревога/нормальный).
Функция: просмотр состояния колец Sy2-RP, для которых включена функция. «Normal» означает, что кольцо Sy2-RP замкнуто. «Alarm» означает, что кольцо разомкнуто или находится в нештатном состоянии.

4. Настройка и отображение сигнала тревоги электропитания и температуры.
Нажмите [Device Advanced Configuration] → [Alarm] → [Alarm Configuration], чтобы перейти на страницу настройки сигнализации электропитания и температуры, как показано на рисунке 195.

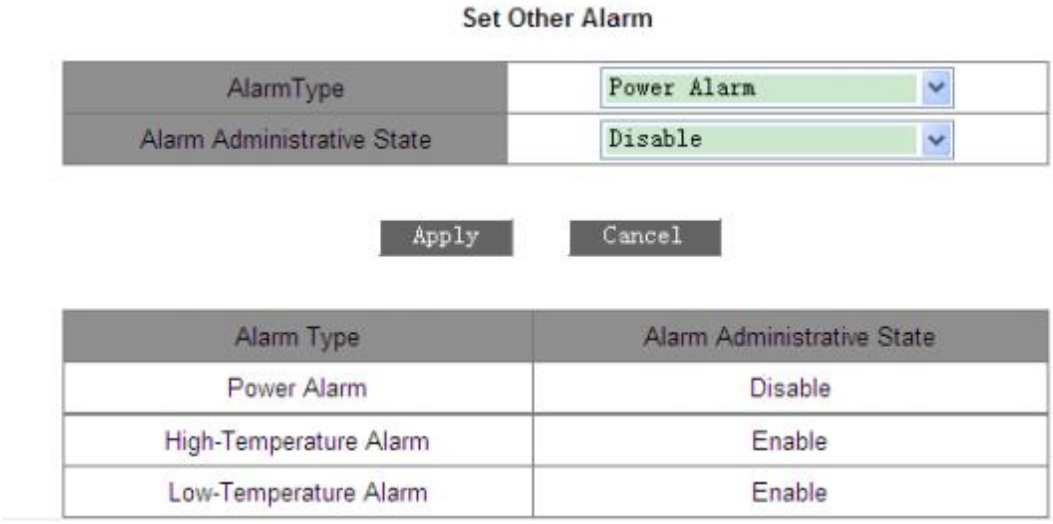



Рисунок 195 – Настройка сигнализации электропитания и температуры

**Alarm type (тип тревоги)**
Варианты: Power Alarm/High-Temperature Alarm/Low-Temperature Alarm (аварийная сигнализация питания/высокой температуры/низкой температуры).
Функция: выбор типа сигнализации.

**Alarm Administrative State (статус сигнализации)**
Варианты: Disable/Enable (отключить/включить).
По умолчанию: сигнализация питания выключена, сигнализация температуры включена.
Функция: включить/выключить определённый тип сигнализации.

Нажмите [Device Advanced Configuration] → [Alarm] → [Alarm Show], чтобы отобразить сигнализацию электропитания и температуры, как показано на рисунке 196.

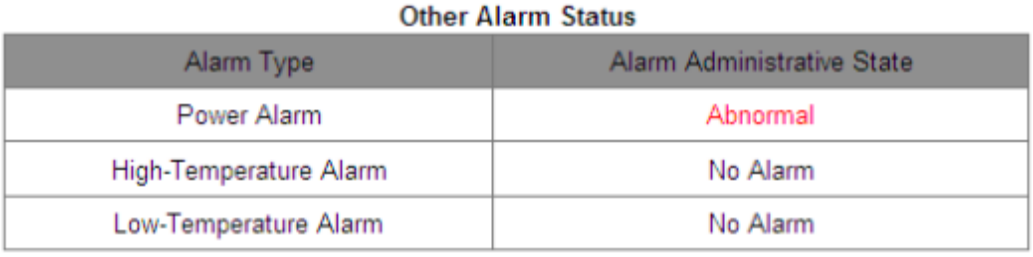



Рисунок 196 – Статус сигнализации

**Power Alarm administrative state (статус сигнализации питания)**
Варианты: Normal/Abnormal (нормальный/ненормальный).
Функция: просмотр состояния аварийного сигнала питания.
Описание: «Abnormal»: для продуктов с резервным питанием. Когда один из модулей питания выходит из строя или работает ненормально, срабатывает аварийный сигнал.

«Normal»: для устройств с одним источником питания модуль питания подает питание в обычном режиме; для устройств с резервным питанием оба силовых модуля обеспечивают питание в штатном режиме.

**High-Temperature alarm administrative state (статус сигнализации высокой температуры)**
Варианты: No Alarm/Alarm (нет тревоги/тревога).
Функция: просмотр рабочей температуры коммутатора.
Описание: «Alarm» означает, что температура коммутатора превышает установленный порог и вызывает аварийный сигнал. «No Alarm» означает, что рабочая температура коммутатора в норме.

**Low-Temperature alarm administrative state (статус сигнализации низкой температуры)**
Варианты: No Alarm/Alarm (нет тревоги/тревога).
Функция: просмотр рабочей температуры коммутатора.
Описание: «Alarm» означает, что температура коммутатора ниже установленного порога и вызывает аварийный сигнал. «No Alarm» означает, что рабочая температура коммутатора в норме.

## 6.11 Оповещение о трафике порта

### 6.11.1 Введение

С помощью функции оповещения о трафике портов коммутатор генерирует аварийный сигнал, если скорость трафика порта превышает указанный порог или возникает ошибка CRC. Режимы тревоги включают в себя ведение журнала, мигание светодиода на передней панели, срабатывание клеммного блока сигнализации и отправку trap-сообщений SNMP.

---

- Функция оповещения о трафике зависит от настроек порта. Такой аварийный сигнал генерируется только в том случае, если функция включена на порту.
- Функция оповещения о трафике зависит от направления. Входящему и исходящему трафику соответствует разные сигналы тревоги.
- При возникновении ошибки CRC генерируется аварийный сигнал.

---

### 6.11.2 Настройка с помощью WEB-интерфейса

1. Настройка оповещений о трафике портов.
Нажмите [Device Advanced Configuration] → [Alarm] → [Alarm about PortRate/CRC], чтобы перейти на страницу настройки оповещения о трафике портов, как показано на рисунке 197.

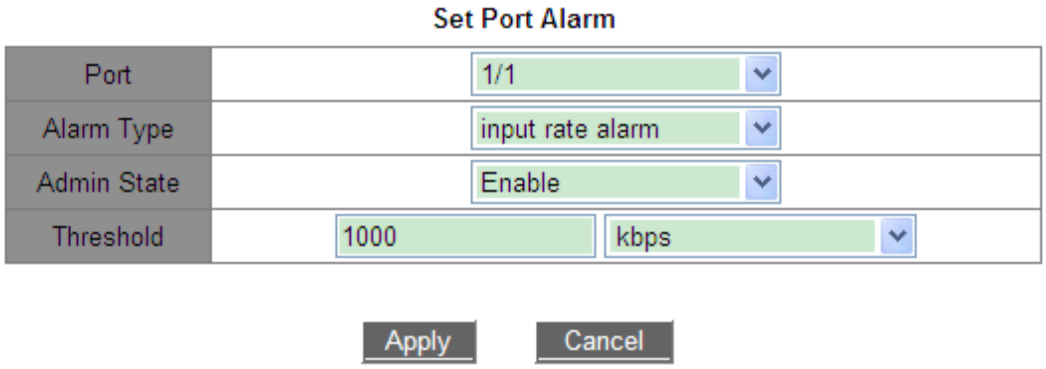



Рисунок 197 – Настройка аварийной сигнализации трафика порта

**Alarm Type (тип сигнала тревоги)**
Варианты: input rate alarm/output rate alarm/CRC (сигнализация входящего трафика / исходящего трафика / CRC).
Функция: настройка типа сигнала тревоги для оповещения о трафике порта.

**Admin State (статус сигнализации)**
Варианты: Enable/Disable (включить/отключить).
Функция: включение/выключение соответствующей тревоги.

**Threshold (порог)**
Диапазон: от 1 до 1000000000 бит/с или от 1 до 1000000 кбит/с.
Функция: настройка порогового значения для скорости трафика.

2. Просмотр информации об аварийных сигналах трафика порта (см рисунок 198).

| Port | input rate alarm | | | output rate alarm | | | CRC | |
|---|---|---|---|---|---|---|---|---|
| | Admin State | Threshold | Current State | Admin State | Threshold | Current State | Admin State | Current State |
| 1/1 | Enable | 1000kbps | Normal | Enable | 100bps | Normal | Disable | Normal |
| 1/2 | Disable | | Normal | Disable | | Normal | Disable | Normal |
| 1/3 | Disable | | Normal | Disable | | Normal | Disable | Normal |
| 1/4 | Disable | | Normal | Disable | | Normal | Disable | Normal |
| 1/5 | Disable | | Normal | Disable | | Normal | Disable | Normal |
| 1/6 | Disable | | Normal | Disable | | Normal | Disable | Normal |
| 1/7 | Disable | | Normal | Disable | | Normal | Disable | Normal |
| 1/8 | Enable | 10bps | Alarm | Enable | 10kbps | Alarm | Disable | Normal |
| 1/9 | Disable | | Normal | Disable | | Normal | Disable | Normal |
| 1/10 | Disable | | Normal | Disable | | Normal | Disable | Normal |
| 1/11 | Disable | | Normal | Disable | | Normal | Disable | Normal |
| 1/12 | Disable | | Normal | Disable | | Normal | Disable | Normal |

Рисунок 198 – Информация аварийной сигнализации трафика порта

# 6.12 Журнал событий

## 6.12.1 Введение

Функция системного журнала предназначена для записи состояние системы, информацию о неисправностях и другую информацию. При соответствующей конфигурации коммутатор может выгружать файлы с записями на сервер, поддерживающий Syslog, в режиме реального времени.
Протокольные записи делятся на 4 уровня, в зависимости от их значимости. По уменьшению степени значимости: Critical (критический), Warning (предупреждение), Information (информация) и Debugging (отладка). Чем меньше значение, тем более экстренной является информация.

Таблица 11. Уровни информации

| **Уровень информации** | **Значение** | **Описание** |
|---|---|---|
| Critical (критический) | 2 | Серьёзная системная проблема |
| Warning (предупреждение) | 4 | Предупреждающая информация |
| Information (информация) | 6 | Уведомление, которое необходимо записать |
| Debugging (отладка) | 7 | Информация, созданная в процессе отладки |

## 6.12.2 Настройка с помощью WEB-интерфейса

1. Настройка журнала.
Нажмите [Device Advanced Configuration] → [Log Configuration] → [Log Configuration], чтобы открыть страницу настройки журнала, как показано на рисунке 199.

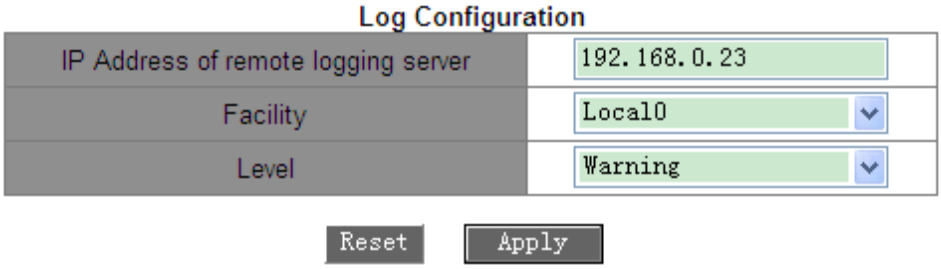



Рисунок 199 – Настройка журнала

**IP Address of remote logging server (IP-адрес удаленного сервера регистрации событий)**
Функция: настройка IP-адреса сервера, на который загружается информация журнала.

**Facility (категория объекта)**
Варианты: Local0 – Local7.
Значение по умолчанию: Local0.

Описание: используется для идентификации различных источников журналов на сервере Syslog.

**Level (уровень)**
Варианты: Critical/Warning/Information/Debugging (критический/предупреждение/информация/отладка).
По умолчанию: Warning (предупреждение).
Функция: выбрать уровень записываемой информации журнала.
Описание: информация журнала может быть отфильтрована по уровням. Правило фильтрации заключается в том, что запрещается вывод информации, значение которой больше значения выбранного информационного уровня. Например, если выбран уровень информации «Предупреждение» и соответствующее ему значение равно 4, система выводит только «Критическая информация» со значением 2 и «Предупреждение» со значением 4.

Вы можете установить программное обеспечение «Syslog Server», например, «Tftp32», на ПК для создания сервера записей системного журнала. Информация системного журнала может отображаться на сервере в режиме реального времени, как показано на рисунке 200.

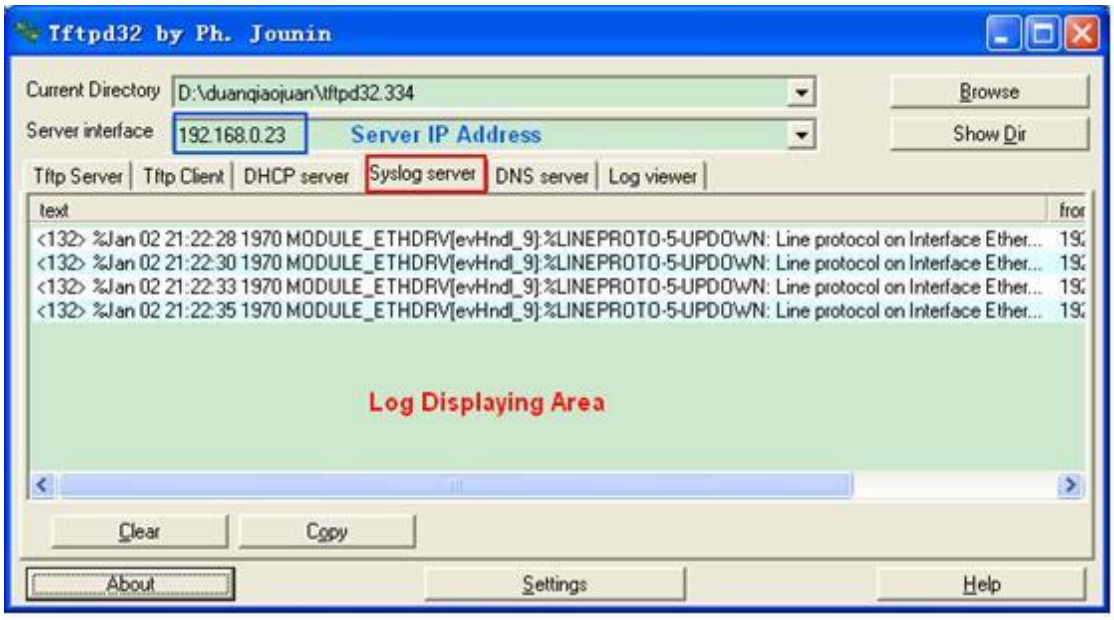



Рисунок 200 – Загрузка информации журнала на сервер в реальном времени

2. Просмотр конфигурации журнала.
Нажмите [Device Advanced Configuration] → [Log Configuration] → [Show Log], чтобы просмотреть журнал, как показано на рисунке 201.

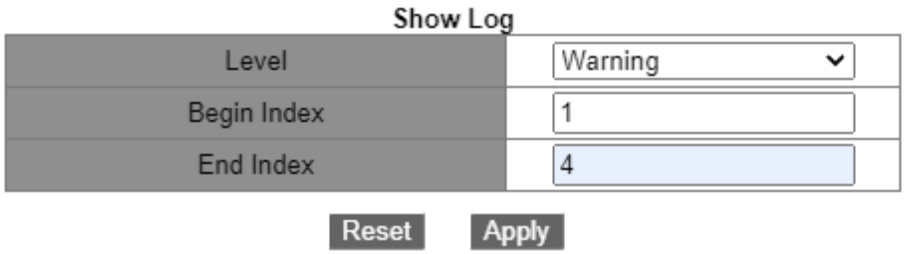



Рисунок 201 – Настройки журнала

**Level (уровень)**
Варианты: Warning/Critical (предупреждение/критический).
Значение по умолчанию: Warning (предупреждение).
Функция: выбрать самый низкий уровень отображаемой информации журнала.

**Begin Index/End Index (начальный указатель/конечный указатель)**
Диапазон: 1~65535.
Функция: просмотр выбранной информации журнала в буфере, где одна строка соответствует одной записи.
На рисунке 202 отображена выбранная информация из буфера.

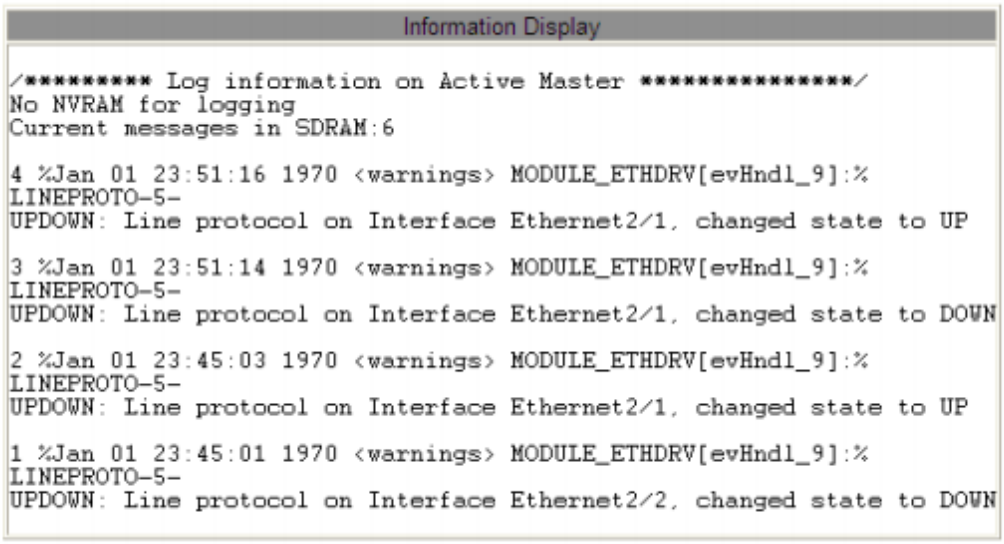



Рисунок 202 – Информация журнала

---

В буфере хранится только информация уровня «Critical» и «Warning», но не «Information» и «Debugging».

---

3. Загрузка журнала.
Нажмите [Device Advanced Configuration] → [Log Configuration] → [Log Transmit], чтобы перейти на страницу загрузки журнала, как показано на рисунке 203.

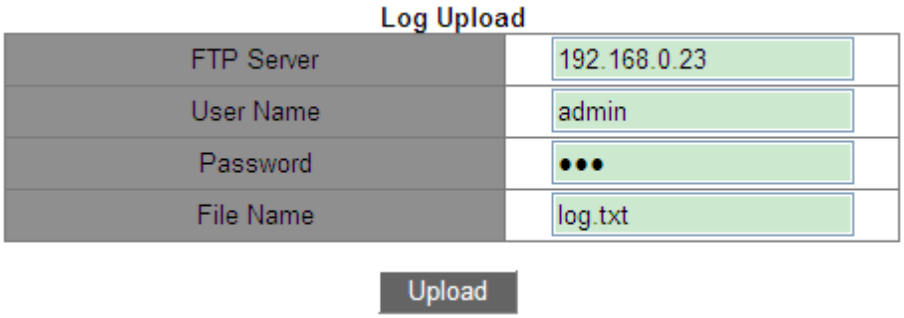



Рисунок 203 – Загрузка журнала

**FTP Server (FTP-сервер)**
Формат: A.B.C.D.
Функция: Установите IP-адрес FTP-сервера.

**User Name (имя пользователя)**
Функция: настройка имени пользователя FTP.

**Password Пароль**
Функция: настройка пароля пользователя FTP.

**File Name (имя файла)**
Диапазон: 1~32 символа.
Функция: указать имя файла, сохраненного на сервере.

---

Во время загрузки журнала необходимо обеспечить устойчивую связь с FTP-сервером.

---

4. Очистить информацию журнала в буфере.
Нажмите [Device Advanced Configuration] → [Log Configuration] → [Clear Log], чтобы очистить журнал, как показано на рисунке 204.


Рисунок 204 – Очистка журнала

## 6.13 Настройка маршрутизации

Чтобы получить доступ к удаленному узлу в Интернете, хост должен выбрать соответствующий маршрут с помощью маршрутизаторов или коммутаторов 3-го уровня. В процессе выбора пути каждый коммутатор 3-го уровня выбирает путь к следующему

коммутатору 3-го уровня в соответствии с адресом получателя пакета до тех пор, пока последний коммутатор 3-го уровня не отправит пакет узлу-получателю. Путь, который выбирает каждый коммутатор 3-го уровня, называется маршрутом. Маршруты делятся на следующие типы:
Прямой – маршрут, обнаруженный протоколом канального уровня.
Статический – маршрут, настроенный сетевым администратором вручную.
Динамический – маршрут, обнаруженный протоколом маршрутизации.

## 6.13.1 Статическая маршрутизация

### 6.13.1.1 Введение

Статические маршруты настраиваются вручную. Если топология сети достаточно проста, вам нужно всего лишь настроить статические маршруты для сети, чтобы она работала соответствующим образом. Статические маршруты просты в настройке и стабильны. Они могут быть использованы для достижения балансировки нагрузки и резервирования маршрутов, предотвращая неправомерные изменения маршрута. Недостатком использования статических маршрутов является то, что они не могут приспособиться к изменениям сетевой топологии. Если в сети появится неисправность или произойдет изменение топологии, соответствующие маршруты будет недоступны, что приведет к прерываниям передачи данных. Когда это происходит, сетевой администратор должен изменить статические маршруты вручную.

### 6.13.1.2 Таблица маршрутизации

Каждый коммутатор 3-го уровня содержит таблицу маршрутизации, где прописаны все маршруты, которые используются маршрутизатором. Каждая запись в таблице определяет, какой из пакетов VLAN, предназначенный для определенной подсети или хоста, должен быть отправлен к следующему маршрутизатору или напрямую подключенному к маршрутизатору адресату.
Запись маршрута включает в себя следующие пункты.
Назначение: указывает IP адрес получателя или сети.
Маска подсети: определяет, какая часть IP-адреса коммутатора 3-го уровня относится к адресу сети, а какая к адресу самого узла в этой сети. Логическая операция AND между адресом назначения и маской подсети дает адрес сети назначения. Например, если адрес получателя 129.102.8.10 и маска 255.255.0.0, адрес сети назначения будет 129.102.0.0. Маска подсети состоит из определенного числа последовательных битов. Это значение может быть выражено как десятичном формате, так и по количеству битов.
Выход: определяет порт, через который соответствующий пакет IP должен быть отправлен.
IP адрес следующего коммутатора 3-го уровня (следующий хоп): указывает новый маршрутизатор, через который будет пропущен пакет IP.
Приоритет: маршруты для одной и той же точки назначения, но имеющие различные следующие хопы, могут иметь разный уровень приоритета и определяются различными протоколами маршрутизации или конфигурируются вручную. Оптимальным маршрутом является маршрут с наивысшим приоритетом.

### 6.13.1.3 Маршрут по умолчанию

Для ограничения слишком большого количества записей в таблице маршрутизации, вы можете настроить маршрут по умолчанию. Маршрут по умолчанию является статическим маршрутом. Если пакету данных не удается найти соответствие в таблице маршрутизации, он передается в соответствии с маршрутом по умолчанию. В таблице маршрутизации маршрутом по умолчанию является маршрут с адресом назначения и маской 0.0.0.0. Если пакет не соответствует ни одной записи в таблице маршрутизации и маршрут по умолчанию не настроен, маршрутизатор отбрасывает пакет и возвращает пакет ICMP с информацией о том, что адрес назначения или сеть недостижимы.

### 6.13.1.4 Настройка с помощью WEB-интерфейса

1. Настройка статического маршрута.
Нажмите [Device Advanced Configuration] → [Route configuration] → [Static route configuration] → [Static route configuration], чтобы открыть страницу конфигурации статического маршрута, как показано на рисунке 205.

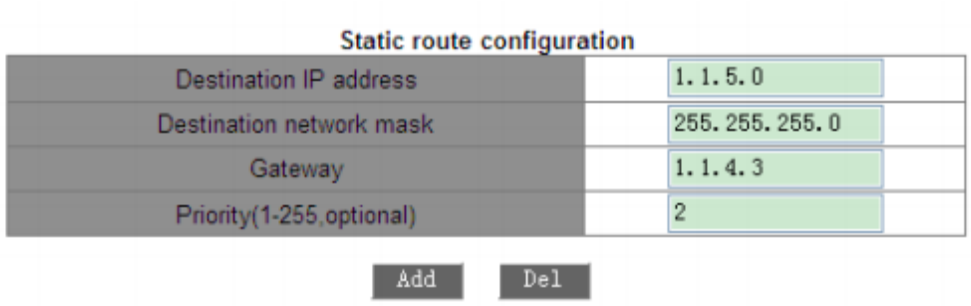



Рисунок 205 – Настройка статического маршрута

Destination IP address (IP адрес назначения)
Формат: A.B.C.D.
Функция: назначить IP адрес сети назначения.
**Destination network mask (маска сети получателя)**
Функция: назначить маску для сети, где находится хост назначения или коммутатор 3-го уровня.
**Gateway (шлюз)**
Формат: A.B.C.D.
Функция: назначить IP адрес следующего узла.
**Приоритет**
Варианты: 1~255.
Значение по умолчанию: 1.
Функция: назначить приоритет текущего маршрута. Маршрут с наименьшим значением приоритета выбирается в качестве оптимального маршрута для пересылки пакетов.

Чтобы удалить запись маршрута, необходимо настроить все параметры так, чтобы они соответствовали параметрам маршрута; в противном случае маршрут не сможет быть удален из-за ошибок соответствия.
После настройки маршрута он отображается в списке статических маршрутов, как показано на рисунке 206.

Static ip route list

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

Рисунок 206 – Список статических маршрутов

### 6.13.1.5 Пример типовой настройки

Как показано на рисунке 207, маска подсети всех коммутаторов 3-го уровня и компьютеров в сети — 255.255.255.0. Требуется настроить статические маршруты, чтобы любые из хостов могли общаться друг с другом.

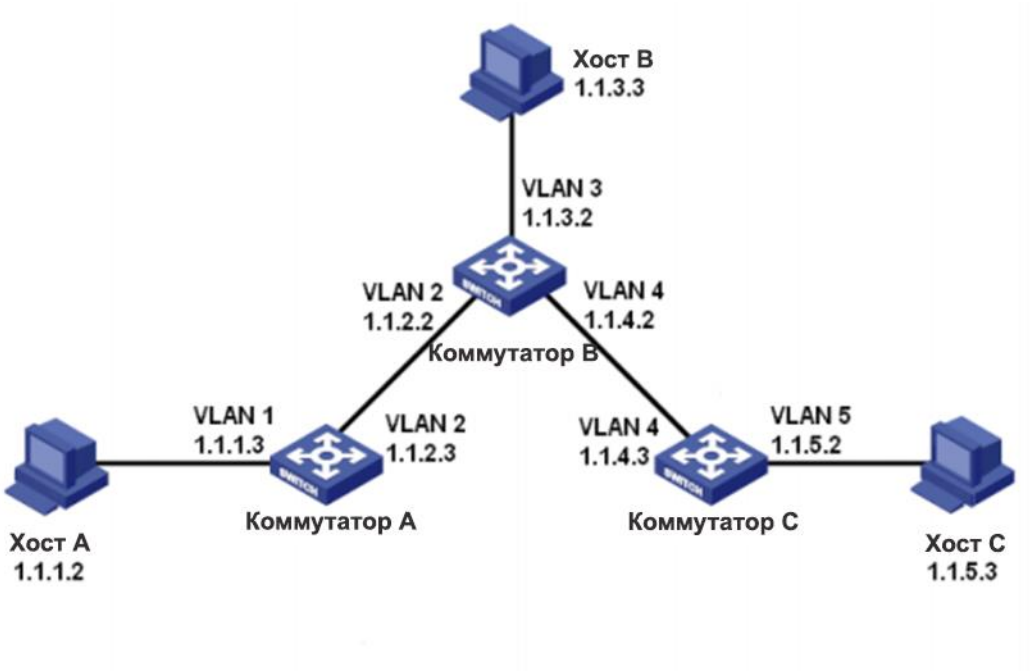



Рисунок 207 – Пример для настройки статических маршрутов

Конфигурация коммутатора A:
1. Задайте IP-адреса для интерфейсов VLAN.
2. Настройте статический маршрут со следующими параметрами:
IP-адрес назначения: 1.1.3.0; маска сети назначения: 255.255.255.0; шлюз по умолчанию: 1.1.2.2; приоритет: 1, как показано на рисунке 205.
IP-адрес назначения: 1.1.5.0; маска сети назначения: 255.255.255.0; шлюз по умолчанию: 1.1.2.2; приоритет: 1, как показано на рисунке 205.

Конфигурация коммутатора B:
3. Задайте IP-адреса для интерфейсов VLAN.
4. Настройте статический маршрут со следующими параметрами:
IP-адрес назначения: 1.1.1.0; маска сети назначения: 255.255.255.0; шлюз по умолчанию: 1.1.2.3; приоритет: 1, как показано на рисунке 205.
IP-адрес назначения: 1.1.5.0; маска сети назначения: 255.255.255.0; шлюз по умолчанию: 1.1.4.3; приоритет: 1, как показано на рисунке 205.

Конфигурация коммутатора C:
5. Задайте IP-адреса для интерфейсов VLAN.
6. Настройте статический маршрут со следующими параметрами:
IP-адрес назначения: 0.0.0.0; маска сети назначения: 0.0.0.0; шлюз по умолчанию: 1.1.4.2; приоритет: 1, как показано на рисунке 205.

7. Настройте шлюзы по умолчанию для хоста A, хоста B и хоста C как 1.1.1.3, 1.1.3.2 и 1.1.5.2 соответственно.

## 6.13.2 Настройка RIP

### 6.13.2.1 Введение

Маршрутизаторы в этой главе относятся к коммутаторам 3-го уровня.

RIP (Routing Information Protocol) — это внутренний протокол маршрутизации дистанционно-векторного типа, использующий пакеты UDP для обмена информацией через порт 520. Каждый коммутатор 3-го уровня, на котором работает RIP, имеет базу данных маршрутизации. База данных содержит записи маршрутизации ко всем доступным пунктам назначения этого коммутатора, на основе которых создается таблица маршрутизации. Когда коммутатор 3-го уровня, использующий RIP, отправляет пакет обновления маршрута своим соседним устройствам, этот пакет содержит всю таблицу маршрутизации, установленную коммутатором на основе базы данных маршрутизации. Следовательно, в крупномасштабной сети каждый коммутатор 3-го уровня должен передавать и обрабатывать большой объем данных маршрутизации, что снижает общую производительность сети. RIP позволяет вносить в таблицу информацию, обнаруженную другими протоколами маршрутизации.
RIP имеет две версии: RIP-1 и RIP-2. RIP-1 использует для сообщений только широковещательную рассылку, не поддерживает маску подсети и аутентификацию. Некоторые поля в сообщении RIP-1 должны быть заполнены нулями. Эти поля называются нулевыми, их следует проверять при получении сообщения RIP-1. Если такое поле содержит ненулевое значение, сообщение RIP-1 не будет обработано. RIP-2 –

усовершенствованная версия на основе RIP-1. В RIP-2 пакеты протокола отправляются в многоадресном режиме, а адрес назначения — 224.0.0.9. Кроме того, в RIP-2 добавлены домен маски подсети и домен проверки RIP (поддерживается простой текстовый пароль и проверка пароля MD5), а также поддерживаются маски подсети переменной длины (VLSM). RIP-2 сохраняет часть нулевых доменов в RIP-1, и поэтому нет необходимости проверять все нулевые домены. По умолчанию коммутатор 3-го уровня передает сообщение RIP-2 в многоадресном режиме, а принимает сообщения RIP-1 и RIP-2.
Для измерения расстояния до пункта назначения RIP использует количество переходов (хопов). Количество хопов от маршрутизатора к сети с прямым подключением равно 0. Количество переходов от маршрутизатора к маршрутизатору с прямым подключением равно 1. Чтобы ограничить время конвергенции, диапазон значений метрики RIP составляет от 0 до 15. Значение метрики 16. и более считается бесконечным, и это означает, что сеть назначения недоступна. Именно поэтому RIP подходит только для сетей небольшого размера.

### 6.13.2.2 Предотвращение петель маршрутизации

В сети с протоколом RIP, когда маршрут RIP становится недоступным, коммутатор 3-го уровня не будет отправлять пакет обновления маршрута немедленно, пока не истечет интервал обновления маршрута (30 с). Если соседний коммутатор отправляет пакет, содержащий информацию о его собственной таблице маршрутизации до того, как будет получен пакет обновления маршрута, произойдет бесконечный подсчет. То есть, метрика для выбора маршрута к недостижимому коммутатору 3-го уровня постепенно увеличивается. Это заметно влияет на время маршрутизации и время агрегации маршрутов.
Чтобы избежать бесконечного подсчета и образования циклического маршрута (петли), RIP предоставляет механизмы расщепления горизонта и триггерного обновления. Расщепление горизонта (split horizon) направлено на то, чтобы избежать отправки маршрутов на шлюз, из которого они были получены. Технология включает в себя простое расщепление горизонта и расщепление горизонта с «отравлением» обратного маршрута (poisoned reverse). Простое расщепление горизонта удаляет маршруты, которые должны быть отправлены на соседний шлюз, от которого эти маршруты были получены. Расщепление горизонта с отравлением обратного маршрута удаляет предыдущие маршруты из пакета обновления и устанавливает метрики этих маршрутов на 16. В механизме триггерного обновления всякий раз, когда шлюз изменяет метрику маршрута, пакет обновления маршрута будет передан немедленно, без учета состояния 30-секундного таймера обновления.

### 6.13.2.3 Принцип работы

1. После включения RIP маршрутизатор отправляет сообщения-запросы соседним маршрутизаторам. Соседние маршрутизаторы возвращают ответные сообщения, включая информацию о своих таблицах маршрутизации.
2. Получив такую информацию, маршрутизатор обновляет свою локальную таблицу маршрутизации и отправляет инициированные сообщения об обновлении соседним узлам. Все маршрутизаторы в сети делают то же самое, чтобы сохранить самую последнюю информацию о маршрутизации.

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

### 6.13.2.4 Настройка с помощью WEB-интерфейса

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

1. Включение RIP.
Нажмите [Device Advanced Configuration] → [Route configuration] → [RIP configuration] → [Enable RIP] → [Enable RIP], чтобы включить RIP, как показано на рисунке 208.

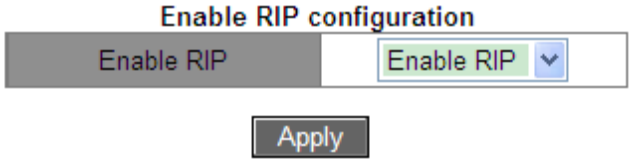



Рисунок 208 – Включение RIP

**Enable RIP (включение RIP)**
Варианты: Enable RIP/Disable RIP (включить RIP/выключить RIP).
Значение по умолчанию: Disable RIP (выключить RIP).
Функция: включение/выключение RIP.

2. Включение RIP на интерфейсе.
Нажмите [Device Advanced Configuration] → [Route configuration] → [RIP configuration] → [Enable RIP] → [Enable port to receive/transmit RIP packet], чтобы включить RIP на интерфейсе, как показано на рисунке 209.

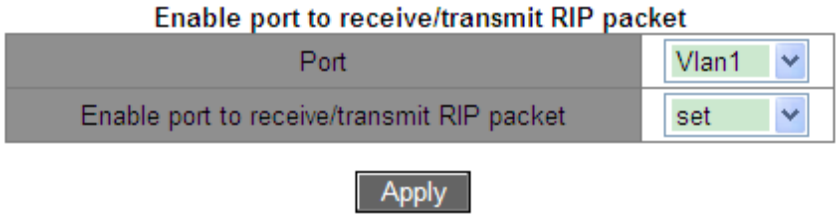



Рисунок 209 – Включение RIP на интерфейсе

**Enable port to receive/transmit RIP packet (разрешить порту прием/передачу RIP-пакета)**
Варианты: set/cancel (установить/отменить).
По умолчанию: set (установить).
Функция: включить/отключить RIP на интерфейсе.

3. Настройка импортированного маршрута.
Нажмите [Device Advanced Configuration] → [Route configuration] → [RIP configuration] → [RIP parameter configuration] → [Enable imported route], чтобы открыть страницу конфигурации импортированного маршрута, как показано на рисунке 210.

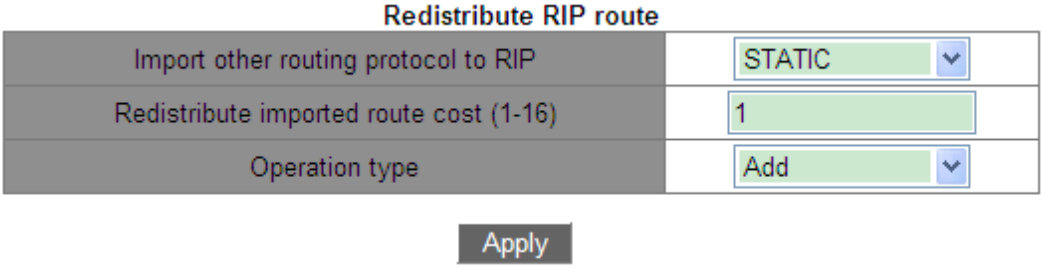



Рисунок 210 – Настройка импортированного маршрута

**Import other routing protocol to RIP (импорт другого протокола маршрутизации в RIP)**
Варианты: STATIC/OSPF.
Функция: импорт другого протокола маршрутизации в RIP. Можно импортировать только активные маршруты.

**Redistribute imported route cost (перераспределить стоимость импортированного маршрута)**
Диапазон: 1~16.
Функция: перераспределить значение метрики импортированного маршрута. Этот параметр является необязательным. Если параметр не настроен, он будет перераспределен в соответствии со значением метрики по умолчанию.

**Operation type (тип операции)**
Варианты: Add/Del (добавить/удалить).
Функция: добавить/отменить импорт другого протокола маршрутизации в RIP. По умолчанию никакие другие протоколы маршрутизации в RIP не импортируются.

4. Настройка дополнительной метрики маршрутизации.

Нажмите [Device Advanced Configuration] → [Route configuration] → [RIP configuration] → [RIP parameter configuration] → [Metricin/out configuration] для входа на страницу настройки дополнительной метрики маршрутизации, как показано на рисунке 211.

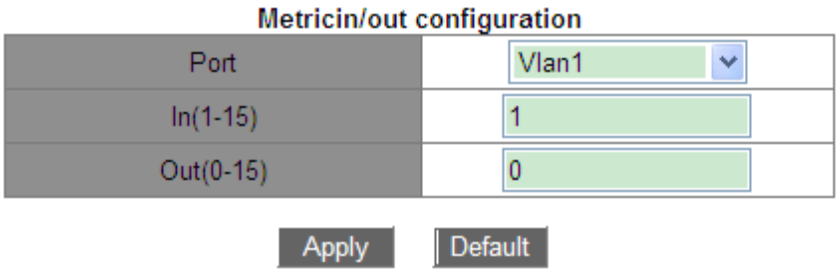



Рисунок 211 – Настройка дополнительной метрики маршрутизации

**In (входящая)**
Диапазон: 1~15.
Значение по умолчанию: 1.
Функция: настройка входящей дополнительной метрики маршрутизации. Входящая дополнительная метрика добавляется к метрике полученного маршрута перед добавлением маршрута в таблицу маршрутизации, и метрика маршрута изменяется. Если сумма дополнительной метрики и исходной метрики больше 16, метрика маршрута будет равна 16.

**Out (исходящая)**
Диапазон: 0~15.
Значение по умолчанию: 0.
Функция: настройка исходящей дополнительной метрики маршрутизации. Исходящая дополнительная метрика добавляется к метрике отправленного маршрута, а метрика маршрута в таблице маршрутизации не изменяется.

5. Настройка RIP-порта.
Нажмите [Device Advanced Configuration] → [Route configuration] → [RIP configuration] → [RIP parameter configuration] → [RIP port configuration], чтобы открыть страницу настройки порта RIP, как показано на рисунке 212.

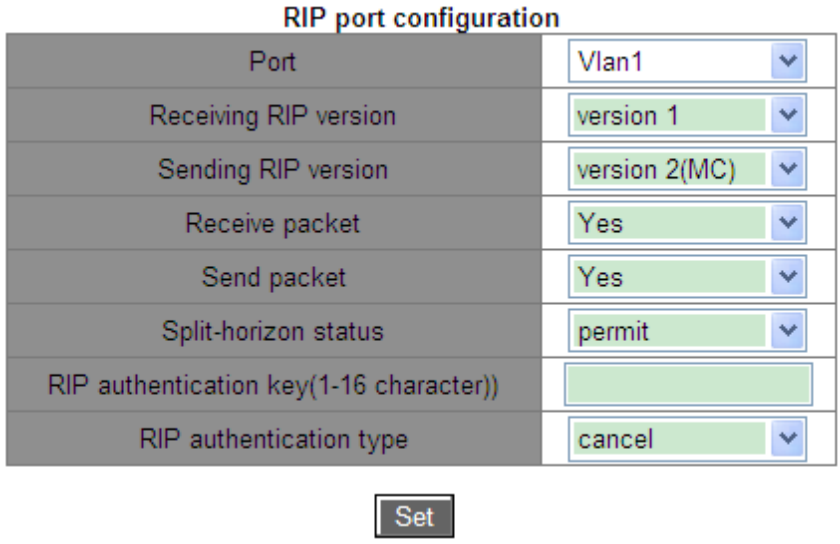



Рисунок 212 – Настройка RIP-порта

**Receiving RIP version (принимаемая версии RIP)**
Варианты: version 1/version 2/version 1 and 2.
Значение по умолчанию: version 1 and 2.
Функция: установить версию сообщения RIP, принимаемую интерфейсом. Версия 1 означает сообщение RIP-1, версия 2 означает RIP-2, а версия 1 и 2 означают приём сообщений RIP-1 и RIP-2.

**Sending RIP version (передаваемая версия RIP)**
Варианты: version 1/version 2 (BC)/version 2 (MC).
Значение по умолчанию: version 2 (MC).
Функция: настройка версии сообщения RIP, передаваемого интерфейсом. Версия 1 означает сообщение RIP-1, версия 2 (BC) – сообщение RIP-2, передаваемое интерфейсом в широковещательном режиме, версия 2 (MC) означает сообщение RIP-2, передаваемое в многоадресном режиме.

**Receive packet (получение пакета)**
Варианты: Yes/No (да/нет).
Значение по умолчанию: Yes (да).
Функция: разрешить интерфейсу получать RIP-сообщения или нет.

**Send packet (отправка пакета)**
Варианты: Yes/No (да/нет).
Значение по умолчанию: Yes (да).
Функция: разрешить интерфейсу отправлять RIP-сообщения или нет.

**Split-horizon status (статус расщепленного горизонта)**
Варианты: permit/forbid (разрешить/запретить).
Значение по умолчанию: permit (разрешить).

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

**RIP authentication key (ключ аутентификации RIP)**
Диапазон: 1~16 символов.
Функция: назначение ключа аутентификации RIP.

**RIP authentication type (тип аутентификации RIP)**
Варианты: text /Cisco MD5/MD5/cancel.
Значение по умолчанию: cancel (отменить).
Функция: установить тип аутентификации RIP. «text» означает текстовую аутентификацию; MD5 означает общую аутентификацию MD5; Cisco MD5 означает аутентификацию Cisco MD5; «cancel» означает восстановление аутентификации по умолчанию: текстовая аутентификация. RIP-1 не поддерживает аутентификацию.

6. Настройка режима RIP.
Нажмите [Device Advanced Configuration] → [Route configuration] → [RIP configuration] → [RIP parameter configuration] → [RIP mode configuration] чтобы открыть страницу настройки режима RIP, как показано на рисунке 213.

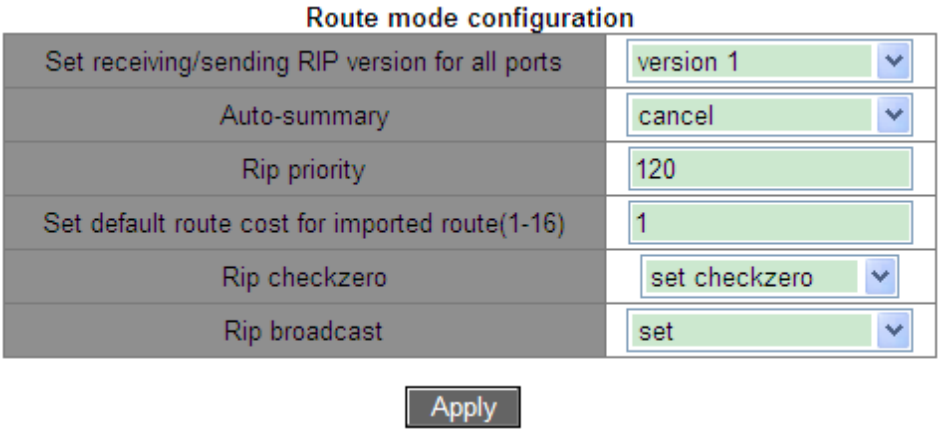



Рисунок 213 – Настройка режима RIP

**Set receiving/sending RIP version for all ports (установка версии RIP приема/отправки для всех портов)**
Варианты: version 1/version 2/cancel (версия 1/версия 2/отмена).
Значение по умолчанию: передача сообщения RIP-2, получение сообщения RIP 1 и RIP 2.
Функция: настройка версии сообщения RIP, передаваемого и принимаемого всеми интерфейсами маршрутизации. Версия 1 означает, что сообщение RIP-1 передается и принимается всеми интерфейсами маршрутизации, версия 2 означает RIP-2, отмена означает восстановление конфигурации по умолчанию.

**Auto-summary (автоматическое суммирование)**
Варианты: cancel/set (отменить/установить).

Значение по умолчанию: cancel (отменить).
Функция: установить/отменить агрегацию маршрутов. Агрегация – процесс объединения мелких префиксов с длинной маской и малым количеством хостов в крупные — с короткой маской и множеством хостов. С помощью агрегации минимизируется необходимая информация для маршрутизатора, которую он использует для поиска пути передачи в сети.
RIP-1 не поддерживает маску подсети, поэтому всегда включает функцию агрегации маршрутизации. Для RIP-2, если вы хотите транслировать маршруты подсети, отключите функцию объединения маршрутов.

**Rip priority (приоритет RIP)**
Диапазон: 0~255
Значение по умолчанию: 120
Функция: Укажите приоритет RIP. Чем меньше значение, тем выше приоритет. Приоритет определяет маршруты в базовой таблице маршрутизации, выбирая, какой алгоритм будет использоваться для получения наилучшей маршрутизации.

**Set default route cost for imported route (установить стоимость маршрута по умолчанию для импортированного маршрута)**
Диапазон: 1~16.
Значение по умолчанию: 1.
Функция: настройка значения метрики по умолчанию для импортированного маршрута.

**Rip checkzero (проверка нулевых полей сообщений RIP)**
Варианты: set checkzero/cancel checkzero.
Значение по умолчанию: set checkzero.
Функция: проверять нулевое поле сообщения RIP-1 или нет. Некоторые поля в сообщении RIP-1 должны содержать нули. Эти поля называются нулевыми полями. Вы можете включить проверку нулевого поля в полученном сообщении RIP-1. Если такое поле содержит ненулевое значение, сообщение RIP-1 не будет обработано. Поскольку в сообщении RIP-2 нет нулевого поля, для RIP-2 эта функция не работает.

**Rip broadcast** (RIP-трансляция)
Опции: set/cancel (установить/отменить).
Значение по умолчанию: set (установить).
Функция: «set» разрешает всем интерфейсам коммутатора 3-го уровня передавать широковещательные пакеты RIP или многоадресные пакеты; «cancel» — запретить всем интерфейсам коммутатора 3-го уровня передавать широковещательные или многоадресные пакеты RIP, а только передавать пакеты данных RIP между соседними коммутаторами.

7. Настройка таймеров RIP.
Нажмите [Device Advanced Configuration] → [Route configuration] → [RIP configuration] → [RIP parameter configuration] → [RIP timer configuration], чтобы перейти на страницу конфигурации таймеров RIP, как показано на рисунке 214.

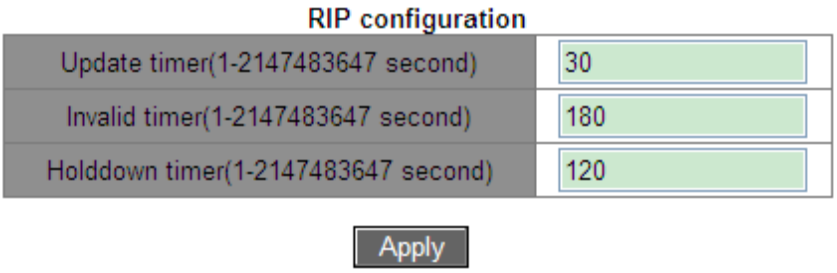



Рисунок 214 – Настройка таймеров RIP

**Update timer (таймер обновления)**
Диапазон: 1~2147483647.
Значение по умолчанию: 30.
Функция: настройка временного интервала между обновлениями маршрутизации.

**Invalid timer (таймер недостоверности)**
Диапазон: 1~2147483647.
Значение по умолчанию: 180.
Функция: настройка диапазона времени, после которого маршрутизация RIP объявляется недействительной. Если коммутатор 3-го уровня не получает информацию об обновлении маршрута от соседнего узла в течение заданного этим таймером интервала, все маршруты от этого узла будут считаться недопустимыми, и маршрут переходит в состояние подавления. Invalid timer > Update timer.

**Holddown timer (таймер удержания)**
Значение по умолчанию: 120.
Функция: настройка времени, в течение которого маршрут RIP остается в подавленном состоянии. Если в течение этого периода (значение таймера удержания) от соседнего коммутатора не будет получена информация об обновлении, этот маршрут удаляется из таблицы маршрутизации. Holddown timer > Update timer.

### 6.13.2.5 Пример типовой настройки

Как показано на рисунке 215, коммутатор B подключен к коммутатору A через интерфейс VLAN 2 и к коммутатору C через интерфейс VLAN 4. Все три коммутатора работают по протоколу маршрутизации RIP. Маска подсети у всех коммутаторов — 255.255.255.0.

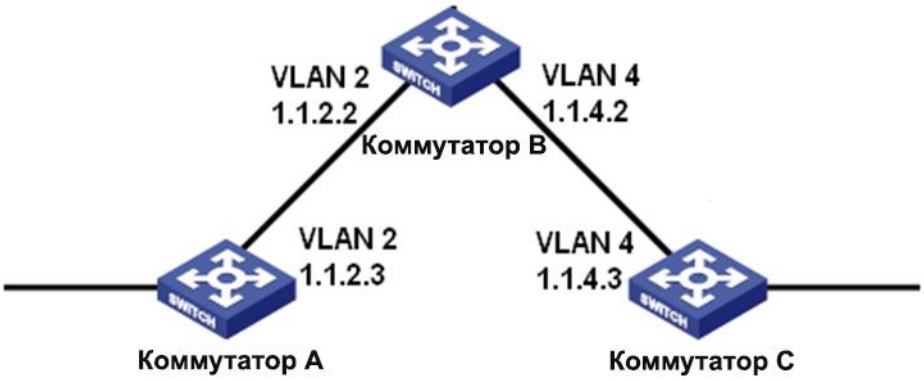



Рисунок 215 – Пример конфигурации RIP

**Настройка коммутатора A:**
1. Установите IP-адрес для интерфейса VLAN 2.
2. Включите протокол RIP, как показано на рисунке 208.
3. Включите интерфейс VLAN 2 для передачи/приема сообщения RIP, как показано на рисунке 209.

**Настройка коммутатора B:**
1. Установите IP-адреса для интерфейсов VLAN 2 и VLAN 4.
2. Включите протокол RIP, как показано на рисунке 208.
3. Включите интерфейсы VLAN 2 и VLAN 4 для передачи/приема сообщения RIP, как показано на рисунке 209.

**Настройка коммутатора C:**
1. Установите IP-адрес для интерфейса VLAN 4.
2. Включите протокол RIP, как показано на рисунке 208.
3. Включите интерфейс VLAN 4 для передачи/приема сообщения RIP, как показано на рисунке 209.

## 6.13.3 Настройка OSPF

### 6.13.3.1 Введение

OSPF (Open Shortest Path First) – протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала. Маршрутизаторы 3-го уровня обмениваются информацией о состоянии канала с базой данных LSDB (Link State Database), содержащей список всех записей о состоянии каналов. Затем каждый из маршрутизаторов использует алгоритм SPF (Shortest Path First), базирующийся на LSDB, для генерации таблицы маршрутизации. Данная серия маршрутизаторов поддерживает OSPF версии 2.

Маршрутизаторы в этой главе относятся к коммутаторам 3-го уровня.

### 6.13.3.2 Основные понятия

**1. AS (автономная система)**

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

**2. Router ID (идентификатор маршрутизатора)**

ID маршрутизатора (RID): маршрутизатор с включенным протоколом OSPF должен иметь свой собственный ID, который является уникальным идентификатором маршрутизатора в AS. При этом RID может быть либо настроен как вручную, так и автоматически. Автоматически созданным RID является основной IP-адрес порта VLAN с самым маленьким ID на коммутаторе.

**3. Пакеты OSPF**

- Hello: периодическая отправка к соседним узлам пакета, содержащего значения некоторых таймеров, а также информацию о выделенном маршрутизаторе (DR), резервном выделенном маршрутизаторе (BDR) и известных соседних узлах.
- Database description (DD): показывает справочную информацию о каждом LSA (Link State Advertisement) в LSDB, передаваемых между двумя маршрутизаторами для синхронизации данных.
- Link state request (LSR): после обмена пакетами DD, два маршрутизатора знают, какие LSA соседних узлов исчезли из их LSDB. Затем они передают пакет LSR друг другу с запросом о потерянных LSA. Пакет LSA содержит справочную информацию о потерянных LSA.
- Link state update (LSU): передает пакеты LSA о состоянии каналов в ответ на запрос соседнего узла. Каждый пакет LSU может включать в себя несколько пакетов LSA.
- Link state acknowledgment (LSAck): Подтверждает принятые пакеты LSU. Содержит заголовки принятых пакетов LSA (Пакет LSAck может подтвердить несколько пакетов LSA).

**4. Соседние и смежные узлы**

- Соседний: когда маршрутизатор с OSPF включается в работу, он передает пакет Hello через порт с протоколом OSPF, а маршрутизатор, который принимает пакет Hello, проверяет параметры, содержащиеся в пакете. Если параметры в обоих маршрутизаторах совпадают, они становятся соседними.
- Смежный: два соседних OSPF-устройства устанавливают смежные связи для синхронизации своих LSDB. Таким образом, любые два соседних узла без обмена информацией о маршрутизации не могут установить смежность.

**5. Типы LSA**

Пакетами LSA могут обмениваться только смежные маршрутизаторы. Различные типы пакетов LSA описываются сетевой топологией OSPF. Все пакеты LSA записаны в LSDB. Информация, содержащаяся в LSDB, используется для вычисления оптимального маршрута по алгоритму SPF.

- Network LSA (Type 2): возникает на выделенном маршрутизаторе (Designated Router, DR) и заполняет всю генерируемую зону. Этот пакет LSA содержит информацию о состоянии портов всех маршрутизаторов на сегменте сети.
- Network Summary LSA (Type 3): возникает на граничном маршрутизаторе (Area Border Routers, ABR) и распространяется в других зонах. Пакет LSA описывает информацию о маршрутизации в зоне.
- ASBR Summary LSA (Type 4): возникает на граничных маршрутизаторах (ABR) и распространяется в смежных зонах. Пакеты LSA четвёртого типа описывают маршруты в граничном маршрутизаторе автономной системы (Autonomous System Boundary Router, ASBR).
- AS External LSA (Type 5): возникает на маршрутизаторах ASBR, и заполняет всю AS (except stub areas). Каждый пакет LSA 5-го типа описывает маршрут к другому AS.

### 6.13.3.3 Зона и маршрутизатор

1. Разделение зон.

OSPF делит AS на несколько зон, которые идентифицированы посредством ID зон. Области классифицируют маршрутизаторы в сети по нескольким логическим группам, как показано на рисунке 216. Суммарная информация о маршрутизации распределена между зонами.

Зона 0, опорная зона, является основной зоной всей сети OSPF. Все зоны, не являющиеся опорными, должны быть напрямую подключены к опорной зоне. Информация о маршрутизации не опорных зон должна быть направлена посредством опорной зоны.

Чтобы уменьшить размер базы данных топологии, OSPF может разделить определенные зоны на несколько тупиковых зон. 4-й и 5-й типы LSA не допускают тупиковых зон. Чтобы убедиться, что маршруты к другим областям в AS или в другие AS, по-прежнему доступны, ABR генерирует маршрут по умолчанию и рассылает его другим маршрутизаторам в этой зоне.

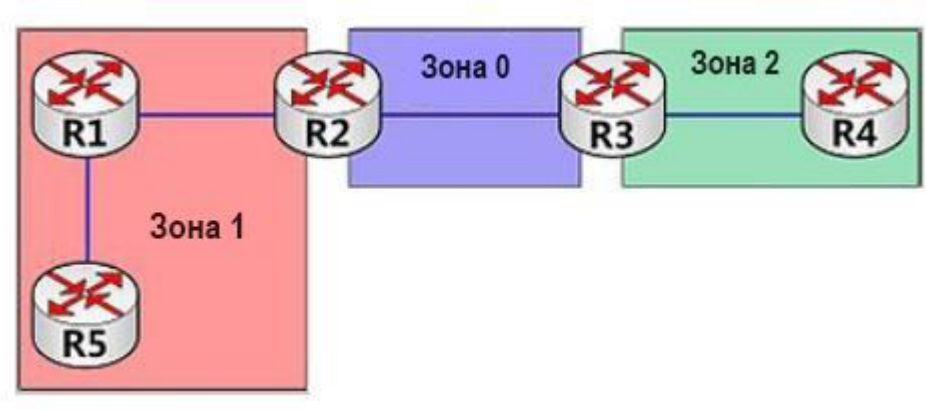



Рисунок 216 – Разделение зон

Разделение зон основано на портах. Таким образом, маршрутизатор с несколькими портами может принадлежать нескольким зонам, но при этом, каждый порт принадлежит

только одной зоне. Если маршрутизатор принадлежит нескольким зонам, он поддерживает LSDB для каждой зоны. Сетевое разделение имеет следующие преимущества:

- Маршрутизаторы в каждой зоне поддерживают только LSDB зоны, но не OSPF всей сети.
- Если топология сети ограничивается зоной, это не влияет на OSPF всей сети, снижая частоту подсчета SPF.
- Ограничивая передачу пакетов LSA к одной зоне, можно сократить данные OSPF.

2. Типы маршрутизаторов.

В зависимости от расположения коммутатора 3-го уровня в AS, он может выполнять роль внутреннего маршрутизатора (internal router), пограничного маршрутизатора (ABR), опорного маршрутизатора (backbone router), или пограничного маршрутизатора автономной системы (ASBR), как показано на рисунке 217.

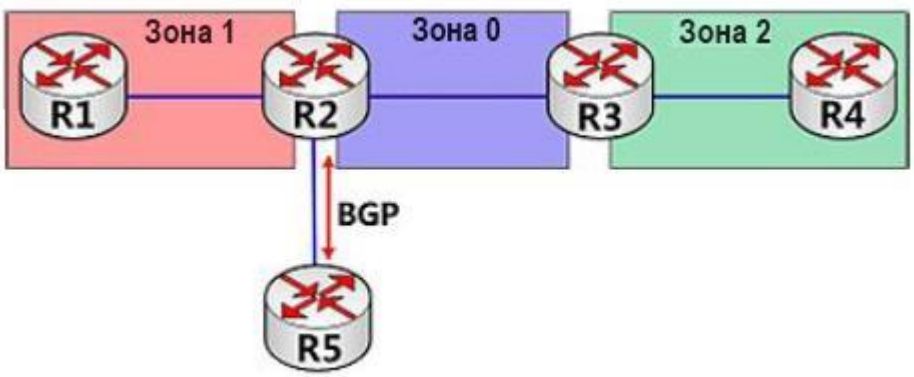



Рисунок 217 – Типы маршрутизаторов OSPF

Внутренний маршрутизатор: маршрутизатор, все порты которого принадлежат одной зоне OSPF.

Пограничный маршрутизатор (ABR) соединяет одну или больше зон с опорной зоной. У маршрутизатора ABR всегда хотя бы один порт принадлежит опорной зоне.

Опорный маршрутизатор (backbone router): маршрутизатор, у которого по крайней мере один порт принадлежит опорной зоне. Все маршрутизаторы ABR и внутренние маршрутизаторы, находящиеся в зоне 0, являются опорными маршрутизаторами.

Пограничный маршрутизатор автономной системы (ASBR): маршрутизатор, который обменивается маршрутной информацией с маршрутизаторами, принадлежащими другой автономной система (AS).

Один маршрутизатор может быть одновременно нескольких типов. Например, R2 на рисунке 217 — это опорный маршрутизатор, ABR и ASBR.

3. Виртуальный канал.

Если зоны, не являющиеся опорными, не могут подключиться к опорной зоне из-за определенных ограничений, виртуальные каналы OSPF могут быть сконфигурированы таким образом, чтобы создать логические связи между ними.

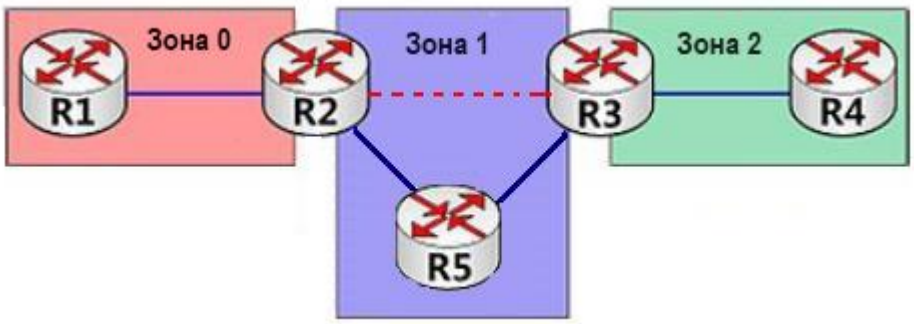



Рисунок 218 – Виртуальный канал

Виртуальный канал, который сконфигурирован на обоих маршрутизаторах ABR, представляет собой логическое соединение, которое устанавливается между двумя маршрутизаторами ABR через зону, не являющуюся опорной. Зона, не являющаяся опорной, называется транзитной зоной. Например, красная пунктирная линия на рисунке 218 — это виртуальный канал, а область 1 — транзитная зона для виртуального канала.

4. Типы маршрутов.
Маршруты OSPF существуют в четырех уровнях приоритета в порядке убывания: Внутренние маршруты зоны (intra-area), маршруты между зонами (inter-area), внешние маршруты 1-го типа (E1) и внешние маршруты 2-го типа (E2). Внутризонные и межзонные маршруты описывают топологию сети автономной системы (AS). Внешние маршруты описывают маршруты к внешним автономным системам (AS)

### 6.13.3.4 Выделенный маршрутизатор и резервный выделенный маршрутизатор

В сетях NBMA (Non Broadcast Multiple Access – нешироковещательные сети со множественным доступом), любые два маршрутизаторы обмениваются маршрутной информацией друг с другом. В результате генерируется много ненужных пакетов LSA. Выделенный маршрутизатор (DR) был применен для решения именно этой проблемы. Все остальные маршрутизаторы устанавливают смежную связь и обмениваются информацией о маршрутизации с DR-маршрутизатором. DR извещает о состоянии каналов сети другие маршрутизаторы. Для предотвращения одиночных, точечных отказов, вызванных неисправностью DR, OSPF определяет резервный выделенный маршрутизатор (BDR). BDR-маршрутизаторы также устанавливают смежную связь с другими маршрутизаторами. BDR является резервной копией DR. Когда DR неисправен, BRD начинает выполнять функции DR. Поскольку с другими маршрутизаторами были установлены смежные связи, отказ DR-маршрутизатора оказывает минимальное влияние на работу сети.

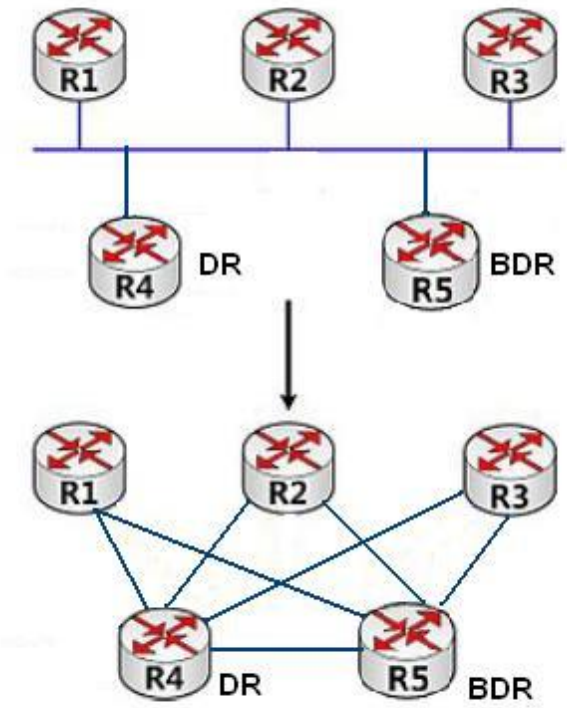



Рисунок 219 – DR и BDR.

Верхняя часть рисунка 219 показывает физические соединения Ethernet, а нижняя — установленные смежные отношения. После принятия DR/BDR для пяти маршрутизаторов требуется только семь смежных связей.

Правила для выбора DR/BDR следующие:

- Маршрутизатор с приоритетом 0 не может стать DR или BDR.
- Маршрутизатор с наивысшим приоритетом сегмента сети становится DR, а маршрутизатор со вторым по значимости после наивысшего становится BDR.
- Если несколько маршрутизаторов имеют одинаковый приоритет, в качестве DR-маршрутизатора выбирается маршрутизатор с наибольшим RID.
- Когда происходит отказ DR-маршрутизатора, BDR-маршрутизатор берёт на себя роль DR-маршрутизатора, при этом другой маршрутизатор будет выбран в качестве BDR.
- Понятие DR основано на портах. Маршрутизатор может быть DR с точки зрения одного порта, либо BDR, либо обычным маршрутизатором с точки зрения другого порта.
- Если маршрутизатор с наивысшим приоритетом добавляется в сети после того, как DR/BDR уже выбраны, он не заменит существующие DR или BDR, чтобы стать новым DR или BDR.

### 6.13.3.5 Настройка с помощью WEB-интерфейса

1. Включение OSPF.

Нажмите [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF process configuration] → [OSPF Enable/Disable], чтобы открыть страницу включения OSPF, как показано на рисунке 220.

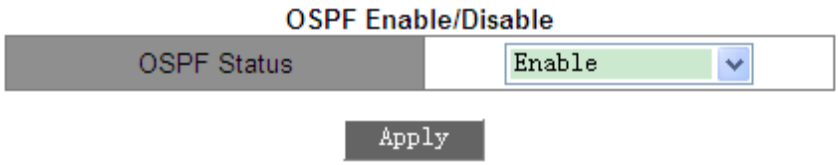



Рисунок 220 – Включение OSPF

**OSPF Status (статус OSPF)**
Варианты: Enable/Disable (включить/выключить).
По умолчанию: Disable (выключить).
Функция: включить или выключить OSPF.

2. Настройка ID маршрутизатора.
Нажмите [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF process configuration] → [Router-ID configuration], чтобы открыть страницу настройки RID, как показано на рисунке 221.

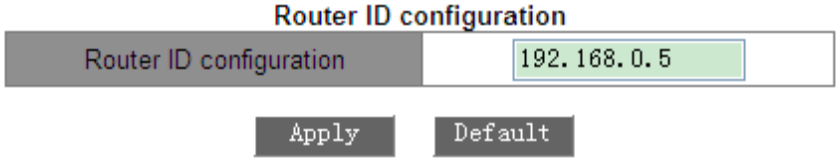



Рисунок 221 – Настройка RID

**Router ID configuration (Настройка ID маршрутизатора)**
Формат: A.B.C.D.
По умолчанию: основной IP адрес порта VLAN с наименьшим ID VLAN на маршрутизаторе.
Функция: настройка ID маршрутизаторов с включенным OSPF. Каждый маршрутизатор с включенным OSPF имеет уникальный ID в AS.

---

Изменение RID вступает в силу только после повторного включения OSPF.

---

3. Настройка сетевого диапазона OSPF.
Нажмите [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF process configuration] → [OSPF network range configuration], чтобы перейти на страницу настройки диапазона сети OSPF, как показано на рисунке 222.

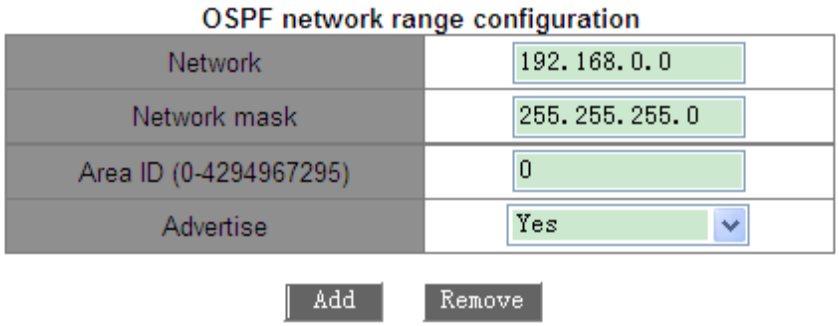



Рисунок 222 – Настройка сетевого диапазона OSPF

**Network (сеть)**
Формат: A.B.C.D.
Функция: настройка IP адреса сети.

**Network mask (маска сети)**
Функция: настройка маски подсети.
Описание: маска сети и IP-адрес определяют сетевой диапазон адресов маршрутизации.

**Area ID (идентификатор зоны)**
Диапазон: 0~4294967295.
Функция: настройка параметра зоны для сетевого диапазона.
Описание: если сетевой диапазон добавлен к вышеупомянутой зоне, все внутренние маршруты сетевого диапазона не объявляются в других зонах.

**Advertise (объявление)**
Варианты: Yes/No (да/нет).
По умолчанию: Yes (да).
Функция: объявлять или нет сводную информацию о маршрутах в заданном сетевом диапазоне.

4. Настройка зоны для порта VLAN.
Нажмите [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF process configuration] → [OSPF area configuration for port (must)], чтобы открыть страницу настройки зоны для интерфейса VLAN, как показано на рисунке 223.

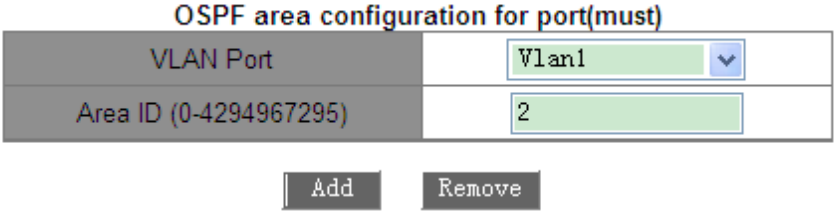



Рисунок 223 – Настройка зоны для порта VLAN

**Area ID (ID зоны)**
Диапазон: 0~4294967295.
Функция: настройка зоны для порта VLAN.
Описание: если порт VLAN добавлен к вышеупомянутой зоне OSPF, OSPF будет включен на порту VLAN.

5. Настройка параметров аутентификации OSPF.
Нажмите [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF TX-parameter configuration] → [OSPF authentication parameter configuration], чтобы открыть страницу настройки аутентификации OSPF, как показано на рисунке 224.

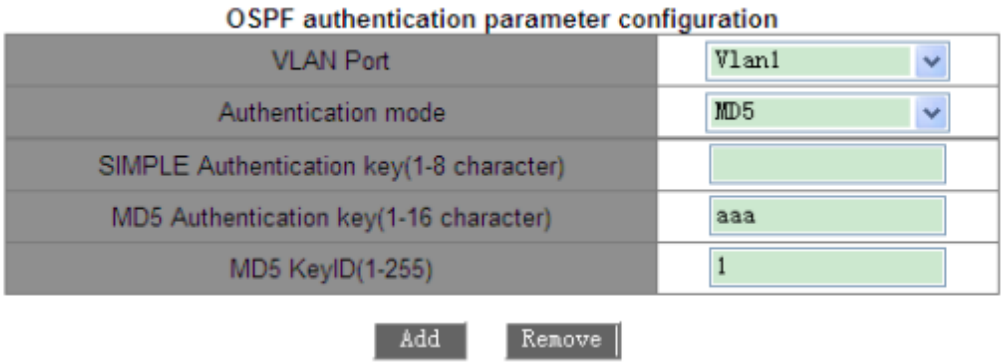



Рисунок 224 – Настройка зоны для порта VLAN

**Authentication mode (режим аутентификации)**
Варианты: SIMPLE/MD5
Функция: настройка режима аутентификации для пакетов OSPF, получаемых на указанный порт.
Описание: SIMPLE подразумевает аутентификацию простым текстом. MD5 подразумевает аутентификацию в зашифрованном режиме.

**SIMPLE Authentication key (аутентификационный ключ SIMPLE)**
Диапазон: 1~8 символов.
Функция: настройка ключа аутентификации для SIMPLE.
Описание: значение этого параметра вступает в силу только при выборе SIMPLE в качестве режима аутентификации.

**MD5 Authentication key (аутентификационный ключ MD5)**
Диапазон: 1~16 символов.
Функция: настройка ключа аутентификации для MD5.
Описание: значение этого параметра вступает в силу только при выборе MD5 в качестве режима аутентификации.

**MD5 Key ID (ID ключа MD5)**

Диапазон: 1~255.
Функция: настройка идентификатора ключа MD5.

---

Для отправки и получения OSPF должным образом, идентичные параметры аутентификации должны быть настроены на обоих концах.

---

6. Настройка режима приема/передачи OSPF для интерфейса VLAN.
Нажмите [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF TX-parameter configuration] → [Passive interface configuration], чтобы открыть страницу настройки режима приёма/передачи OSPF, как показано на рисунке 225.

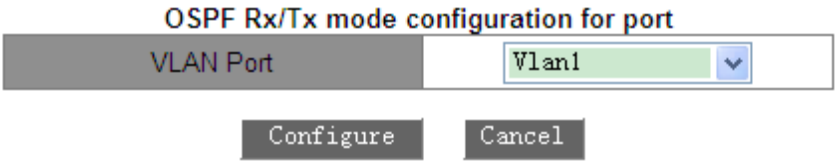



Рисунок 225 – Настройка режима приёма/передачи OSPF для порта VLAN

**VLAN Port (порт VLAN)**
Варианты: порты VLAN, на которых включен OSPF.
Функция: настройка указанного порта VLAN только на прием (но не передачу) OSPF пакетов.
Описание: изначально все порты с включенным OSPF могут передавать и получать OSPF пакеты.

7. Настройка параметров таймера отправки OSPF-пакетов.
Нажмите [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF TX-parameter configuration] → [OSPF packet sending timer configuration], чтобы открыть страницу настройки таймера отправки пакетов, как показано на рисунке 226.

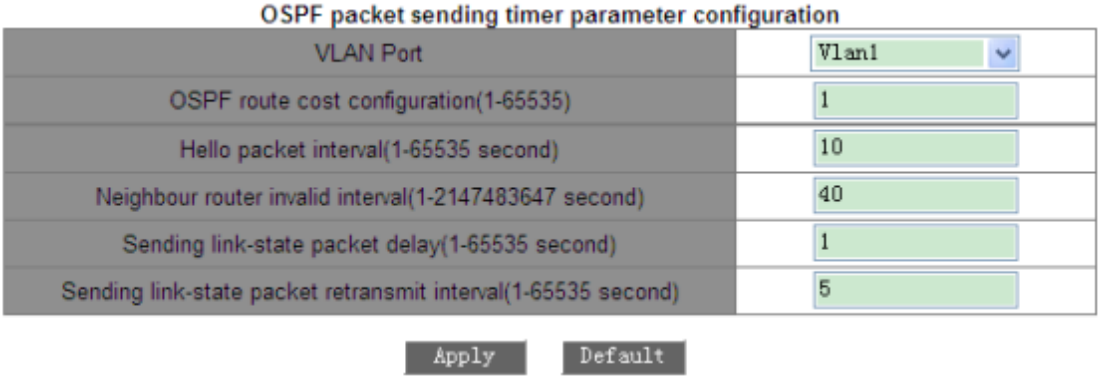



Рисунок 226 – Настройка параметров таймера отправки OSPF-пакетов

**OSPF route cost configuration (настройка стоимости маршрута OSPF)**
Диапазон: 1~65535 с.
Значение по умолчанию: 1 с.
Функция: настройка стоимости маршрута OSPF для указанного порта.

**Hello packet interval (интервал пакета Hello)**
Диапазон: 1~65535 с.
Значение по умолчанию: 10 с.
Функция: настройка интервала передачи пакетов Hello через указанный порт.
Описание: коммутатор периодически посылает пакеты Hello смежным устройствам, чтобы обнаруживать и поддерживать смежные связи, а также осуществлять выбор DR и BDR.

**Neighbour router invalid interval (интервал недоступности соседнего маршрутизатора)**
Диапазон: 1~2147483647 с.
Значение по умолчанию: 40 с.
Функция: настройка временного интервала, по истечении которого смежный коммутатор считается недоступным. Данное значение должно быть больше или равно значению четырех интервалов пакета Hello.
Описание: если коммутатор не получает пакеты Hello от смежного устройства в определенный период, находящееся рядом устройство считается недоступным и нерабочим.

**Sending link-state packet delay (задержка передачи пакета состояния канала)**
Диапазон: 1~65535 с.
Значение по умолчанию: 1 с.
Функция: настройка задержки передачи пакета LSA по определенному порту.

**Sending link-state packet retransmit interval (интервал повторной передачи пакета состояния канала)**
Диапазон: 1~65535 с.
Значение по умолчанию: 5 с.
Функция: настройка интервала для повторной передачи пакета LSA к смежным коммутаторам через указанный порт.
Описание: После отправки пакета LSA к смежному устройству, коммутатор сохраняет пакет LSA, пока не получит подтверждение от смежного устройства. Если коммутатор не получает подтверждение в течение определенного времени, он повторно передает пакет LSA.

---

Для обеспечения нормальной работы OSPF, параметры таймера должны быть идентичны между смежными OSPF.

---

8. Настройка параметров импортирования маршрутов OSPF.

Нажмите [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [Imported route parameter configuration] → [Imported route parameter configuration], чтобы открыть страницу настройки параметров импортирования маршрутов OSPF, как показано на рисунке 227.

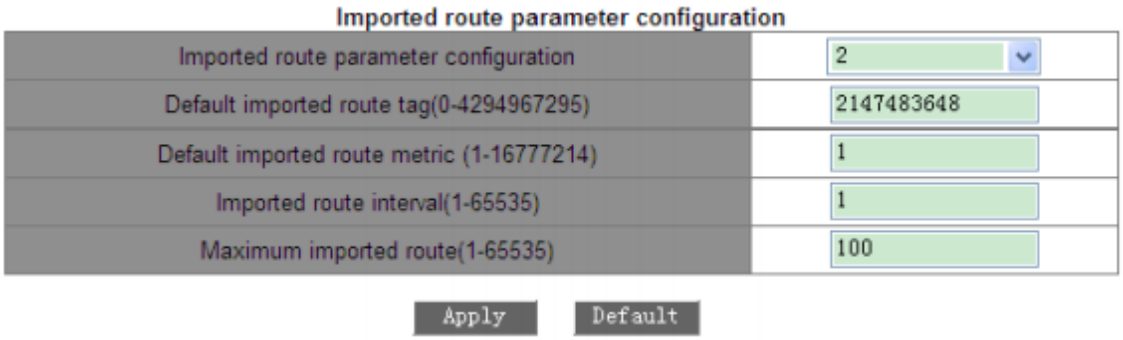



Рисунок 227 – Настройка параметров импортирования маршрутизатора

**Imported route parameter configuration (настройка параметра импортированного маршрута)**
Варианты: 1/2.
Значение по умолчанию: 2.
Функция: настроить тип импортируемых маршрутов по умолчанию.
Описание: значение 1 определяет Тип 1 внешних маршрутов, а значение 2 определяет Тип 2 внешних маршрутов. Стоимость маршрута от маршрутизатора к месту назначения внешнего маршрута Типа 1 будет эквивалентна стоимости маршрута от маршрутизатора к соответствующему ASBR плюс стоимость маршрута от ASBR к месту назначения внешнего маршрута. Стоимость маршрута от внутреннего маршрутизатора к месту назначения внутреннего маршрута Типа 2 будет эквивалентна стоимости маршрута от ASBR к месту назначения внешнего маршрута Типа 2.

**Default imported route tag (значение по умолчанию тега импортированного маршрута)**
Диапазон: 0~4294967295.
Значение по умолчанию: 2147483648.
Функция: настройка тега по умолчанию для импортированного маршрута.
**Default imported route metric (значение по умолчанию метрики импортированного маршрута)**
Диапазон: 1~16777214.
Значение по умолчанию: 1.
Функция: настройка значения стоимости импортированного маршрута по умолчанию.
**Imported route interval (интервал импортированного маршрута)**
Диапазон: 1~65535 с.
Значение по умолчанию: 1 с.
Функция: настройка интервала для импортированных внешних маршрутов. OSPF периодически импортирует информацию о внешних маршрутах и заполняет этой информацией всю AS.

**Maximum imported route (максимальное количество импортированных маршрутов)**
Диапазон: 1~65535.
Значение по умолчанию: 100.
Функция: настройка максимального количества маршрутов, которые могут быть единовременно импортированы OSPF.

9. Настройка импортирования маршрутов на основе других протоколов.
Нажмите [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [Imported route parameter configuration] → [Import external routing information], чтобы открыть страницу настройки импорта внешних маршрутов, как показано на рисунке 228.

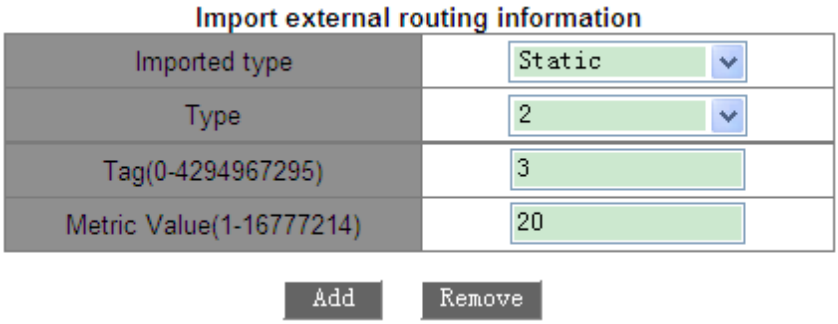



Рисунок 228 – Настройка импортирования маршрутов на основе других протоколов

**Imported type (импортируемый тип)**
Варианты: Static/RIP/Connected/BGP.
Функция: Настройка протокола маршрутизации.
Описание: «Static» указывает на импорт статических маршрутов; «RIP» указывает на импорт маршрутов RIP; «Connected» указывает на импорт маршрутов с прямым подключением; BGP указывает на импорт маршрутов BGP.

**Type (тип)**
Варианты: 1/2.
Функция: настройка типа импортируемых маршрутов.
Описание: 1 указывает на внешние маршруты Типа 1, а 2 указывает на внешние маршруты Типа 2.

**Tag (тег)**
Диапазон: 0~4294967295.
Функция: настройка тега импортированных маршрутов.

**Metric Value (значение метрики)**
Диапазон: 1~16777214.
Функция: настроить значение метрики импортированных маршрутов.

10. Установка приоритетов для протоколов маршрутизации.

Нажмите [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [Other parameter configuration] → [OSPF priority configuration], чтобы открыть страницу настройки приоритета протокола маршрутизации, как показано на рисунке 229.

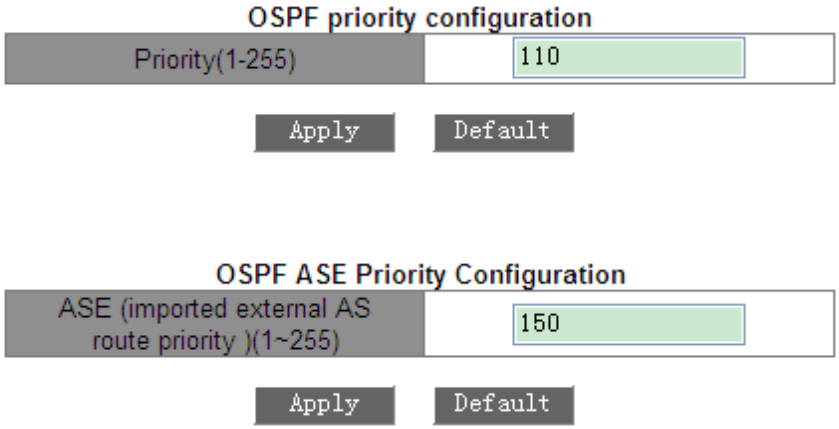



Рисунок 229 – Установка приоритета для протокола маршрутизации

**Priority (приоритет)**
Диапазон: 1~255.
Значение по умолчанию: 110.
Функция: настройка приоритета OSPF.

**ASE (приоритет импортирования внешнего маршрута AS)**
Диапазон: 1~255.
Значение по умолчанию: 150.
Функция: настройка приоритета импортированных маршрутов.
Описание: поскольку на коммутаторах 3-го уровня может быть включено несколько протоколов маршрутизации, важное значение приобретают совместное использование и выбор маршрута. Следовательно, приоритет должен быть установлен для каждого протокола маршрутизации. Если один и тот же маршрут обнаруживается несколькими протоколами маршрутизации, действительным считается протокол с наивысшим приоритетом (наименьшее число значения).

11. Настройка тупиковой зоны.
Нажмите [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [Other parameter configuration] → [OSPF STUB area and default route cost], чтобы открыть страницу тупиковой зоны, как показано на рисунке 230.

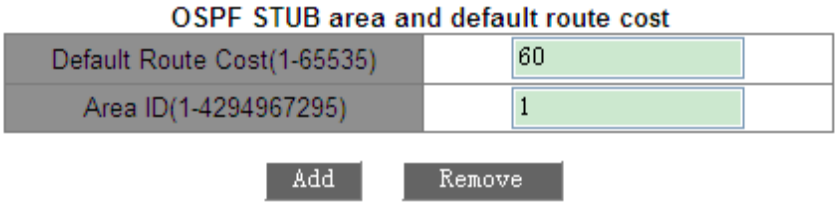



Рисунок 230 – Настройка тупиковой зоны

**Default Route Cost (стоимость маршрута по умолчанию)**
Диапазон: 1~65535.
Функция: настройка стоимости маршрута по умолчанию для тупиковой зоны.
**Area ID (идентификатор зоны)**
Диапазон: 1~4294967295.
Функция: настройка указанной зоны в качестве тупиковой.

---

Опорная зона, обозначенная как 0, не может быть настроена в качестве тупиковой.

---

12. Настройка виртуального канала OSPF.
Нажмите [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [Other parameter configuration] → [OSPF virtual link configuration], чтобы открыть страницу настройки виртуального канала OSPF, как показано на рисунке 231.

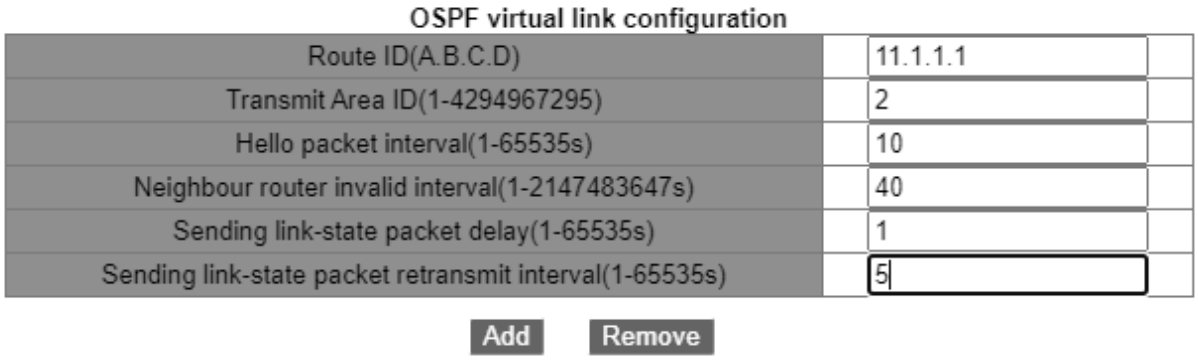



Рисунок 231 – Настройка виртуального канала OSPF

**Route ID (идентификатор маршрута)**
Формат: A.B.C.D.
Функция: настройка идентификатора (RID) для оконечного пира виртуального канала.

**Transit Area ID (идентификатор транзитной зоны)**
Диапазон: 1~4294967295.
Функция: указать значение транзитной зоны для виртуального канала.

**Hello packet interval (интервал пакета Hello)**
Диапазон: 1~65535 с.
По умолчанию: 10 с.
Функция: настройка интервала для передачи пакета Hello через указанный порт.
Описание: коммутатор периодически посылает пакеты Hello смежным устройствам, чтобы обнаруживать и поддерживать смежные связи, а также осуществлять выбор DR и BDR.

**Neighbour router invalid interval (интервал недоступности соседнего маршрутизатора)**
Диапазон: 1~2147483647 с.
По умолчанию: 40 с.
Функция: Настройка временного интервала, по истечении которого смежный коммутатор считается недоступным. Данное значение должно быть больше или равно значению четырех интервалов пакета Hello.
Описание: если коммутатор не получает пакеты Hello от смежного устройства в определенный период, находящееся рядом устройство считается недоступным и нерабочим.

**Sending link-state packet delay (задержка передачи пакета состояния канала)**
Диапазон: 1~65535 с.
По умолчанию: 1 с.
Функция: настройка задержки передачи пакетов LSA через указанный порт.

**Sending link-state packet retransmit interval (интервал повторной передачи пакета состояния канала)**
Диапазон: 1~65535 с.
По умолчанию: 5 с.
Функция: Настройка интервала для повторной передачи пакета LSA к смежным коммутаторам через указанный порт.
Описание: после отправки пакета LSA к смежному устройству, коммутатор сохраняет пакет LSA, пока не получит подтверждение от смежного устройства. Если коммутатор не получает подтверждение в течение определенного времени, он повторно передает пакет LSA.

Настройки параметров на обоих сторонах виртуального канала должны быть эквивалентны.

13. Настройка приоритета порта VLAN.
Нажмите [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [Other parameter configuration] → [Port DR priority configuration], чтобы открыть страницу настройки приоритета интерфейса VLAN, как показано на рисунке 232.

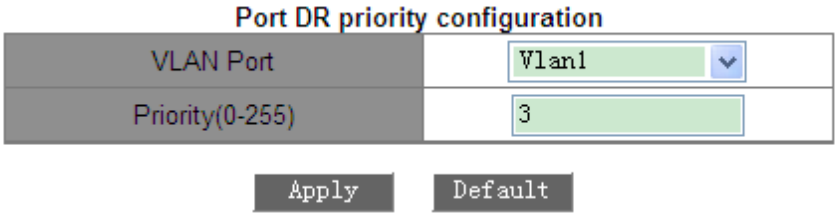



Рисунок 232 – Настройка приоритета порта VLAN

**Priority (приоритет)**
Диапазон: 0~255.
Значение по умолчанию: 1.
Функция: настройка приоритета порта VLAN с включенным OSPF.
Описание: в процессе выбора DR или BDR, коммутатор с наивысшим значением этого параметра будет указан как DR.

14. Просмотр информации OSPF.
Нажмите [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF debug] → [show ip ospf], чтобы открыть страницу информации OSPF, как показано на рисунке 233.

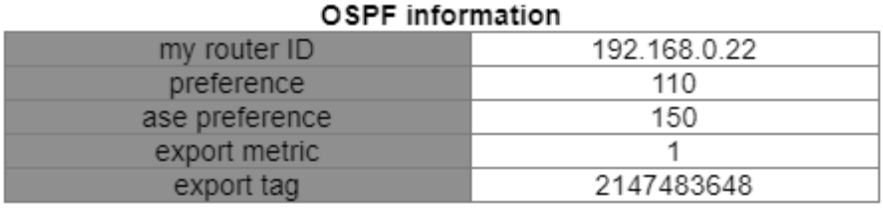



Рисунок 233 – Информация OSPF

15. Просмотр информации о внешних маршрутах OSPF.
Нажмите [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF debug] → [show ip ospf ase], чтобы открыть страницу информации о внешнем маршруте OSPF, как показано на рисунке 234.

**OSPF Imported External AS Route Information**

| Destination | AdvRouter | NextHop | Age | SeqNumber | Type | Cost |
|---|---|---|---|---|---|---|
| 7.7.7.0 | 2.2.2.2 | 2.2.2.3 | 1145 | -2147483506 | DTYPE_ASBR | 1 |

Рисунок 234 – Информация OSPF о внешнем импортированном маршруте

16. Просмотр статистики OSPF.
Нажмите [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF debug] → [show ip ospf cumulative], чтобы открыть страницу статистики OSPF, как показано на рисунке 235.

**OSPF Cumulative information**

| Type | In | Out |
|---|---|---|
| HELLO | 23674 | 23823 |
| DD | 19 | 22 |
| LS Req | 8 | 6 |
| LS Update | 1394 | 548 |
| LS Ack | 406 | 970 |
| ASE count | 1 | checksum 7938 |

Рисунок 235 – Статистика OSPF

17. Просмотр информации базы данных OSPF
Нажмите [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF debug] → [show ip ospf database], чтобы открыть страницу базы данных OSPF, как показано на рисунке 236.

**OSPF database information**

**AREA 0**

| Router LSAs | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| LS ID(Router ID) | ADV rtr | Age | Sequence | Cost | Checksum | | | | |
| 2.2.2.2 | 2.2.2.2 | 331 | 0x800001ea | 1 | 49246 | Type : Transit net | Cost : 1 | DR : 2.2.2.2 | Address: 2.2.2.2 |
| | | | | | | Type : Virtual link | Cost : 1 | RouterID : 3.3.3.3 | Address: 3.3.3.1 |
| 1.1.1.1 | 1.1.1.1 | 340 | 0x80000228 | 0 | 59435 | Type : Transit net | Cost : 1 | DR : 2.2.2.2 | Address: 2.2.2.1 |
| 3.3.3.3 | 3.3.3.3 | 330 | 0x80000231 | 2 | 36454 | Type : Virtual link | Cost : 1 | RouterID : 2.2.2.2 | Address: 3.3.3.2 |

| Network LSAs | | | | | |
|---|---|---|---|---|---|
| LS ID(DR's IP) | ADV rtr | Age | Sequence | Cost | Checksum |
| 2.2.2.2 | 2.2.2.2 | 336 | 0x800000c0 | 1 | 64898 |

| Summary Network LSAs | | | | | |
|---|---|---|---|---|---|
| LS ID(Net's IP) | ADV rtr | Age | Sequence | Cost | Checksum |
| 20.1.1.0 | 1.1.1.1 | 521 | 0x80000178 | 65535 | 26468 |
| 5.5.5.0 | 3.3.3.3 | 333 | 0x80000006 | 4 | 33976 |
| 4.4.4.255 | 3.3.3.3 | 416 | 0x8000021e | 3 | 26814 |
| 3.3.3.0 | 3.3.3.3 | 333 | 0x80000119 | 3 | 39318 |
| 3.3.3.0 | 2.2.2.2 | 336 | 0x800001ef | 2 | 2643 |

| ASBR Summary LSAs | | | | | |
|---|---|---|---|---|---|
| LS ID(Net's IP) | ADV rtr | Age | Sequence | Cost | Checksum |

**AREA 4**

| Router LSAs | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| LS ID(Router ID) | ADV rtr | Age | Sequence | Cost | Checksum | | | | |
| 1.1.1.1 | 1.1.1.1 | 746 | 0x8000010e | 0 | 13044 | Type : Stub net | Cost : 1 | Network : 20.1.1.0 | NetMask: 255.255.255.0 |

| Network LSAs | | | | | |
|---|---|---|---|---|---|
| LS ID(Router ID) | ADV rtr | Age | Sequence | Cost | Checksum |

| Summary Network LSAs | | | | | |
|---|---|---|---|---|---|
| LS ID(Net's IP) | ADV rtr | Age | Sequence | Cost | Checksum |
| 5.5.5.0 | 1.1.1.1 | 319 | 0x80000001 | 65535 | 56937 |
| 2.2.2.255 | 1.1.1.1 | 319 | 0x80000007 | 65535 | 8493 |
| 4.4.4.255 | 1.1.1.1 | 319 | 0x80000001 | 65535 | 63571 |
| 3.3.3.0 | 1.1.1.1 | 319 | 0x80000003 | 65535 | 3903 |

| ASBR Summary LSAs | | | | | |
|---|---|---|---|---|---|
| LS ID(ASBR's Rtr ID) | ADV rtr | Age | Sequence | Cost | Checksum |
| 2.2.2.2 | 1.1.1.1 | 335 | 0x80000001 | 65535 | 2886 |

| AS External LSAs | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| LS ID(ASBR's Rtr ID) | ADV rtr | Age | Sequence | Cost | Checksum | Is_type | metric | ese_type | forward | tag |

Рисунок 236 – База данных OSPF

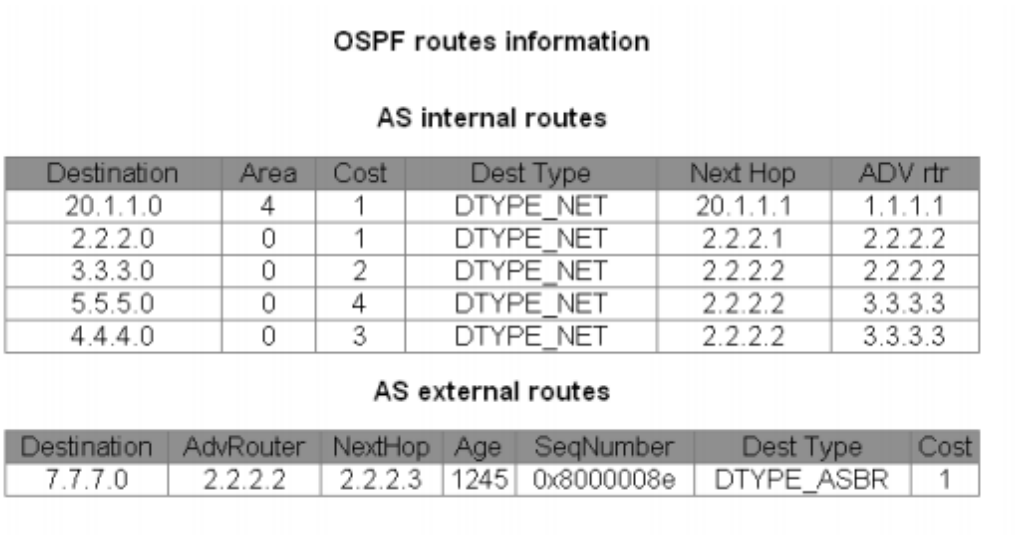
18. Просмотр информации о соседних OSPF-устройствах.
Нажмите [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF debug] → [show ip ospf neighbor], чтобы открыть страницу информации о смежном узле OSPF, как показано на рисунке 237.

**OSPF Neighbor**

| interface p :20.1.1.1 | | | | | | |
|---|---|---|---|---|---|---|
| neighbor: area | router id | router IP | state | priority | DR | BDR |
| interface ip :2.2.2.1 | | | | | | |
| neighbor: area | router id | router IP | state | priority | DR | BDR |
| 0 | 2.2.2.2 | 2.2.2.2 | NFULL | 1 | 2.2.2.2 | 2.2.2.1 |

Рисунок 237 – Информация о смежном узле OSPF

19. Просмотр информации о маршрутизации OSPF.
Нажмите [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [OSPF debug] → [show ip ospf routing], чтобы открыть страницу информации о маршрутизации OSPF, как показано на рисунке 238.



OSPF routes information

AS internal routes

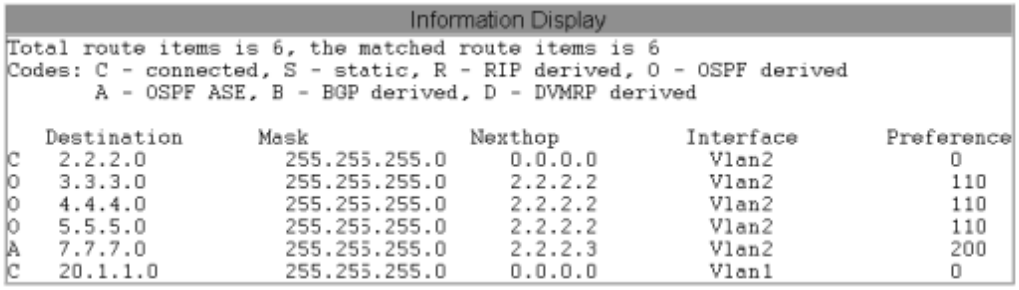
| Destination | Area | Cost | Dest Type | Next Hop | ADV rtr |
|---|---|---|---|---|---|
| 20.1.1.0 | 4 | 1 | DTYPE_NET | 20.1.1.1 | 1.1.1.1 |
| 2.2.2.0 | 0 | 1 | DTYPE_NET | 2.2.2.1 | 2.2.2.2 |
| 3.3.3.0 | 0 | 2 | DTYPE_NET | 2.2.2.2 | 2.2.2.2 |
| 5.5.5.0 | 0 | 4 | DTYPE_NET | 2.2.2.2 | 3.3.3.3 |
|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

AS external routes

| Destination | AdvRouter | NextHop | Age | SeqNumber | Dest Type | Cost |
|---|---|---|---|---|---|---|
| 7.7.7.0 | 2.2.2.2 | 2.2.2.3 | 1245 | 0x8000008e | DTYPE_ASBR | 1 |

Рисунок 238 – Информация о маршрутах OSPF

20. Просмотр записей маршрутов.
Нажмите [Device Advanced Configuration] → [Route configuration] → [OSPF configuration] → [show ip route], чтобы открыть страницу информации о маршрутизации, как показано на рисунке 239.



Information Display

```
Total route items is 6, the matched route items is 6
Codes: C - connected, S - static, R - RIP derived, O - OSPF derived
       A - OSPF ASE, B - BGP derived, D - DVMRP derived

   Destination       Mask             Nexthop          Interface        Preference
C    2.2.2.0          255.255.255.0      0.0.0.0          Vlan2              0
O    3.3.3.0          255.255.255.0      2.2.2.2          Vlan2              110
O    4.4.4.0          255.255.255.0      2.2.2.2          Vlan2              110
O    5.5.5.0          255.255.255.0      2.2.2.2          Vlan2              110
A    7.7.7.0          255.255.255.0      2.2.2.3          Vlan2              200
C    20.1.1.0         255.255.255.0      0.0.0.0          Vlan1              0
```

Рисунок 239 – Таблица маршрутизации

### 6.13.3.5 Пример типовой настройки

Необходимо включить OSPF на всех коммутаторах и разделить всю AS на три области. Зона 2 не связана напрямую с зоной 0. Требуется виртуальный канал между маршрутизаторами R2 и R3. В качестве транзитной зоны, зона 1 соединяет зону 2 с зоной 0. Маршрутизаторы R2 и R3 служат в качестве ABR для пересылки информации о маршрутах между зонами (inter-area).

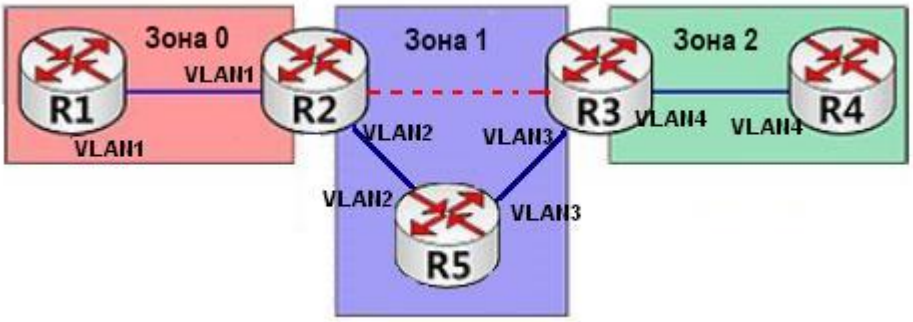



Рисунок 240 – Пример типовой настройки OSPF

**Настройки маршрутизатора R1:**

1. Установите IP-адрес интерфейса VLAN1 192.168.1.1 и маску подсети 255.255.255.0.
2. Установите для RID значение 192.168.1.1, как показано на рисунке 221.
3. Включите OSPF, как показано на рисунке 220.
4. Настройте диапазон сети. Установите IP-адрес сети 192.168.1.0, маску 255.255.255.0, идентификатор зоны 0 и объявление «Yes», как показано на рисунке 222.
5. Добавьте интерфейс VLAN1 в зону 0, как показано на рисунке 223.

**Настройки маршрутизатора R2:**

1. Установите IP-адрес для интерфейса VLAN1 192.168.1.2 и маску подсети 255.255.255.0, а для VLAN2 – 192.168.2.1 и 255.255.255.0.
2. Установите для RID значение 192.168.1.2, как показано на рисунке 221.
3. Включите OSPF, как показано на рисунке 220.
4. Настройте диапазон сети. Установите IP-адрес сети 192.168.1.0, маску 255.255.255.0, идентификатор зоны 0 и объявление «Yes». Установите IP-адрес сети 192.168.2.0, маску 255.255.255.0, идентификатор зоны 1 и объявление «Yes», как показано на рисунке 222.
5. Добавьте интерфейс VLAN1 в зону 0 и VLAN2 в зону 1, как показано на рисунке 223.
6. Настройте виртуальный канал. Установите идентификатор RID 192.168.3.2, идентификатор транзитной зоны 1 и оставьте значения по умолчанию для других параметров, как показано на рисунке 231.

**Настройки маршрутизатора R3:**

1. Установите IP-адрес для интерфейса VLAN3 192.168.3.2 и маску подсети 255.255.255.0, а для VLAN4 – 192.168.4.1 и 255.255.255.0.
2. Установите для RID значение 192.168.3.2, как показано на рисунке 221.
3. Включите OSPF, как показано на рисунке 220.
4. Настройте диапазон сети. Установите IP-адрес сети 192.168.3.0, маску 255.255.255.0, идентификатор зоны 1 и объявление «Yes». Установите IP-адрес сети 192.168.4.0, маску 255.255.255.0, идентификатор зоны 2 и объявление «Yes», как показано на рисунке 222.
5. Добавьте интерфейс VLAN3 в зону 1 и VLAN4 в зону 2, как показано на рисунке 223.
6. Настройте виртуальный канал. Установите идентификатор RID 192.168.1.2, идентификатор транзитной зоны 1 и оставьте значения по умолчанию для других параметров, как показано на рисунке 231.

**Настройки маршрутизатора R4:**

1. Установите IP-адрес для интерфейса VLAN4 192.168.4.2 и маску подсети 255.255.255.0.
2. Установите для RID значение 192.168.4.2, как показано на рисунке 221.
3. Включите OSPF, как показано на рисунке 220.
4. Настройте диапазон сети. Установите IP-адрес сети 192.168.4.0, маску 255.255.255.0, идентификатор зоны 2 и объявление «Yes», как показано на рисунке 222.
5. Добавьте интерфейс VLAN4 в зону 2, как показано на рисунке 223.

**Настройки маршрутизатора R5:**

1. Установите IP-адрес для интерфейса VLAN2 192.168.2.2 и маску подсети 255.255.255.0, а для VLAN3 – 192.168.3.1 и 255.255.255.0.
2. Установите для RID значение 192.168.2.2, как показано на рисунке 221.
3. Включите OSPF, как показано на рисунке 220.
4. Настройте диапазон сети. Установите IP-адрес сети 192.168.2.0, маску 255.255.255.0, идентификатор зоны 1 и объявление «Yes». Установите IP-адрес сети 192.168.3.0, маску 255.255.255.0, идентификатор зоны 1 и объявление «Yes», как показано на рисунке 222.
5. Добавьте интерфейс VLAN2 в зону 1 и VLAN3 в зону 1, как показано на рисунке 223.

## 6.14 DHCP

В связи с постоянным увеличением масштаба сети и ростом её сложности, в условиях частого перемещения компьютеров (таких как ноутбуки или устройства с беспроводным подключением), а также ввиду того, что число компьютеров значительно превышает выделяемые для них IP-адреса, протокол BootP, предназначенный для статической конфигурации хоста, всё чаще становится неспособным удовлетворить существующие потребности. Для быстрого доступа в сеть, выхода из сети и улучшения коэффициента использования ресурсов IP-адресов было необходимо разработать автоматический механизм распределения IP-адресов на основе протокола BootP, в результате чего был представлен протокол DHCP (протокол динамической конфигурации хоста).

Данный протокол работает по модели «клиент-сервер». На этапе конфигурации клиент обращается к серверу, который в ответ сообщает необходимые параметры настроек, такие как IP-адрес, использую динамическую конфигурацию IP-адресов. На рисунке 241 показана типичная структура применения DHCP-протокола.

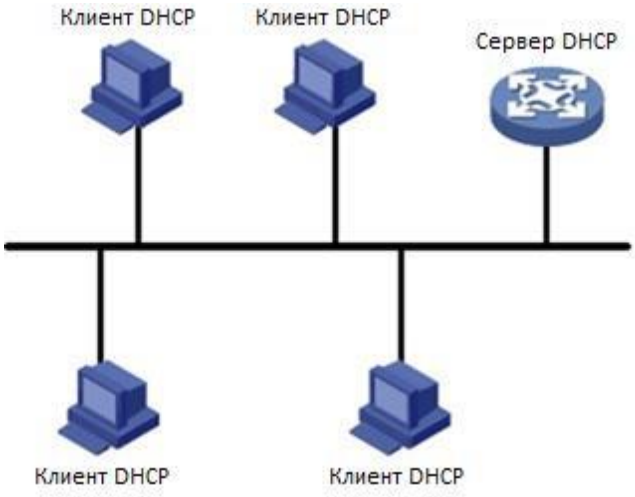



Рисунок 241 – Типовая схема DHCP

---

В процессе динамического распределения IP-адресов происходит отправка широковещательного сообщения, поэтому необходимо, чтобы DHCP-клиент и DHCP-сервер находились в одном сегменте. Если они находятся в разных сегментах, чтобы получить IP-адрес и другие параметры конфигурации, клиент может связаться с сервером через ретранслятор DHCP-протокола.

---

Протокол DHCP поддерживает два механизма распределения IP-адресов. Статическое распределение: сетевой администратор статично привязывает фиксированные IP-адреса к нескольким конкретным клиентам, таким как, например, WWW-сервер, и отсылает привязанные IP-адреса клиентам через протокол DHCP. Динамическое распределение: DHCP-сервер производит динамическую раздачу IP-адреса клиенту. Этот механизм распределения может назначить постоянный IP-адрес или IP-адрес с ограниченным сроком пользования для клиента. Когда время аренды адреса истекает, клиент должен повторно запросить IP-адрес. Сетевой администратор может выбирать для каждого клиента свой механизм распределения по протоколу DHCP.

## 6.14.1 Настройка сервера DHCP

### 6.14.1.1 Введение

DHCP-сервер – это поставщик услуг DHCP-протокола. Он использует DHCP-сообщения для связи с DHCP-клиентом, чтобы выделить подходящий IP-адрес и при необходимости сообщить другие сетевые параметры. DHCP-сервер обычно используется для выделения IP-адресов в следующих случаях:

- большой масштаб сети. При ручном распределении рабочая нагрузка возрастает и управлять всей сетью становится трудно;
- количество хостов превышает число распределяемых IP-адресов, отчего становится невозможно выделить фиксированный IP-адрес каждому хосту;
- только несколько хостов в сети нуждаются в фиксированных IP-адресах.

### 6.14.1.2 Пул адресов DHCP

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

1. IP-адрес статически привязывается к MAC-адресу клиента;
2. IP-адрес, записанный на DHCP-сервере, который когда-либо был выделен клиенту;
3. IP-адрес, указанный в сообщении запроса клиента;
4. Первый выделяемый IP-адрес, найденный в пуле адресов;
5. Если доступный IP-адрес отсутствует, необходимо проверить IP-адрес, срок аренды которого истекает и у которого был конфликт. Если такой IP-адрес найден, происходит его выделение, если IP-адрес не найден, подключение отсутствует.

### 6.14.1.3 Настройка с помощью WEB-интерфейса

1. Включение DHCP-сервера.
Нажмите [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Enable DHCP], чтобы включить сервер DHCP, как показано на рисунке 242.

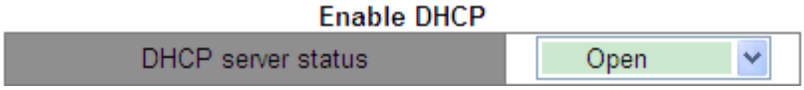



Рисунок 242 – Включение DHCP-сервера

**DHCP server status (состояние DHCP-сервера)**
Опция: Open/Close (открыть/закрыть).
По умолчанию: Close (закрыть).
Функция: выбор данного коммутатора в качестве сервера DHCP для назначения клиенту IP адреса.

2. Назначение статического IP-адреса.
Нажмите [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Address pool configuration], чтобы создать пул адресов DHCP, как показано на рисунке 243.

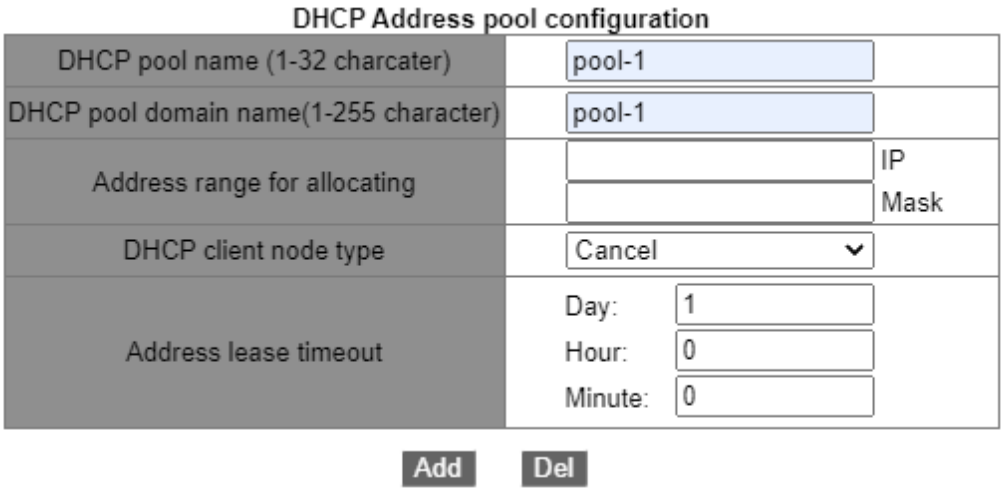



Рисунок 243 – Создание пула адресов

**DHCP pool name (имя пула DHCP)**
Диапазон: 1~32 символа.
Функция: настроить имя пула IP-адресов.

**DHCP pool domain name (доменное имя пула DHCP)**
Диапазон: 1~255 символов.
Функция: настроить доменное имя пула IP-адресов. При назначении IP-адреса клиенту необходимо также отправить ему суффикс доменного имени.

**Address lease timeout (срок аренды адреса)**
Диапазон: 0 дней 0 часов 0 минут ~ 365 дней 23 часов 59 минут.
Описание: срок аренды статического адреса бесконечен. Поэтому настройка этого параметра недопустима для статического распределения.

---

- Статическое выделение IP-адреса можно рассматривать как получение IP-адреса из специального пула адресов, который содержит только один конкретный IP-адрес. Следовательно, пул адресов DHCP должен быть создан до статического выделения IP-адреса.
- Для каждого пула адресов DHCP можно настроить только один тип механизма распределения IP-адресов.

---

Нажмите [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Manual address pool configuration], чтобы открыть страницу настройки статического распределения, как показано на рисунке 244.

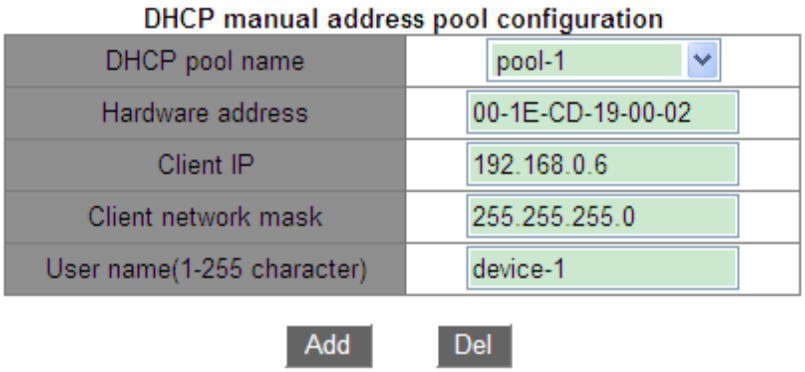



Рисунок 244 – Статическое распределение IP-адресов

**DHCP pool name (имя пула DHCP)**
Функция: выбрать имя созданного пула.

**Hardware address (аппаратный адрес)**
Формат: HH-HH-HH-HH-HH-HH (H — шестнадцатеричное число).
Функция: настройка MAC-адреса клиента со статическим ограничением.

**Client IP (IP-адрес клиента)**
Формат: A.B.C.D.
Функция: настройка IP-адреса клиента со статическим ограничением.
Описание: распределение статических IP-адресов реализуется путем привязки IP-адреса к MAC-адресу клиента. Когда клиент с этим MAC-адресом запрашивает IP-адрес, DHCP-сервер находит IP-адрес, соответствующий данному MAC-адресу, и выделяет его клиенту. Приоритет этого режима распределения выше, чем при динамическом распределении IP-адресов, а срок аренды является постоянным.

**Client network mask (сетевая маска клиента)**
Маска подсети представляет собой число длиной 32 бита, состоящее из единиц и нулей. «1» соответствует полям номера сети и подсети, в то время как «0» соответствует полям номера хоста. Обычно маска настраивается как 255.255.255.0.

**User name (имя пользователя)**
Диапазон: 1~255 символов.
Функция: настройка имени пользователя клиента.

3. Динамическое выделение IP-адреса.
Нажмите [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Address pool configuration], чтобы открыть страницу настройки динамического распределения, как показано на рисунке 245.

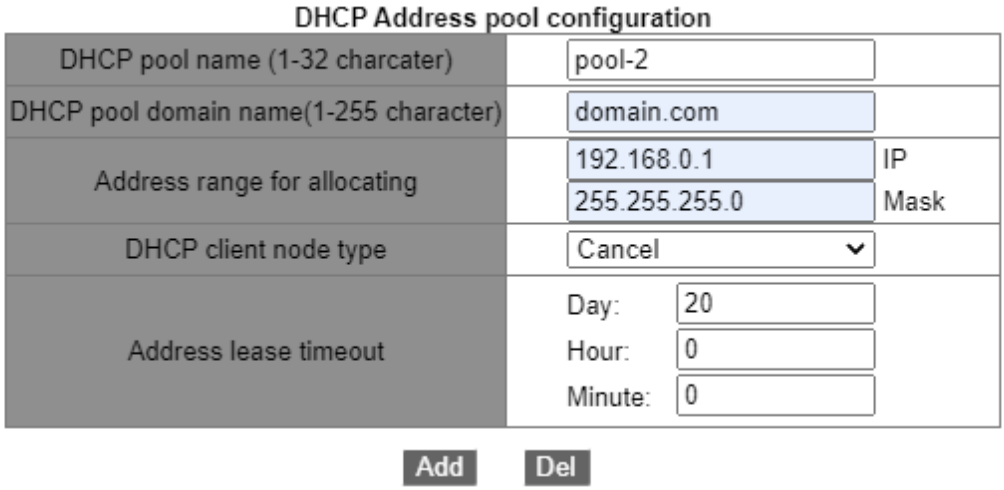



Рисунок 245 – Динамическое распределение IP-адресов

**DHCP pool name (имя пула DHCP)**
Диапазон: 1~32 символа.
Функция: настроить имя пула IP-адресов.

**DHCP pool domain name (доменное имя пула DHCP)**
Диапазон: 1~255 символов.
Функция: настроить доменное имя пула IP-адресов. При назначении IP-адреса клиенту необходимо также отправить ему суффикс доменного имени.

**Address range of allocating {IP, MASK} (диапазон распределяемых адресов)**
Функция: настройка диапазона пула IP-адресов, определяемого маской подсети. Маска подсети представляет собой число длиной 32 бита, состоящее из единиц и нулей. «1» соответствует полям номера сети и подсети, в то время как «0» соответствует полям номера хоста. Обычно маска настраивается как 255.255.255.0.

В каждом пуле могут быть настроены адреса только из одного сетевого сегмента.

**DHCP client node type (тип клиентского узла DHCP)**
Варианты: Cancel/Broadcast node/Peer-to-peer node/Mixed node/Hybrid node.
Значение по умолчанию: Cancel (отмена).
Функции: настройка типа клиентского узла NetBIOS. Когда DHCP-клиент использует протокол NetBIOS для связи в сети, необходимо установить соответствие между именем хоста и IP-адресом. Различные типы узлов реализуют сопоставление в разных режимах.
Описание: Broadcast node использует широковещательные запросы на регистрацию и разрешение имен NetBIOS. Peer-to-peer node отправляет одноадресный пакет для связи с WINS-сервером. Mixed node сначала отправляет широковещательный пакет. Если Mixed node не может получить ответ сразу, он отправляет одноадресный пакет для связи с WINS-сервером. Hybrid node сначала отправляет одноадресный пакет для связи с WINS-

сервером. Если Hybrid node не может разрешить имя с помощью сервера имен NetBIOS, он использует широковещание.

**Address lease timeout (Срок аренды адреса)**
Диапазон: 0 дней 0 часов 0 минут ~ 365 дней 23 часов 59 минут.
Описание: настройка времени аренды динамического адреса. Для разных пулов адресов сервер DHCP может установить разное время аренды адреса, но адреса в одном пуле всегда имеют одинаковое время аренды.

4. Настройка шлюза DHCP-клиента.
Нажмите [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Default Gateway Configuration], чтобы открыть страницу настройки шлюза DHCP-клиента, как показано на рисунке 246.

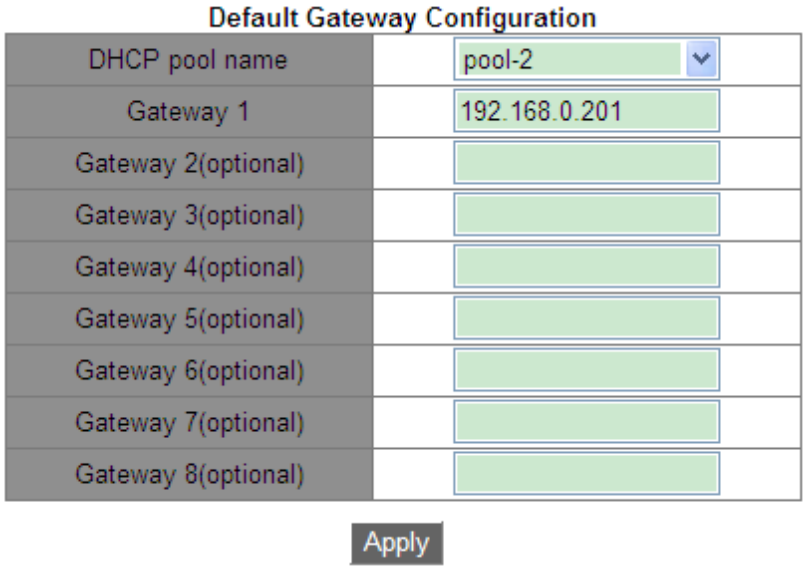



Рисунок 246 – Настройка шлюза DHCP-клиента

**DHCP pool name (имя пула DHCP)**
Функция: выбор созданного имени пула IP-адресов.

**Gateway 1~Gateway 8 (шлюз 1~шлюз 8)**
Функция: настройка адреса клиентского шлюза, выделяемого DHCP-сервером.
Пояснение: когда DHCP-клиент посещает хост, находящийся в другом сегменте, данные должны пересылаться через шлюзы. Выделяя IP-адреса клиентам, DHCP-сервер может одновременно указывать адреса шлюза. Пул адресов DHCP может настроить до восьми шлюзов. Шлюз 1 имеет наивысший приоритет, а шлюз 8 — наименьший.

5. Настройка DNS-сервера DHCP-клиента.
Нажмите [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Client DNS server configuration], чтобы открыть страницу настройки клиентского DNS-сервера, как показано на рисунке 247.

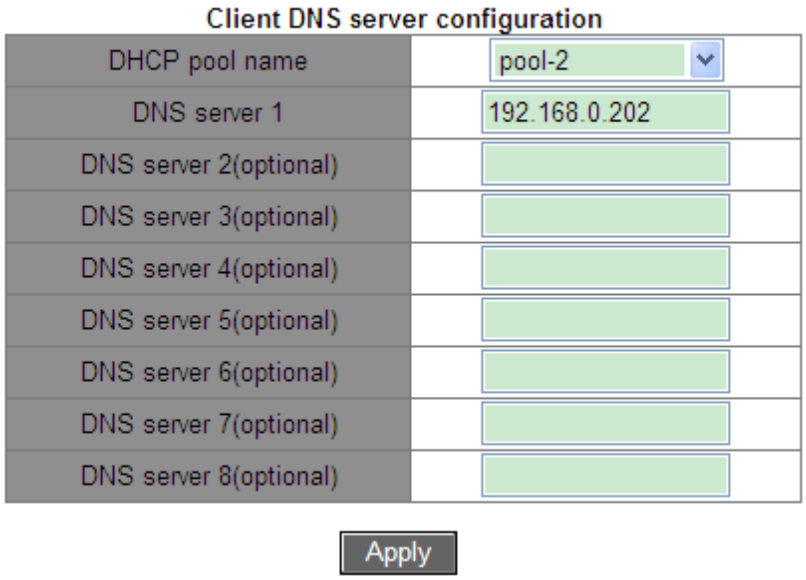



Рисунок 247 – DNS-сервера DHCP-клиента

**DHCP pool name (имя пула DHCP)**
Функция: выбор созданного имени пула IP-адресов.

**DNS server 1~DNS server 8 (DNS-сервер 1~DNS-сервер 8)**
Функция: настройка адреса клиентского DNS-сервера, назначаемого DHCP-сервером.
Пояснение: при посещении сетевого узла через доменное имя, доменное имя должно быть преобразовано в IP-адрес. Это преобразование реализуется при помощи DNS (система доменных имен). Чтобы DHCP-клиент мог посещать сетевой хост через доменное имя, выделяя IP-адреса клиентам, DHCP-сервер может одновременно указывать IP-адреса серверов доменных имен. Пул адресов DHCP может настроить до восьми DNS-серверов. DNS-сервер 1 имеет наивысший приоритет, а DNS-сервер 8 — наименьший.

6. Настройка WINS-сервера DHCP-клиента.
Нажмите [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Client WINS server configuration], чтобы открыть страницу настройки WINS-сервера DHCP-клиента, как показано на рисунке 248.

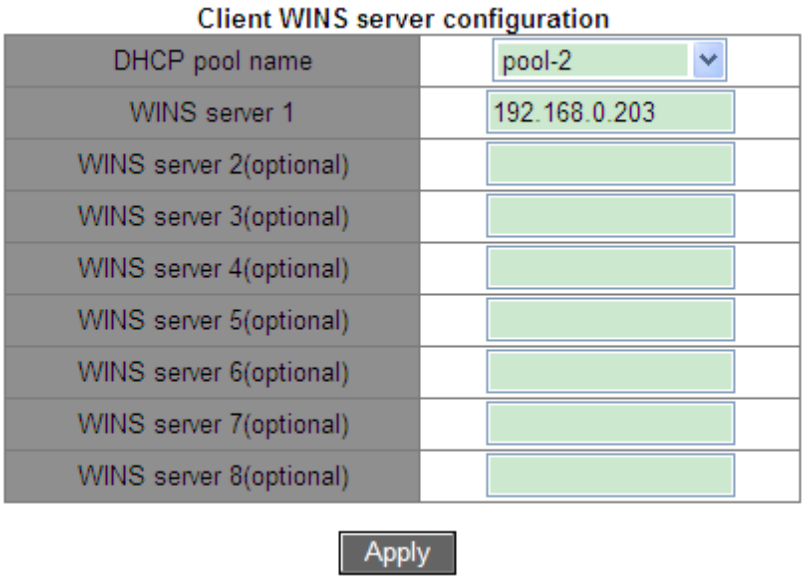



Рисунок 248 – Настройка WINS-сервера DHCP-клиента

**DHCP pool name (имя пула DHCP)**
Функция: выбор созданного имени пула IP-адресов.

**WINS server 1~WINS server 8 (WINS-сервер 1~WINS-сервер 8)**
Функция: настройка адреса клиентского WINS-сервера, выделяемого DHCP-сервером.
Пояснение: для клиента, работающего под управлением операционной системы (ОС) Microsoft Windows, сервер Windows Internet Naming Service (WINS) предоставляет услугу преобразования имени хоста, использующего для связи протокол NetBIOS, в IP-адрес. Следовательно, для большинства клиентов на базе ОС Windows требуется настройка WINS. Чтобы DHCP-клиент мог преобразовать имя хоста в IP-адрес, необходимо указать адрес WINS-сервера. Он будет передаваться, когда DHCP-сервер выделяет IP-адрес клиенту. Пул адресов DHCP позволяет настроить до 8 серверов WINS. WINS-сервер 1 имеет самый высокий приоритет, а WINS-сервер 8 — самый низкий.

7. Настройка адреса TFTP-сервера DHCP-клиента и имени загрузочного файла.
Нажмите [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [DHCP file server address configuration], чтобы открыть страницу настройки адреса клиентского TFTP-сервера и имени загрузочного файла, как показано на рисунке 249.

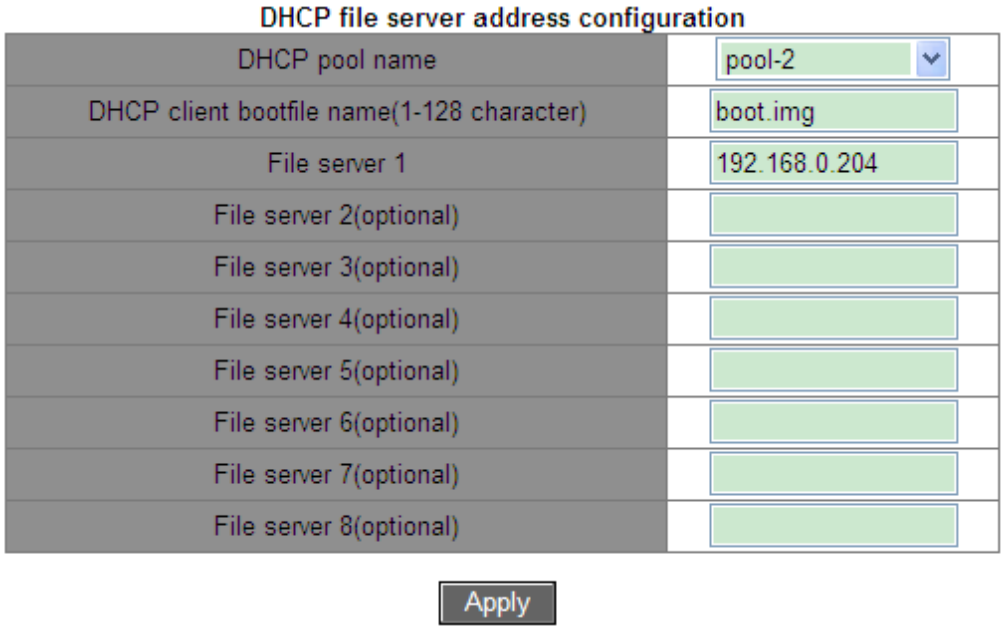



Рисунок 249 – Настройка адреса TFTP-сервера и имени загрузочного файла

**DHCP pool name (имя пула DHCP)**
Функция: выбор созданного имени пула IP-адресов.

**DHCP client bootfile name (имя загрузочного файла DHCP-клиента)**
Диапазон: 1~128 символов.
Функция: настройка имени файла, назначаемого DHCP-сервером для начальной загрузки клиента. При запуске бездискового устройства загрузочный файл необходимо загрузить с сервера, а затем импортировать.

**File server 1~File server 8 (файловый сервер 1~файловый сервер 8)**
Функция: настройка адреса клиентского TFTP-сервера, выделяемого DHCP-сервером. Пул адресов DHCP может настроить до восьми файловых серверов. Файловый сервер 1 имеет наивысший приоритет, а файловый сервер 8 — самый низкий.

8. Настройка сетевых параметров DHCP.
Нажмите [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [DHCP network parameter configuration], чтобы открыть страницу конфигурации сетевых параметров DHCP, как показано на рисунке 250.

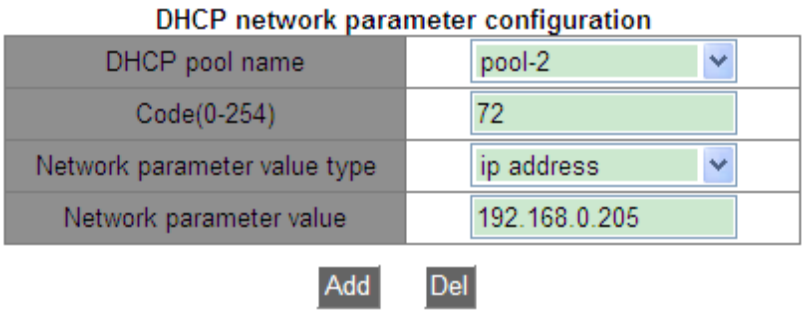



Рисунок 250 – Настройка сетевых параметров DHCP

**DHCP pool name (имя пула DHCP)**
Функция: выбор созданного имени пула IP-адресов.

**Code (код)**
Диапазон: 0~254.
Функция: настройка опций DHCP. DHCP сохраняет формат сообщения BootP для совместимости с этим протоколом. Недавно добавленная функция BootP реализуется через поле «Option». DHCP передает управляющую информацию и параметры конфигурации сети через поле «Option», реализуя назначение IP-адреса и предоставляя клиенту более подробную информацию о конфигурации. Например, «Option72» — параметр WWW-сервера. Эта опция используется для указания адреса WWW-сервера, выделяемого клиенту.

---

Подробную информацию об опциях DHCP см. в документе RFC2132.
Веб-интерфейс обеспечивает настройку общих параметров (например, адрес шлюза, адрес сервера DNS и адрес сервера WINS). Коды сетевых параметров нельзя настраивать как эти общие параметры.

---

**Network parameter value type (тип значения сетевого параметра)**
Варианты: ascii/hex/ip address
Функция: настройка типа значения сетевого параметра. «ascii» — это строка символов ASCII, и ее диапазон составляет от 1 до 255 символов. «hex» — это шестнадцатеричное число, и его конфигурация должна быть чётным числом в диапазоне от 1 до 510.

**Network parameter value (значение сетевого параметра)**
Функция: настройка соответствующего значения сетевого параметра на основе типа значения сетевого параметра.

9. Запрос конфигурации пула адресов DHCP.
Нажмите [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Query address pool configuration], чтобы запросить конфигурацию пула адресов DHCP, как показано на рисунке 251.

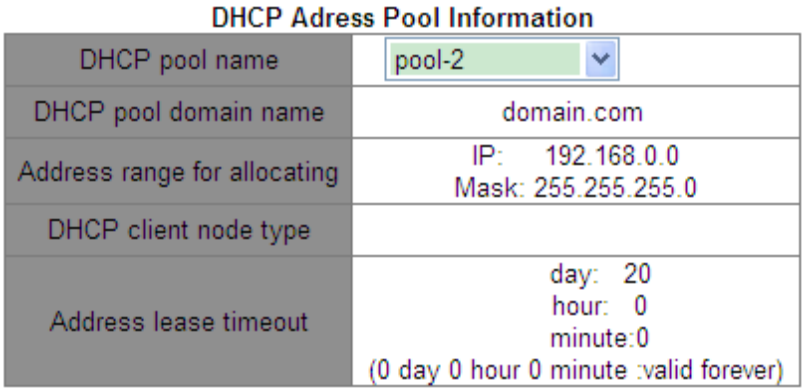



Рисунок 251 – Запрос конфигурации пула адресов DHCP

**DHCP pool name (имя пула DHCP)**
Функция: выбор созданного имени пула IP-адресов.

10. Настройка диапазона IP-адресов, которые не распределяются динамически в пуле адресов DHCP.
Нажмите [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [Excluded address configuration], чтобы перейти на страницу настройки исключений, как показано на рисунке 252.

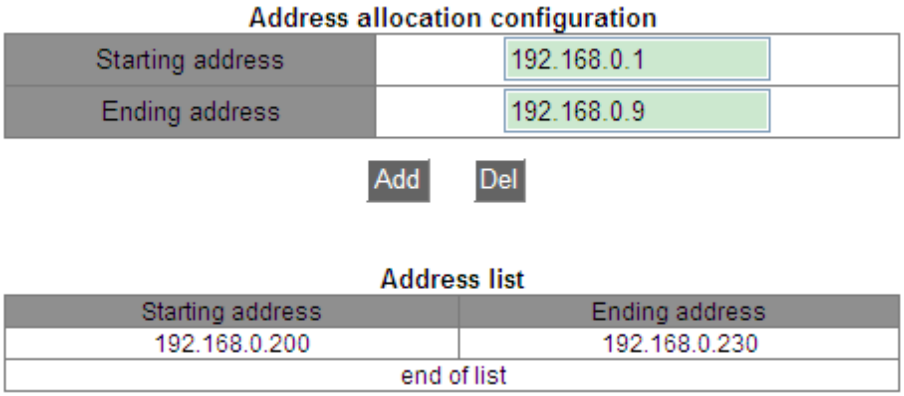



Рисунок 252 – Настройка диапазона не распределяемых динамически IP-адресов

**Starting address/Ending address (начальный адрес/конечный адрес)**
Функция: настройка диапазона IP-адресов, которые не распределяются динамически в пуле адресов DHCP. При распределении IP-адресов DHCP-сервер должен исключить занятый IP-адрес (например, адреса шлюза и DNS-сервера). В противном случае один и тот же IP-адрес может быть назначен двум клиентам, что приведет к конфликту IP-адресов.

11. Отображение статистики пакетов DHCP.
Нажмите [Device Advanced Configuration] → [DHCP configuration] → [DHCP server configuration] → [DHCP packet statistics], чтобы просмотреть статистику пакетов DHCP, как показано на рисунке 253.

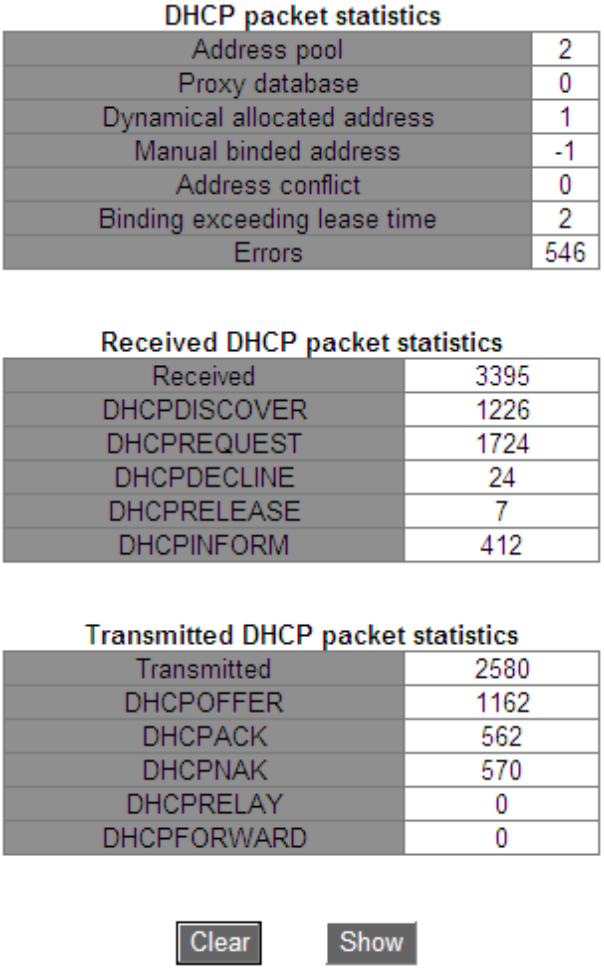



Рисунок 253 – Отображение статистики DHCP-пакетов

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

12. Удаление журнала статистики DHCP-сервера.
Нажмите [Device Advanced Configuration] → [DHCP configuration] → [DHCP debugging] → [Delete DHCP server statistics log], чтобы удалить журнал статистики DHCP-сервера, как показано на рисунке 254.

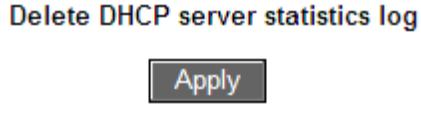



Рисунок 254 – Удаление журнала статистики DHCP-сервера

Нажмите кнопку <Apply>, чтобы очистить статистику принятых/отправленных пакетов DHCP.

13. Отображение информации о привязке IP-MAC.
Нажмите [Device Advanced Configuration] → [DHCP configuration] → [DHCP debugging] → [Show IP-MAC binding], чтобы отобразить информацию о привязке IP-MAC, как показано на рисунке 255.

```
Information Display
IP address          Hardware adress        Lease expiration
Type
192.168.0.23        44-37-E6-88-6E-90      Infinite
Manual
192.168.0.6         00-1E-CD-19-00-02      Infinite
Manual
Total dhcp binding items: 2, the matched: 2
```

Рисунок 255 – Отображение информации о привязке IP-MAC

### 6.14.1.4 Пример типовой настройки

Как показано на рисунке 256, коммутатор A работает как DHCP-сервер, а коммутатор B – как DHCP-клиент. Порт 3 коммутатора A соединяется с портом 4 коммутатора B. Клиент отправляет сообщения с запросом IP-адреса, и сервер может назначить IP-адрес клиенту двумя способами. Диапазон исключенных IP-адресов составляет 192.168.0.1~192.168.0.10, в том случае, если DHCP-сервер динамически выделяет IP-адрес.

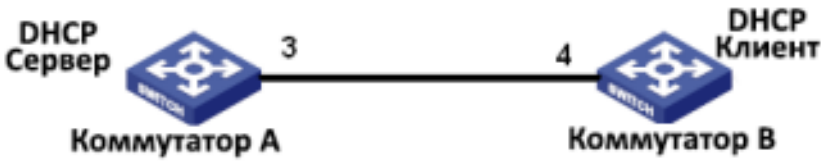



Рисунок 256 – Пример типовой настройки DHCP

**Назначение статических IP-адресов.**

- Настройка коммутатора A:

1. Установите статус сервера DHCP в состояние «Enable», как показано на рисунке 242.
2. Создайте пул IP-адресов DHCP: pool-1, как показано на рисунке 243.
3. Свяжите MAC-адрес коммутатора B: 00-1e-cd-19-00-02 с IP-адресом 192.168.0.6, установите маску подсети 255.255.255.0, как показано на рисунке 244.

- Настройка коммутатора B:

1. Установите режим получения IP-адреса bootp-client или dhcp-client, как показано на рисунке 118.
2. Коммутатор B получает IP-адрес 192.168.0.6 и маску подсети 255.255.255.0 от DHCP-сервера, как показано на рисунке 257.

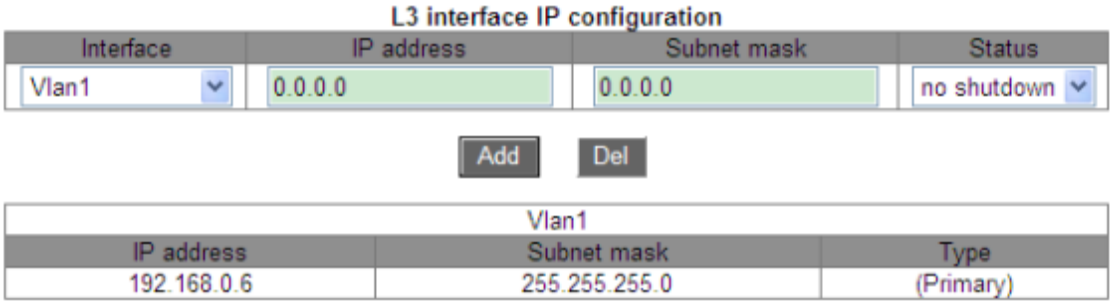



Рисунок 257 – DHCP-клиент получает IP-адрес-1

**Назначение динамических IP-адресов.**

- Настройка коммутатора A:

1. Установите статус сервера DHCP в состояние «Enable», как показано на рисунке 242.
2. Создайте пул IP-адресов DHCP: pool-2, укажите доменное имя domain.com, диапазон адресов для распределения 192.168.0.3(IP) и 255.255.255.0(MASK) и срок аренды до 20 дней, как показано на рисунке 245.
3. Установите диапазон исключений для IP-адресов 192.168.0.1~192.168.0.9, как показано на рисунке 252.

- Настройка коммутатора B:

1. Установите режим получения IP-адреса bootp-client или dhcp-client, как показано на рисунке 118.
2. DHCP-сервер ищет подходящие для присвоения IP-адреса в пуле по порядку и выделяет первый найденный IP-адрес и другие сетевые параметры коммутатору B. Маска подсети — 255.255.255.0, как показано на рисунке 258.

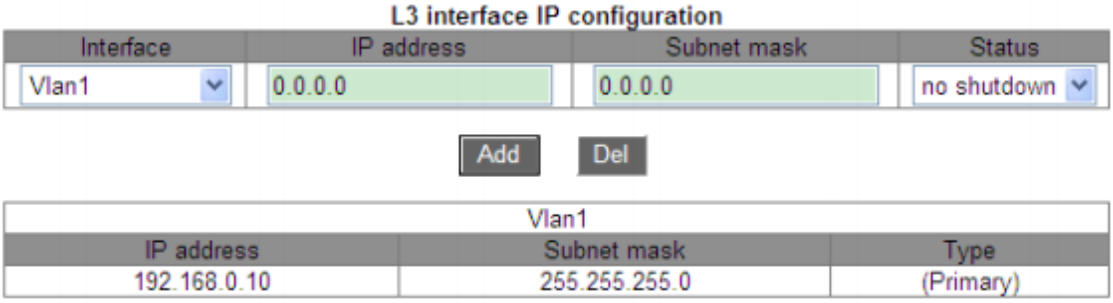



Рисунок 258 – DHCP-клиент получает IP-адрес-2

## 6.15 Настройка QoS

### 6.15.1 Введение

Quality of Service (QoS) позволяет дифференцировать сервисы, в зависимости от разных требований в условиях ограниченной пропускной способности путём контроля трафика и изменения движения трафика в IP сетях. QoS пытается оптимизировать передачу данных

различных сервисов, снизить задержки передачи и минимизировать их эффект в зависимости от приоритета сервиса.
Основная задача QoS – идентификация сервисов, управление задержками передачи данных и их предотвращение.
Идентификация сервисов: разделение сервисов происходит в зависимости от соответствующих правил или объектов. Например, объектами могут быть поля приоритетов в пакетах; приоритеты, определяемые по портам и сетям VLAN, либо другая информация о приоритетах. Идентификация сервисов – основополагающая функция QoS.

Управление перегрузками: это обязательная функция 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 нарастания перегрузки функция использует упреждающее отбрасывание пакетов и регулирует объем трафика для решения возникшей проблемы.

## 6.15.2 QoS CAR

Committed access rate (CAR) – гарантированная скорость доступа QoS. Это тип политики ограничения скорости. Данная политика цитирует правило ACL для идентификации потока, ограничивает скорость порта для соответствующего пакета и отбрасывает поток, выходящий за пределы диапазона (ширина и значение пакета), предусмотренного политикой QoS для пакета.

## 6.15.3 QoS Remark

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

## 6.15.4 Принцип работы

Каждый порт коммутаторов данной серии поддерживает 8 приоритетных очередей, с приоритетами от 0 до 7 (чем выше число - тем выше приоритет).
Вы можете указать соответствие между приоритетом и очередью. При поступлении кадра на порт, коммутатор определяет подходящую для него очередь в зависимости от его заголовка. Коммутатор поддерживает два режима определения соответствия очередей и приоритетов: CoS и DSCP.

- Значение CoS зависит от приоритета в поле 802.1Q кадра. Соответствие между значением CoS и очередью можно настраивать.
- Значение DSCP зависит от TOD/DSCP полей кадра. Соответствие между значением DSCP и очередью также можно настраивать.

При передаче данных, для распределения кадров по 8 приоритетным очередям порт использует режим планирования. Данные коммутаторы используют два режима постановки в очередь: WRR (взвешенный циклический перебор – Weighted Round Robin) и приоритетные очереди.

- WRR планирует распределение потоков данных в зависимости от весового коэффициента. На его основе очереди получают свою полосу пропускания. WRR отдает приоритет очередям с высоким весовым коэффициентом. Для них выделяется бóльшая ширина полосы пропускания.
- Приоритетные очереди гарантируют, что данные с максимальным приоритетом будут передаваться в первую очередь. Как только на коммутатор поступают данные с высоким приоритетом, устройство прекращает обработку данных с более низкими приоритетами и начинает передачу тех, у которых приоритет выше. Только когда очередь максимального приоритета пуста, устройство переходит к передаче данных следующей по важности очереди и так далее.

## 6.15.5 Настройка с помощью WEB-интерфейса

1. Включение функции QoS.
Нажмите [Device Advanced Configuration] → [QoS configuration] → [Enable QoS] → [Enable/Disable QoS], чтобы включить QoS, как показано на рисунке 259.


Рисунок 259 – Включение QoS

**QoS Status (состояние QoS)**
Варианты: Open/Close (открыть/закрыть).
По умолчанию: Close (закрыть).
Функция: включение/отключение глобальной функции QoS.

2. Добавление/удаление карты классов.
Нажмите [Device Advanced Configuration] → [QoS configuration] → [Class-map configuration] → [Add/Remove class-map], чтобы добавить/удалить карту классов, как показано на рисунке 260.

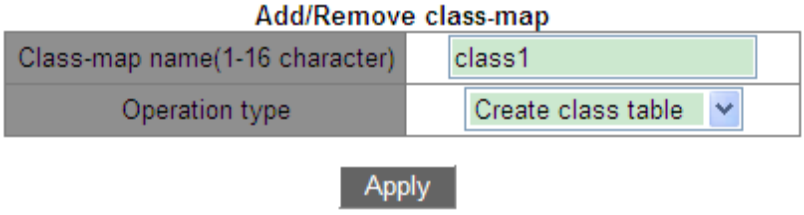



Рисунок 260 – Добавление/удаление карты классов

**Class-map name (имя карты классов)**
Диапазон: 1~16 символов.
Функция: настройка имени карты классов.

**Operation type (тип операции)**
Варианты: Create class table/Remove class table (создать таблицу классов/удалить таблицу классов).
Функция: создать/удалить таблицу классов.

3. Настройка сопоставления карты классов.
Нажмите [Device Advanced Configuration] → [QoS configuration] → [Class-map configuration] → [Class-map configuration], чтобы открыть страницу настройки карты классов, как показано на рисунке 261.

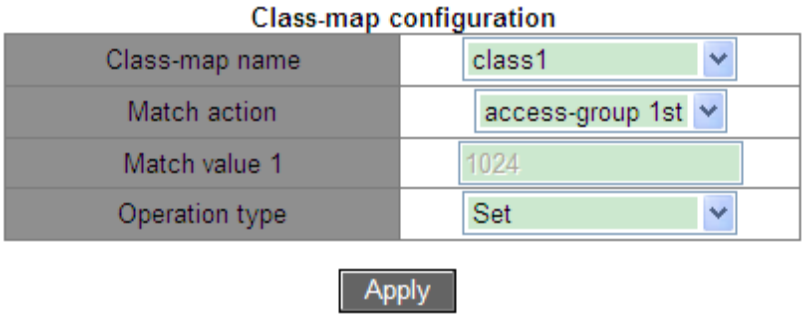



Рисунок 261 – Настройка сопоставления карты классов

**Class-map name (имя карты классов)**
Варианты: все созданные карты классов.

**Match action** (действие сопоставления)
По умолчанию: access-group 1st.
Функция: настроить действие сопоставления карты классов.

**Match value 1 (значение совпадения 1)**
Значение по умолчанию: 1024.
Функция: соответствие с указанной записью ACL. Запись ACL 1024 существует на коммутаторе по умолчанию, и эта запись соответствует всем пакетам.

**Operation type (тип операции)**
Варианты: Set/Del (установить/удалить).
Функция: установить/удалить действие сопоставления карты классов.

4. Добавление/удаление карты политик.
Нажмите [Device Advanced Configuration] → [QoS configuration] → [Policy-map configuration] → [Add/Remove policy-map], чтобы добавить/удалить карту политик, как показано на рисунке 262.

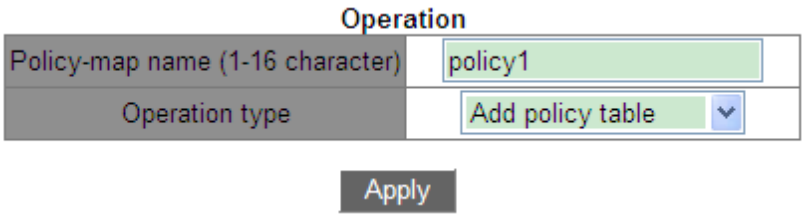



Рисунок 262 – Добавление/удаление карты политик

**Policy-map name (имя карты политик)**
Диапазон: 1~16 символов.
Функция: настройка имени карты политик.

**Operation type (тип операции)**
Варианты: Create policy table/Remove policy table (создать таблицу политик/удалить таблицу политик).
Функция: создать/удалить карту политик.

5. Настройка пропускной способности карты политик.
Нажмите [Device Advanced Configuration] → [QoS configuration] → [Policy-map configuration] → [Policy-map bandwidth configuration], чтобы открыть страницу настройки полосы пропускания в карте политик, как показано на рисунке 263.

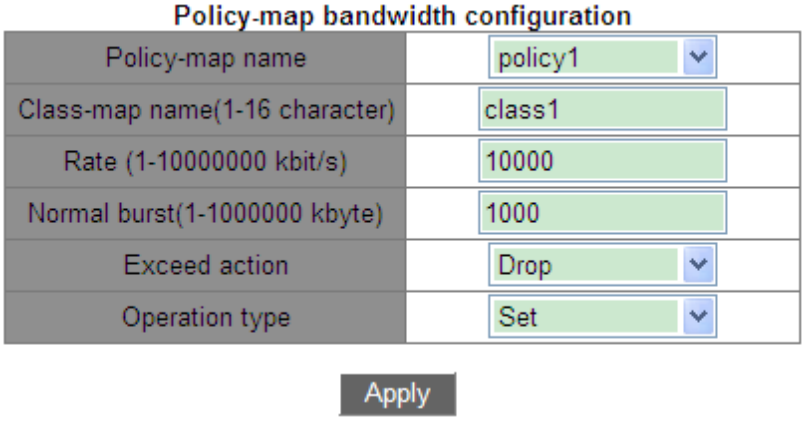



Рисунок 263 – Настройка полосы пропускания карты политик

**Policy-map name (имя карты политик)**
Варианты: все созданные карты политик.

**Class-map name (имя карты классов)**
Варианты: все созданные карты классов.

**Rate (скорость)**
Диапазон: 1-10000000 кбит/с
Функция: настройка значения скорости.

**Normal burst (нормальный пакет)**
Диапазон: 11000-1000000 байт.
Функция: настройка значения размера нормального пакета.

**Exceed action (превышение)**
Варианты: Drop (отбросить).
Функция: применить политику отбрасывания для пакета, соответствующего карте классов, но превышающего значение «Rate».

**Operation type (тип операции)**
Варианты: Set/Del (установить/удалить).
Функция: установка/удаление настройки пропускной способности в карте политик.

6. Настройка приоритетной перемаркировки карты политик.
Нажмите [Device Advanced Configuration] → [QoS configuration] → [Policy-map configuration] → [Policy-map priority configuration], чтобы перейти на страницу настройки приоритета карты политик, как показано на рисунке 264.

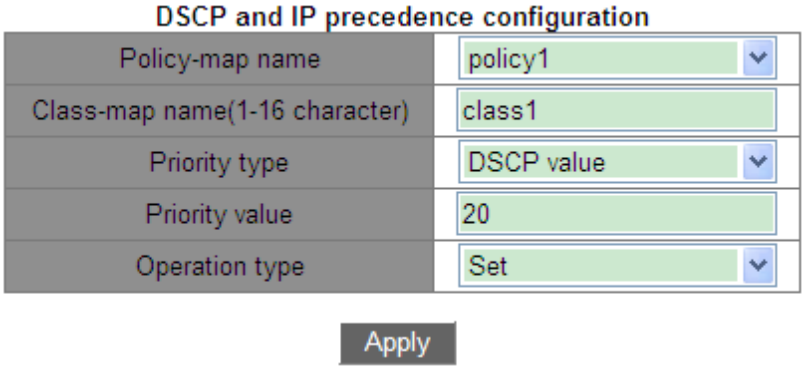



Рисунок 264 – Настройка приоритетной перемаркировки

**Policy-map name (имя карты политик)**
Варианты: все созданные карты политик.

**Class-map name (имя карты классов)**
Варианты: все созданные карты классов.

**Priority type (тип приоритета)**
Варианты: DSCP value/ COS value.
Функция: выбор типа приоритета, который необходимо маркировать.

**Priority value (значение приоритета)**
Варианты: 0–63 (значение DSCP) / 0–7 (значение COS).
Функция: настройка значения перемаркировки приоритета.
Описание: выполнение политики перемаркировки для пакета, соответствующего карте классов.

**Operation type (тип операции)**
Варианты: Set/Del (установить/удалить).
Функция: установка/удаление функции перемаркировки приоритета в карте политик.

7. Применение карты политик к порту.
Нажмите [Device Advanced Configuration] → [QoS configuration] → [Apply QoS to the port] → [Apply policy-map to port], чтобы применить карту политик к порту, как показано на рисунке 265.

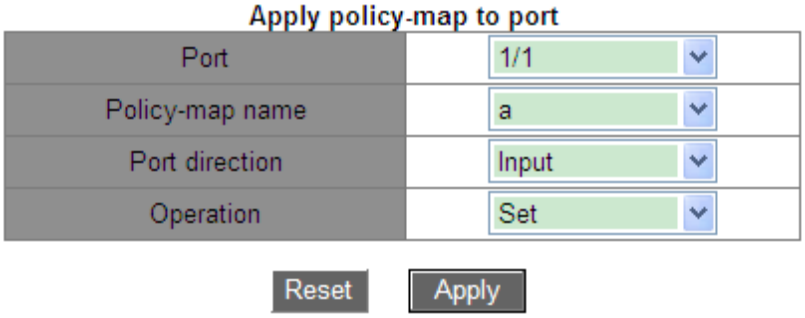



Рисунок 265 – Применение карты политик к порту.

**Policy-map name (имя карты политик)**
Варианты: все созданные карты политик.

**Port direction (направление порта)**
Опции: Input (ввод).
Функция: применение таблицы политик на приёмнике порта для реализации ограничения скорости или перемаркировки приоритета пакета, полученного через порт.

**Operation type (тип операции)**
Варианты: Set/Del (установить/удалить).
Функция: установка/удаление функции применения карты политик к порту.

---

- К одному порту применяется одна карта политик.
- Применение к порту карты политик и его настройка в режиме trust mode – взаимоисключающие функции.

---

8. Настройка режима доверия порта (trust mode).
Нажмите [Device Advanced Configuration] → [QoS Configuration] → [Apply QoS to port] → [Port trust mode configuration], чтобы открыть страницу конфигурации режима доверия порта, как показано на рисунке 266.

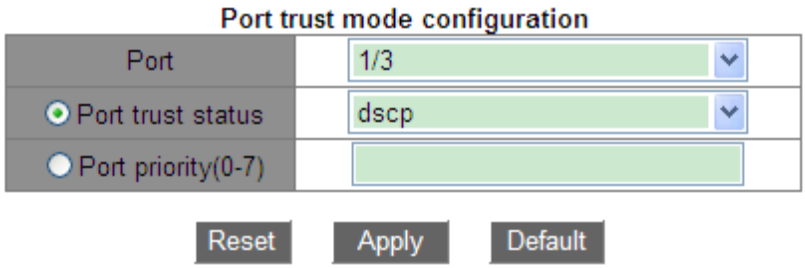



Рисунок 266 – Настройка trust mode для порта

**Port (порт)**
Варианты: все порты коммутатора.

**Port trust status (статус режима доверия порта)**
Варианты: cos/cos and pass through dscp/dscp/dscp and pass through cos/port.
По умолчанию: если порт получает IP пакет, то значение по умолчанию «dscp»; если это не IP пакет, но имеет поле приоритета, значение по умолчанию «cos». Если это не IP пакет, и у него нет поля приоритета, то trust mode не будет выбран, а данные будут обработаны с приоритетом 0.
Функция: определить режим доверия для порта коммутатора.
Описание: «cos» и «cos and pass through dscp» означает, что порт доверяет значению CoS. Очередь, куда будут помещены данные будет определяться по значению CoS. Если у кадра нет поля CoS, данные будут помещаться в очередь, соответствующую приоритету CoS = 0. Разница между режимами «cos» и «cos and pass through dscp» в том, что «cos» во время передачи данных будет изменять приоритет DSCP согласно правилам соответствия CoS и DSCP, а «cos and pass through dscp» не будет изменять значение приоритета DSCP пакетов.
«dscp» и «dscp and pass through cos» означает, что порт доверяет значению DSCP. Очередь, куда будут помещены данные будет определяться по значению DSCP. Если у кадра нет поля DSCP, данные будут помещаться в очередь, соответствующая приоритету DSCP = 0. Разница между «dscp» и «dscp and pass through cos» в том, что «dscp» во время передачи данных будет изменять приоритет CoS согласно правилам соответствия DSCP и CoS, а «dscp and pass through cos» не будет изменять значение приоритета CoS пакетов.

**Port priority (приоритет портов)**
Варианты: 0~7.
Значение по умолчанию: 0.
Функция: настройка приоритета физического порта. Данные, полученные на указанном порту ставятся в очередь согласно выбранному приоритету порта, а не приоритету самих кадров. Пакеты, полученные от порта с приоритетом «0» попадут в приоритетную очередь 0, а от порта с приоритетом «1» – соответственно, в очередь 1, и так далее.

9. Настройка значения CoS порта по умолчанию.

Нажмите [Device Advanced Configuration] → [QoS Configuration] → [Apply QoS to port] → [Port default CoS configuration], чтобы открыть страницу настройки CoS порта по умолчанию, как показано на рисунке 267.

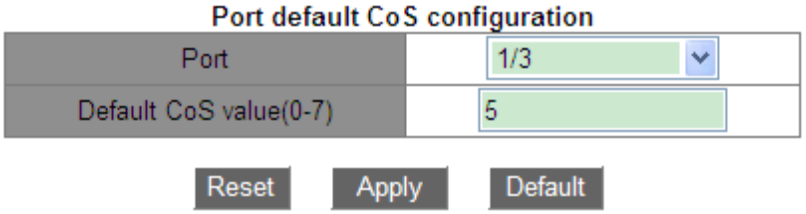



Рисунок 267 – Настройка CoS порта по умолчанию

**Port (порт)**
Варианты: все порты коммутатора.

**Default CoS value (значение CoS по умолчанию)**
Варианты: 0~7.
Значение по умолчанию: 0.
Функция: настройка значения CoS по умолчанию для данного порта.
Пояснение: если принимаемые данные не имеют тега CoS, он добавляется, и используется данное значение по умолчанию.

10. Настройка режима планирования исходящей очереди порта согласно приоритетам.
Нажмите [Device Advanced Configuration] → [QoS Configuration] → [Egress-queue configuration] → [Port Egress-queue work mode configuration], чтобы перейти на страницу настройки режима планирования приоритетной очереди, как показано на рисунке 268.

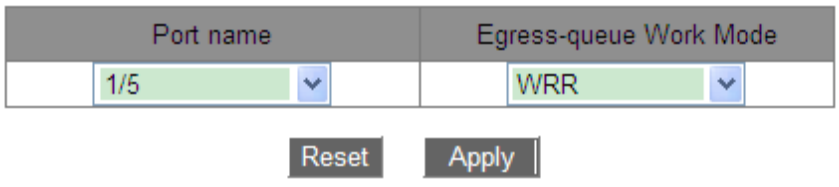



Рисунок 268 – Настройка режима исходящей очереди

**Egress-queue Work Mode (режим работы исходящей очереди)**
Варианты: PQ/WRR.
По умолчанию: PQ.
Функция: настроить режим исходящей очереди для выбранного порта.

11. Настройка взвешенных коэффициентов WRR очереди порта.
Нажмите [Device Advanced Configuration] → [QoS Configuration] → [Egress-queue configuration] → [Port Egress-queue wrr weight configuration], чтобы открыть страницу настройки веса WRR исходящей очереди, как показано на рисунке 269.

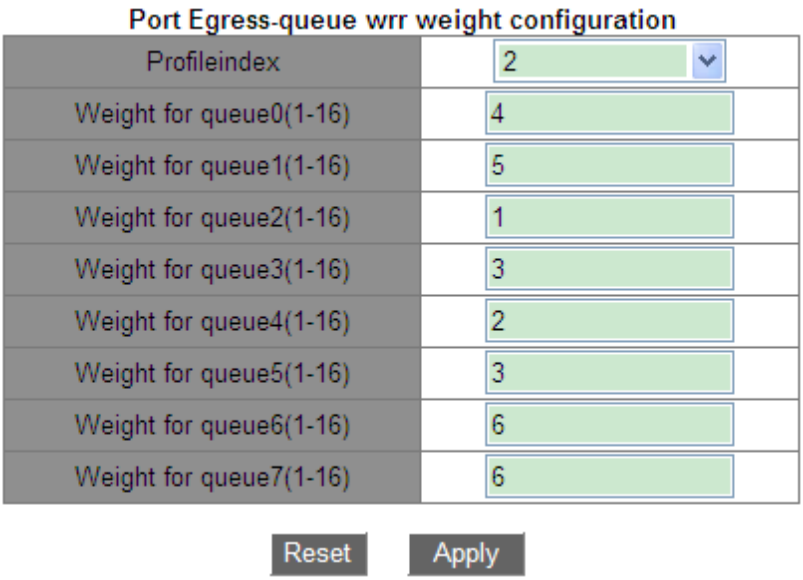



Рисунок 269 – Настройка взвешенных коэффициентов

**Profileindex (индекс профиля)**
Варианты: 1~6.
Значение по умолчанию: 1.
Функция: настройка группы взвешенных значений.
Пояснение: коммутатор поддерживает до 6 групп взвешенных значений.

**{Weight for queue0, Weight for queue1, Weight for queue2, Weight for queue3, Weight for queue4, Weight for queue5, Weight for queue6, Weight for queue7} – {Вес для очереди0, Вес для очереди1, Вес для очереди2, Вес для очереди3, Вес для очереди4, Вес для очереди5, Вес для очереди6, Вес для очереди7}.**
Варианты: {0~15, 0~15, 0~15, 0~15, 0~15, 0~15, 0~15}.
По умолчанию: {1, 2, 3, 4, 5, 6, 7, 8}.
Функция: настройка взвешенных значений. Абсолютное значение веса не имеет смысла. WRR распределяет полосу пропускания в соответствии с 8 соотношениями весовых значений.
Описание: если значение веса одной очереди равно 0, её данные имеют наивысший приоритет. Если значение веса нескольких очередей равно 0, наивысший приоритет пересылки отдается данным из очереди с высоким приоритетом, имеющим значение 0. Затем пересылаются данные со значением веса 0 из очереди с низким приоритетом. Когда отправлены все данные со значением веса 0, коммутатор начинает пересылать данные других очередей в соответствии с коэффициентом веса.

12. Настройка режим планирования WRR для порта и привязка к порту весового коэффициента (см. рисунок 270).

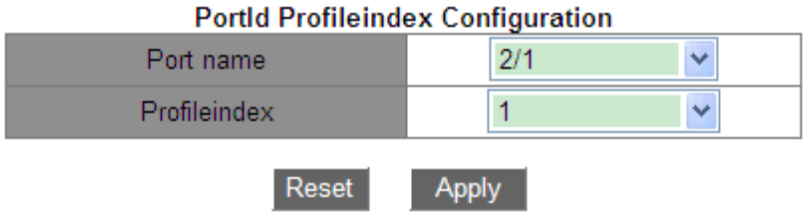



Рисунок 270 – Настройка режима планирования WRR

**Port name (имя порта)**
Варианты: все порты коммутатора.
Функция: выбрать порт, чтобы установить для него режим планирования WRR.

**Profileindex (индекс профиля)**
Варианты: 1~6.
Функция: выбрать весовой коэффициент WRR порта.

13. Настройка соответствия между значениями CoS и исходящими очередями.
Нажмите [Device Advanced Configuration] → [QoS Configuration] → [Egress-queue configuration] → [Mapping CoS values to egress queue], чтобы открыть страницу настройки сопоставления CoS и очереди, как показано на рисунке 271.

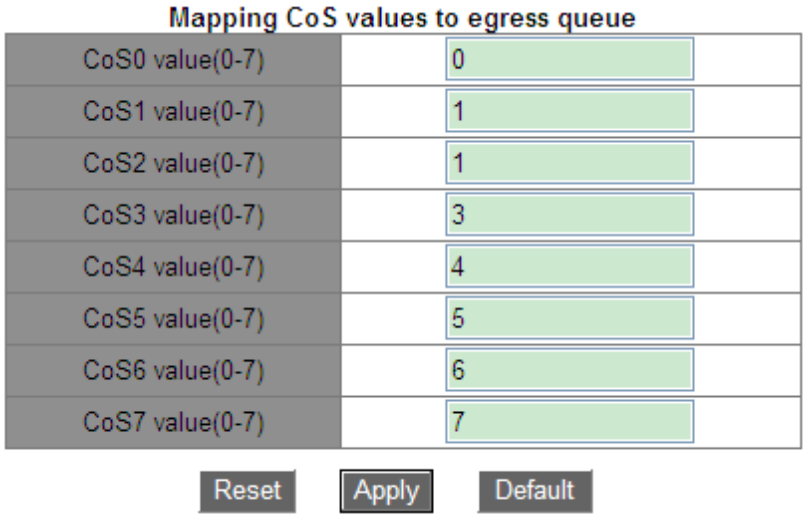



Рисунок 271 – Сопоставление значений CoS и очередей.

**{COS value, Queue-ID} {значение приоритета COS, идентификатор очереди}**
Варианты: {0~7, 0~7}.
По умолчанию:
значение CoS=0 привязывается к очереди 0; значение CoS=1 привязывается к очереди 1;
значение CoS=2 привязывается к очереди 2; значение CoS=3 привязывается к очереди 3;
значение CoS=4 привязывается к очереди 4; значение CoS=5 привязывается к очереди 5;
значение CoS=6 привязывается к очереди 6; значение CoS=7 привязывается к очереди 7.
Функция: настройка соответствия между приоритетами CoS и очередями.

Примечание: каждое значение CoS может быть привязано только к одной очереди. При этом, к одной очереди можно привязать множество CoS-приоритетов.

14. Настройка соответствия между значениями DSCP и исходящими очередями.
Нажмите [Device Advanced Configuration] → [QoS Configuration] → [Egress-queue configuration] → [Mapping DSCP values to egress queue], чтобы открыть страницу настройки сопоставления DSCP и очереди, как показано на рисунке 272.

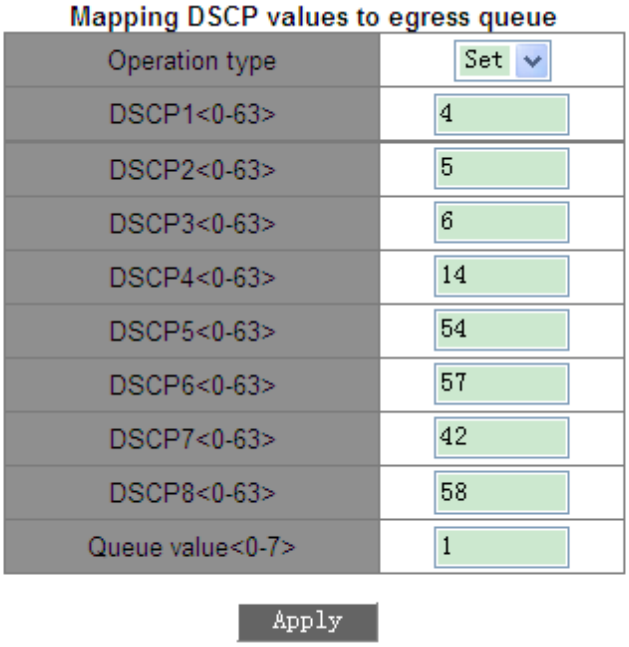



Рисунок 272 – Сопоставление значений DSCP и очередей

**Operation type (тип операции)**
Варианты: Set/Del (установить/удалить).
По умолчанию: Set (установить).
Функция: настройка соответствия между DSCP и очередью.
Описание: «Set» устанавливает новое соответствие между значением DSCP и очередью. «Del» восстанавливает соответствие по умолчанию.

**{DSCP, Queue value} – (значения DSCP и очереди)**
Варианты: {0~63, 0~7}.
По умолчанию:
значения DSCP=0~7 привязываются к очереди 0; значения DSCP=8~15 привязываются к очереди 1;
значения DSCP=16~23 привязываются к очереди 2; значения DSCP=24~31 привязываются к очереди 3;
значения DSCP=32~39 привязываются к очереди 4; значения DSCP=40~47 привязываются к очереди 5;

значения DSCP=48~55 привязываются к очереди 6; значения DSCP=56~63 привязываются к очереди 7.
Функция: настройка соответствия между значениями приоритетов DSCP и очередями.
Пояснение: каждое значение DSCP может быть привязано только к одной очереди. При этом, к одной очереди можно привязать множество DSCP-приоритетов.

15. Настройка соответствия между значениями CoS и DSCP.
[Device Advanced Configuration] → [QoS Configuration] → [QoS mapping configuration] → [CoS-to-DSCP mapping], чтобы открыть страницу сопоставления CoS и DSCP, как показано на рисунке 273.

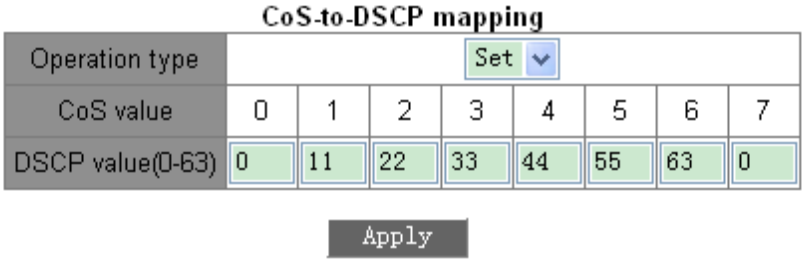



Рисунок 273 – Сопоставление значений CoS и DSCP

**Operation type (тип операции)**
Варианты: Set/Del (установить/удалить).
По умолчанию: Set (установить).
Функция: настройка соответствия между CoS и DSCP.
Описание: «Set» устанавливает новое соответствие между значениями CoS и DSCP. «Del» восстанавливает соответствие по умолчанию.

**DSCP value (значение DSCP)**
Варианты: 0~63.
По умолчанию:
значение CoS 0 соответствует значению DSCP 0; значение CoS 1 соответствует значению DSCP 8;
значение CoS 2 соответствует значению DSCP 16; значение CoS 3 соответствует значению DSCP 24;
значение CoS 4 соответствует значению DSCP 32; значение CoS 5 соответствует значению DSCP 40;
значение CoS 6 соответствует значению DSCP 48; значение CoS 7 соответствует значению DSCP 56.
Функция: настройка сопоставления CoS и DSCP. Когда режим доверия порта — CoS, значение приоритета DSCP-пакета может быть изменено в соответствии с этим сопоставлением.
Пояснение: одному значению DSCP можно сопоставить несколько значений CoS.

16. Настройка соответствия между значениями DSCP и CoS.

Нажмите [Device Advanced Configuration] → [QoS Configuration] → [QoS mapping configuration] → [DSCP-to-CoS mapping], чтобы открыть страницу сопоставления DSCP и CoS, как показано на рисунке 274.

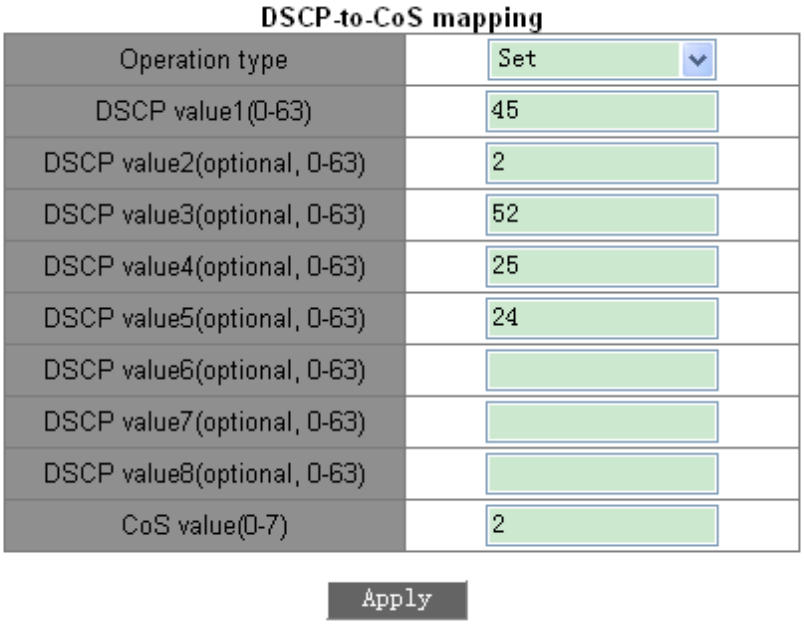



Рисунок 274 – Сопоставление значений DSCP и CoS

**Operation type (тип операции)**
Варианты: Set/Del (установить/удалить).
По умолчанию: Set (установить).
Функция: настройка соответствия между DSCP и CoS.
Описание: «Set» устанавливает новое соответствие между значениями DSCP и CoS. «Del» восстанавливает соответствие по умолчанию.

**{DSCP value, COS value} – {значение DSCP, значение COS}**
Варианты: {0~63, 0~7}.
По умолчанию:
значение DSCP 0~7 соответствует значению CoS 0;
значение DSCP 8~15 соответствует значению CoS 1;
значение DSCP 16~23 соответствует значению CoS 2;
значение DSCP 24~31 соответствует значению CoS 3;
значение DSCP 32~39 соответствует значению CoS 4;
значение DSCP 40~47 соответствует значению CoS 5;
значение DSCP 48~55 соответствует значению CoS 6;
значение DSCP 56~63 соответствует значению CoS 7.
Функция: настройка сопоставления DSCP и CoS. Когда режим доверия порта — DSCP, значение приоритета пакета CoS может быть изменено в соответствии с этим сопоставлением.
Пояснение: одному значению CoS можно сопоставить до восьми значений DSCP.

7. Настройка изменения значений приоритета DSCP.
Нажмите [Device Advanced Configuration] → [QoS Configuration] → [QoS mapping configuration] → [DSCP-to-DSCP mutation mapping], чтобы открыть страницу настройки сопоставления значений DSCP, как показано на рисунке 275.

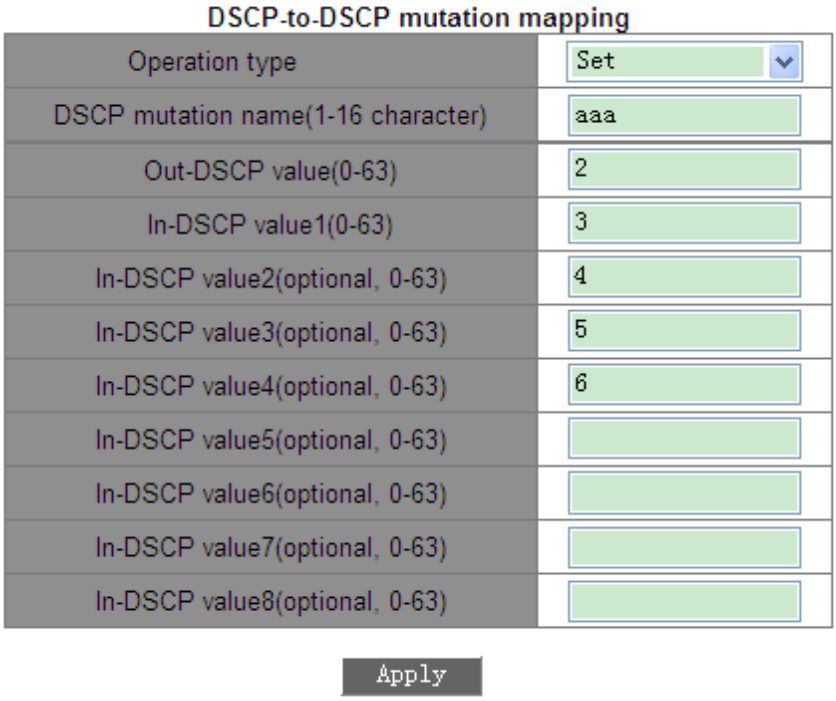



Рисунок 275 – Сопоставление значений DSCP

**Operation type (тип операции)**
Варианты: Set/Del (установить/удалить).
По умолчанию: Set (установить).
Функция: настройка соответствия между DSCP и DSCP.
Описание: «Set» устанавливает новое соответствие между значениями DSCP и DSCP. «Del» удаляет соответствие. Коммутаторы серии поддерживают до 28 сопоставлений DSCP-DSCP.

**DSCP mutation name (имя алгоритма изменения DSCP)**
Диапазон: 1~16 символов.
Функция: установить имя для алгоритма изменения DSCP.

**{Out-DSCP value, In-DSCP value} – {исходящее значение DSCP, входящее значение DSCP}**
Варианты: {0~63, 0~63}.
Функция: настройка сопоставление между DSCP и DSCP. Данная функция используется, если необходимо изменить значение DSCP-приоритета передаваемого пакета.

Пояснение: одному значению приоритета DSCP можно сопоставить до восьми значений DSCP.

---

Очередь обработки данных определяется в соответствии с изначальным приоритетом DSCP.

---

18. Применение алгоритма изменения DSCP к порту.
Нажмите [Device Advanced Configuration] → [QoS Configuration] → [Apply QoS to port] → [Apply DSCP mutation mapping], чтобы открыть страницу конфигурации, как показано на рисунке 276.

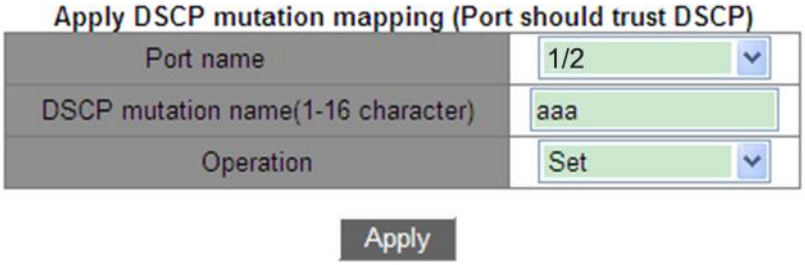



Рисунок 276 – Применение DSCP mutation на порту

**Port name** имя порта
Опции: все порты коммутатора
Функция: выбор порта для использования сопоставления DSCP-DSCP.

**DSCP mutation name (имя алгоритма изменения DSCP)**
Варианты: имя записи DSCP mutation.
Функция: настройка DSCP mutation на данном порту.

**Operation (операция)**
Опции: Set/Del (установить/удалить).
Функция: добавление/удаление алгоритма DSCP mutation, используемого портом.

## 6.15.6 Пример типовой настройки

Как показано на рисунке 277, порты 1, 2, 3 и 4 пересылают пакеты на порт 5.

- Значение DSCP принятого пакета порта 1 равно 6, режим доверия — DSCP pass CoS, а пакеты, поступающие на порт 1, соответствуют очереди 3.
- Значение CoS принятого пакета порта 2 равно 2, режим доверия — CoS pass DSCP, а пакеты, поступающие на порт 2, соответствуют очереди 1.
- Значение CoS принятого пакета порта 3 равно 2, значение DSCP для него равно 32, режим доверия — DSCP, а пакеты, поступающие на порт 3, соответствуют очереди 2.
- Значение DSCP принятого пакета порта 4 равно 26, значение CoS для него равно 3, режим доверия — CoS, а пакеты, поступающие на порт 4, соответствуют очереди 3.
- Порт 5 использует режим планирования WRR.

**Процесс настройки:**

1. Включите QoS, как показано на рисунке 259.
2. Установите режим доверия порта 1 на DSCP pass CoS, порта 2 на CoS pass DSCP, порта 3 на DSCP и порта 4 на CoS, как показано на рисунке 266.
3. Режимы CoS-to-DSCP и DSCP-to-CoS используют сопоставление по умолчанию; это означает, что значение CoS для пересылаемых пакетов порта 3 изменяется на 4, а значение DSCP для пересылаемых пакетов порта 4 изменяется на 24.
4. Привяжите значение CoS 2 к очереди 1, а значение CoS 3 – к очереди 3, как показано на рисунке 271.
5. Привяжите значение DSCP 6 к очереди 3, а значение DSCP 32 – к очереди 2, как показано на рисунке 272.
6. Настройте режим планирования очереди порта 5 на WRR (см. рисунок 268); используйте весовой коэффициент очереди по умолчанию, как показано на рисунке 270.


Рисунок 277 – Пример конфигурации QoS

Пакеты порта 1 и порта 4 попадают в очередь 3, пакеты порта 2 – в очередь 1, а пакеты порта 3 – в очередь 2. Согласно соответствию между очередью и весом, вес очереди 1 равен 2, вес очереди 2 равен 3, а вес очереди 3 равен 4, поэтому доля полосы пропускания, выделенная пакетам во входящей очереди 1, равна 2/(2+3+4), доля полосы пропускания, выделенная пакетам во входящей очереди 2, равна 3/(2+3+4), а для пакетов во входящей очереди 3 выделяется 4/(2+3+4). Среди них пакеты порта 1 и порта 4 попадают в очередь 3, поэтому они пересылаются в соответствии с правилом «первым пришёл — первым ушёл» (FIFO), но общая пропорция пропускной способности порта 1 и порта 4 должна быть 4/(2+3+4).

## 6.16 Настройка IEC61850

### 6.16.1 Введение

IEC 61850 (МЭК-61850) – это международный стандарт, определяющий протоколы связи для интеллектуальных электронных устройств (ИЭУ) на электрических подстанциях. В настоящее время для мониторинга коммутаторов необходимы инструменты, отличные от IEC61850, такие как EMS, Web, CLI и OPC, что приводит к несогласованности настройки и неудобству управления сетью. Для решения этой проблемы коммутаторы данной серии

разрабатываются с учётом стандарта IEC 61850 и могут быть включены в системы автоматизации подстанций в качестве ИЭУ. Тем самым обеспечивается единое представление мониторинга, упрощаются задачи планирования и интеграции, а также снижаются затраты на создание автоматизированных систем и их последующее техническое обслуживание.

---

Файл моделирования по умолчанию switch.cid, предоставленный производителем, уже импортирован в коммутатор. Если необходимо импортировать другие файлы моделирования, обратитесь к разделу 5.13 «Служба передачи файлов».

---

## 6.16.2 Настройка с помощью WEB-интерфейса

1. Включение IEC61850.
Нажмите [Device Advanced Configuration] → [IEC61850 Configuration] → [IEC61850 Configuration], чтобы открыть страницу настройки IEC61850, как показано на рисунке 278.


Рисунок 278 – Включение IEC61850

**IEC61850 Function (функционирование IEC61850)**
Варианты: Enable/Disable (включить/отключить).
По умолчанию: Disable (отключить).
Функция: включение или выключение функции IEC61850.

2. Настройка IEC61850.

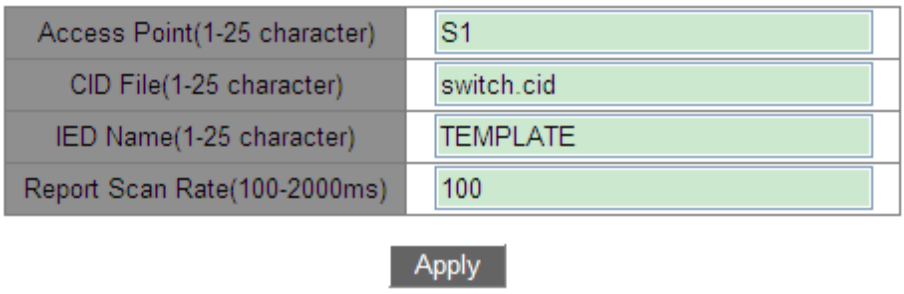



Рисунок 279 – Настройка IEC61850

**Access Point (точка доступа)**
Диапазон: 1~25 символов.

По умолчанию: S1.
Функция: настройка имени точки доступа, соответствующей IED в файле CID.

**CID File (CID-файл)**
Диапазон: 1~25 символов.
По умолчанию: switch.cid
Функция: настройка имени актуального файла моделирования CID при запуске функции IEC61850.

**IED Name (имя ИЭУ)**
Диапазон: 1~25 символов.
По умолчанию: TEMPLATE (шаблон).
Функция: настройка имени логического устройства, соответствующего значению IED, в файле CID.

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

---

Настройки имени точки доступа и устройства ИЭУ должны соответствовать имени точки доступа и устройства ИЭУ в указанном файле моделирования. В противном случае функция IEC61850 не сможет быть активирована.

---

# 6.17 IGMP Snooping

## 6.17.1 Введение

Internet Group Management Protocol Snooping (IGMP Snooping) – многоадресный протокол второго уровня. Он используется для управления и настройки мультикастовых групп передачи данных. Коммутаторы с поддержкой IGMP Snooping анализируют принимаемые IGMP пакеты, осуществляют сопоставление между портами и мультикастовыми MAC-адресами и отправляют мультикастовые данные в соответствии с этим сопоставлением.

## 6.17.2 Основные понятия

Мастер запросов: периодически отправляет IGMP-запросы для проверки и обновления информации о мультикастовых группах. Если в сети присутствует несколько мастеров запросов, они автоматически определяют одного (с наименьшим IP адресом), который непосредственно и будет осуществлять запросы, остальные будут только получать и передавать IGMP-запросы.
Маршрутизирующий порт: получает общие запросы (на IGMP-коммутаторе) от мастера. При получении IGMP ответа, коммутатор инициализирует мультикастовую группу и добавляет в неё порт, на который пришёл ответ. Если настроен маршрутизирующий порт,

он также добавляется. Затем коммутатор ретранслирует IGMP ответ другим устройствам через маршрутизирующий порт.

## 6.17.3 Принцип работы

IGMP Snooping управляет участниками групп многоадресной рассылки путём обмена связанными пакетами между поддерживающих IGMP устройствами.

- Пакет общего запроса: мастер запросов периодически отправляет общие запросы (с IP адресом назначения: 224.0.0.1) для уточнения, есть ли у мультикастовой группы порты-участники. При получении запроса, устройство, не являющееся мастером запросов, ретранслирует пакет на все свои порты.
- Пакет конкретного запроса: Если устройство хочет покинуть мультикастовую группу, оно отправляет пакет «IGMP leave». После получения такого пакета, мастер запросов отправляет пакет конкретного запроса (с IP адресом назначения, равным IP адресу мультикастовой группы) для удостоверения, что у коммутатора остались какие-либо порты-участники данной группы.
- Пакет отчёта о принадлежности: Если устройство хочет получить данные мультикастовой группы, оно отправляет пакет IGMP оповещения (с IP адресом назначения, равным IP адресу мультикастовой группы) в ответ на IGMP запрос группы.
- Пакет «IGMP leave»: Если устройство хочет покинут мультикастовую группу, оно отправляет пакет «IGMP leave» (с IP адресом назначения: 224.0.0.2).

## 6.17.4 Настройка с помощью WEB-интерфейса

1. Включение IGMP Snooping.
Нажмите [Device Advanced Configuration] → [Multicast protocol configuration] → [IGMP Snooping configuration] → [Enable IGMP Snooping], чтобы открыть страницу глобальной конфигурации IGMP Snooping, как показано на рисунке 280.


Рисунок 280 – Включение IGMP Snooping

**IGMP Snooping**
Варианты: Open/Close (открыть/закрыть).
По умолчанию: Close (закрыть).
Функция: включить или отключить глобальный протокол IGMP Snooping. IGMP Snooping и GMRP нельзя включить одновременно.

2. Настройка параметров IGMP Snooping.
Нажмите [Device Advanced Configuration] → [Multicast protocol configuration] → [IGMP Snooping configuration] → [IGMP Snooping configuration], чтобы открыть страницу настройки IGMP Snooping, как показано на рисунке 281.


Рисунок 281 – Настройка IGMP Snooping

**VLAN ID (идентификатор VLAN)**
Варианты: все созданные идентификаторы VLAN.

**Snooping state (состояние отслеживания)**
Варианты: Open/Close (открыть/закрыть).
По умолчанию: Close (закрыть).
Функция: включение или выключение IGMP Snooping для данной VLAN. Предварительным условием для этой функции является включение глобальной функции IGMP Snooping.

**Static IP (статический IP-адрес)**
Формат: A.B.C.D.
По умолчанию: 192.168.0.2.
Функция: настроить исходный IP-адрес для отправки пакетов.

3. Настройка параметров мастера запросов IGMP (см. рисунок 282).

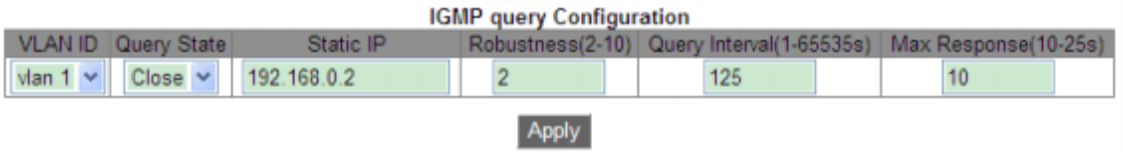



Рисунок 282 – Настройка мастера запросов IGMP

**VLAN ID (идентификатор VLAN)**
Варианты: все созданные идентификаторы VLAN.
Функция: выбор идентификатора VLAN, для которой будет разрешена функция запроса IGMP.

**Query State (статус запросов)**
Варианты: Open/Close (открыть/закрыть).
По умолчанию: Close (закрыть).
Функция: включение или отключение мастера IGMP-запросов для выбранной VLAN. Предварительным условием для этой функции является включение глобальной функции IGMP Snooping.
Описание: если в сети несколько мастеров запросов, они автоматически выберут одного с наименьшим IP, который станет единственным мастером в сети.

Функции мастера запросов и IGMP Snooping – взаимоисключающие для каждой VLAN. Это означает, что если мастер запросов включен, то IGMP Snooping должен быть выключен для данной VLAN, и наоборот.

**Static IP (статический IP-адрес)**
Формат: A.B.C.D.
Функция: назначение IP адреса отправителя для запроса.

**Robustness (надежность)**
Диапазон: 2~10.
Значение по умолчанию: 2.
Функция: настройка параметра надежности функции запроса IGMP.
Описание: чем больше значение, тем ненадёжнее сеть. Пользователь может самостоятельно выбирать значение данного параметра в зависимости от состояния сети.

**Query Interval (интервал между запросами)**
Диапазон: 1~65535 с.
Значение по умолчанию: 125 с.
Функция: настройка интервала для отправки пакета запроса.

**Max Response (максимальное время ответа)**
Диапазон: 10~25 с.
Значение по умолчанию: 10 с.
Функция: настроить максимальное время ответа на запрос.

После завершения настройки в разделе «IGMP Configuration» отображается информация о настройках IGMP, как показано на рисунке 283.

IGMP Configuration

| VLAN ID | Snooping State | Query State | Static IP | Robustness | Query Interval(s) | Max Response(s) |
|---|---|---|---|---|---|---|
| 1 | Close | Open | 192.168.0.2 | 2 | 125 | 10 |
| 2 | Open | Close | 192.168.0.2 | 0 | 0 | 0 |

Рисунок 283 – Информация о настройках IGMP

4. Настройка статических параметров многоадресной рассылки IGMP Snooping.
Нажмите [Device Advanced Configuration] → [Multicast protocol configuration] → [IGMP Snooping configuration] → [IGMP Snooping static multicast configuration], чтобы открыть страницу статической настройки IGMP Snooping, как показано на рисунке 284.

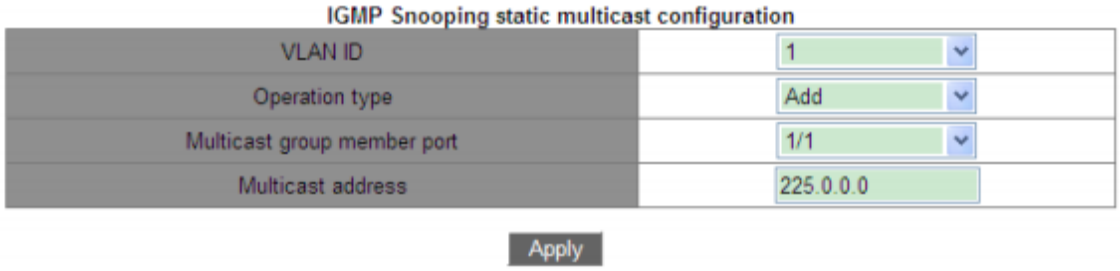



Рисунок 284 – Конфигурация статической многоадресной группы IGMP Snooping

**VLAN ID (идентификатор VLAN)**
Варианты: все созданные идентификаторы VLAN.

**Operation type (тип операции)**
Варианты: Add/Del (добавить/удалить).
По умолчанию: Add (добавить).
Функция: добавить/удалить участника мультикастовой группы.

**Multicast group member port (порт-участник мультикастовой группы)**
Варианты: все порты коммутатора
Действие: выберите порт для добавления или исключения из мультикастовой группы. Если порт подключён к устройству, получающему данные какой-либо мультикастовой группы, он может быть настроен как участник статической мультикастовой группы.

**Multicast address (мультикастовый адрес)**
Диапазон: 224.0.1.0~239.255.255.255.
Действие: введите адрес мультикастовой группы.
Описание: Если мультикастовая группа получена динамически, статическая запись её перезапишет.

5. Отображение многоадресных записей.
Нажмите [Device Advanced Configuration] → [Multicast protocol configuration] → [IGMP Snooping configuration] → [Show IGMP Snooping information], чтобы отобразить записи многоадресной рассылки, как показано на рисунке 285.

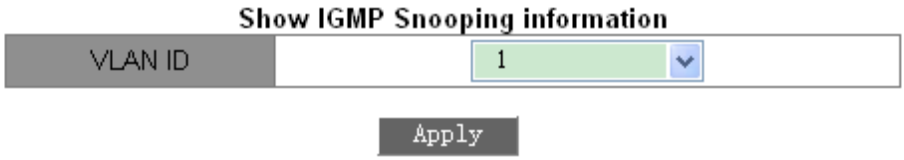



Рисунок 285 – Список участников многоадресной рассылки.

Просмотрите мультикастовые записи в выбранной VLAN.

## 6.17.5 Пример типовой настройки

Как показано на рисунке 286, включите функцию IGMP Snooping на коммутаторе 1, коммутаторе 2 и коммутаторе 3.

Включите автоматический запрос на коммутаторе 2 и коммутаторе 3. IP-адрес коммутатора 2 — 192.168.1.2, а коммутатора 3 — 192.168.0.2, поэтому коммутатор 3 выбран в качестве мастера запросов.

1. Включите IGMP Snooping.
2. Включите IGMP Snooping и автоматический запрос.
3. Включите IGMP Snooping и автоматический запрос.

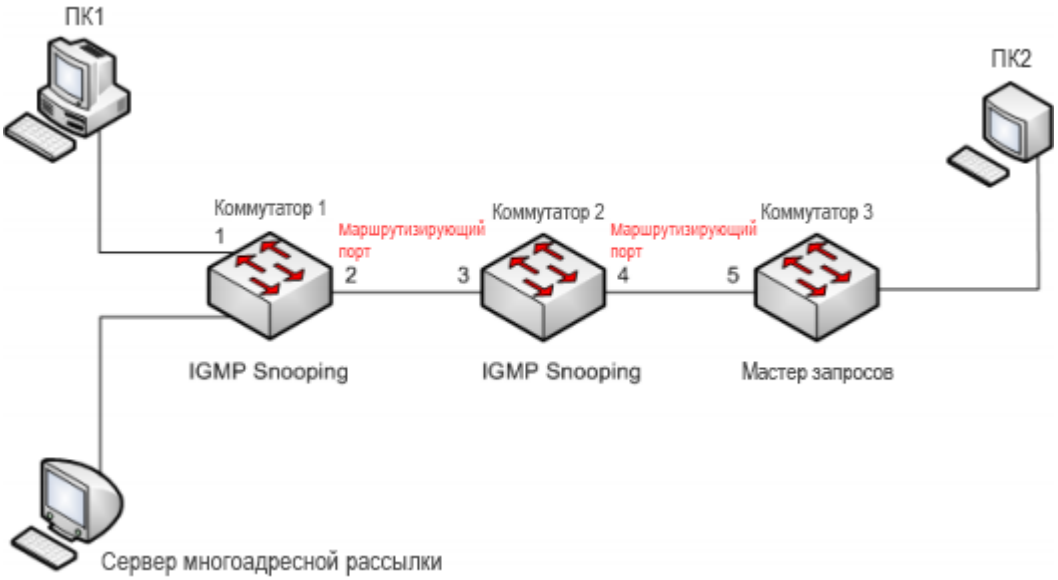



Рисунок 286 – Пример применения IGMP Snooping

- Поскольку коммутатор 3 выбран в качестве мастера запросов, он периодически отправляет сообщение общего запроса.
- Порт 4 коммутатора 2 получает сообщение запроса. Он становится маршрутизирующим портом. Тем временем коммутатор 2 пересылает запрос с порта 3. Затем порт 2 коммутатора 1 выбирается в качестве маршрутизирующего порта, как только он получает запрос от коммутатора 2.
- Когда ПК 1 присоединяется к группе многоадресной рассылки 225.1.1.1, он отправляет отчётное сообщение IGMP, поэтому порт 1 и маршрутизирующий порт 2 коммутатора 1 также присоединяются к группе многоадресной рассылки 225.1.1.1. Затем сообщение с отчётом IGMP будет перенаправлено на коммутатор 2 через маршрутизирующий порт 2, поэтому порт 3 и порт 4 коммутатора 2 также присоединятся к 225.1.1.1, а затем сообщение с отчётом IGMP будет перенаправлено на коммутатор 3 через маршрутизирующий порт 4, поэтому порт 5 коммутатора 3 также присоединится к 225.1.1.1.
- Когда данные сервера многоадресной рассылки достигают коммутатора 1, они будут перенаправлены на ПК1 через порт 1. Поскольку маршрутизирующий порт 2 также является членом группы многоадресной рассылки, данные будут пересылаться через

него. Таким образом, когда данные достигают порта 5 коммутатора 3, он прекратит пересылку, потому что получателя больше нет. Но если ПК2 также присоединится к группе 255.1.1.1, многоадресные данные будут перенаправлены на ПК2.

# 6.18 GMRP

## 6.18.1 GARP. Введение

Generic Attribute Registration Protocol (GARP) используется для распространения, регистрации и удаления определённой информации (VLAN, адреса многоадресных групп) между коммутаторами сети.
Благодаря GARP, информация о настройках коммутатора может быть передана по всей локальной сети. Объекты GARP, передают друг другу инструкции о регистрации или отмене тех или иных настроек путём отправки соответствующих join и leave-сообщений.
GARP предусматривает три типа сообщений: Join, Leave и LeaveAll.

- Когда объект GARP хочет передать свои настройки другим коммутаторам, он отсылает Join-сообщение. Join-сообщения бывают двух типов: JoinEmpty и JoinIn. Сообщение JoinIn отправляется для зарегистрированного свойства, в то время как JoinEmpty – для свойства, которое ещё не было зарегистрировано.
- Когда объект GARP хочет удалить свои настройки с других коммутаторов, он отправляет сообщение Leave. Сообщения Leave делятся на два типа: LeaveEmpty и LeaveIn. Сообщение LeaveIn отправляется для отмены зарегистрированного атрибута, а сообщение LeaveEmpty – для отмены еще не зарегистрированного атрибута.
- После запуска объекта GARP, он начинает отсчитывать период LeaveAll. Когда период заканчивается, объект отсылает сообщение LeaveAll.

---

«Объект» означает порт, на котором включен GARP.

---

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

**Таймер Hold.** При получении сообщения о регистрации настроек, объект GARP не отправляет сообщение Join сразу, а запускает таймер Hold. Когда таймер заканчивает отсчёт, объект отправляет все сообщения о настройках, полученные за этот период в одном Join-сообщении, что уменьшает количество передаваемых данных по сети.

**Таймер Join.** Для того, чтобы убедиться, что Join-сообщения получены другими объектами, после отправки сообщения Join объект GARP запускает таймер Join. Если за период до истечения установленного срока в ответ не получено JoinIn-сообщение, объект отправляет Join-сообщение снова. В противном случае, сообщение Join не отправляется.

**Таймер Leave.** Если объект GARP хочет удалить информацию об атрибуте, он отсылает Leave-сообщение. Объект, получивший это сообщение, запускает таймер Leave. Если он не получает ни одного Join-сообщения до истечения таймера, он удаляет информацию о данном атрибуте.

**Таймер LeaveAll.** При старте объекта GARP, запускается таймер LeaveAll. По его истечении, объект отправляет LeaveAll-сообщение для того, чтобы другие объекты GARP перерегистрировали все свои свойства. После этого объект запускает таймер LeaveAll заново.

## 6.18.2 Протокол GMRP

GARP Multicast Registration Protocol (GMRP) – многоадресный протокол регистрации, основанный на принципах GARP. Он используется для поддержки информации о мультикастовых группах на коммутаторах. Все коммутаторы, поддерживающие GMRP, могут получать регистрационную информацию от других коммутаторов, динамически обновлять информацию о зарегистрированных мультикастовых группах, а также передавать собственную регистрационную информацию другим коммутаторам. Механизм обмена информации гарантирует единообразие информации о многоадресной рассылке на всех GMRP-коммутаторах сети.
Если коммутатор или терминал хотят войти или выйти из мультикастовой группы, GMRP-порт передаёт информацию об этом в широковещательном режиме на все порты своей VLAN.

## 6.18.3 Пояснение

Порт-агент: обозначает порт, на котором включены функции GMRP и агента.
Порт распространения: обозначает порт, на котором включена только функция GMRP, без функции прокси.
Динамически полученные мультикастовые записи GMRP и информация об агенте передаётся портом распространения на порты распространения устройств нижнего уровня.
Все таймеры GMRP одной сети должны подчиняться одним и тем же правилам во избежание взаимоисключений. Таймеры должны следовать следующим правилам: таймер Hold < таймер Join, 2*(таймер Join) < таймер Leave, а таймер Leave < таймер LeaveAll.

## 6.18.4 Настройка с помощью WEB-интерфейса

1. Включение протокола GMRP.
Нажмите [Device Advanced Configuration] → [Multicast protocol configuration] → [GMRP configuration] → [GMRP configuration], чтобы открыть страницу конфигурации GMRP, как показано на рисунке 287.

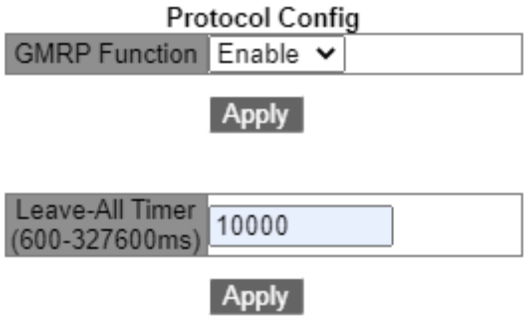



Рисунок 287 – Настройка протокола GMRP

**GMRP function (функция GMRP)**
Варианты: Enable/Disable (включить/выключить).
По умолчанию: Disable (выключено).
Функция: включение/выключение функции GMRP. Протокол не может работать одновременно с протоколом IGMP Snooping.

**Leave-All timer таймер (Leave-All)**
Диапазон: 100 мс~327600 мс.
По умолчанию: 10000 мс.
Функция: настройка временного интервала для отправки сообщений "LeaveAll". Интервал должен быть кратен 100.
Пояснение: если на разных устройствах таймеры LeaveAll истекут одновременно, они отправят множество сообщений "LeaveAll" одновременно. Для того, чтобы избежать подобной ситуации, которая может повысить нагрузку на сеть, рабочее значение таймеров LeaveAll должно быть случайным значением, которое больше изначального значения таймера LeaveAll, но меньше чем 1.5 значения этого таймера.

2. Настройка функции GMRP для порта (см. рисунок 288).

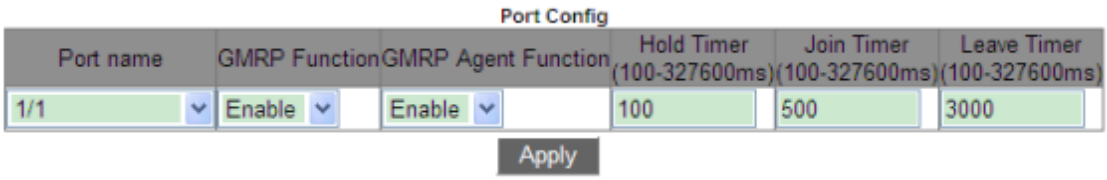



Рисунок 288 – Настройка GMRP для порта

**Port name (имя порта)**
Варианты: все порты коммутатора.

**Функция GMRP**
Варианты: Enable/Disable (включить/выключить).
По умолчанию: Disable (выключено).
Функция: включение или выключение функции GMRP на порту.

**Функция агента GMRP**
Варианты: Enable/Disable (включить/выключить).
По умолчанию: Disable (выключено).
Функция: включение или выключение функции GMRP агента на порту

---

- Порт-агент не может распространять информацию об агенте.
- До включения функции GMRP агента нужно включить функцию GMRP на данном порту.

---

**Hold Timer (таймер Hold)**
Диапазон: 100 мс~327600 мс.
Значение по умолчанию: 100 мс.
Описание: значение должно быть кратно 100. Рекомендуется устанавливать одинаковое значение для всех GMRP портов.

**Join Timer (таймер Join)**
Диапазон: 100 мс~327600 мс.
Значение по умолчанию: 500 мс.
Значение должно быть кратно 100. Рекомендуется устанавливать одинаковое значение для всех GMRP портов.

**Leave Timer (таймер Leave)**
Диапазон: 100 мс~327600 мс.
Значение по умолчанию: 3000 мс.
Значение должно быть кратно 100. Рекомендуется устанавливать одинаковое значение для всех GMRP портов.

3. Добавление записи агента GMRP.
Нажмите [Device Advanced Configuration] → [Multicast protocol configuration] → [GMRP configuration] → [GMRP agent configuration], чтобы открыть страницу настройки агента GMRP, как показано на рисунке 289.

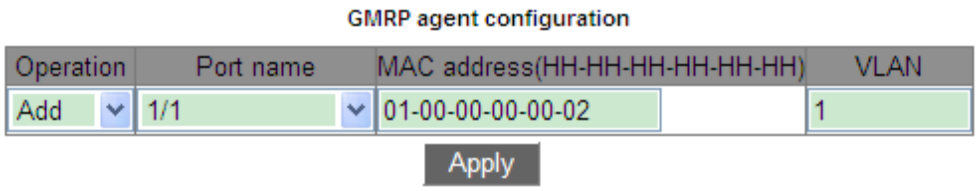



Рисунок 289 – Настройка записи GMRP-агента

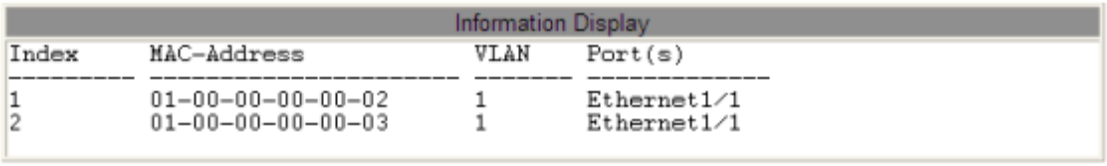
**Operation (действие)**
Варианты: Add/Del (добавить/удалить).
По умолчанию: Add (добавить).
Действие: добавить или удалить запись.

**Port name (имя порта)**
Варианты: все настроенные порты-агенты

**MAC address (MAC-адрес)**
Формат: FF-FF-FF-FF-FF-FF (F – это шестнадцатеричное число).
Функция: настройка MAC-адреса мультикастовой группы. Младший бит первого байта равен 1.

**VLAN**
Варианты: все созданные VLAN.
Функция: настройка номера VLAN для GMRP агента.
Описание: информация о GMRP агенте может передаваться через порты распространения только с тем же VLAN ID, что указан для порта-агента.

4. Просмотр записей агентов GMRP.
Нажмите [Device Advanced Configuration] → [Multicast protocol configuration] → [GMRP configuration] → [Show GMRP agent configuration], чтобы отобразить записи GMRP-агентов, как показано на рисунке 290.


Information Display

| Index | MAC-Address | VLAN | Port(s) |
|---|---|---|---|
| 1 | 01-00-00-00-00-02 | 1 | Ethernet1/1 |
| 2 | 01-00-00-00-00-03 | 1 | Ethernet1/1 |

Рисунок 290 – Записи агентов GMRP

5. Участники многоадресной рассылки этой агентской записи на подключенном соседнем устройстве отображаются как показано на рисунке 291.
Подключение должно удовлетворять следующим условиям:

- Функция GMRP включена на взаимосвязанных устройствах.
- Два порта, которые соединяют устройства, должны быть портами распространения, а порт распространения на локальном устройстве должен соответствовать VLAN ID записи агента.

**GMRP Dynamic Multicast List**

| Index | Multicast MAC | VLAN ID | Member Port |
|---|---|---|---|
| 1 | 01-00-00-00-00-03 | 1 | FE15 |
| 2 | 01-00-00-00-00-02 | 1 | FE15 |

Рисунок 291 – Таблица динамической многоадресной рассылки GMRP

**GMRP dynamic multicast (динамическая многоадресная рассылка GMRP)**
Шаблоны: {Index, Multicast MAC, VLAN ID, Member Port} – {индекс, MAC-адрес многоадресной рассылки, VLAN ID, порт-участник}

Функция: просмотр динамических многоадресных записей GMRP.

## 6.18.5 Пример типовой настройки

Как показано на рисунке 292, коммутатор A и коммутатор B подключены через порт 2. Порт 1 коммутатора A настроен как порт-агент и создает две многоадресные записи:
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.

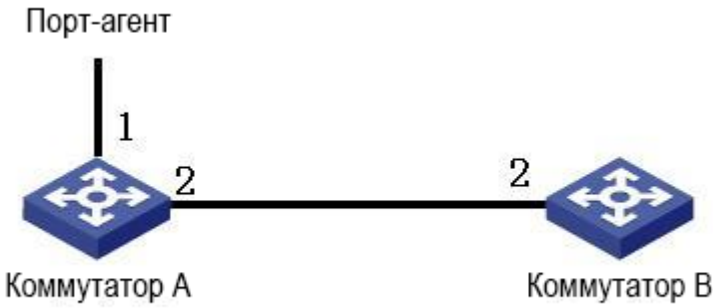



Рисунок 292 – Сеть GMRP

**Настройка коммутатора A:**
1. Включите глобальную функцию GMRP на коммутаторе A; установите для таймера LeaveAll значение по умолчанию, как показано на рисунке 287.
2. Включите функцию GMRP и функцию агента для порта 1; включите только функцию GMRP для порта 2; установите для таймеров значения по умолчанию, как показано на рисунке 288.
3. Настройте многоадресную запись агента. Установите <MAC-адрес, идентификатор VLAN, порт-участник> на <01-00-00-00-00-01, 1, 1> и <01-00-00-00-00-02, 2, 1>, как показано на рисунке 289.

**Настройка коммутатора B:**
4. Включите глобальную функцию GMRP на коммутаторе B; установите для таймера LeaveAll значение по умолчанию, как показано на рисунке 287.
5. Включите функцию GMRP на порту 2; установите для таймеров значения по умолчанию, как показано на рисунке 288.
В таблице 12 перечислены динамические записи многоадресной рассылки GMRP на коммутаторе B.

Таблица 12 – Динамические мультикастовые записи

| Атрибут порта 2 на коммутаторе A | Атрибут порта 2 на коммутаторе B | Многоадресные записи, полученные на коммутаторе B |
|---|---|---|
| Access VID=1 | Access VID=1 | MAC: 01-00-00-00-00-01<br>VLAN ID: 1<br>Member port: 2 |
| Access VID=2 | Access VID=2 | MAC: 01-00-00-00-00-02<br>VLAN ID: 2<br>Member port: 2 |
| Access VID=1 | Access VID=2 | MAC: 01-00-00-00-00-01<br>VLAN ID: 2<br>Member port: 2 |

## 6.19 Настройка действия с незарегистрированными многоадресными данными

### 6.19.1 Введение

Незарегистрированные многоадресные пакеты – это пакеты, которые отправлены на групповой адрес, который не был объявлен или зарегистрирован на сетевом устройстве. Такие пакеты могут появиться, например, в случае, если отправитель пытается передавать данные на новый групповой адрес, который еще не известен в сети. При получении незарегистрированного многоадресного пакета коммутатор транслирует его всем портам, находящимся в данной VLAN, кроме порта на котором данный пакет был получен. Это требует значительной ширины полосы пропускания сети, что отрицательно влияет на скорость передачи. В таком случае может быть включена функция отбрасывания незарегистрированных мультикастовых пакетов. Если эта функция включена, после получения незарегистрированного пакета коммутатор отбрасывает его, а не пересылает.

### 6.19.2 Настройка с помощью WEB-интерфейса

1. Настройка незарегистрированного многоадресного действия.
Нажмите [Device Advanced Configuration] → [Multicast protocol configuration] → [Unregistered multicast action configuration], чтобы открыть страницу настройки действия с незарегистрированными многоадресными пакетами, как показано на рисунке 293.


Рисунок 293 – Настройка действия с незарегистрированными многоадресными данными

**Unregistered multicast action (действие с незарегистрированным мультикастом)**
Варианты: Forward/Discard (переслать/отбросить).
По умолчанию: Forward (переслать).
Функция: настройка действия с незарегистрированными многоадресными данными.

2. Настройка порта отслеживания многоадресного потока (см. рисунок 294).

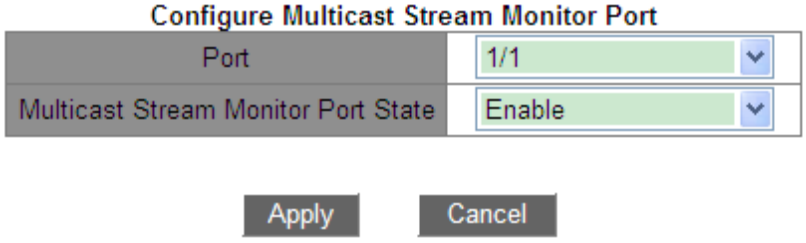



Рисунок 294 – Настройка порта отслеживания многоадресного потока

**Multicast Stream Monitor Port State (состояние порта отслеживания многоадресного потока)**
Варианты: Disable/Enable (отключить/включить).
По умолчанию: Disable (отключить).
Функция: настройка порта отслеживания многоадресного потока. Этот порт перенаправляет потоки службы многоадресной рассылки (включая зарегистрированный и незарегистрированный поток), полученные другими портами в той же сети VLAN. Функция в основном используется для многоадресного мониторинга.

---

- Если для незарегистрированного многоадресного действия настроено отбрасывание, порт отслеживания многоадресного потока настроить нельзя.
- Если порт отслеживания многоадресной рассылки доступен, незарегистрированный поток многоадресной рассылки перенаправляется только на него. Если недоступен, поток перенаправляется на все порты VLAN.
- Порт отслеживания не поддерживает протокол многоадресной рассылки; следовательно, он не может быть настроен как участник мультикастовой группы.

---

# 6.20 Статическая настройка многоадресной рассылки

## 6.20.1 Введение

Таблица мультикастовых адресов может быть настроена статически. В таблицу добавляется запись в виде {VLAN ID, Multicast MAC address, Multicast member port}, и сообщение многоадресной рассылки будет перенаправлено на соответствующий порт-участник в соответствии с записью.

## 6.20.2 Настройка с помощью WEB-интерфейса

1. Добавление статической многоадресной записи.
Нажмите [Device Advanced Configuration] → [Multicast protocol configuration] → [Static Multicast Configuration], чтобы перейти на страницу статической настройки многоадресной рассылки, как показано на рисунке 295.

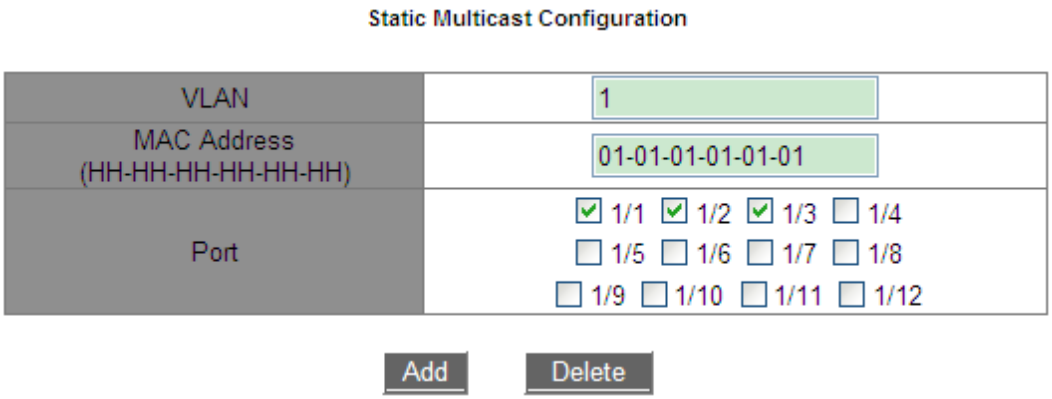



Рисунок 295 – Добавление статической многоадресной записи

**VLAN**
Варианты: все существующие идентификаторы VLAN.
Функция: указать значение идентификатора VLAN для статической многоадресной записи. Только порты-участники данной VLAN могут пересылать это многоадресное сообщение.

**MAC Address (MAC-адрес)**
Формат: HH-HH-HH-HH-HH-HH (H — шестнадцатеричное число).
Функция: настройка адреса группы многоадресной рассылки. Младший бит старшего байта равен 1.

**Port (порт)**
Функция: выбрать порты мультикастового адреса. Если хост, подключенный к порту, хочет получать определенные данные группы многоадресной рассылки, статически добавьте этот порт в группу многоадресной рассылки и назначьте статическим портом-участником. Нажмите кнопку <Add>, чтобы добавить статическую многоадресную запись; нажмите кнопку <Delete>, чтобы удалить запись.

2. Отображение статических многоадресные записей (см. рисунок 296).

| VLAN | MAC Address | Port |
|---|---|---|
| 2 | 03-01-01-01-01-01 | 1/1 1/4 |
| 1 | 01-01-01-01-01-01 | 1/1 1/2 1/3 |
| 1 | 01-00-00-00-00-01 | 1/1 1/2 |

Рисунок 296 – Таблица статических многоадресные записей

# 6.21 LLDP

## 6.21.1 Введение

LLDP (Link Layer Discovery Protocol) предоставляет стандартный механизм поиска второго уровня. Он собирает информацию, такую как возможности устройства, адрес, идентификатор устройства и интерфейса в пакет Link Layer Discovery Protocol Data Unit (LLDPDU), и передаёт LLDPDU своим непосредственно подключенным соседям. При получении LLDPDU, соседние устройства сохраняют эту информацию в MIB для предоставления NMS данной информации, а также информации о состоянии соединения между устройствами.

## 6.21.2 Настройка с помощью WEB-интерфейса

1. Включение LLDP.
Нажмите [Device Advanced Configuration] → [LLDP configuration] → [LLDP configuration], чтобы открыть страницу настройки LLDP, как показано на рисунке 297.


Рисунок 297 – Включение LLDP

**LLDP configuration (настройка LLDP)**
Варианты: Enable/Disable (включить/отключить).
По умолчанию: Disable (отключить).
Функция: включение LLDP.

2. Включение функции адреса управления в TLV (Type-Length-Value), как показано на рисунке 298.


Рисунок 298 – Включение адреса управления TLV

**TLV Management Address (адрес управления TLV)**
Варианты: Enable/Disable (включить/отключить).
По умолчанию: Disable (отключить).
Функция: отправка IP-адреса интерфейса (то есть основного IP-адреса первого интерфейса VLAN, в котором находится этот порт) на подключенное устройство, когда эта функция отключена. Если IP-адрес не настроен для интерфейса VLAN, где находится данный порт, IP-адрес интерфейса — 127.0.0.1. После включения данной функции на соседнее устройство отправляется IP-адрес интерфейса и все IP-адреса, настроенные для текущего устройства. Можно отправить до 64 адресов управления.

---

Когда адрес управления на локальном устройстве включен в TLV, и подключающееся соседнее устройство может анализировать функцию TLV, оно будет корректно отображать все настроенные IP-адреса локального коммутатора.

---

3. Просмотр информации LLDP.
Нажмите [Device Advanced Configuration] → [LLDP configuration] → [Show lldp], чтобы отобразить информацию LLDP, как показано на рисунках 299 –302.

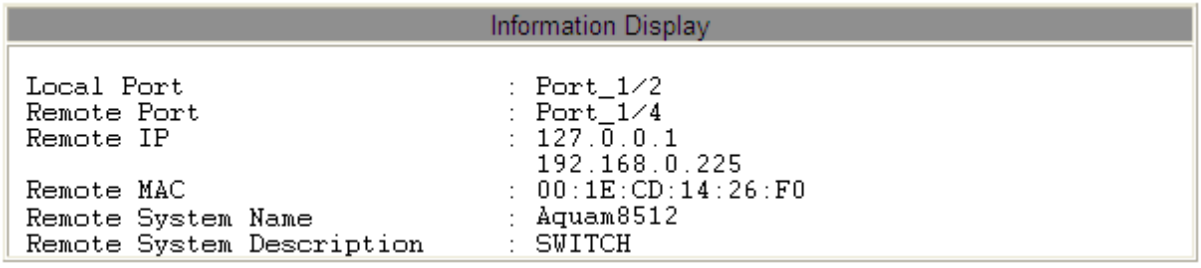



Рисунок 299 – Информация LLDP-1, когда адрес управления включен в TLV

На предыдущем рисунке показано условие, при котором IP-адрес не настроен для первого интерфейса VLAN, где находится порт 3/4.

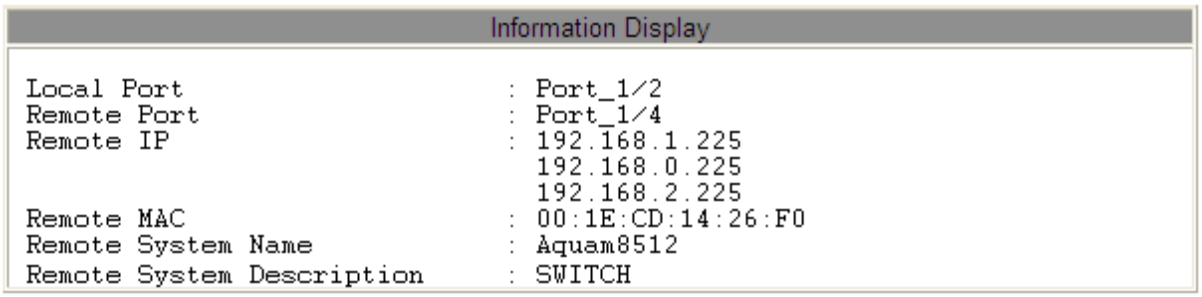



Рисунок 300 – Информация LLDP-2, когда адрес управления включен в TLV

На предыдущем рисунке показано условие, при котором первичный IP-адрес первого интерфейса VLAN, где находится порт 3/4, настроен как 192.168.1.225.
Когда в TLV разрешён адрес управления, отображаемая информация LLDP включает в себя подключенный локальный порт коммутатора, удаленный порт соседнего устройства, IP-адрес интерфейса, все настроенные IP-адреса, MAC-адрес и системную информацию соседнего устройства.

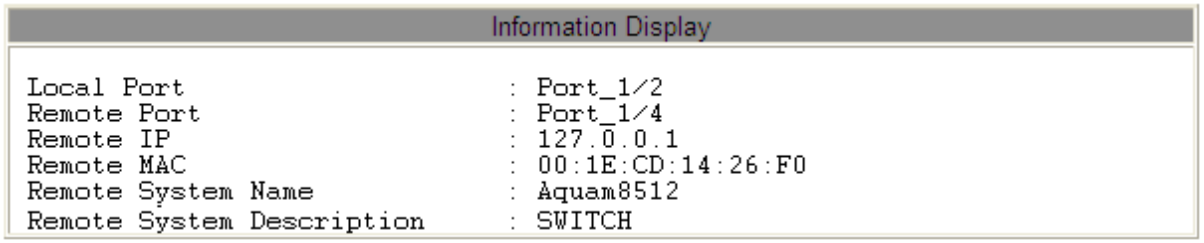



Рисунок 301 – Информация LLDP-1, когда адрес управления не включен в TLV

На предыдущем рисунке показано условие, при котором IP-адрес не настроен для первого интерфейса VLAN, где находится порт 3/4.

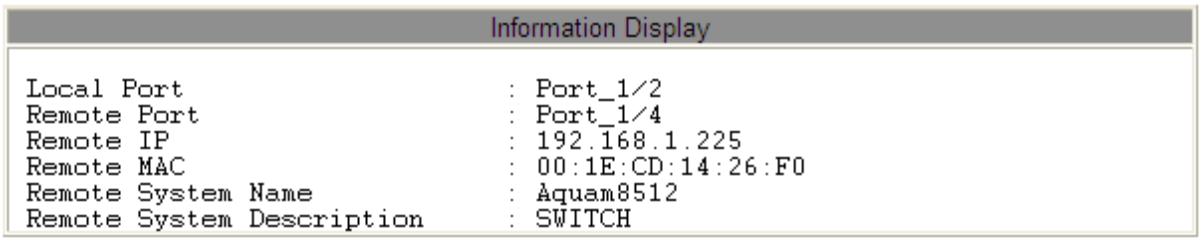



Рисунок 302 – Информация LLDP-1, когда адрес управления не включен в TLV

На предыдущем рисунке показано условие, при котором первичный IP-адрес первого интерфейса VLAN, где находится порт 3/4, настроен как 192.168.1.225.
Когда в TLV не разрешён адрес управления, отображаемая информация LLDP включает в себя подключенный локальный порт коммутатора, удаленный порт соседнего устройства, IP-адрес интерфейса, MAC-адрес и системную информацию соседнего устройства.

Для отображения информации LLDP устройства с поддержкой этой функции должны быть подключены друг к другу.

## 6.22 VRRP

Маршрутизаторы в этой главе относятся к коммутаторам 3-го уровня.

### 6.22.1 Введение

VRRP (Virtual Router Redundancy Protocol) добавляет несколько маршрутизаторов, которые могут действовать как сетевые шлюзы, в группу VRRP, которая образует виртуальный маршрутизатор. С помощью механизма выбора VRRP в группе определяется мастер, остальные маршрутизаторы становятся резервными. В случае выхода мастера из строя, среди резервных маршрутизаторов выбирается новый мастер, что обеспечивает бесперебойную передачу данных без изменения конфигурации.

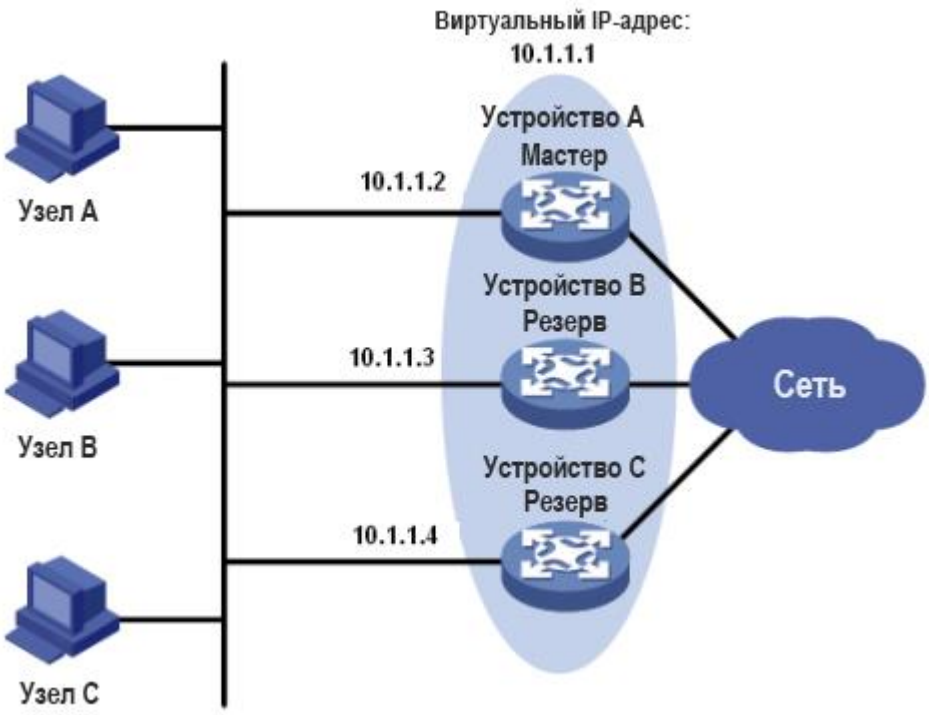



Рисунок 303 – VRRP

Как показано на рисунке 303, устройства A, B и C образуют виртуальный маршрутизатор с IP-адресом. Узлы могут взаимодействовать с внешними сетями через виртуальный маршрутизатор только в том случае, если его IP-адрес настроен как следующий переход (хоп) маршрута по умолчанию на узлах. Виртуальный маршрутизатор состоит из одного

главного и нескольких резервных коммутаторов. Мастер действует как шлюз. В случае сбоя один из резервных коммутаторов возьмет на себя функции вышедшего из строя мастера и будет выступать в качестве шлюза.

- IP-адрес виртуального маршрутизатора может быть либо неиспользуемым IP-адресом в сегменте, где находится группа VRRP, либо IP-адресом интерфейса маршрутизатора из этой группы.
- Маршрутизатор, IP-адрес интерфейса которого совпадает с адресом виртуального маршрутизатора, является владельцем IP-адреса.
- В каждой группе VRRP может быть только один владелец IP-адреса.

## 6.22.2 Выбор мастера

1. Маршрутизатор с наивысшим приоритетом в группе VRRP выбирается в качестве мастера. Он периодически отправляет объявления VRRP, чтобы информировать другие маршрутизаторы в группе о том, что он работает корректно.

Приоритет VRRP находится в диапазоне от 0 до 255. Чем больше число, тем выше приоритет. Приоритеты от 1 до 254 настраиваются. Приоритет 0 зарезервирован для специального использования, а приоритет 255 — для владельца IP-адреса.

2. Резервные маршрутизаторы получают приоритеты других маршрутизаторов в группе путем обмена пакетами VRRP.

- Если приоритет мастера в объявлении выше его собственного приоритета, маршрутизатор остается резервным.
- Если приоритет мастера в объявлении ниже, чем собственный приоритет маршрутизатора, маршрутизатор берет на себя роль мастера в вытесняющем режиме и остается резервным в невытесняющем режиме.
- Если в течение определенного периода не было получено объявлений VRRP, маршрутизатор считает, что мастер вышел из строя, и отправляет объявления VRRP, чтобы начать новый выбор мастера.

- Невытесняющий режим: когда маршрутизатор в группе VRRP становится ведущим, он остается ведущим до тех пор, пока работает нормально, даже если резервному маршрутизатору позднее будет присвоен более высокий приоритет.
- Вытесняющий режим: когда резервный маршрутизатор обнаруживает, что его приоритет выше приоритета мастера, он отправляет объявления VRRP, чтобы начать новый выбор мастера в группе VRRP.

## 6.22.3 Мониторинг указанного интерфейса

Если интерфейс восходящей линии связи маршрутизатора в группе VRRP выходит из строя, обычно группа не может знать об отказе такого интерфейса. Если маршрутизатор является мастером, узлы в локальной сети не могут получить доступ к внешним сетям. Эту проблему можно решить, отслеживая указанный интерфейс восходящей линии связи. В случае сбоя интерфейса приоритет ведущего устройства автоматически снижается на указанное значение, и маршрутизатор с более высоким приоритетом в группе VRRP становится ведущим.

## 6.22.4 Настройка с помощью WEB-интерфейса

1. Создание/удаление группы VRRP.
Нажмите [Device Advanced Configuration] → [VRRP Configuration] → [Create/Remove VRRP], чтобы открыть страницу настройки группы VRRP, как показано на рисунке 304.

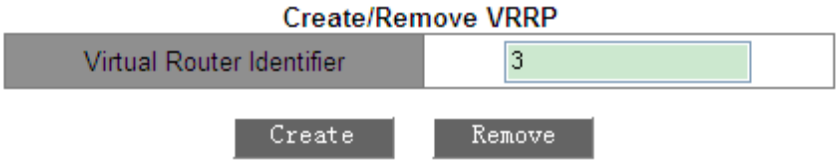



Рисунок 304 – Создание группы VRRP

**Virtual Router Identifier (идентификатор виртуального маршрутизатора)**
Диапазон: 1~255.
Функция: назначить идентификатор группы VRRP.
Примечание. Коммутаторы серии поддерживают до 10 групп VRRP.

2. Настройка IP-адреса виртуального маршрутизатора.
Нажмите [Device Advanced Configuration] → [VRRP Configuration] → [VRRP Initialization], чтобы открыть страницу инициализации VRRP, как показано на рисунке 305.

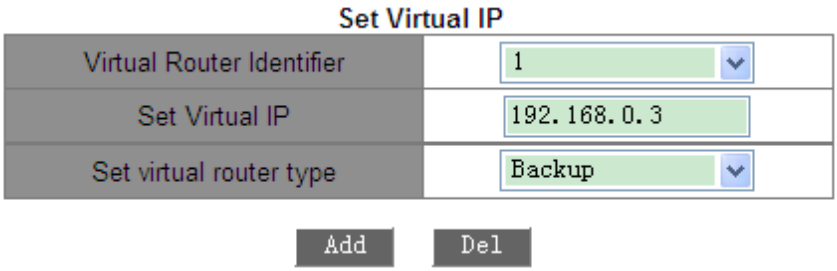



Рисунок 305 – Настройка IP-адреса виртуального маршрутизатора

**Set Virtual IP (настройка виртуального IP-адреса)**
Формат: A.B.C.D.

Функция: настроить IP-адрес виртуального маршрутизатора.
Примечание. IP-адрес виртуального маршрутизатора должен находиться в том же сегменте сети, что и IP-адрес интерфейса.

**Set virtual router type (выбрать тип виртуального маршрутизатора)**
Варианты: Master/Backup (основной/резервный).
Описание: «Master» указывает, что данное устройство является владельцем IP-адреса виртуального маршрутизатора. «Backup» указывает, что данное устройство не является владельцем IP-адреса виртуального маршрутизатора.

3. Настройка интерфейса 3-го уровня для VRRP, как показано на рисунке 306.

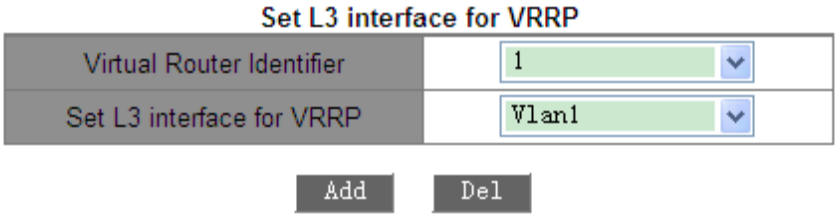



Рисунок 306 – Настройка интерфейса 3-го уровня для VRRP

Функция: настройка интерфейса 3-го уровня для указанной группы VRRP.

4. Настройка режима работы группы VRRP.
Нажмите [Device Advanced Configuration] → [VRRP Configuration] → [Set preempt mode], чтобы открыть страницу конфигурации рабочего режима VRRP, как показано на рисунке 307.

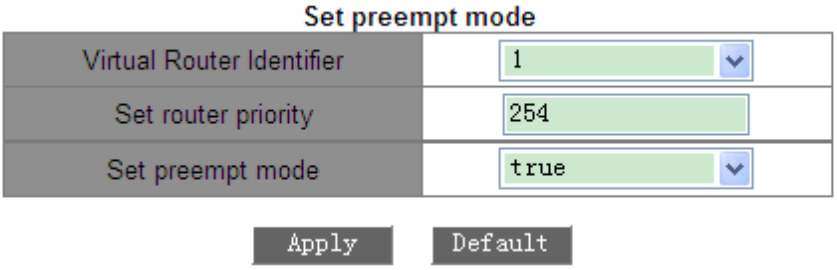



Рисунок 307 – Настройка режима работы группы VRRP

**Set router priority (установить приоритет маршрутизатора)**
Диапазон: 1~254.
По умолчанию: 100 (для не владельцев IP-адресов).
Функция: установить приоритет маршрутизатора в группе VRRP.

**Set preempt mode (установить режим вытеснения)**
Варианты: true/false (правда/ложь).
По умолчанию: true (правда).

Функция: настройка режима работы виртуального маршрутизатора.
Описание: «true» указывает на вытесняющий режим, а «false» – на невытесняющий.

5. Настройка интервала передачи объявлений.
Нажмите [Device Advanced Configuration] → [VRRP Configuration] → [Set advertisement interval, monitor interface and connectivity check], чтобы открыть страницу настройки, как показано на рисунке 308.

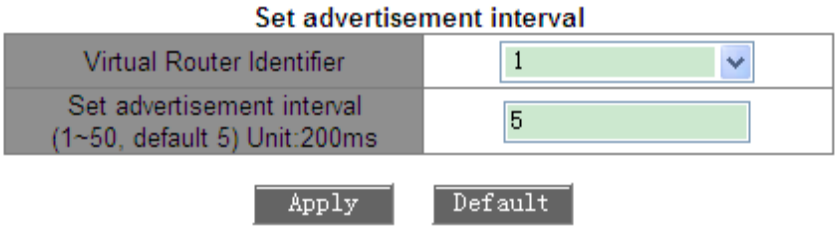



Рисунок 308 – Настройка интервала передачи объявлений

**Set advertisement interval (установить интервал передачи объявлений)**
Диапазон: 1~50 (единица измерения: 200 мс).
Значение по умолчанию: 5×200 мс.
Функция: установка интервала, через который главный маршрутизатор будет отправлять объявления VRRP.

6. Настройка контролируемого интерфейса (см. рисунок 309).

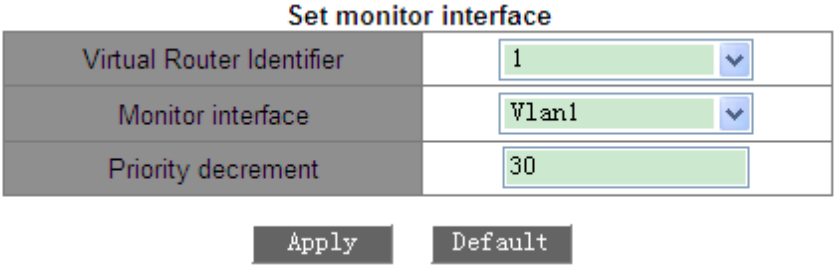



Рисунок 309 – Настройка контролируемого интерфейса

**Monitor Interface (контролируемый интерфейс)**
Функция: выбор интерфейса VLAN для мониторинга.

**Priority decrement (декремент приоритета)**
Диапазон: 1~253.
Функция: настройка, позволяющая выбрать, насколько сильно должен снижаться приоритет маршрутизатора в виртуальной группе.

---

- Владелец IP-адреса виртуального маршрутизатора не может быть настроен в качестве контролируемого интерфейса.

- Приоритет главного маршрутизатора после понижения должен быть меньше, чем у резервного маршрутизатора.

---

7. Настройка параметров аутентификации VRRP.
Нажмите [Device Advanced Configuration] → [VRRP Configuration] → [VRRP Authentication], чтобы открыть страницу настройки аутентификации VRRP, как показано на рисунке 310.

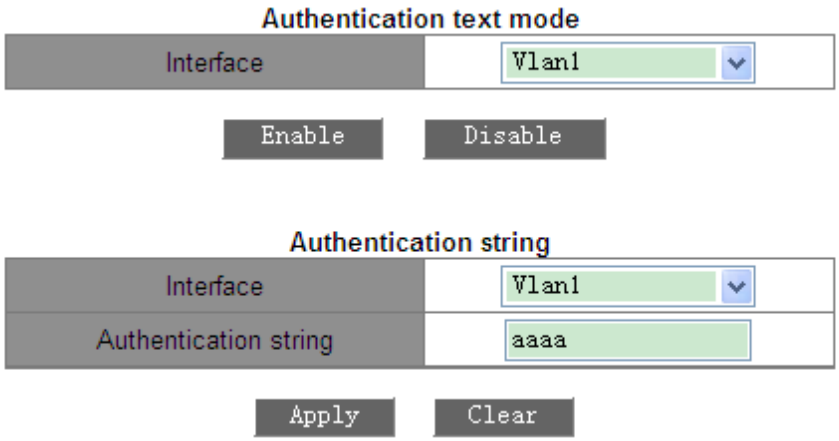



Рисунок 310 – Настройка параметров аутентификации VRRP

**Authentication text mode (текстовый режим аутентификации)**
Функция: включение интерфейса, требующий простой аутентификации. Маршрутизатор, отправляющий пакет VRRP, добавляет в пакет ключ аутентификации. Маршрутизатор, получивший пакет, сравнивает ключ аутентификации в пакете с локальным ключом. Если два ключа аутентификации идентичны, пакет считается законным и истинным. В противном случае пакет является нелегитимным.

**Authentication string (строка аутентификации)**
Диапазон: 1~8 символов.
Функция: настроить строку аутентификации.

9. Инициализация группы VRRP.
Нажмите [Device Advanced Configuration] → [VRRP Configuration] → [VRRP Initialization], чтобы открыть страницу инициализации VRRP, как показано на рисунке 311.

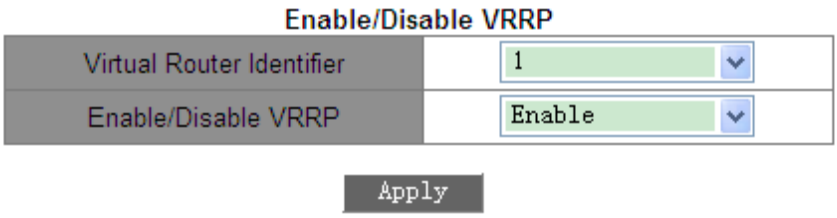



Рисунок 311 – Включение группы VRRP

## 6.22.5 Пример типовой настройки

Как показано на рисунке 312, коммутатор A и коммутатор B образуют виртуальный маршрутизатор с IP-адресом 192.168.2.4. Узел A может связываться с узлом B через виртуальный маршрутизатор. Когда коммутатор A работает правильно, он является мастером в группе VRRP. Когда коммутатор A или VLAN 3 выходит из строя, коммутатор B становится мастером.

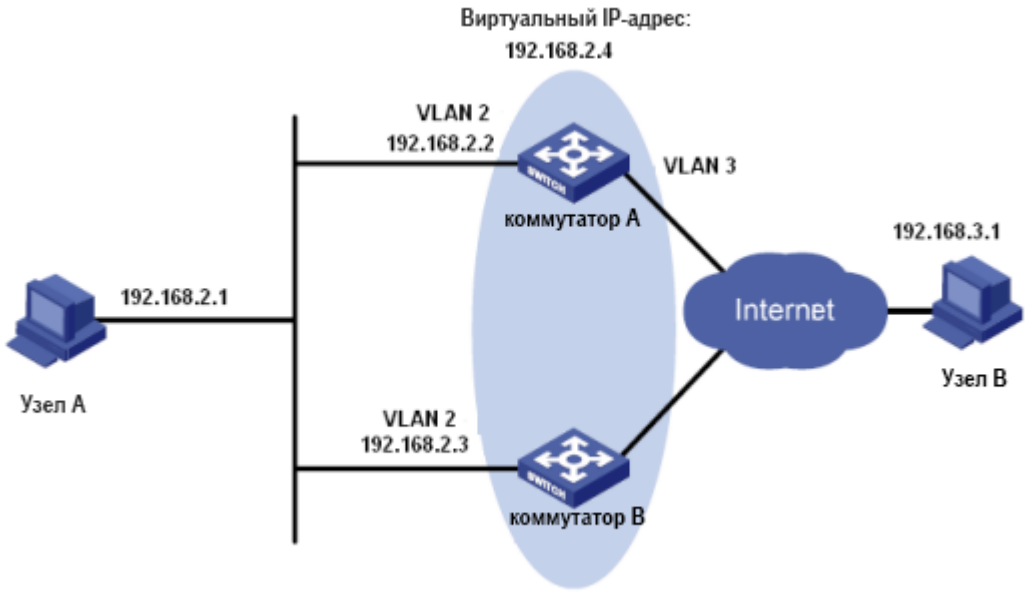



Рисунок 312 – Пример типовой настройки VRRP

**Настройка коммутатора A:**

1. Установите IP-адрес VLAN 2 на 192.168.2.2 и маску подсети на 255.255.255.0.
2. Создайте группу VRRP 1, как показано на рисунке 304.
3. Установите виртуальный IP-адрес группы VRRP 1 на 192.168.2.4 и тип маршрутизатора на Backup, как показано на рисунке 305.
4. Настройте VLAN 2 в качестве интерфейса 3-го уровня для группы VRRP 1, как показано на рисунке 306.
5. Установите для коммутатора A в группе VRRP приоритет 110, а для режима вытеснения — значение false, как показано на рисунке 307.
6. Настройте VLAN 3 в качестве отслеживаемого интерфейса и установите значение декремента приоритета на 30, как показано на рисунке 309.
7. Включите группу VRRP 1, как показано на рисунке 311.

**Настройка коммутатора B:**

1. Установите IP-адрес VLAN 2 на 192.168.2.3 и маску подсети на 255.255.255.0.
2. Создайте группу VRRP 1, как показано на рисунке 304.
3. Установите виртуальный IP-адрес группы VRRP 1 на 192.168.2.4 и тип маршрутизатора на Backup, как показано на рисунке 305.

4. Настройте VLAN 2 в качестве интерфейса 3-го уровня для группы VRRP 1, как показано на рисунке 306.
5. Установите для коммутатора B в группе VRRP приоритет 100, а для режима вытеснения — значение false, как показано на рисунке 307.
6. Включите группу VRRP 1, как показано на рисунке 311.

## 6.23 Настройка SNTP

### 6.23.1 Введение

SNTP (Simple Network Time Protocol) синхронизирует время между сервером и клиентом путём запросов и ответов. В роли клиента коммутатор синхронизирует своё время с временем сервера. Для одного коммутатора можно назначить множество SNTP серверов, однако активным из них может быть только один.
Клиент SNTP отправляет запрос каждому серверу. Первый ответивший сервер будет активным. Остальные серверы будут неактивны.

---

- Для синхронизации времени по SNTP должен существовать активный сервер SNTP.
- Вся информация о времени, передаваемая в протоколе SNTP, является стандартной информацией о времени для часового пояса 0.

---

### 6.23.2 Настройка с помощью WEB-интерфейса

1. Включение протокола SNTP.
Нажмите [Device Advanced Configuration] → [SNTP configuration] → [SNTP server configuration], чтобы перейти на страницу настройки SNTP, как показано на рисунке 313.

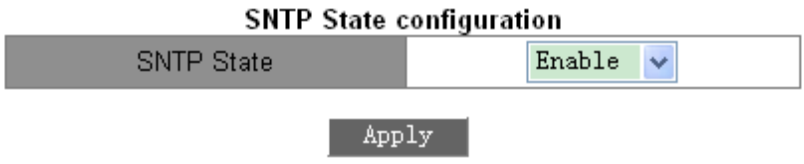



Рисунок 313 – Включение SNTP

**SNTP State (Состояние SNTP)**
Варианты: Enable/Disable (Включить/Выключить).
По умолчанию: Disable (Выключено).
Функция: включить или выключить SNTP.

---

Протоколы SNTP и NTP являются взаимоисключающими из-за того, что NTP и SNTP используют один UDP порт.

---

2. Настройка SNTP-сервера (см. рисунок 314).

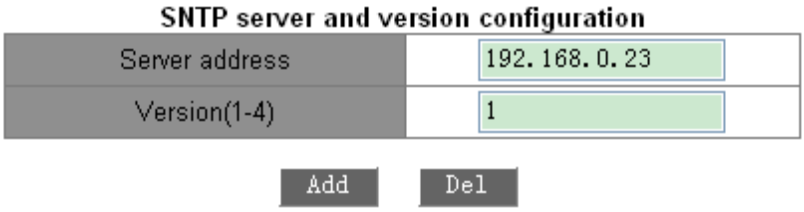



Рисунок 314 – Настройка сервера SNTP

**Server address (адрес сервера)**
Формат: A.B.C.D.
Функция: настройка IP-адреса сервера SNTP. Клиенты будут синхронизировать время в соответствии с пакетами сервера.

**Version (версия)**
Варианты: 1~4.
Функция: настройка версии SNTP.

---

Количество SNTP-серверов не ограничено, но для обеспечения корректной работы рекомендуется использовать не более 5 серверов.

---

3. Настройка временного интервала отправки запросов на синхронизацию, как показано на рисунке 315.

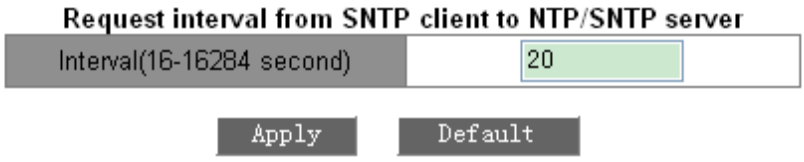



Рисунок 315 – Установка временного интервала для отправки запросов на синхронизацию

**Interval (интервал)**
Варианты: 16~16284 с.
Функция: настройка временного интервала для отправки запросов на синхронизацию.

4. Проверка синхронизации часов с сервера.
Нажмите [Device Basic Configuration] → [Switch Basic Configuration] → [clock config], чтобы открыть страницу с информацией о часах, как показано на рисунке 316.

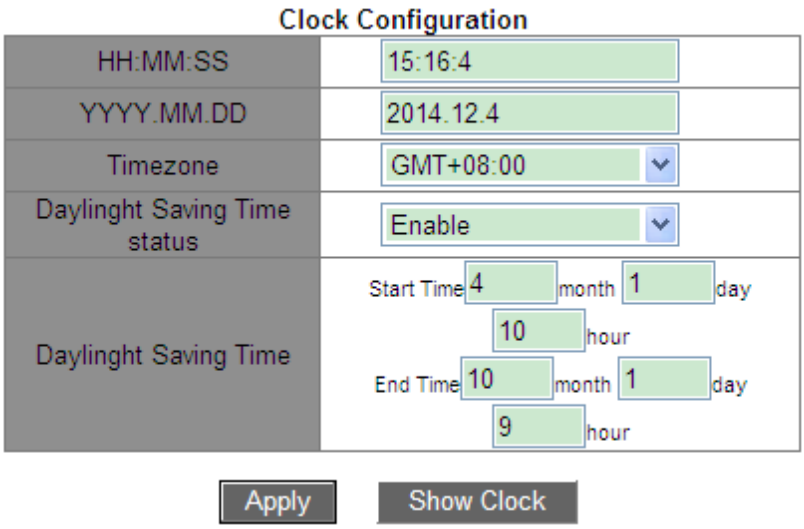



Рисунок 316 – Синхронизация часов

Нажмите <Show Clock>. На странице информационного дисплея отображается информация о часах после синхронизации с сервером SNTP.

5. Просмотр информации о конфигурации SNTP.
Нажмите [Device Advanced Configuration] → [SNTP configuration] → [SNTP information], чтобы просмотреть конфигурацию SNTP, как показано на рисунке 317.


Рисунок 317 – Информация о настройках SNTP

Значение «Last receive» отображает время, прошедшее с момента последней синхронизации.

## 6.24 Настройка NTP

### 6.24.1 Введение

NTP (Network Time Protocol) синхронизирует время между серверами и клиентами. NTP синхронизируют часы всех сетевых устройств, обеспечивая единое время на всех устройствах в сети. Таким образом может быть обеспечена работа множества систем, зависящих от точно синхронизированного времени. NTP-устройство не только может синхронизировать свои часы с источником, но и само служить источником для других устройств.

Как показано на рисунке 318, двусторонняя задержка «(T4-T1) - (T3-T2)» и смещение часов «((T2-T1) + (T3-T4)) / 2» могут быть рассчитаны на основе обмена NTP-пакетами, благодаря чему достигается высокоточная синхронизация часов между устройствами.

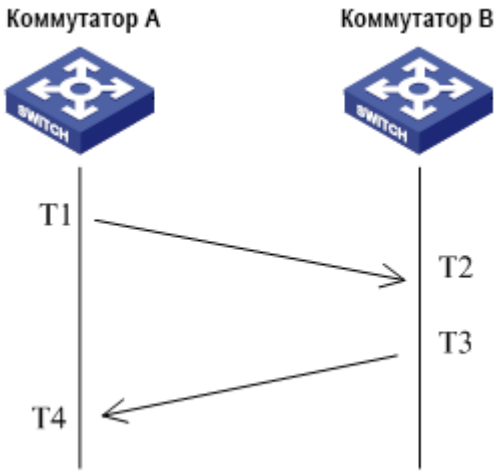



Рисунок 318 – NTP

## 6.24.2 Режимы работы NTP

NTP способен работать в различных режимах синхронизации времени. Вы можете выбрать наиболее подходящий вам режим.

Режим «клиент-сервер». В этом режиме клиент отправляет данные синхронизации на сервер (клиентский режим). Приняв данные, сервер автоматически возвращает ответ (серверный режим). После получения ответа клиент синхронизируется с часами сервера.

Одноранговый режим (Peer mode). В этом режиме, активное устройство (active peer) отсылает данные синхронизации неактивному (passive peer). После получения данных, неактивный узел отправляет ответ. Активные и пассивные узлы могут взаимно синхронизироваться. Если оба одноранговых узла синхронизировали время с других устройств, узел, имеющий более высокую страту часов, синхронизирует время с узлом, чья страта часов ниже.

Широковещательный режим. В этом режиме широковещательный сервер периодически рассылает пакеты синхронизации. При получении данных, клиенты отправляют ответ. После получения ответов, сервер отправляет синхронизационные данные, и так далее. Синхронизация включает обмен восемью пакетами запросов и ответов.

Многоадресный режим. Мультикастовый клиент периодически отправляет мультикастовые запросы синхронизации мультикастовому серверу. После получения пакетов сервер отправляет одноадресные ответные пакеты. Затем сервер и клиент выполняют синхронизацию часов, обмениваясь одноадресными запросами синхронизации часов и ответными пакетами.

## 6.24.3 Настройка с помощью WEB-интерфейса

1. Включение NTP.

Нажмите [Device Advanced Configuration] → [NTP configuration] → [NTP Global Configuration], чтобы открыть страницу глобальной настройки NTP, как показано на рисунке 319.

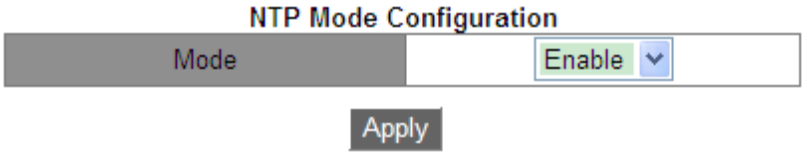



Рисунок 319 – Включение NTP

**Mode (режим)**
Варианты: Enable/Disable (включить/отключить).
По умолчанию: Disable (отключено).
Функция: включение или отключение функции глобальной службы NTP.

---

- NTP и SNTP нельзя запускать одновременно, поскольку они используют один и тот же номер порта UDP.
- Вы также можете настроить параметры NTP и сохранить конфигурацию, когда служба NTP отключена. Включение службы NTP не влияет на её настройку.

---

2. Настройка одноадресной передачи NTP (см. рисунок 320).

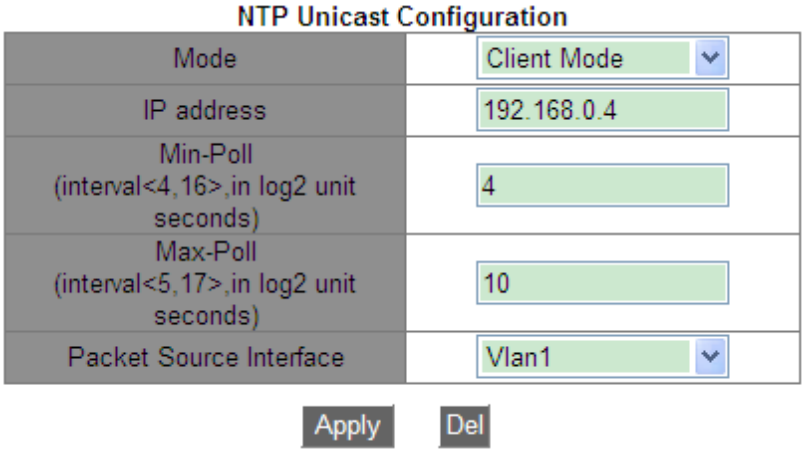



Рисунок 320 – Настройка одноадресной передачи NTP

**Mode (режим)**
Варианты: Client Mode/Peer Mode (режим клиента/одноранговый режим).
Функция: выбор режима работы NTP.
Описание: режим «Client Mode» означает, что NTP работает в режиме «клиент-сервер»; «Peer Mode» означает работу в одноранговом режиме.

**IP address (IP адрес)**
Формат: A.B.C.D.
Описание: если выбран режим «клиент-сервер», IP адрес является адресом NTP сервера. Если выбран одноранговый режим, IP адрес будет адресом пассивного узла.

**Min-Poll**
Диапазон: от 4 до 16. Интервал = $2^n$ с (n – значение этого параметра).
Значение по умолчанию: 4. В этом случае интервал равен 16 с ($2^4$).
Функция: настройка минимального интервала для NTP запросов между устройством и сервером.

**Max-Poll**
Диапазон: от 5 до 17. Интервал = $2^n$ с (n – значение этого параметра).
Значение по умолчанию: 10. В этом случае интервал равен 1024 с ($2^{10}$).
Функция: настройка максимального интервала для NTP запросов между устройством и сервером.

**Packet source interface (интерфейс отправки пакетов)**
Функция: настройка порта для отправки NTP пакетов.
Описание: когда используется архитектура «клиент-сервер», устройство отправляет NTP запросы на сервер. IP адрес источника запроса будет равен основному IP адресу порта.
В одноранговом режиме устройство отправляет NTP запросы соседнему узлу. IP адрес источника запроса будет равен основному IP адресу порта.

---

- Если выбран режим «клиент-сервер», для клиента достаточно вышеуказанных настроек.
- Указанный NTP сервер должен быть глобально синхронизирован перед тем, как предоставлять синхронизацию клиентам.
- Если выбран одноранговый режим, для активного узла достаточно вышеуказанных настроек.
- Min-Poll ≤ Max-Poll.
- Значения Min-Poll для узлов NTP должны быть одинаковыми.

---

3. Настройка сервера многоадресной передачи NTP.
Нажмите [Device Advanced Configuration] → [NTP configuration] → [Multicast Server Configuration], чтобы открыть страницу конфигурации сервера многоадресной рассылки, как показано на рисунке 321.

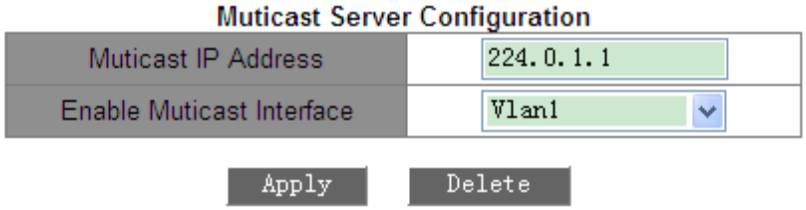



Рисунок 321 – Настройка многоадресного сервера

**Multicast IP Address (мультикастовый IP адрес)**
Формат: A.B.C.D.
Функция: настройка мультикастового IP адреса. Если адрес не указать, по умолчанию будет принят 224.0.1.1.

**Enable Multicast Interface (включить мультикастовый интерфейс)**
Функция: выбор мультикастового порта.

4. Настройка многоадресного клиента NTP.
Нажмите [Device Advanced Configuration] → [NTP configuration] → [Multicast Client Configuration], чтобы открыть страницу конфигурации клиента многоадресной рассылки, как показано на рисунке 322.

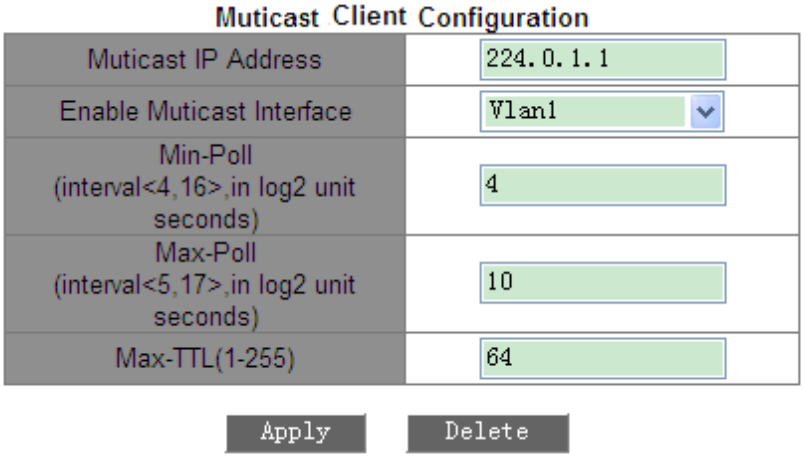



Рисунок 322 – Настройка многоадресного клиента

**Multicast IP Address (мультикастовый IP адрес)**
Формат: A.B.C.D.
Функция: настройка мультикастового IP адреса. Если адрес не указать, по умолчанию будет принят 224.0.1.1.

**Enable Multicast Interface (включить мультикастовый интерфейс)**
Функция: настройка мультикастового порта.

**Min-Poll**

Диапазон: от 4 до 16. Интервал = $2^n$ с (n – значение этого параметра.)
По умолчанию: 4. В этом случае, интервал равен 16 с ($2^4$).
Функция: настройка минимального интервала для NTP запросов между устройством и сервером.

**Max-Poll**
Диапазон: от 5 до 17. Интервал = $2^n$ с (n – значение этого параметра).
По умолчанию: 10. В этом случае, интервал равен 1024 с ($2^{10}$).
Функция: настройка максимального интервала для NTP запросов между устройством и сервером.

**Max-TTL**
Диапазон: 1~255.
Значение по умолчанию: 64.
Функция: настройка максимального TTL для запросов многоадресной рассылки, отправляемых клиентом.

5. Настройка широковещательного сервера NTP.
Нажмите [Device Advanced Configuration] → [NTP configuration] → [Broadcast Server Configuration], чтобы открыть страницу настройки широковещательного сервера, как показано на рисунке 323.

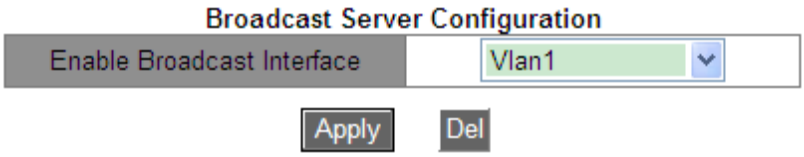



Рисунок 323 – Настройка широковещательного сервера

**Enable Broadcast Interface (включить широковещательный интерфейс)**
Функция: указать широковещательный порт.

6. Настройка широковещательного клиента NTP.
Нажмите [Device Advanced Configuration] → [NTP configuration] → [Broadcast Client Configuration], чтобы открыть страницу настройки широковещательного клиента, как показано на рисунке 324.

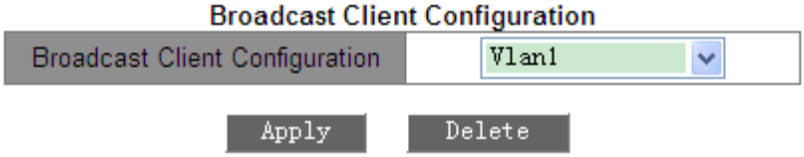



Рисунок 324 – Настройка широковещательного клиента

**Broadcast Client Configuration (настройка широковещательного клиента)**

Функция: указать широковещательный порт.

7. Настройка эталонных часов.
Нажмите [Device Advanced Configuration] → [NTP configuration] → [Reference Clock Configuration], чтобы открыть страницу конфигурации эталонных часов, как показано на рисунке 325.

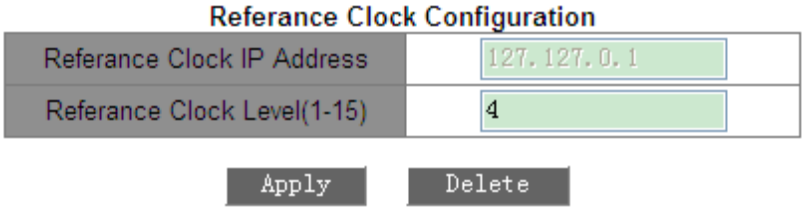



Рисунок 325 – Настройка эталонных часов

**Reference Clock IP Address (IP адрес эталонных часов)**
Формат: 127.127.t.u.
По умолчанию: 127.127.0.1.
Описание: «t» в 127.127.0.1 означает тип эталонных часов, а «u» означает ID экземпляра. На данный момент поддерживается только 127.127.0.1. То есть, системные часы являются эталонными.

**Reference Clock Level (уровень эталонных часов)**
Диапазон: 1~15.
По умолчанию: 4.
Функция: настройка страты эталонных часов.
Описание: параметр «страта» определяет погрешность часов. Чем выше её уровень, тем ниже точность. Если параметр равен 16, часы не синхронизированы и не могут служить эталонными часами.

---

На данный момент, только сам коммутатор может служить эталонными часами. Перед изменением данных параметров, выясните требования к синхронизации в сети.

---

## 6.24.4 Пример типовой настройки

- Настройка одноранговой режима:

Как показано на рисунке 326, необходимо настроить локальные часы на коммутаторе D в качестве эталонных часов и установить для их страты значение 2. Коммутатор A работает в режиме клиента, а коммутатор D служит NTP-сервером. Коммутатор B работает в одноранговом режиме, а коммутатор A является его одноранговым узлом. Коммутатор B является активным узлом, а коммутатор A — пассивным.

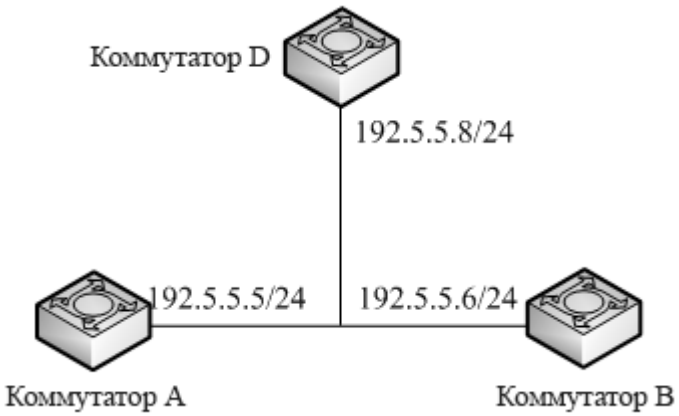



Рисунок 326 – Работа в одноранговом режиме

**Настройка коммутатора D:**
1. Включите NTP, как показано на рисунке 319.
2. Установите IP-адрес эталонных часов 127.127.0.1 и страту часов 2, как показано на рисунке 325.

**Настройка коммутатора A:**
3. Включите NTP, как показано на рисунке 319.
4. Установите IP-адрес NTP-сервера 192.5.5.8, Min-Poll – 4, Max-Poll – 10 и источник пакетов NTP – VLAN 1, как показано на рисунке 320.

**Настройка коммутатора B:**
5. Включите NTP, как показано на рисунке 319.
6. Установите IP-адрес одноранговой узла NTP 192.5.5.5, Min-Poll – 4, Max-Poll – 10 и источник пакетов NTP – VLAN 1, как показано на рисунке 320.

- Настройка многоадресного режима:

Как показано на рисунке 327, необходимо настроить локальные часы на коммутаторе D в качестве эталонных часов и установить для страты значение 2. Коммутатор D работает в режиме многоадресного сервера. Режим многоадресного сервера настроен на порту VLAN 2. Коммутатор A и коммутатор B работают в режиме многоадресного клиента. Режим многоадресного клиента настроен на VLAN 2.

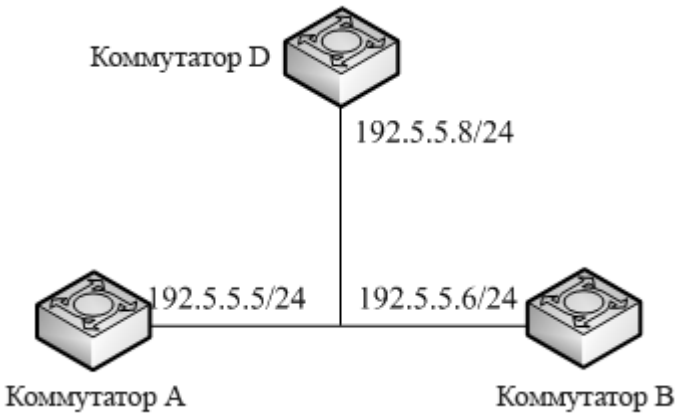



Рисунок 327 – Работа в многоадресном режиме

**Настройка коммутатора D:**

1. Включите NTP, как показано на рисунке 319.
2. Установите IP-адрес эталонных часов 127.127.0.1 и значение страты 2, как показано на рисунке 325.
3. Настройте сервер многоадресной рассылки: укажите IP-адрес многоадресной рассылки 224.0.1.1 и мультикастовый интерфейс VLAN 2, как показано на рисунке 321.

**Настройка коммутаторов A и B:**

4. Включите NTP, как показано на рисунке 319.
5. Настройте клиент многоадресной рассылки: укажите IP-адрес многоадресной рассылки 224.0.1.1, порт – VLAN 2, Min-Poll – 4, Max-Poll – 10 и Max-TTL – 64, как показано на рисунке 322.

- Настройка широковещательного режима:

Как показано на рисунке 328, необходимо настроить локальные часы на коммутаторе D в качестве эталонных часов и установить значение их страты 2. Коммутатор D работает в режиме широковещательного сервера. Режим широковещательного сервера настроен на порту VLAN 2. Коммутатор A и коммутатор B работают в режиме широковещательного клиента. Режим широковещательного клиента настроен на VLAN 2.

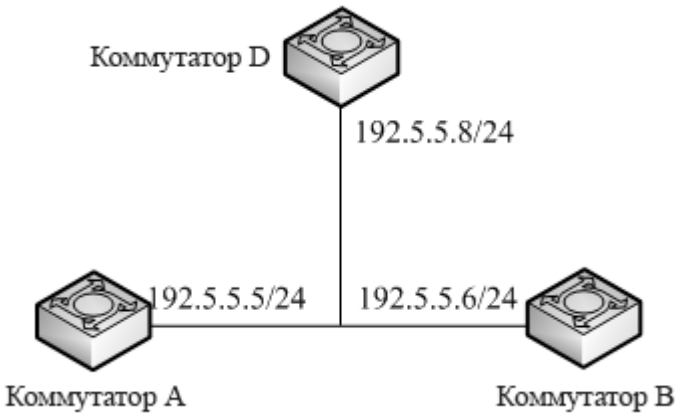



Рисунок 328 – Работа в широковещательном режиме

**Настройка коммутатора D:**
1. Включите NTP, как показано на рисунке 319.
2. Установите IP-адрес эталонных часов на 127.127.0.1 и значение их страты 2, как показано на рисунке 325.
3. Настройте широковещательный сервер: укажите широковещательный порт VLAN 2, как показано на рисунке 323.

**Настройка коммутаторов A и B:**
4. Включите NTP, как показано на рисунке 319.
5. Настройте широковещательный клиент: установите для широковещательного порта значение VLAN 2, как показано на рисунке 324.

## 6.25 Настройка TACACS+

### 6.25.1 Введение

TACACS+ (Terminal Access Controller Access Control System) – протокол аутентификации, авторизации и учета доступа (AAA), который используется для централизованного управления доступом и контроля сетевых устройств. Это система, основанная на TCP. Для передачи данных между сервером сетевого доступа NAS (Network Access Server) и сервером TACACS+ она использует клиент-серверную архитектуру. Клиент функционирует на NAS, а пользовательская информация контролируется на централизованном сервере (см. рисунок 329). NAS является сервером для пользователей, но клиентом для сервера TACACS+.

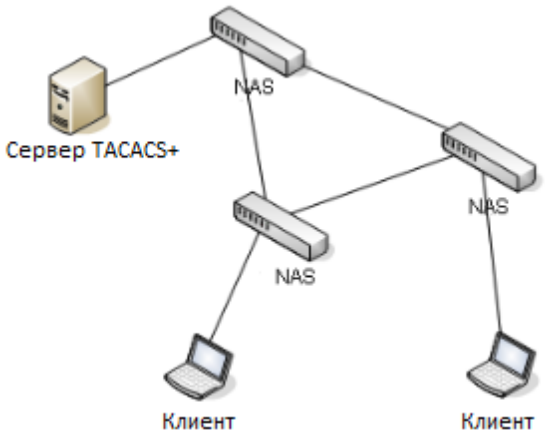



Рисунок 329 – Структура TACACS+

Протокол аутентифицирует, авторизует и управляет терминальными пользователями, которым необходимо заходить на сетевые устройства для каких-либо действий. Устройство работает как клиент TACACS+ и отправляет логин и пароль на TACACS+ сервер для аутентификации. Сервер принимает данные, отвечает на запросы и проверяет корректность присланных данных. Если пользователь проходит аутентификацию, он может зайти на устройство.

## 6.25.2 Настройка с помощью WEB-интерфейса

1. Включение TACACS+.
Нажмите [Device Advanced Configuration] → [TACACS-PLUS Configuration] → [TACACS-PLUS configuration], чтобы открыть страницу конфигурации TACACS+, как показано на рисунке 330.

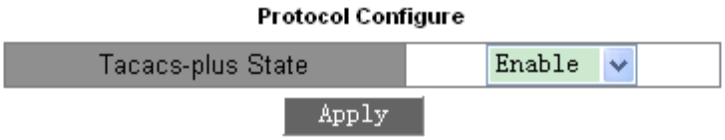



Рисунок 330 – Включение TACACS+

**TACACS-PLUS State (статус TACACS+)**
Варианты: Enable/Disable (включить/отключить).
По умолчанию: Disable (отключить).
Функция: включить/выключить TACACS+.

2. Настройка сервера TACACS+ (см. рисунок 331).

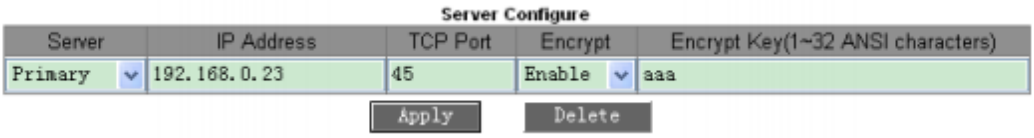



Рисунок 331 – Настройка сервера TACACS+

**Server (сервер)**
Варианты: Primary/Secondary (первичный/вторичный).
По умолчанию: Primary (первичный).
Функция: выбор типа сервера.

**IP Address (IP-адрес)**
Формат: A.B.C.D.
Функция: настройка IP адреса сервера.

**TCP port (порт TCP)**
Диапазон: 1~65535.
Значение по умолчанию: 49.
Функция: настройка номера порта, который будет принимать запросы аутентификации NAS.

**Encrypt (шифрование)**
Варианты: Enable/Disable (включить/отключить).
По умолчанию: Disable (отключить).
Функция: включение и выключение шифрования. Если оно включено, необходимо ввести его ключ.

**Encrypt Key (ключ шифрования)**
Диапазон: 1~32 символов.
Описание: введите ключ для установки безопасного соединения между клиентом и сервером TACACS+. Для проверки достоверности передаваемых данных два устройства должны иметь один и тот же ключ шифрования. Таким образом, необходимо убедиться в том, что ключ такой же, как на сервере TACACS+.
После завершения настройки в следующем разделе «Server Configured» отображается информация о конфигурации сервера, как показано на рисунке 332.

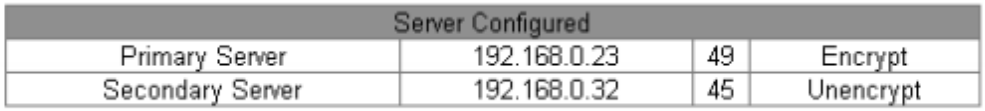



Рисунок 332 – Список серверных настроек

### 6.25.3 Пример типовой настройки

Как показано на рисунке 333, сервер TACACS+ может аутентифицировать и авторизовать пользователей с помощью коммутатора. IP-адрес сервера — 192.168.0.23, а общий ключ, используемый при обмене пакетами между коммутатором и сервером, — ааа.

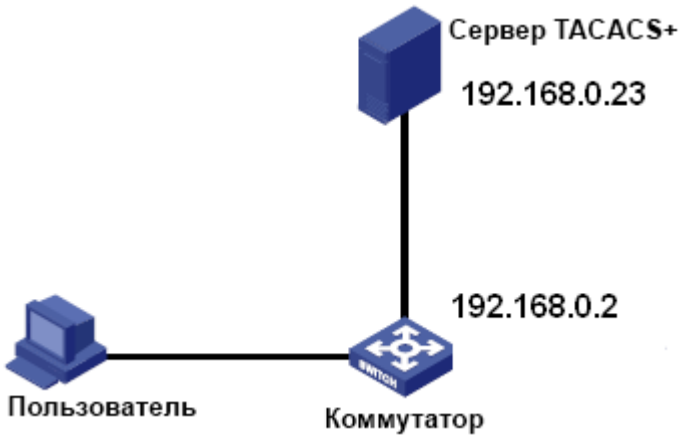



Рисунок 333 – Пример аутентификации TACACS+

1. Включите TACACS+, как показано на рисунке 330.
2. Настройка сервера TACACS+. Установите IP-адрес сервера 192.168.0.23 и ключ шифрования «ааа». Включите шифрование, как показано на рисунке 331.
3. При входе на коммутатор через веб-интерфейс выберите «Local», при входе через telnet выберите «TACACS+», как показано на рисунке 345.
4. Настройте имя пользователя и пароль «bbb», зашифруйте ключ «ааа» на сервере TACACS+.
5. При входе на коммутатор через веб-интерфейс введите имя пользователя «admin» и пароль «123», чтобы пройти локальную аутентификацию.
6. При входе на коммутатор через Telnet введите имя пользователя и пароль «bbb», чтобы пройти аутентификацию TACACS+.

## 6.26 Настройка RADIUS

### 6.26.1 Введение

RADIUS (служба удаленной аутентификации пользователей) является распространенным протоколом передачи данных. Он определяет формат RADIUS-кадра на основе UDP и механизм передачи данных, гарантируя защиту сетей от несанкционированного доступа. Как правило, RADIUS используется в сетях с высокими требованиями безопасности и удаленным доступом пользователей.

RADIUS поддерживает режим клиент/сервер, обеспечивая соединение между сервером сетевого доступа NAS и RADIUS-сервером. RADIUS-клиент работает на NAS-сервере. RADIUS-сервер осуществляет централизованное управление информацией о

пользователе. NAS-сервер выполняет функции сервера для пользователей и функции клиента для сервера RADIUS. На рисунке 334 показана структура.

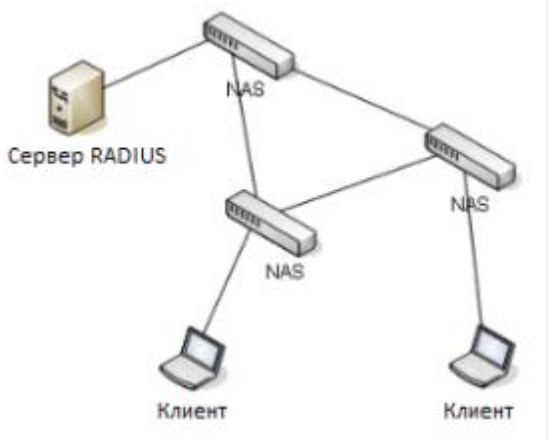



Рисунок 334 – Структура RADIUS

Протокол проводит аутентификацию конечных пользователей, которым необходимо авторизоваться в системе устройства для работы. Действуя как RADIUS клиент, устройство отправляет информацию о пользователе на RADIUS сервер для аутентификации и разрешает или запрещает пользователям войти в систему устройства по результатам процесса аутентификации.

## 6.26.2 Настройка с помощью WEB-интерфейса

1. Настройка параметров RADIUS.
Нажмите [Device Advanced Configuration] → [RADIUS configuration] → [RADIUS configuration], чтобы открыть страницу конфигурации RADIUS, как показано на рисунке 335.

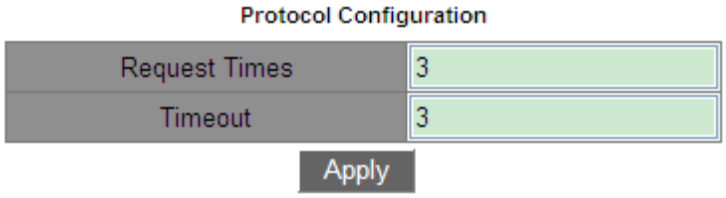



Рисунок 335 – Настройка параметров RADIUS

**Request Times (количество запросов)**
Диапазон: 1~3.
По умолчанию: 3.
Функция: установить максимальное количество попыток повторной передачи для пакетов запроса RADIUS. Если устройство по-прежнему не получает ответные пакеты от сервера RADIUS после максимального количества попыток повторной передачи, устройство считает, что аутентификация не удалась.

**Timeout (время ожидания)**
Диапазон: 1~3.
По умолчанию: 3.
Функция: установить дополнительное время для ответа от сервера RADIUS. После отправки пакета запроса RADIUS устройство повторит передачу пакета запроса RADIUS, если оно по-прежнему не получит ответа от сервера RADIUS по истечении указанного времени.

2. Настройка RADIUS-сервера, как показано на рисунке 336.

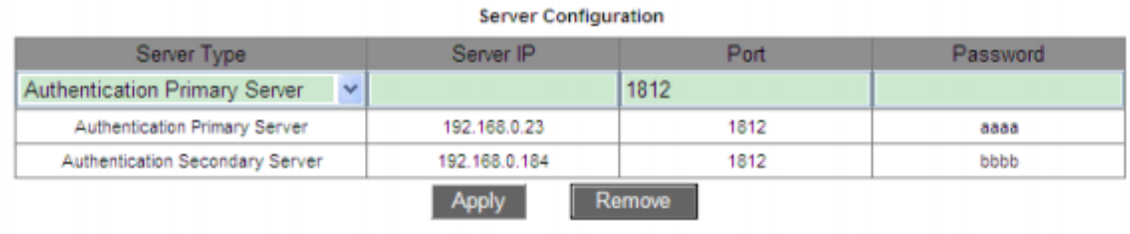



Рисунок 336 – Настройка сервера RADIUS

**Server Type (тип сервера)**
Варианты: Authentication Primary Server/Authentication Secondary Server (первичный сервер аутентификации/вторичный сервер аутентификации).
Функция: настроить первичный или вторичный сервер RADIUS. Если первичный сервер недоступен, для аутентификации будет использоваться вторичный сервер.

**Server IP (IP-адрес сервера)**
Формат: A.B.C.D.
Функция: настройка IP-адреса сервера RADIUS.

**Port (порт)**
Диапазон: 1~65535.
Значение по умолчанию: 1812.
Функция: настройка UDP-порта сервера RADIUS.

**Password (пароль)**
Диапазон: 1~32 символа.
Функция: настройка пароля сервера RADIUS.

## 6.26.3 Пример типовой настройки

Как показано на рисунке 337, на порту 1 коммутатора включена работа протокола (стандарта) IEEE802.1x. Соответственно, пользователи могут зайти на коммутатор через порт 1 после прохождения аутентификации на сервере RADIUS. IP-адрес сервера 192.168.0.23. Ключ для обмена пакетами между коммутатором и сервером – aaaa.

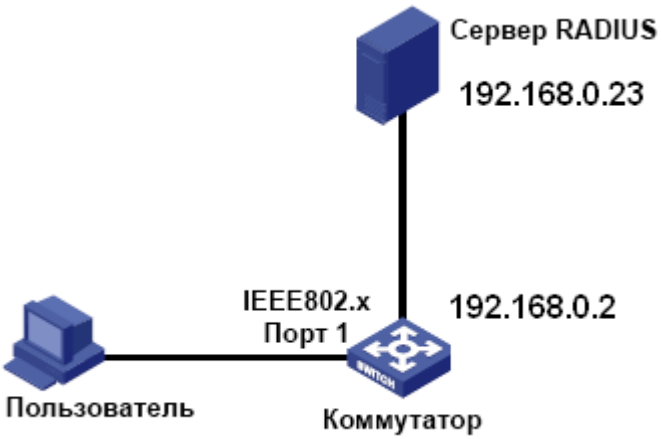



Рисунок 337 – Пример аутентификации RADIUS

1. Установите для IP-адреса основного сервера аутентификации значение 192.168.0.23 и пароль «аааа», как показано на рисунке 336.
2. Настройки IEEE802.1x: включите IEEE802.1x глобально. Включите IEEE802.1x на порту 1. Оставьте значения по умолчанию для других параметров. Подробнее см. в разделе 6.27 «Настройка IEEE802.1x».
3. Установите для dot1x аутентификацию RADIUS, как показано на рисунке 345.
4. Установите для имени пользователя и пароля на сервере RADIUS значение «ссс», для ключа шифрования — «аааа».
5. Установите и запустите клиентское программное обеспечение 802.1x на ПК. Введите «ссс» в качестве имени пользователя и пароля.

Таким образом, пользователь может пройти аутентификацию и получить доступ к коммутатору через порт 1.

# 6.27 Настройка IEEE802.1x

## 6.27.1 Введение

Для обеспечения безопасности WLAN комитет IEEE802 LAN/WAN предложил протокол 802.1x. В качестве стандартного механизма управления доступа к портам LAN в Ethernet стандарт 802.1x обеспечивает аутентификацию. Стандарт 802.1x – это управление доступом к сети на основе портов. Управление доступом к сети на основе портов предназначено для аутентификации и управления портами устройств при доступе к локальной сети. Если пользователь проходит аутентификацию, он может получить доступ к ресурсам в локальной сети. Если аутентификация не пройдена, ресурсы в локальной сети для пользователя недоступны. Стандарт 802.1x имеет структуру клиент/сервер. Аутентификация и авторизация пользователя при условии управления доступом на основе порта требует следующих элементов:

**Клиент:** обычно обозначает пользовательский терминал. Когда пользователь хочет выйти в Интернет, он запускает клиентскую программу и вводит требуемые имя пользователя и пароль. Клиентская программа отправит запрос на подключение.

**Устройство:** означает коммутатор аутентификации в системе Ethernet. Он загружает и доставляет информацию об аутентификации пользователя, а также включает или отключает порт в зависимости от результата аутентификации.
**Сервер аутентификации:** означает объект, который предоставляет услугу аутентификации для устройств. Он проверяет, есть ли у пользователей разрешения на использование сетевых служб в соответствии с идентификаторами (именами пользователей и паролями), отправляемыми клиентом и включает или отключает порты в соответствии с результатами аутентификации.

## 6.27.2 Настройка с помощью WEB-интерфейса

1. Включение глобального протокола IEEE802.1x.
Нажмите [Device Advanced Configuration] → [IEEE802.1x configuration] → [IEEE802.1x configuration], чтобы открыть страницу конфигурации IEEE802.1x, как показано на рисунке 338.

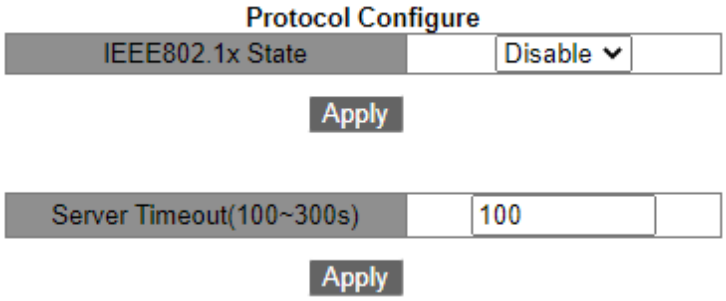



Рисунок 338 – Включение глобального IEEE802.1x

**IEEE802.1x State (состояние IEEE802.1x)**
Варианты: Enable/Disable (включить/выключить).
По умолчанию: Disable (выключено).
Функция: включение/отключение глобальной функции безопасности IEEE802.1x.

**Server Timeout (время ожидания сервера)**
Диапазон: 100~300 с.
Значение по умолчанию: 100 с.
Функция: после того, как устройство отправляет сообщение RADIUS Access-Request на сервер аутентификации, устройство запускает этот таймер. Если устройство не получит ответ от сервера аутентификации до истечения времени ожидания, устройство повторно отправит запрос аутентификации.

2. Настройка порта, на котором включен IEEE802.1x (см. рисунок 339).

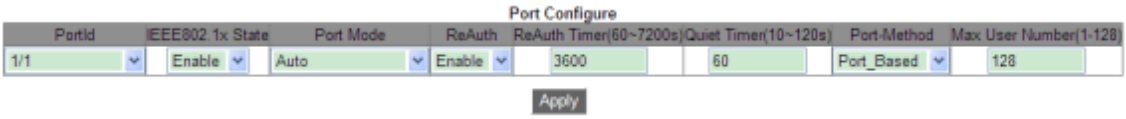



Рисунок 339 – Настройка порта IEEE802.1x

**PortId (идентификатор порта)**
Варианты: все порты коммутатора.

**IEEE802.1x State (состояние IEEE802.1x)**
Варианты: Enable/Disable (включить/выключить).
По умолчанию: Disable (выключено).
Функция: включение/отключение IEEE802.1x на порту.
Описание: когда эта функция включена, связь пользователей через порт зависит от режима порта IEEE802.1x.

**Port Mode (режим порта)**
Варианты: Unauthorized-force/Auto/Authorized-force (принудительно неавторизован/авто/ принудительно авторизован).
По умолчанию: Auto.
Функция: выбор режима аутентификации порта.
Описание: «Unauthorized-force» означает, что порт всегда находится в «неавторизованном» состоянии и не позволяет пользователям проводить аутентификацию, а коммутатор не предоставляет услуги аутентификации клиентам, которые получают доступ к коммутатору с этого порта. Авто означает, что начальное состояние порта «неавторизованное», и порт не позволяет пользователям получать доступ к сетевым ресурсам. Если пользователь проходит аутентификацию, порт переходит в «авторизованное» состояние и позволяет пользователям получать доступ к сетевым ресурсам. Если пройти аутентификацию не удастся, порт перейдет в «неавторизованное состояние» и закроет пользователям доступ. «Authorized-force» означает, что порт всегда находится в авторизованном состоянии и позволяет пользователям получать доступ к сетевым ресурсам без аутентификации.

**ReAuth (повторная аутентификация)**
Варианты: Enable/Disable (включить/выключить).
По умолчанию: Disable (выключено).
Функция: настройка необходимости регулярной повторной аутентификации при успешном выполнении аутентификации.

**ReAuth Timer (таймер повторной аутентификации)**
Диапазон: 60~7200 с.
Значение по умолчанию: 3600 с.
Функция: установка временного интервала для принудительной повторной аутентификации после успешного входа.

**Quiet Timer (таймер периода молчания)**
Диапазон: 10~120 с.
Значение по умолчанию: 60 с.
Функция: если аутентификация не удалась, начинается период молчания (QuietPeriod). В течение периода молчания сервер не отвечает на запросы аутентификации от клиента. После окончания периода молчания сервер снова начинает принимать запросы аутентификации.

**Port-Method (метод порта)**
Варианты: Port_ Based/ MAC_ Based (на основе порта/на основе MAC-адреса).
По умолчанию: Port_ Based (на основе порта).
Функция: настройка режима управления доступом к портам с поддержкой IEEE802.1x.
Описание: MAC_Based указывает, что все пользователи, использующие порт, должны пройти аутентификацию соответственно. Когда пользователь находится в автономном режиме, только он не может использовать сеть. Port_Based указывает, что пользователи аутентифицируются на основе порта. После того как первый пользователь, использующий порт, проходит аутентификацию, всем другим пользователям, использующим этот порт, аутентификация не требуется. Однако, когда первый пользователь переходит в автономный режим, порт отключается, и все остальные пользователи, подключенные через этот порт, не могут использовать сеть.

**Max User Number (максимальное количество пользователей)**
Диапазон: 1~128.
Значение по умолчанию: 128.
Функция: настроить максимальное количество пользователей доступа, использующих порт с поддержкой IEEE802.1x.
Описание: эта настройка действует только для портов с управлением доступом на основе MAC-адресов.

3. Просмотр конфигурации IEEE802.1x.
Нажмите [Device Advanced Configuration] → [IEEE802.1x configuration] → [IEEE802.1x information], чтобы просмотреть конфигурацию IEEE802.1x, как показано на рисунке 340.

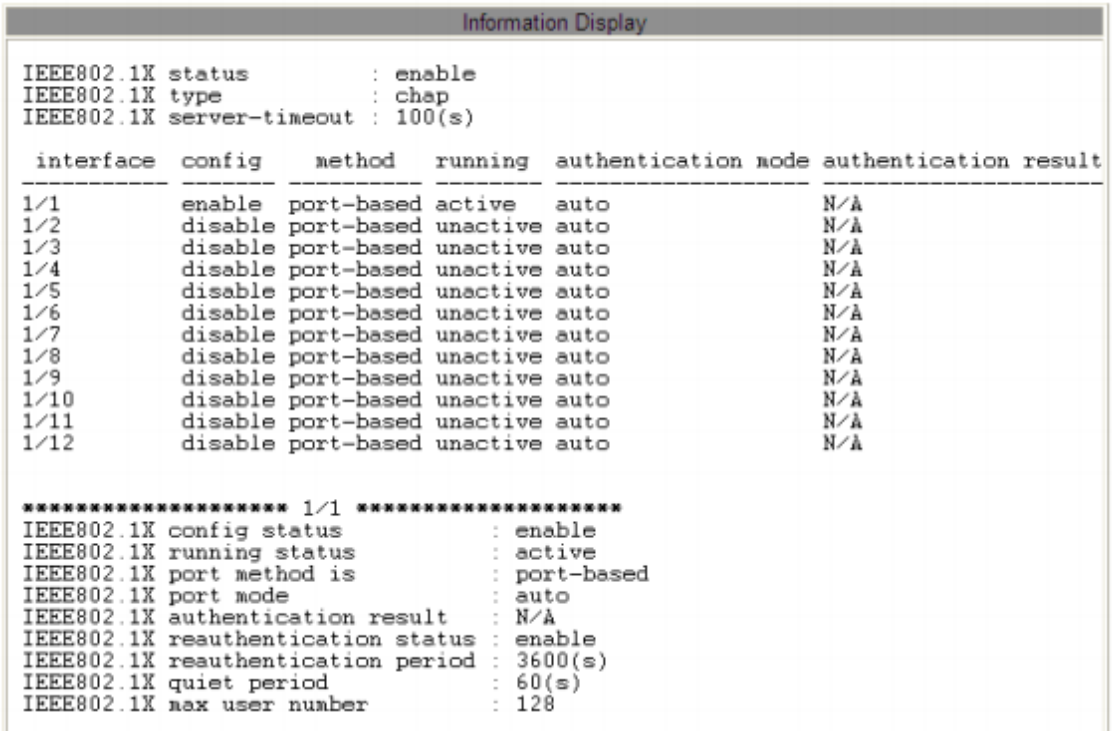



Рисунок 340 – Отображение настроек IEEE802.1x.

4. Настройка группы IEEE802.1x.
Нажмите [Device Advanced Configuration] → [IEEE802.1x configuration] → [IEEE802.1x Group configuration], чтобы открыть страницу настройки группы IEEE802.1x, как показано на рисунке 341.

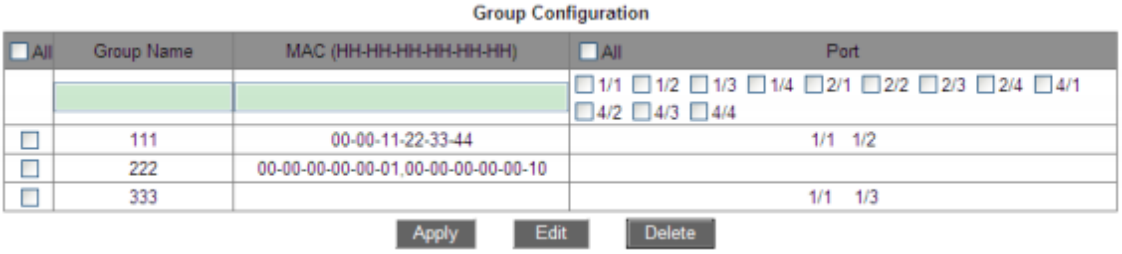



Рисунок 341 – Настройка группы IEEE802.1x

**Group Name (имя группы)**
Диапазон: 1~16 символов.
Функция: настройка имени группы.

**MAC (MAC-адрес)**
Формат: HH-HH-HH-HH-HH-HH (H — шестнадцатеричное число).
Функция: настройка MAC-адреса для группы. В одну группу можно добавить несколько MAC-адресов, при этом MAC-адреса разделяются однобайтовыми запятыми.

**Port (порт)**
Функция: добавление портов для группы.

---

Группа аутентификации пользователей позволяет настраивать только MAC-адрес или номер порта.

---

5. Настройка информации пользователя IEEE802.1x.
Нажмите [Device Advanced Configuration] → [IEEE802.1x configuration] → [IEEE802.1x User configuration], чтобы открыть страницу настройки пользователя IEEE802.1x, как показано на рисунке 342.

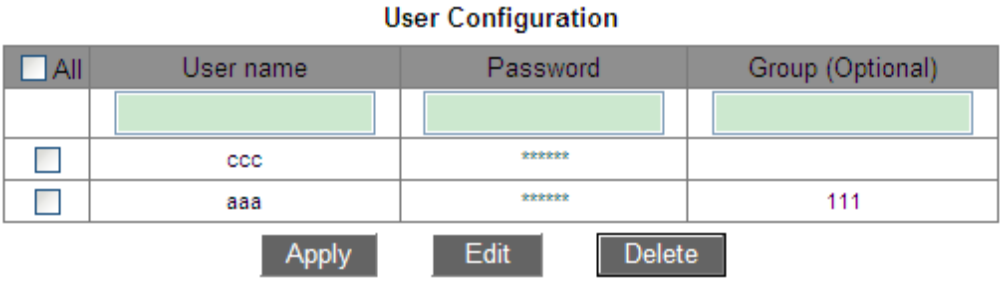



Рисунок 342 – Настройка пользователя IEEE802.1x

**User Name (имя пользователя)**
Диапазон: 1~16 символов.
Функция: настройка имени пользователя IEEE802.1x.

**Password (пароль)**
Диапазон: 1~16 символов.
Функция: настройка пароля IEEE802.1x.

**Group (группа)**
Функция: привязать пользователя к группе.
Описание: если текущий пользователь привязан к группе аутентификации пользователей, только пользователь, чей MAC-адрес и номер порта доступа совпадают с привязанной группой, может пройти аутентификацию и получить доступ к коммутатору. Также допускается, чтобы текущий пользователь не был привязан к какой-либо группе проверки подлинности пользователя. В этом случае пользователи могут проводить аутентификацию, используя любой MAC-адрес и номер порта.

6. Просмотр информации о пользователях IEEE802.1x, находящихся в режиме онлайн.
Нажмите [Device Advanced Configuration] → [IEEE802.1x configuration] → [IEEE802.1x On-line user], чтобы просмотреть информацию о пользователе IEEE802.1x в сети, как показано на рисунке 343.

On-line user

| All | User Name | MAC | Port | Authentication Mode | Time(min) |
|---|---|---|---|---|---|
| ☐ | ccc | 44-37-e6-88-6e-90 | Ethernet1/1 | port-based | 2 |

Disconnect

Рисунок 343 – Отображение информации о пользователе IEEE802.1x в сети

Вы можете выбрать одного или нескольких пользователей и нажать <Disconnect>, чтобы отключить выбранных пользователей от коммутатора.

## 6.27.3 Пример типовой настройки

Как показано на рисунке 344, клиент подключен к порту 1 коммутатора. Включите IEEE802.1x на порту 1 и выберите режим автоматической аутентификации. Имя пользователя и пароль для локальной аутентификации — ccc, а имя пользователя и пароль для удаленной аутентификации — ddd. Оставьте значения по умолчанию для других параметров.

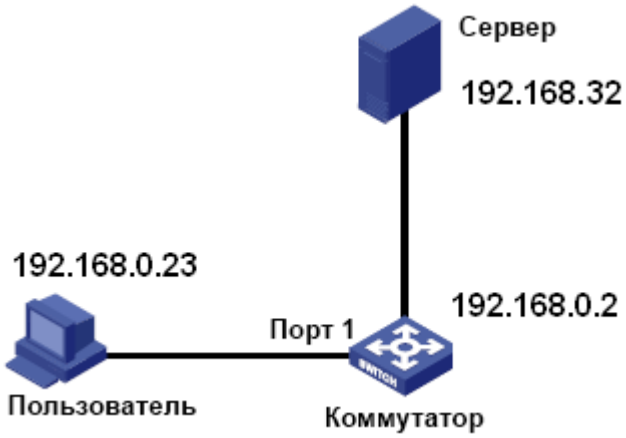



Рисунок 344 – Пример конфигурации IEEE802.1x

➢ Настройка локальной аутентификации.

1. Включите глобальный протокол IEEE802.1x, как показано на рисунке 338.
2. Установите для dot1x локальную аутентификацию, как показано на рисунке 345.
3. Установите для имени пользователя и пароля значение «ccc», как показано на рисунке 342.
4. Включите IEEE802.1x на порту 1 и установите для режима аутентификации значение Auto, как показано на рисунке 339.
5. Установите клиентское программное обеспечение аутентификации 802.1x и запустите его. Введите имя пользователя и пароль «ccc», чтобы пройти аутентификацию. После это вы сможете получить доступ к коммутатору.

➢ Настройка удаленной аутентификации.

Вы можете обратиться к примеру типовой настройки в разделе 6.26 «Настройка RADIUS».

## 6.28 Настройка режима аутентификации

Настройка режима доступа к коммутатору, режима и порядка аутентификации.
Нажмите [Device Advanced Configuration] → [Authentication login configuration] → [Authentication login configuration], чтобы открыть страницу конфигурации входа для аутентификации, как показано на рисунке 345.

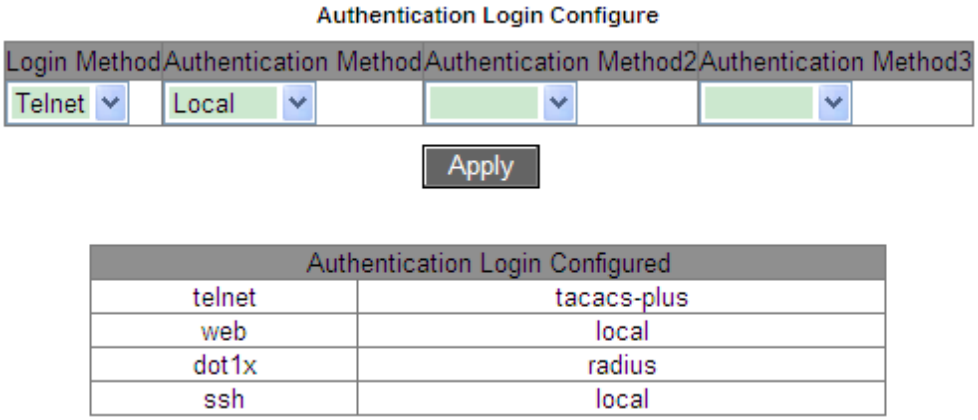



Рисунок 345 – Настройка аутентификации

**Login Method (метод входа)**
Опции: Telnet/Web/dot1x/SSH
Функция: выберите режим доступа к коммутатору.

**Authentication Method/Authentication Method 2/Authentication Method 3**
Варианты: Local/TACACS+/RADIUS/ RADIUS+ Local/ TACACS Plus+ Local.
По умолчанию: Local.
Функция: выбор порядка аутентификации. Сначала выполняется метод аутентификации 1. Если аутентификация не удалась, выполняется метод аутентификации 2. Если выполнение обоих методов не приносит результата, выполняется метод аутентификации 3.
Описание: «Local» означает использование для выполнения аутентификации имени пользователя и пароля, установленных локально. «TACACS+» означает использование для аутентификации имени пользователя и пароля, установленных на сервере TACACS+. «RADIUS» означает использование имени пользователя и пароля, установленных на сервере RADIUS.

---

Если для доступа к коммутатору используется dot1x, можно выбрать только один режим аутентификации.

---

# 6.29 Проверка связи

## 6.29.1 Введение

Проверка канала использует периодическое взаимодействие протокольных пакетов для оценки состояния связи и отображения статуса подключения порта. В случае неисправности проблема может быть вовремя обнаружена и устранена.
Порт, для которого включена проверка состояния соединения, периодически (каждую секунду) отправляет контрольные пакеты своему одноранговому устройству. Если порт не получает пакет проверки связи от удаленного устройства в течение 5 секунд, это означает, что связь не работает, и порт отображает ошибку приема (Rx). Если порт получает пакет проверки связи от удаленного устройства, и этот пакет показывает, что пакет проверки связи был отправлен локальным устройством в пределах времени ожидания (5 секунд), то порт отображает нормальное состояние. Если порт получает пакет проверки связи от удаленного устройства, но этот пакет показывает, что пакет проверки связи не был получен от локального устройства в пределах времени ожидания (5 секунд), то порт отображает ошибку передачи (Tx). Если связь с портом не работает, порт отображает состояние «Link Down».
Порт, для которого отключена проверка состояния связи, работает в пассивном режиме. То есть он самостоятельно не отправляет пакет «link-check». Однако после получения такого пакета от удаленного узла этот порт немедленно возвращает свой пакет проверки, чтобы проинформировать удаленный узел о нормальном состоянии связи.

---

Если кольцевой/резервный порт Sy2-RP, для которого включена проверка канала, неисправен (например, ненормальный прием, ненормальная передача или отключение), кольцевой протокол Sy2-RP заблокирует этот кольцевой/резервный порт.

---

## 6.29.2 Настройка с помощью WEB-интерфейса

1. Включение функции проверки связи на порту.
Нажмите [Device Advanced Configuration] → [Diagnosis Configuration] → [Link Check], чтобы перейти на страницу конфигурации проверки связи, как показано на рисунке 346.

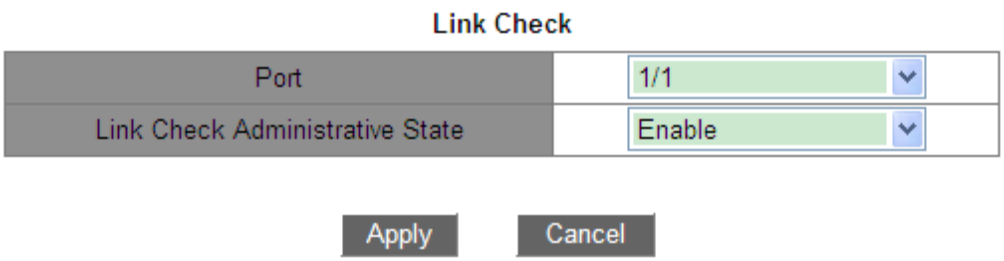



Рисунок 346 – Включение проверки связи на порту

**Link Check Administrative State (состояние активной проверки связи)**

Варианты: Enable/Disable (включить/выключить).
По умолчанию: Disable (выключено).
Функция: включить/отключить проверку связи на порту.

Если одноранговое устройство не поддерживает эту функцию, она должна быть отключена на соответствующем порту локального устройства.

2. Отображение состояния проверки связи на порту показано на рисунке 347.

| Port | Link Check State |
|---|---|
| 1/1 | Normal |
| 1/2 | Link Down |
| 1/3 | Disable |
| 1/4 | Disable |
| 1/5 | Disable |
| 1/6 | Disable |
| 1/7 | Disable |
| 1/8 | Rx Fault |
| 1/9 | Disable |
| 1/10 | Disable |
| 1/11 | Disable |
| 1/12 | Disable |

Рисунок 347 – Отображение состояния проверки связи на порту

**Link Check State (состояние проверки связи)**
Варианты: Normal / Rx Fault / Disable / Tx Fault / Link Down (нормальный / ошибка приёма / отключено / ошибка передачи / отсутствие связи.
Описание: если для порта включена проверка связи и порт нормально отправляет и принимает данные, отображается «Normal». Если одноранговая сторона не получает пакеты проверки от устройства, отображается «Tx Fault». Если устройство не получает пакеты проверки от одноранговой стороны, отображается «Rx Fault». Если порт отключен, отображается «Link Down». Если функция проверки связи не включена для порта, отображается «Disable».

# 6.30 Настройка функции Loop Detect

## 6.30.1 Введение

После того, как на порту будет включена функция обнаружения петель (Loop Detect), через порт будут отправляться специальные пакеты для обнаружения петель. Данная функция определяет, существуют ли петли в сети, подключенной к порту. ЦП (CPU) периодически передает на порт пакеты «Loop detect». Если какой-либо порт коммутатора получает пакеты «Loop detect», можно сказать, что в сети существуют петли. Перезагрузите порт, который отправляет пакеты «Loop detect», и через некоторое время порт будет автоматически подключен и продолжит обнаружение. Интервал времени для отправки пакетов обнаружения петель и время восстановления порта можно настроить в программном обеспечении.

---

Обнаружение петель Loop Detect и резервирование Sy2-Ring/Sy2-RP/RSTP/MSTP – взаимоисключающие функции. Они не могут быть работать одновременно на одном порту.

---

## 6.30.2 Настройка с помощью WEB-интерфейса

Настройка функции обнаружения петель порта.
Нажмите [Device Advanced Configuration] → [Loop Detect configuration] → [Loop Detect configuration], чтобы открыть страницу настройки Loop Detect, как показано на рисунке 384.

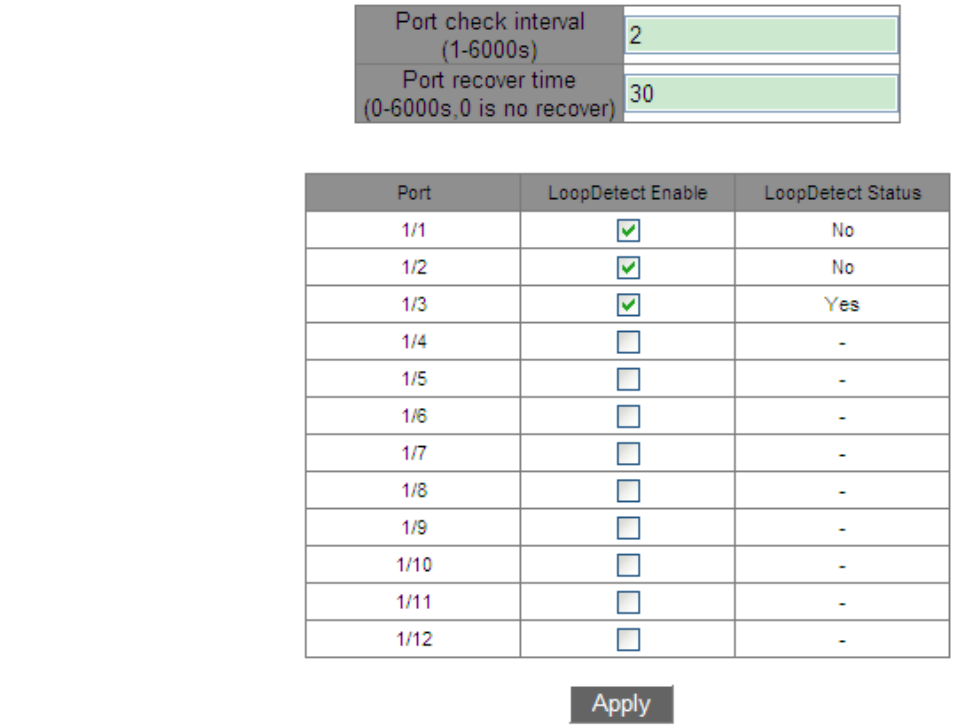



Рисунок 348 – Включение функции обнаружения петель для порта

**Port check interval (интервал проверки порта)**
Диапазон: 1~6000 с
Значение по умолчанию: 2 с.
Функция: настройка временного интервала для отправки пакетов обнаружения петель.

**Port recovery time (время восстановления порта)**
Диапазон: 0~6000 с.
Значение по умолчанию: 30 с.
Функция: настройка времени восстановления работы порта; 0 указывает, что порт не может быть подключен автоматически.

**Loop Detect Enable (включение обнаружения петель)**
Варианты: Enable/Disable (включить/выключить).
По умолчанию: Disable (выключено).
Функция: включение или отключение функции Loop Detect для порта.

**Loop Detect Status (статус функции обнаружения петель)**
Варианты: Yes/No (да/нет).
Функция: показывает наличие петель в сети, где на порту включена функция Loop Detect. «Yes» указывает на наличие петель, а «No» – на их отсутствие.

## 6.30.3 Пример типовой настройки

Требования к сети:
порт 3 коммутатора подключен к внешней сети. Когда в сети есть петли, отключите порт 3, как показано на рисунке 349.

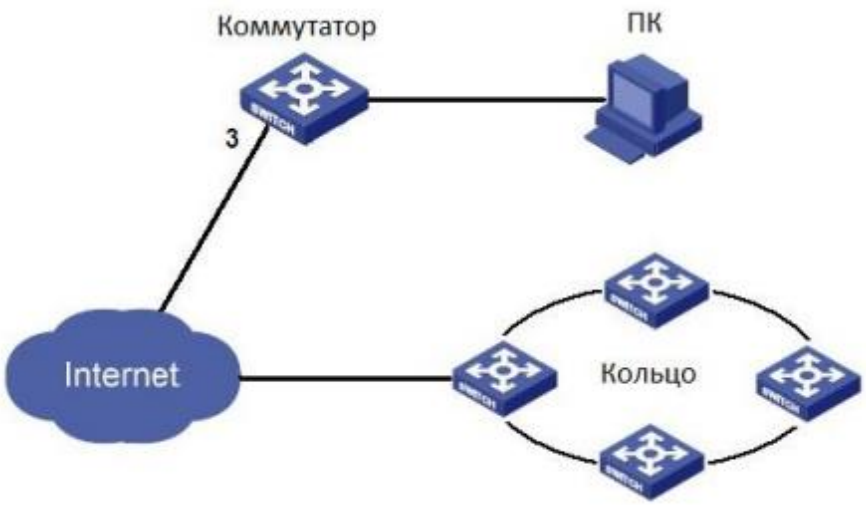



Рисунок 349 – Схема сети

Настройка:
включите функцию обнаружения петель на порту 3, как показано на рисунке 348.

# 6.31 Защита CRC-кода порта

## 6.31.1 Введение

При включении защиты CRC порта, функция реализует периодическое обнаружение пакетов с ошибками CRC. Если количество таких пакетов превышает ожидаемый порог, выключите порт. Подключите порт через некоторое время и продолжайте обнаружение. Время обнаружения пакетов с ошибками CRC и время возобновления работы порта можно настроить в программном обеспечении.

## 6.31.2 Настройка с помощью WEB-интерфейса

Настройка функции защиты CRC для портов.
Нажмите [Device Advanced Configuration] → [CRC Protect configuration] → [CRC Protect configuration], чтобы открыть страницу конфигурации защиты CRC, как показано на рисунке 350.

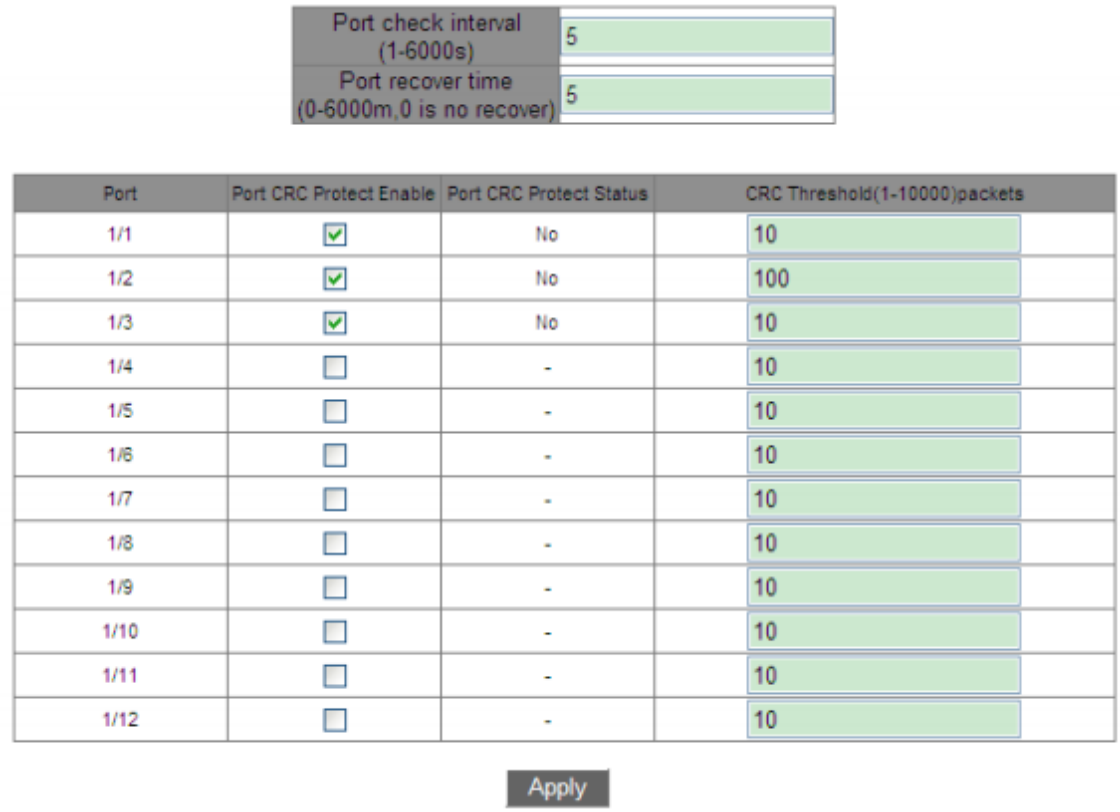



Рисунок 350 – Включение функции защиты CRC

**Port check interval (интервал проверки порта)**
Диапазон: 1~6000 с.
Значение по умолчанию: 5 с.

Функция: настройка времени обнаружения пакетов с ошибками CRC. Если количество пакетов ошибок CRC превышает пороговое значение, выключите порт.

**Port recover time (время восстановление порта)**
Диапазон: 0~6000 мин.
По умолчанию: 5 мин.
Функция: настройка времени восстановления порта; 0 указывает, что порт не может возобновить работу автоматически.

**Port CRC Protect Enable (включить защиту CRC для портов)**
Варианты: Enable/Disable (включить/выключить).
По умолчанию: Disable (выключено).
Функция: включить или отключить функцию защиты CRC портов. Механизм обнаружения ошибок работает только для порта с включенной функцией защиты CRC.

**Port CRC Protect Status (статус защиты CRC портов)**
Варианты: -- /Yes/No.
Описание: «Yes»: функция защиты портов CRC включена, а порт находится в состоянии «link down» из-за ошибки CRC. «No»: функция защиты порта CRC включена, а порт находится в состоянии «link up». «--»: функция защиты CRC порта отключена.

**CRC Threshold (пороговое значение CRC)**
Диапазон: 1~10000 пакетов.
По умолчанию: 10 пакетов.
Функция: настроить пороговое значение количества пакетов с ошибками CRC.

# 7. Расшифровка аббревиатур

| | | |
|---|---|---|
| ABR | Area Border Router | Граничный маршрутизатор |
| AS | Autonomous System | Автономная система |
| ASBR | Autonomous System Boundary Router | Граничный маршрутизатор автономной системы |
| ARP | Address Resolution Protocol | Протокол определения адреса |
| BDR | Backup Designated Router | Резервный выделенный маршрутизатор |
| BootP | Bootstrap Protocol | Протокол, используемый для автоматического получения клиентом IP-адреса |
| BPDU | Bridge Protocol Data Unit | Протокол управления сетевыми мостами |
| CAR | Committed Access Rate | Гарантированная скорость доступа |
| CIST | Common and Internal Spanning Tree | Общее и внутреннее связующее дерево |
| CLI | Command Line Interface | Интерфейс командной строки |
| CoS | Class of Service | Класс сервиса |
| CST | Common Spanning Tree | Общее связующее дерево |
| DD | Database Description | Описание базы данных |
| DHCP | Dynamic Host Configuration Protocol | Протокол динамической настройки узла |
| DHP | Dual Homing Protocol | Протокол, позволяющий подключить устройство к двум разным коммутаторам, обеспечивая резервирование подключения |
| DNS | Domain Name System | Система доменных имен |
| DR | Designated Router | Назначенный маршрутизатор |
| DSCP | Differentiated Services CodePoint | Точка кода дифференцированных услуг |
| DST | Daylight Saving Time | Переход на летнее время |
| FTP | File Transfer Protocol | Протокол передачи файлов |
| GARP | Generic Attribute Registration Protocol | Протокол регистрации основных атрибутов |
| GMRP | GARP Multicast Registration Protocol | Протокол GARP для регистрации многоадресных групп |
| GVRP | GARP VLAN Registration Protocol | Протокол GARP для регистрации VLAN |
| HTTP | Hyper Text Transfer Protocol | Протокол передачи гипертекста |
| ICMP | Internet Control Message Protocol | Протокол межсетевых управляющих сообщений |
| IED | Intelligent Electronic Device | Интеллектуальное электронное устройство |
| IGMP | Internet Group Management Protocol | Протокол управления группами Интернета (протокол управления групповой (multicast) передачей данных в сетях, основанных на протоколе IP) |

| | | |
|---|---|---|
| IGMP Snooping | Internet Group Management Protocol Snooping | Протокол отслеживания сетевого трафика IGMP |
| IST | Internal Spanning Tree | Внутреннее связующее дерево |
| LLDP | Link Layer Discovery Protocol | Протокол обнаружения уровня канала |
| LLDPDU | Link Layer Discovery Protocol Data Unit | Блок данных протокола обнаружения уровня канала |
| LSA | Link State Advertisement | Сообщение с описанием локального состояния маршрутизатора или сети |
| LSAck | Link State Acknowledgment | Пакет подтверждения состояния канала |
| LSDB | Link State Database | База данных о состоянии каналов |
| LSR | Link State Request | Пакет запроса о состоянии канала |
| LSU | Link State Update | Пакет подтверждения состояния канала |
| MIB | Management Information Base | Пакет обновления информации о состоянии канала |
| MSTI | Multiple Spanning Tree Instance | Экземпляр множественного связующего дерева |
| MSTP | Multiple Spanning Tree Protocol | Протокол множественного связующего дерева (в один экземпляр MSTP могут входить несколько виртуальных сетей при условии, что их топология одинакова) |
| NAS | Network Access Server | Сервер сетевого доступа |
| NetBIOS | Network Basic Input/Output System | Базовая сетевая система ввода-вывода |
| NMS | Network Management Station | Станция управления сетью |
| NTP | Network Time Protocol | Сетевой протокол синхронизации времени |
| OID | Object Identifier | Идентификатор объекта |
| OSPF | Open Shortest Path First | Протокол динамической маршрутизации, основанный на технологии отслеживания состояния канала и передающий информацию по наилучшему пути |
| PVLAN | Private VLAN | Частная виртуальная локальная сеть |
| QoS | Quality of Service | Качество обслуживания (технология предоставления различным классам трафика различных приоритетов в обслуживании) |
| RADIUS | Remote Authentication Dial-In User Service | Служба удалённой аутентификации пользователей |
| RID | Router ID | Идентификатор маршрутизатора |
| RIP | Routing Information Protocol | Протокол дистанционно-векторной маршрутизации |
| RMON | Remote Network Monitoring | Дистанционный мониторинг сети (расширение SNMP, разработанное IETF) |
| RSTP | Rapid Spanning Tree Protocol | Быстрый протокол связующего дерева (версия протокола STP с ускоренной реконфигурацией дерева) |

| | | |
|---|---|---|
| RTC | Real Time Clock | Часы реального времени |
| SNMP | Simple Network Management Protocol | Простой протокол сетевого управления (интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP) |
| SNTP | Simple Network Time Protocol | Простой протокол синхронизации времени (является упрощённой реализацией протокола NTP) |
| SSH | Secure Shell | «Безопасная оболочка», сетевой протокол прикладного уровня |
| SSL | Secure Sockets Layer | Уровень защищённых сокетов; криптографический протокол, который отвечает за безопасную передачу данных на сеансовом уровне |
| STP | Spanning Tree Protocol | Протокол связующего дерева |
| TACACS+ | Terminal Access Controller Access Control System | Сеансовый протокол аутентификации, авторизации и учета доступа |
| TCP | Transmission Control Protocol | Протокол управления передачей |
| TFTP | Trivial File Transfer Protocol | Простой протокол передачи файлов |
| UDP | User Datagram Protocol | Протокол пользовательских дейтаграмм |
| USM | User-Based Security Model | Модель безопасности на основе пользователей |
| VLAN | Virtual Local Area Network | Виртуальная локальная сеть |
| VRRP | Virtual Router Redundancy Protocol | Протокол резервирования виртуальных маршрутизаторов |
| WINS | Windows Internet Naming Service | Служба разрешения NetBIOS-имен компьютеров в локальных сетях на основе MS Windows |
| WRR | Weighted Round Robin | Взвешенная очередь |